ASA Cluster

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

Some features are not supported when using clustering. See Unsupported Features with Clustering, on page 11.

- About ASA Clustering, page 1
- Licensing for ASA Clustering, page 18
- Prerequisites for ASA Clustering, page 19
- Guidelines for ASA Clustering, page 21
- Defaults for ASA Clustering, page 26
- Configure ASA Clustering, page 26
- Manage ASA Cluster Members, page 60
- Monitoring the ASA Cluster, page 64
- Examples for ASA Clustering, page 70
- History for ASA Clustering, page 90

About ASA Clustering

This section describes the clustering architecture and how it works.

How the ASA Cluster Fits into Your Network

The cluster consists of multiple ASAs acting as a single unit. To act as a cluster, the ASAs need the following infrastructure:
• Isolated, high-speed backplane network for intra-cluster communication, known as the cluster control link.

• Management access to each ASA for configuration and monitoring.

When you place the cluster in your network, the upstream and downstream routers need to be able to load-balance the data coming to and from the cluster using one of the following methods:

• Spanned EtherChannel (Recommended)—Interfaces on multiple members of the cluster are grouped into a single EtherChannel; the EtherChannel performs load balancing between units.

• Policy-Based Routing (Routed firewall mode only)—The upstream and downstream routers perform load balancing between units using route maps and ACLs.

• Equal-Cost Multi-Path Routing (Routed firewall mode only)—The upstream and downstream routers perform load balancing between units using equal cost static or dynamic routes.

**Performance Scaling Factor**

When you combine multiple units into a cluster, you can expect a performance of approximately:

• 70% of the combined throughput

• 60% of maximum connections

• 50% of connections per second

For example, for throughput, the ASA 5585-X with SSP-40 can handle approximately 10 Gbps of real world firewall traffic when running alone. For a cluster of 8 units, the maximum combined throughput will be approximately 70% of 80 Gbps (8 units x 10 Gbps): 56 Gbps.

**Cluster Members**

Cluster members work together to accomplish the sharing of the security policy and traffic flows. This section describes the nature of each member role.

**Bootstrap Configuration**

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.

**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.

**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. See About Cluster Interfaces, on page 26 for more information.

**Cluster Control Link**

Each unit must dedicate at least one hardware interface as the cluster control link. See About the Cluster Control Link, on page 26 for more information.

**High Availability Within the ASA Cluster**

ASA Clustering provides high availability by monitoring unit and interface health and by replicating connection states between units.
**Unit Health Monitoring**

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. If the unit health check fails, the unit is removed from the cluster.

**Interface Monitoring**

Each unit monitors the link status of all named 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.

When you enable health monitoring, all physical interfaces (including the main EtherChannel and redundant interface types) are monitored by default; you can optionally disable monitoring per interface. Only named interfaces can be monitored. For example, the named EtherChannel must fail to be considered failed, which means all member ports of an EtherChannel must fail to trigger cluster removal (depending on your minimum port bundling setting).

A unit is removed from the cluster if its monitored interfaces fail. The amount of time before the ASA removes a member from the cluster depends on the type of interface and whether the unit is an established member or is joining the cluster. For EtherChannels (spanned or not), if the interface is down on an established member, then the ASA removes the member after 9 seconds. The ASA does not monitor interfaces for the first 90 seconds that a unit joins the cluster. Interface status changes during this time will not cause the ASA to be removed from the cluster. For non-EtherChannels, the unit is removed after 500 ms, regardless of the member state.

**Status After Failure**

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 unit.

The ASA automatically tries to rejoin the cluster, depending on the failure event.

---

**Note**

When the 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 disabled. 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 when initially joining**—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 group name`, and then `enable`.

- **Failed cluster control link after joining the cluster**—The ASA automatically tries to rejoin every 5 minutes, indefinitely. This behavior is configurable.

- **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 group name`, and then `enable`. This behavior is configurable.

- **Failed ASA FirePOWER module on the ASA 5585-X**—The ASA automatically tries to rejoin at 5 minutes.

- **Failed ASA FirePOWER software module**—After you resolve the problem with the module, you must manually enable clustering at the console port by entering `cluster group name`, and then `enable`.

- **Failed unit**—If the unit was removed from the cluster because of a unit health check failure, then rejoining the cluster depends on the source of the failure. For example, a temporary power failure means the unit will rejoin the cluster when it starts up again as long as the cluster control link is up and clustering is still enabled with the `enable` command. The ASA attempts to rejoin the cluster every 5 seconds.

- **Internal error**—Internal failures include: application sync timeout; inconsistent application statuses; and so on. After you resolve the problem, you must manually rejoin the cluster by re-enabling clustering at the console port by entering `cluster group name`, and then `enable`.

See Configure the Master Unit Bootstrap Settings, on page 45.

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. The backup owner is usually also the director.

Some traffic requires state information above the TCP or UDP layer. See the following table for clustering support or lack of support for this kind of traffic.

<table>
<thead>
<tr>
<th>Traffic</th>
<th>State Support</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up time</td>
<td>Yes</td>
<td>Keeps track of the system up time.</td>
</tr>
<tr>
<td>ARP Table</td>
<td>Yes</td>
<td>Transparent mode only.</td>
</tr>
<tr>
<td>MAC address table</td>
<td>Yes</td>
<td>Transparent mode only.</td>
</tr>
</tbody>
</table>
### Configuration Replication

All units in the cluster share a single configuration. You can only make configuration changes on the master unit, and changes are automatically synced to all other units in the cluster.

### ASA Cluster Management

One of the benefits of using ASA clustering is the ease of management. This section describes how to manage the cluster.

#### Management Network

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

<table>
<thead>
<tr>
<th>Traffic</th>
<th>State Support</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Identity</td>
<td>Yes</td>
<td>Includes AAA rules (uauth) and identity firewall.</td>
</tr>
<tr>
<td>IPv6 Neighbor database</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Dynamic routing</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>SNMP Engine ID</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Centralized VPN (Site-to-Site)</td>
<td>No</td>
<td>VPN sessions will be disconnected if the master unit fails.</td>
</tr>
</tbody>
</table>
master unit, so management of the cluster continues seamlessly. The Local IP address is used for routing, and is also useful for troubleshooting.

For example, you can manage the cluster by connecting to the Main cluster IP address, which is always attached to the current master unit. To manage an individual member, you can connect to the Local IP address.

For outbound management traffic such as TFTP or syslog, each unit, including the master unit, uses the Local IP address to connect to the server.

For a Spanned EtherChannel interface, you can only configure one IP address, and that IP address is always attached to the master unit. You cannot connect directly to a slave unit using the EtherChannel interface; we recommend configuring the management interface as an Individual interface so that you can connect to each unit. Note that you can use a device-local EtherChannel for management.

Master Unit Management Vs. Slave Unit Management

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 (except for syslogs sent to the console when console replication is enabled).
- SNMP
- NetFlow

RSA Key Replication

When you create an RSA key on the master unit, the key is replicated to all slave units. If you have an SSH session to the Main cluster IP address, you will be disconnected if the master unit fails. The new master unit uses the same key for SSH connections, so that you do not need to update the cached SSH host key when you reconnect to the new master unit.

ASDM Connection Certificate IP Address Mismatch

By default, a self-signed certificate is used for the ASDM connection based on the Local IP address. If you connect to the Main cluster IP address using ASDM, then a warning message about a mismatched IP address appears because the certificate uses the Local IP address, and not the Main cluster IP address. You can ignore the message and establish the ASDM connection. However, to avoid this type of warning, you can enroll a certificate that contains the Main cluster IP address and all the Local IP addresses from the IP address pool. You can then use this certificate for each cluster member.

Inter-Site Clustering

For inter-site installations, you can take advantage of ASA clustering as long as you follow the recommended guidelines.
You can configure each cluster chassis to belong to a separate site ID. Site IDs work with site-specific MAC addresses. Packets sourced from the cluster use a site-specific MAC address, while packets received by the cluster use a global MAC address. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address. Site-specific MAC addresses are supported for routed mode using Spanned EtherChannels only.

Site IDs are also used to enable flow mobility using LISP inspection. See the following sections for more information about inter-site clustering:

- Sizing the Data Center Interconnect—Prerequisites for ASA Clustering, on page 19
- Inter-Site Guidelines—Guidelines for ASA Clustering, on page 21
- Configure Cluster Flow Mobility—Configure Cluster Flow Mobility, on page 56
- Inter-Site Examples—Examples for Inter-Site Clustering, on page 85

### How the ASA Cluster Manages Connections

Connections can be load-balanced to multiple members of the cluster. Connection roles determine how connections are handled in both normal operation and in a high availability situation.

#### Connection Roles

See the following roles defined for each connection:

- **Owner**—Usually, the unit that initially receives the connection. The owner maintains the TCP state and processes packets. A connection has only one owner. If the original owner fails, then when new units receive packets from the connection, the director chooses a new owner from those units.

- **Backup owner**—The unit that stores TCP/UDP state information received from the owner, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner does not take over the connection in the event of a failure. If the owner becomes unavailable, then 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.

  As long as the director (see below) is not the same unit as the owner, then the director is also the backup owner. If the owner chooses itself as the director, then a separate backup owner is chosen.

  For inter-chassis clustering on the Firepower 9300, which can include up to 3 cluster units in one chassis, if the backup owner is on the same chassis as the owner, then an additional backup owner will be chosen from another chassis to protect flows from a chassis failure.

- **Director**—The unit that handles owner lookup requests from forwarders. When the owner receives a new connection, it chooses a director based on a hash of the source/destination IP address and 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. If a director fails, the owner chooses a new director.

  As long as the director is not the same unit as the owner, then the director is also the backup owner (see above). If the owner chooses itself as the director, then a separate backup owner is chosen.
• 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.

When a connection uses Port Address Translation (PAT), then the PAT type (per-session or multi-session) influences which member of the cluster becomes the owner of a new connection:

• Per-session PAT—The owner is the unit that receives the initial packet in the connection.
  By default, TCP and DNS UDP traffic use per-session PAT.

• Multi-session PAT—The owner is always the master unit. If a multi-session PAT connection is initially received by a slave unit, then the slave unit forwards the connection to the master unit.
  By default, UDP (except for DNS UDP) and ICMP traffic use multi-session PAT, so these connections are always owned by the master unit.

You can change the per-session PAT defaults for TCP and UDP so connections for these protocols are handled per-session or multi-session depending on the configuration. For ICMP, you cannot change from the default multi-session PAT. For more information about per-session PAT, see the firewall configuration guide.

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.

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 one ASA (based on the load balancing method), which becomes the owner. The owner creates a flow, encodes owner information into a SYN cookie, and forwards the packet to the server.

2 The SYN-ACK packet originates from the server and is delivered to a different ASA (based on the load balancing method). This ASA is the forwarder.

3 Because the forwarder does not own the connection, it decodes owner information from the SYN cookie, creates a forwarding flow to the owner, and forwards the SYN-ACK to the owner.

4 The owner sends a state update to the director, and forwards the SYN-ACK to the client.

5 The director receives the state update from the owner, creates a flow to the owner, and records the TCP state information as well as the owner. The director acts as the backup owner for the connection.

6 Any subsequent packets delivered to the forwarder will be forwarded to the owner.

7 If packets are delivered to any additional units, it will query the director for the owner and establish a flow.

8 Any state change for the flow results in a state update from the owner to the director.

**Rebalancing New TCP Connections Across the Cluster**

If the load balancing capabilities of the upstream or downstream routers result in unbalanced flow distribution, you can configure overloaded units to redirect new TCP flows to other units. No existing flows will be moved to other units.

**ASA Features and Clustering**

Some ASA features are not supported with ASA clustering, and some are only supported on the master unit. Other features might have caveats for proper usage.
Unsupported Features with Clustering

These features cannot be configured with clustering enabled, and the commands will be rejected.

- Unified Communication features that rely on TLS Proxy
- Remote access VPN (SSL VPN and IPsec VPN)
- The following application inspections:
  - CTIQBE
  - H323, H225, and RAS
  - IPsec passthrough
  - MGCP
  - MMP
  - RTSP
  - SCCP (Skinny)
  - WAAS
  - WCCP

- Botnet Traffic Filter
- Auto Update Server
- DHCP client, server, and proxy. DHCP relay is supported.
- VPN load balancing
- Failover
- ASA CX module

Centralized Features for Clustering

The following features are only supported on the master unit, and are not scaled for the cluster. For example, you have a cluster of eight units (5585-X with SSP-60). The Other VPN license allows a maximum of 10,000 site-to-site IPsec tunnels for one ASA 5585-X with SSP-60. For the entire cluster of eight units, you can only use 10,000 tunnels; the feature does not scale.

Note
Traffic for centralized features is forwarded from member units to the master unit over the cluster control link.

If you use the rebalancing feature, traffic for centralized features may be rebalanced to non-master units before the traffic is classified as a centralized feature; if this occurs, the traffic is then sent back to the master unit.

For centralized features, if the master unit fails, all connections are dropped, and you have to re-establish the connections on the new master unit.
• Site-to-site VPN

• The following application inspections:
  ◦ DCERPC
  ◦ ESMTP
  ◦ IM
  ◦ NetBIOS
  ◦ PPTP
  ◦ RADIUS
  ◦ RSH
  ◦ SNMP
  ◦ SQLNET
  ◦ 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 3 units and with traffic evenly distributed, the conform rate actually becomes 3 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.
• LISP traffic—LISP traffic on UDP port 4342 is inspected by each receiving unit, but is not assigned a director. Each unit adds to the EID table that is shared across the cluster, but the LISP traffic itself does not participate in cluster state sharing.

• ASA Firepower module—There is no configuration sync or state sharing between ASA Firepower modules. You are responsible for maintaining consistent policies on the ASA Firepower modules in the cluster using Firepower Management Center. Do not use different ASA-interface-based zone definitions for devices in the cluster.

• ASA IPS module—There is no configuration sync or state sharing between IPS modules. Some IPS signatures require IPS to keep the state across multiple connections. For example, the port scanning signature is used when the IPS module detects that someone is opening many connections to one server but with different ports. In clustering, those connections will be balanced between multiple ASA devices, each of which has its own IPS module. Because these IPS modules do not share state information, the cluster may not be able to detect port scanning as a result.

### AAA for Network Access and Clustering

AAA for network access consists of three components: authentication, authorization, and accounting. Authentication and authorization 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.

### FTP and Clustering

• If FTP data channel and control channel flows are owned by different cluster members, then 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 re-loaded, 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.

### Identity Firewall and Clustering

Only the master unit retrieves the user-group from the AD and the user-ip mapping from the AD agent. The master unit then populates the user information to slaves, and slaves can make a match decision for user identity based on the security policy.

### Multicast Routing and Clustering

Multicast routing behaves differently depending on the interface mode.
Multicast Routing in Spanned EtherChannel Mode

In Spanned EtherChannel mode, the master unit handles all multicast routing packets and data packets until fast-path forwarding is established. After the connection is established, each slave can forward multicast data packets.

Multicast Routing in Individual Interface Mode

In Individual interface mode, units do not act independently with multicast. All data and routing packets are processed and forwarded by the master unit, thus avoiding packet replication.

NAT and Clustering

NAT can affect 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 the 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.

• No PAT with Port Block Allocation—This feature is not supported for the cluster.

• PAT with Port Block Allocation—See the following guidelines for this feature:
  ◦ Maximum-per-host limit is not a cluster-wide limit, and is enforced on each unit individually. Thus, in a 3-node cluster with the maximum-per-host limit configured as 1, if the traffic from a host is load-balanced across all 3 units, then it can get allocated 3 blocks with 1 in each unit.
  ◦ Port blocks created on the backup unit from the backup pools are not accounted for when enforcing the maximum-per-host limit.
  ◦ When a PAT IP address owner goes down, the backup unit will own the PAT IP address, corresponding port blocks, and xlates. But it will not use these blocks to service new requests. As the connections eventually time out, the blocks get freed.
  ◦ On-the-fly PAT rule modifications, where the PAT pool is modified with a completely new range of IP addresses, will result in xlate backup creation failures for the xlate backup requests that were still in transit while the new pool became effective. This behavior is not specific to the port block allocation feature, and is a transient PAT pool issue seen only in cluster deployments where the pool is distributed and traffic is load-balanced across the cluster units.

• 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, then 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, whereas ICMP and all other UDP traffic uses multi-session. You can configure per-session NAT rules to change these defaults for TCP and UDP, but you cannot configure per-session PAT for ICMP. For traffic that benefits from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT for the associated TCP ports (the UDP ports for those H.323 and SIP are already multi-session by default). For more information about per-session PAT, see the firewall configuration guide.

- No static PAT for the following inspections—
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP

**Dynamic Routing and Clustering**

This section describes how to use dynamic routing with clustering.
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 1: Dynamic Routing in Spanned EtherChannel Mode*

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

The OSPF LSA database is not synchronized from the master unit to slave units. If there is a master unit switchover, the neighboring router will detect a restart; the switchover is not transparent. The OSPF process picks an IP address as its router ID. Although not required, you can assign a static router ID to ensure a consistent router ID is used across the cluster. See the OSPF Non-Stop Forwarding feature to address the interruption.
Dynamic Routing in Individual Interface Mode

In Individual interface mode, each unit runs the routing protocol as a standalone router, and routes are learned by each unit independently.

**Figure 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. EIGRP does not form neighbor relationships with cluster peers in individual interface mode.

---

**Note**

If the cluster has multiple adjacencies to the same router for redundancy purposes, asymmetric routing can lead to unacceptable traffic loss. To avoid asymmetric routing, group all of these ASA interfaces into the same traffic zone. See [Configure a Traffic Zone](#).

---

**SCTP and Clustering**

An SCTP association can be created on any unit (due to load balancing); its multi-homing connections must reside on the same unit.

**SIP Inspection and Clustering**

A control flow can be created on any unit (due to load balancing); its child data flows must reside on the same unit.

TLS Proxy configuration is not supported.
SNMP and Clustering

An SNMP agent polls each individual ASA by its Local IP address. You cannot poll consolidated data for the cluster.

You should always use the Local address, and not the Main cluster IP address for SNMP polling. If the SNMP agent polls the Main cluster IP address, if a new master is elected, the poll to the new master unit will fail.

Syslog and NetFlow and Clustering

• Syslog—Each unit in the cluster generates its own syslog messages. You can configure logging so that each unit uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all units in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all units look as if they come from a single unit. If you configure logging to use the local-unit name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different units.

• NetFlow—Each unit in the cluster generates its own NetFlow stream. The NetFlow collector can only treat each ASA as a separate NetFlow exporter.

Cisco TrustSec and Clustering

Only the master unit learns security group tag (SGT) information. The master unit then populates the SGT to slaves, and slaves can make a match decision for SGT based on the security policy.

VPN and Clustering

Site-to-site VPN is a centralized feature; only the master unit supports VPN connections.

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.

Licensing for ASA Clustering

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

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

### ASA Hardware and Software Requirements

All units in a cluster:

- Must be the same model with the same DRAM. You do not have to have the same amount of flash memory.
- Must run the identical software except at the time of an image upgrade. Hitless upgrade is supported.
- Must be in the same security context mode, single or multiple.
- (Single context mode) Must be in the same firewall mode, routed or transparent.
- New cluster members must use the same SSL encryption setting (the `ssl encryption` command) as the master unit for initial cluster control link communication before configuration replication.
- Must have the same cluster, encryption and, for the ASA 5585-X, 10 GE I/O licenses.

### Switch Prerequisites

- Be sure to complete the switch configuration before you configure clustering on the ASAs.
- For a list of supported switches, see [Cisco ASA Compatibility](#).

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
</table>
| ASA 5585-X | Cluster License, supports up to 16 units.  
**Note** Each unit must have the same encryption license; each unit must have the same 10 GE I/O/Security Plus license (ASA 5585-X with SSP-10 and -20). |
| ASA 5516-X | Base license, supports 2 units.  
**Note** Each unit must have the same encryption license. |
| ASA 5512-X | 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 | Base License, supports 2 units.  
**Note** Each unit must have the same encryption license. |
| ASA on the Firepower 9300 Chassis | See [ASA Cluster Licenses for the ASA on the Firepower 9300 Chassis](#). |
| All other models | No support. |
ASA Prerequisites

- Provide each unit with a unique IP address before you join them to the management network.
  - See the Getting Started chapter for more information about connecting to the ASA and setting the management IP address.
  - Except for the IP address used by the master unit (typically the first unit you add to the cluster), these management IP addresses are for temporary use only.
  - After a slave joins the cluster, its management interface configuration is replaced by the one replicated from the master unit.

- To use jumbo frames on the cluster control link (recommended), you must enable Jumbo Frame Reservation before you enable clustering.

Sizing the Data Center Interconnect for Inter-Site Clustering

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 \( (2/2 \times 5 \text{ Gbps}) \).

- For 6 members at 3 sites, the size increases:
  - 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 \( (3/2 \times 10 \text{ Gbps}) \).

- 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)).

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 for ASA Clustering

Context Mode
The mode must match on each member unit.

Firewall Mode
For single mode, the firewall mode must match on all units.

Failover
Failover is not supported with clustering.

IPv6
The cluster control link is only supported using IPv4.

Models
Supported on:
  • ASA 5585-X—For the ASA 5585-X with SSP-10 and SSP-20, which include two Ten Gigabit Ethernet interfaces, we recommend using one interface for the cluster control link, and the other for data (you can use subinterfaces for data). Although this setup does not accommodate redundancy for the cluster control link, it does satisfy the need to size the cluster control link to match the size of the data interfaces.
  • ASA 5516-X
  • ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X

Switches
  • For the ASR 9006, if you want to set a non-default MTU, set the ASR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the mtu-ignore option is used. Note that the cluster device MTU should match the ASR IPv4 MTU.
  • On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit 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. Note that some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.
On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: source-dest-ip or source-dest-ip-port (see the Cisco Nexus OS and Cisco IOS port-channel load-balance command). Do not use a vlan keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster. Do not change the load-balancing algorithm from the default on the cluster device.

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.

Some switches do not support dynamic port priority with LACP (active and standby links). You can disable dynamic port priority to provide better compatibility with spanned EtherChannels.

Switches on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.

Port-channel bundling downtime should not exceed the configured keepalive interval.

On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the cluster device to fixed:

```
router(config)# port-channel id hash-distribution fixed
```

Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.

You should disable the LACP Graceful Convergence feature on all cluster-facing EtherChannel interfaces for Cisco Nexus switches.

EtherChannels

In Catalyst 3750-X Cisco IOS software versions earlier than 15.1(1)S2, the cluster unit did not support connecting an EtherChannel to a switch stack. With default switch settings, if the cluster unit 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. To improve compatibility, set the stack-mac persistent timer command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.

Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.

* Spanned EtherChannels—For cluster unit 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 cluster unit 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 cluster unit EtherChannels into one EtherChannel on the switch.
Inter-Site Guidelines

See the following guidelines for inter-site clustering:

- Supports inter-site clustering in the following interface and firewall modes:

<table>
<thead>
<tr>
<th>Interface Mode</th>
<th>Firewall Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Routed</td>
</tr>
<tr>
<td>Individual Interface</td>
<td>Yes</td>
</tr>
<tr>
<td>Spanned EtherChannel</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- For individual interface mode, when using ECMP towards a multicast Rendezvous Point (RP), we recommend that you use a static route for the RP IP address using the Main cluster IP address as the next hop. This static route prevents sending unicast PIM register packets to slave units. If a slave unit receives a PIM register packet, then the packet is dropped, and the multicast stream cannot be registered.

- The cluster control link latency must be less than 20 ms round-trip time (RTT).
• The cluster control link must be reliable, with no out-of-order or dropped packets; for example, you should use a dedicated link.

• Do not configure connection rebalancing; you do not want connections rebalanced to cluster members at a different site.

• The cluster implementation does not differentiate between members at multiple sites for incoming connections; therefore, connection roles for a given connection may span across sites. This is expected behavior.

• For transparent mode, if the cluster is placed between a pair of inside and outside routers (AKA North-South insertion), you must ensure that both inside routers share a MAC address, and also that both outside routers share a MAC address. When a cluster member at site 1 forwards a connection to a member at site 2, the destination MAC address is preserved. The packet will only reach the router at site 2 if the MAC address is the same as the router at site 1.

• For transparent mode, if the cluster is placed between data networks and the gateway router at each site for firewalling between internal networks (AKA East-West insertion), then each gateway router should use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide identical virtual IP and MAC address destinations at each site. The data VLANs are extended across the sites using Overlay Transport Virtualization (OTV), or something similar. You need to create filters to prevent traffic that is destined to the local gateway router from being sent over the DCI to the other site. If the gateway router becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site’s gateway.

• For routed mode using Spanned EtherChannel, configure site-specific MAC addresses. Extend the data VLANs across the sites using OTV, or something similar. You need to create filters to prevent traffic that is destined to the global MAC address from being sent over the DCI to the other site. If the cluster becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site’s cluster units. Dynamic routing is not supported when an inter-site cluster acts as the first hop router for an extended segment.

Additional Guidelines

• When significant topology changes occur (such as adding or removing an EtherChannel interface, enabling or disabling an interface on the ASA or the switch, adding an additional switch to form a VSS or vPC) you should disable the health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the interface 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.

• We do not support VXLAN in Individual Interface mode. Only Spanned EtherChannel mode supports VXLAN.
Defaults for ASA Clustering

- When using Spanned EtherChannels, the cLACP system ID is auto-generated and the system priority is 1 by default.
- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.
- The cluster auto-rejoin feature for a failed cluster control link is unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection rebalancing is disabled by default. If you enable connection rebalancing, the default time between load information exchanges is 5 seconds.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

Configure ASA Clustering

To configure clustering, perform the following tasks.

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

Cable the Units and Configure Interfaces

Before configuring clustering, cable the cluster control link network, management network, and data networks. Then configure your interfaces.

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

About the Cluster Control Link

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

Cluster Control Link Traffic Overview

Cluster control link traffic includes both control and data traffic.

Control traffic includes:
- Master election.
- Configuration replication.
- Health monitoring.
Data traffic includes:
- State replication.
- Connection ownership queries and data packet forwarding.

**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 FirePOWER module, Cisco recommends that you use ASA interfaces for the cluster control link, and not interfaces on the ASA FirePOWER module. Module interfaces can drop traffic for up to 30 seconds during a module reload, including reloads that occur during a software upgrade. However, if needed, you can use module interfaces and ASA interfaces in the same cluster control link EtherChannel. When the module interfaces drop, the remaining interfaces in the EtherChannel are still up. The ASA 5585-X Network Module does not run a separate operating system, so it is not affected by this issue.

Be aware that data interfaces on the module are also affected by reload drops. Cisco recommends always using ASA interfaces redundantly with module interfaces in an EtherChannel.

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.

You can use an EtherChannel or redundant interface.

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.

**Size the Cluster Control Link**

If possible, you should size the cluster control link to match the expected throughput of each chassis so the cluster-control link can handle the worst-case scenarios. 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. 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.

Cluster Control Link Redundancy

We recommend using an EtherChannel for the cluster control link, so that you can pass traffic on multiple links in the EtherChannel while still achieving redundancy.

The following diagram shows how to use an EtherChannel as a cluster control link in a Virtual Switching System (VSS) or Virtual Port Channel (vPC) environment. All links in the EtherChannel are active. When the switch is part of a VSS or vPC, then you can connect ASA interfaces within the same EtherChannel to separate switches in the VSS or vPC. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch. Note that this EtherChannel is device-local, not a Spanned EtherChannel.

Cluster Control Link Reliability

To ensure cluster control link functionality, be sure the round-trip time (RTT) between units is less than 20 ms. This maximum latency enhances compatibility with cluster members installed at different geographical sites. To check your latency, perform a ping on the cluster control link between units.

The cluster control link must be reliable, with no out-of-order or dropped packets; for example, for inter-site deployment, you should use a dedicated link.

Cluster Control Link Failure

If the cluster control link line protocol goes down for a unit, then clustering is disabled; data interfaces are shut down. After you fix the cluster control link, you must manually rejoin the cluster by re-enabling clustering.

Note
When the 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.

Spanned EtherChannels (Recommended)

You can group one or more interfaces per chassis into an EtherChannel that spans all chassis 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 BVI, not to the bridge group member interface. The EtherChannel inherently provides load balancing as part of basic operation.

**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.

**Guidelines for Maximum Throughput**

To achieve maximum throughput, we recommend the following:

- Use a load balancing hash algorithm that is "symmetric," meaning that packets from both directions will have the same hash, and will be sent to the same ASA in the Spanned EtherChannel. We recommend using the source and destination IP address (the default) or the source and destination port as the hashing algorithm.
- Use the same type of line cards when connecting the ASAs to the switch so that hashing algorithms applied to all packets are the same.
Load Balancing

The EtherChannel link is selected using a proprietary hash algorithm, based on source or destination IP addresses and TCP and UDP port numbers.

Note

On the ASA, do not change the load-balancing algorithm from the default. On the switch, we recommend that you use one of the following algorithms: `source-dest-ip` or `source-dest-ip-port` (see the Cisco Nexus OS or Cisco IOS `port-channel load-balance` command). Do not use a `vlan` keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the ASAs in a cluster.

The number of links in the EtherChannel affects load balancing.

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

EtherChannel Redundancy

The EtherChannel has built-in redundancy. It monitors the line protocol status of all links. If one link fails, traffic is re-balanced between remaining links. If all links in the EtherChannel fail on a particular unit, but other units are still active, then the unit is removed from the cluster.

Connecting to a VSS or vPC

You can include multiple interfaces per ASA in the Spanned EtherChannel. Multiple interfaces per ASA are especially useful for connecting to both switches in a VSS or vPC.

Depending on your switches, you can configure up to 32 active links in the spanned EtherChannel. This feature requires both switches in the vPC to support EtherChannels with 16 active links each (for example the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module).

For switches that support 8 active links in the EtherChannel, you can configure up to 16 active links in the spanned EtherChannel when connecting to two switches in a VSS/vPC.

If you want to use more than 8 active links in a spanned EtherChannel, you cannot also have standby links; the support for 9 to 32 active links requires you to disable cLACP dynamic port priority that allows the use of standby links. You can still use 8 active links and 8 standby links if desired, for example, when connecting to a single switch.

The following figure shows a 32 active link spanned EtherChannel in an 8-ASA cluster and a 16-ASA cluster.
The following figure shows a 16 active link spanned EtherChannel in a 4-ASA cluster and an 8-ASA cluster.
The following figure shows a traditional 8 active/8 standby link spanned EtherChannel in a 4-ASA cluster and an 8-ASA cluster. The active links are shown as solid lines, while the inactive links are dotted. cLACP load-balancing can automatically choose the best 8 links to be active in the EtherChannel. As shown, cLACP helps achieve load balancing at the link level.
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 slave IP address for the master unit; the Local IP address is always the master address for routing. The Main cluster IP address provides consistent management access to an address; when a master unit changes, the Main cluster IP address moves to the new master unit, so management of the cluster continues seamlessly. Load balancing, however, must be configured separately on the upstream switch in this case.

Note

We recommend Spanned EtherChannels instead of Individual interfaces because Individual interfaces rely on routing protocols to load-balance traffic, and routing protocols often have slow convergence during a link failure.
Policy-Based Routing (Routed Firewall Mode Only)

When using Individual interfaces, each ASA interface maintains its own IP address and MAC address. One method of load balancing is Policy-Based Routing (PBR).

We recommend this method if you are already using PBR, and want to take advantage of your existing infrastructure. This method might offer additional tuning options vs. Spanned EtherChannel as well.

PBR makes routing decisions based on a route map and ACL. You must manually divide traffic between all ASAs in a cluster. Because PBR is static, it may not achieve the optimum load balancing result at all times. To achieve the best performance, we recommend that you configure the PBR policy so that forward and return packets of a connection are directed to the same physical ASA. For example, if you have a Cisco router, redundancy can be achieved by using Cisco IOS PBR with Object Tracking. Cisco IOS Object Tracking monitors each ASA using ICMP ping. PBR can then enable or disable route maps based on reachability of a particular ASA. See the following URLs for more details:


Note

If you use this method of load-balancing, you can use a device-local EtherChannel as an Individual interface.

Equal-Cost Multi-Path Routing (Routed Firewall Mode Only)

When using Individual interfaces, each ASA interface maintains its own IP address and MAC address. One method of load balancing is Equal-Cost Multi-Path (ECMP) routing.

We recommend this method if you are already using ECMP, and want to take advantage of your existing infrastructure. This method might offer additional tuning options vs. Spanned EtherChannel as well.
ECMP routing can forward packets over multiple "best paths" that tie for top place in the routing metric. Like EtherChannel, a hash of source and destination IP addresses and/or source and destination ports can be used to send a packet to one of the next hops. If you use static routes for ECMP routing, then an ASA failure can cause problems; the route continues to be used, and traffic to the failed ASA will be lost. If you use static routes, be sure to use a static route monitoring feature such as Object Tracking. We recommend using dynamic routing protocols to add and remove routes, in which case, you must configure each ASA to participate in dynamic routing.

**Note**
If you use this method of load-balancing, you can use a device-local EtherChannel as an Individual interface.

**Nexus Intelligent Traffic Director (Routed Firewall Mode Only)**
When using Individual interfaces, each ASA interface maintains its own IP address and MAC address. Intelligent Traffic Director (ITD) is a high-speed hardware load-balancing solution for Nexus 5000, 6000, 7000, and 9000 switch series. In addition to fully covering the functional capabilities of traditional PBR, it offers a simplified configuration workflow and multiple additional features for a more granular load distribution. ITD supports IP stickiness, consistent hashing for bi-directional flow symmetry, virtual IP addressing, health monitoring, sophisticated failure handling policies with N+M redundancy, weighted load-balancing, and application IP SLA probes including DNS. Due to the dynamic nature of load-balancing, it achieves a more even traffic distribution across all cluster members as compared to PBR. In order to achieve bi-directional flow symmetry, we recommend configuring ITD such that forward and return packets of a connection are directed to the same physical ASA. See the following URL for more details:


**Cable the Cluster Units and Configure Upstream and Downstream Equipment**

Before configuring clustering, cable the cluster control link network, management network, and data networks.

**Note**
At a minimum, an active cluster control link network is required before you configure the units to join the cluster.

You should also configure the upstream and downstream equipment. For example, if you use EtherChannels, then you should configure the upstream and downstream equipment for the EtherChannels.

**Examples**

**Note**
This example uses EtherChannels for load-balancing. If you are using PBR or ECMP, your switch configuration will differ.

For example on each of 4 ASA 5585-Xs, you want to use:

- 2 Ten Gigabit Ethernet interfaces in a device-local EtherChannel for the cluster control link.
- 2 Ten Gigabit Ethernet interfaces in a Spanned EtherChannel for the inside and outside network; each interface is a VLAN subinterface of the EtherChannel. Using subinterfaces lets both inside and outside interfaces take advantage of the benefits of an EtherChannel.
- 1 Management interface.

You have one switch for both the inside and outside networks.

---

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Connect Interfaces on each of 4 ASAs</th>
<th>To Switch Ports</th>
</tr>
</thead>
</table>
| 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. |
To Switch Ports

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Connect Interfaces on each of 4 ASAs</th>
<th>To Switch Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside and outside interfaces</td>
<td>TenGigabitEthernet 0/8 and TenGigabitEthernet 0/9</td>
<td>8 ports total</td>
</tr>
<tr>
<td></td>
<td>Configure a single EtherChannel (across all ASAs).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On the switch, configure these VLANs and networks now; for example, a trunk including VLAN 200 for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the inside and VLAN 201 for the outside.</td>
<td></td>
</tr>
<tr>
<td>Management interface</td>
<td>Management 0/0</td>
<td>4 ports total</td>
</tr>
<tr>
<td></td>
<td>Place all interfaces on the same isolated management VLAN, for example VLAN 100.</td>
<td></td>
</tr>
</tbody>
</table>

**Configure the Cluster Interface Mode on Each Unit**

You can only configure one type of interface for clustering: Spanned EtherChannels or Individual interfaces; you cannot mix interface types in a cluster.

**Before You Begin**

- You must set the mode separately on each ASA that you want to add to the cluster.
- You can always configure the management-only interface as an Individual interface (recommended), even in Spanned EtherChannel mode. The management interface can be an Individual interface even in transparent firewall mode.
- In Spanned EtherChannel mode, if you configure the management interface as an Individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.
- In multiple context mode, you must choose one interface type for all contexts. For example, if you have a mix of transparent and routed mode contexts, you must use Spanned EtherChannel mode for all contexts because that is the only interface type allowed for transparent mode.

**Procedure**

**Step 1**
Show any incompatible configuration so that you can force the interface mode and fix your configuration later; the mode is not changed with this command:

```
cluster interface-mode \{individual | spanned\} check-details
```

**Example:**
```
ciscoasa(config)# cluster interface-mode spanned check-details
```

**Step 2**
Set the interface mode for clustering:
```
cluster interface-mode \{individual | spanned\} force
```
### Example:

```text
ciscoasa(config)# cluster interface-mode spanned force
```

There is no default setting; you must explicitly choose the mode. If you have not set the mode, you cannot enable clustering.

The **force** option changes the mode without checking your configuration for incompatible settings. You need to manually fix any configuration issues after you change the mode. Because any interface configuration can only be fixed after you set the mode, we recommend using the **force** option so that you can at least start from the existing configuration. You can re-run the **check-details** option after you set the mode for more guidance.

Without the **force** option, if there is any incompatible configuration, you are prompted to clear your configuration and reload, thus requiring you to connect to the console port to reconfigure your management access. If your configuration is compatible (rare), the mode is changed and the configuration is preserved. If you do not want to clear your configuration, you can exit the command by typing **n**.

To remove the interface mode, enter the **no cluster interface-mode** command.

---

### Configure Interfaces on the Master Unit

You must modify any interface that is currently configured with an IP address to be cluster-ready before you enable clustering. For other interfaces, you can configure them before or after you enable clustering; we recommend pre-configuring all of your interfaces so that the complete configuration is synced to new cluster members.

This section describes how to configure interfaces to be compatible with clustering. You can configure data interfaces as either Spanned EtherChannels or as Individual interfaces. Each method uses a different load-balancing mechanism. You cannot configure both types in the same configuration, with the exception of the management interface, which can be an Individual interface even in Spanned EtherChannel mode.

### Configure Individual Interfaces (Recommended for the Management Interface)

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 primary 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 primary unit.

### Before You Begin

- Except for the management-only interface, you must be in Individual interface mode.
- For multiple context mode, perform this procedure in each context. If you are not already in the context configuration mode, enter the **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.
- (Optional) Configure the interface as a device-local EtherChannel interface, a redundant interface, and/or configure subinterfaces.
For an EtherChannel, this EtherChannel is local to the unit, and is not a Spanned EtherChannel.

Management-only interfaces cannot be redundant interfaces.

**Procedure**

**Step 1** Configure a pool of Local IP addresses (IPv4 and/or IPv6), one of which will be assigned to each cluster unit for the interface:

(IPv4)

```plaintext
ip local pool poolname first-address — last-address [mask mask]
```

(IPv6)

```plaintext
ipv6 local pool poolname ipv6-address/prefix-length number_of_addresses
```

**Example:**

```plaintext
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8::1002/32 8
```

Include at least as many addresses as there are units in the cluster. If you plan to expand the cluster, include additional addresses. The Main cluster IP address that belongs to the current primary unit is not a part of this pool; be sure to reserve an IP address on the same network for the Main cluster IP address.

You cannot determine the exact Local address assigned to each unit in advance; to see the address used on each unit, enter the `show ip[v6] local pool poolname` command. Each cluster member is assigned a member ID when it joins the cluster. The ID determines the Local IP used from the pool.

**Step 2** Enter interface configuration mode:

```plaintext
interface interface_id
```

**Example:**

```plaintext
ciscoasa(config)# interface tengigabitethernet 0/8
```

**Step 3** (Management interface only) Set an interface to management-only mode so that it does not pass through traffic:

```plaintext
management-only
```

By default, Management type interfaces are configured as management-only. In transparent mode, this command is always enabled for a Management type interface.

This setting is required if the cluster interface mode is Spanned.

**Step 4** Name the interface:

```plaintext
nameif name
```

**Example:**

```plaintext
ciscoasa(config-if)# nameif inside
```

The `name` is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value.
Step 5  Set the Main cluster IP address and identify the cluster pool:

(IPV4)

`ip address ip_address [mask] cluster-pool poolname`

(IPV6)

`ipv6 address ipv6-address/prefix-length cluster-pool poolname`

Example:

```bash
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8::1002/32 cluster-pool insipv6
```

This IP address must be on the same network as the cluster pool addresses, but not be part of the pool. You can configure an IPv4 and/or an IPv6 address.

DHCP, PPPoE, and IPv6 autoconfiguration are not supported; you must manually configure the IP addresses.

Step 6  Set the security level, where `number` is an integer between 0 (lowest) and 100 (highest):

`security-level number`

Example:

```bash
ciscoasa(config-if)# security-level 100
```

Step 7  Enable the interface:

`no shutdown`

---

**Examples**

The following example configures the Management 0/0 and Management 0/1 interfaces as a device-local EtherChannel, and then configures the EtherChannel as an Individual interface:

```bash
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
```
Configure Spanned EtherChannels

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

Before You Begin

• You must be in Spanned EtherChannel interface mode.

• For multiple context mode, start this procedure in the system execution space. If you are not already in the System configuration mode, enter the `changeto system` command.

• For transparent mode, configure the bridge group.

• Do not specify the maximum and minimum links in the EtherChannel—We recommend that you do not specify the maximum and minimum links in the EtherChannel (The `lacp max-bundle` and `port-channel min-bundle` commands) on either the ASA or the switch. If you need to use them, note the following:
  - The maximum links set on the ASA is the total number of active ports for the whole cluster. Be sure the maximum links value configured on the switch is not larger than the ASA value.
  - The minimum links set on the ASA is the minimum active ports to bring up a port-channel interface per unit. On the switch, the minimum links is the minimum links across the cluster, so this value will not match the ASA value.

• Do not change the load-balancing algorithm from the default (see the `port-channel load-balance` command). On the switch, we recommend that you use one of the following algorithms: `source-dest-ip` or `source-dest-ip-port` (see the Cisco Nexus OS and Cisco IOS `port-channel load-balance` command). Do not use a `vlan` keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the ASAs in a cluster.

• The `lacp port-priority` and `lacp system-priority` commands are not used for a Spanned EtherChannel.

• When using Spanned EtherChannels, the port-channel interface will not come up until clustering is fully enabled. This requirement prevents traffic from being forwarded to a unit that is not an active unit in the cluster.

Procedure

Step 1 Specify the interface you want to add to the channel group:
```
interface physical_interface
```

Example:
```
ciscoasa(config)# interface gigabitethernet 0/0
```
The `physical_interface` ID includes the type, slot, and port number as type slot/port. This first interface in the channel group determines the type and speed for all other interfaces in the group.

Step 2 Assign this interface to an EtherChannel:
```
channel-group channel_id mode active [vss-id {1 | 2}]
```
Example:

ciscoasa(config-if)# channel-group 1 mode active

The channel_id is between 1 and 48. If the port-channel interface for this channel ID does not yet exist in the configuration, one will be added automatically:

interface port-channel channel_id

Only active mode is supported for Spanned EtherChannels.

If you are connecting the ASA to two switches in a VSS or vPC, then configure the vss-id keyword to identify to which switch this interface is connected (1 or 2). You must also use the port-channel span-cluster vss-load-balance command for the port-channel interface in Step 6.

Step 3 Enable the interface:
no shutdown

Step 4 (Optional) Add additional interfaces to the EtherChannel by repeating the process.

Example:

ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown

Multiple interfaces in the EtherChannel per unit are useful for connecting to switches in a VSS or vPC. Keep in mind that by default, a spanned EtherChannel can have only 8 active interfaces out of 16 maximum across all members in the cluster; the remaining 8 interfaces are on standby in case of link failure. To use more than 8 active interfaces (but no standby interfaces), disable dynamic port priority using the clacp static-port-priority command. When you disable dynamic port priority, you can use up to 32 active links across the cluster. For example, for a cluster of 16 ASAs, you can use a maximum of 2 interfaces on each ASA, for a total of 32 interfaces in the spanned EtherChannel.

Step 5 Specify the port-channel interface:
interface port-channel channel_id

Example:

ciscoasa(config)# interface port-channel 1

This interface was created automatically when you added an interface to the channel group.

Step 6 Set this EtherChannel as a Spanned EtherChannel:
port-channel span-cluster [vss-load-balance]

Example:

ciscoasa(config-if)# port-channel span-cluster

If you are connecting the ASA to two switches in a VSS or vPC, then you should enable VSS load balancing by using the vss-load-balance keyword. This feature ensures that the physical link connections between the ASAs to the VSS (or vPC) pair are balanced. You must configure the vss-id keyword in the channel-group command for each member interface before enabling load balancing (see Step 2).
**Step 7** (Optional) You can set the Ethernet properties for the port-channel interface to override the properties set on the Individual interfaces. This method provides a shortcut to set these parameters because these parameters must match for all interfaces in the channel group.

**Step 8** (Optional) If you are creating VLAN subinterfaces on this EtherChannel, do so now.

**Example:**

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

The rest of this procedure applies to the subinterfaces.

**Step 9** (Multiple Context Mode) Allocate the interface to a context. Then enter:

```
change to context name
interface port-channel channel_id
```

**Example:**

```
ciscoasa(config)# context admin
```

```
ciscoasa(config)# allocate-interface port-channel1
```

```
ciscoasa(config)# changeto context admin
```

```
ciscoasa(config-if)# interface port-channel 1
```

For multiple context mode, the rest of the interface configuration occurs within each context.

**Step 10** Name the interface:

```
nameif name
```

**Example:**

```
ciscoasa(config-if)# nameif inside
```

The `name` is a text string up to 48 characters, and is not case-sensitive. You can change the name by reentering this command with a new value.

**Step 11** Perform one of the following, depending on the firewall mode.

- **Routed Mode**—Set the IPv4 and/or IPv6 address:
  
  **(IPv4)**
  
  `ip address ip_address [mask]`
  
  **(IPv6)**
  
  `ipv6 address ipv6-prefix/prefix-length`
  
  **Example:**

  ```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ```

  ```
ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  DHCP, PPPoE, and IPv6 autoconfig are not supported.

- **Transparent Mode**—Assign the interface to a bridge group:
**bridge-group number**

Example:

```
ciscoasa(config-if)# bridge-group 1
```

Where *number* is an integer between 1 and 100. You can assign up to 4 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group. Note that the BVI configuration includes the IP address.

**Step 12** Set the security level:
```
security-level number
```

Example:

```
ciscoasa(config-if)# security-level 50
```

Where *number* is an integer between 0 (lowest) and 100 (highest).

**Step 13** Configure a global MAC address for a Spanned EtherChannel to avoid potential network connectivity problems:
```
mac-address mac_address
```

Example:

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

With a manually-configured MAC address, the MAC address stays with the current primary unit. In multiple context mode, if you share an interface between contexts, you should enable auto-generation of MAC addresses so that you only need to set the MAC address manually for a shared interface if you disable auto-generation. Note that you must manually configure the MAC address for non-shared interfaces.

The *mac_address* is in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE is entered as 000C.F142.4CDE.

The first two bytes of a manual MAC address cannot be A2 if you also want to use auto-generated MAC addresses.

**Step 14** (Routed mode) For inter-site clustering, configure a site-specific MAC address for each site:
```
mac-address mac_address site-id number
```

Example:

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
```

```
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1
```

```
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2
```

```
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3
```

```
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4
```

The site-specific MAC address used by a unit depends on the site ID you specify in each unit’s bootstrap configuration.
Create the Bootstrap Configuration

Each unit in the cluster requires a bootstrap configuration to join the cluster.

Configure the Master Unit Bootstrap Settings

Each unit in the cluster requires a bootstrap configuration to join the cluster. Typically, the first unit you configure to join the cluster will be the master unit. After you enable clustering, after an election period, the cluster elects a master unit. With only one unit in the cluster initially, that unit will become the master unit. Subsequent units that you add to the cluster will be slave units.

Before You Begin

- 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.
- You must use the console port to enable or disable clustering. You cannot use Telnet or SSH.
- With the exception of the cluster control link, any interfaces in your configuration must be configured with a cluster IP pool or as a Spanned EtherChannel before you enable clustering, depending on your interface mode. If you have pre-existing interface configuration, you can either clear the interface configuration (`clear configure interface`), or convert your interfaces to cluster interfaces before you enable clustering.
- When you add a unit to a running cluster, you may see temporary, limited packet/connection drops; this is expected behavior.
- Pre-determine the size of the cluster control link. See Size the Cluster Control Link, on page 27.

Procedure

Step 1

Enable the cluster control link interface before you join the cluster.
You will later identify this interface as the cluster control link when you enable clustering.

We recommend that you combine multiple cluster control link interfaces into an EtherChannel if you have enough interfaces. The EtherChannel is local to the ASA, and is not a Spanned EtherChannel.

The cluster control link interface configuration is not replicated from the master unit to slave units; however, you must use the same configuration on each unit. Because this configuration is not replicated, you must configure the cluster control link interfaces separately on each unit.

- You cannot use a VLAN subinterface as the cluster control link.
- You cannot use a Management.x/x interface as the cluster control link, either alone or as an EtherChannel.
- For the ASA 5585-X with an ASA FirePOWER module, Cisco recommends that you use ASA interfaces for the cluster control link, and not interfaces on the ASA FirePOWER module. Module interfaces can drop traffic for up to 30 seconds during a module reload, including reloads that occur during a software upgrade. However, if needed, you can use module interfaces and ASA interfaces in the same cluster.
control link EtherChannel. When the module interfaces drop, the remaining interfaces in the EtherChannel are still up. The ASA 5585-X Network Module does not run a separate operating system, so it is not affected by this issue.

a) Enter interface configuration mode:
interface interface_id

Example:
ciscoasa(config)# interface tengigabitethernet 0/6

b) (Optional, for an EtherChannel) Assign this physical interface to an EtherChannel:
channel-group channel_id mode on

Example:
ciscoasa(config-if)# channel-group 1 mode on

The channel_id is between 1 and 48. If the port-channel interface for this channel ID does not yet exist in the configuration, one will be added automatically:
interface port-channel channel_id

We recommend using the On mode for cluster control link member interfaces to reduce unnecessary traffic on the cluster control link. The cluster control link does not need the overhead of LACP traffic because it is an isolated, stable network. Note: We recommend setting data EtherChannels to Active mode.

c) Enable the interface:
no shutdown

You only need to enable the interface; do not configure a name for the interface, or any other parameters.

d) (For an EtherChannel) Repeat for each additional interface you want to add to the EtherChannel:

Example:
ciscoasa(config)# interface tengigabitethernet 0/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown

Step 2 (Optional) Specify the maximum transmission unit for the cluster control link interface:
mtu cluster bytes

Example:
ciscoasa(config)# mtu cluster 9000

Set the MTU between 1400 and 9198 bytes. The default MTU is 1500 bytes.

We suggest setting the MTU to 1600 bytes or greater, which requires you to enable jumbo frame reservation before continuing with this procedure. Jumbo frame reservation requires a reload of the ASA.

This command is a global configuration command, but is also part of the bootstrap configuration that is not replicated between units.

Step 3 Name the cluster and enter cluster configuration mode:
cluster group name

Example:
ciscoasa(config)# cluster group pod1

The name must be an ASCII string from 1 to 38 characters. You can only configure one cluster group per unit. All members of the cluster must use the same name.

Step 4 Name this member of the cluster:
local-unit unit_name

Use a unique ASCII string from 1 to 38 characters. Each unit must have a unique name. A unit with a duplicated name will not be allowed in the cluster.

Example:
ciscoasa(cfg-cluster)# local-unit unit1

Step 5 Specify the cluster control link interface, preferably an EtherChannel:
cluster-interface interface_id ip ip_address mask

Example:
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2

Subinterfaces and Management interfaces are not allowed.
Specify an IPv4 address for the IP address; IPv6 is not supported for this interface. This interface cannot have a nameif configured.
For each unit, specify a different IP address on the same network.

Step 6 If you use inter-site clustering, set the site ID for this unit so it uses a site-specific MAC address:
site-id number

Example:
ciscoasa(cfg-cluster)# site-id 1

The number is between 1 and 8.

Step 7 Set the priority of this unit for master unit elections:
priority priority_number

Example:
ciscoasa(cfg-cluster)# priority 1

The priority is between 1 and 100, where 1 is the highest priority.

Step 8 (Optional) Set an authentication key for control traffic on the cluster control link:
key shared_secret
**Example:**

ciscoasa(cfg-cluster)# key chuntheunavoidable

The shared secret is an ASCII string from 1 to 63 characters. The shared secret is used to generate the key. This command does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

**Step 9** (Optional) Disable dynamic port priority in LACP:

clap static-port-priority

Some switches do not support dynamic port priority, so this command improves switch compatibility. Moreover, it enables support of more than 8 active spanned EtherChannel members, up to 32 members. Without this command, only 8 active members and 8 standby members are supported. If you enable this command, then you cannot use any standby members; all members are active.

**Step 10** (Optional) Manually specify the cLACP system ID and system priority:

clap system-mac {mac_address | auto} [system-priority number]

**Example:**

ciscoasa(cfg-cluster)# clap system-mac 000a.0000.aaaa

When using Spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch. ASAs in a cluster collaborate in cLACP negotiation so that they appear as a single (virtual) device to the switch. One parameter in cLACP negotiation is a system ID, which is in the format of a MAC address. All ASAs in the cluster use the same system ID: auto-generated by the master unit (the default) and replicated to all secondaries; or manually specified in this command in the form H.H.H, where H is a 16-bit hexadecimal digit. (For example, the MAC address 00-0A-00-00-AA-AA is entered as 000A.0000.AAAA.) You might want to manually configure the MAC address for troubleshooting purposes, for example, so that you can use an easily identified MAC address. Typically, you would use the auto-generated MAC address.

The system priority, between 1 and 65535, is used to decide which unit is in charge of making a bundling decision. By default, the ASA uses priority 1, which is the highest priority. The priority needs to be higher than the priority on the switch.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units. However, you cannot change this value after you enable clustering.

**Step 11** Enable clustering:

enable [noconfirm]

**Example:**

ciscoasa(cfg-cluster)# enable

INFO: Clustering is not compatible with following commands:
policy-map global_policy
class inspection_default
inspect skinny
policy-map global_policy
class inspection_default
inspect sip
Would you like to remove these commands? [Y]es/[N]o: Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done

When you enter the **enable** command, the ASA scans the running configuration for incompatible commands for features that are not supported with clustering, including commands that may be present in the default configuration. You are prompted to delete the incompatible commands. If you respond **No**, then clustering is not enabled. Use the **noconfirm** keyword to bypass the confirmation and delete incompatible commands automatically.

For the first unit enabled, a master unit election occurs. Because the first unit should be the only member of the cluster so far, it will become the master unit. Do not perform any configuration changes during this period.

To disable clustering, enter the **no enable** command.

**Note** If you disable clustering, all data interfaces are shut down, and only the management-only interface is active.

### Examples

The following example configures a management interface, configures a device-local EtherChannel for the cluster control link, and then enables clustering for the ASA called "unit1," which will become the master unit because it is added to the cluster first:

```
  ip local pool mgmt 10.1.1.2-10.1.1.9
  ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
  interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    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
```

### Configure Slave Unit Bootstrap Settings

Perform the following procedure to configure the slave units.

**Before You Begin**

- You must use the console port to enable or disable clustering. You cannot use Telnet or SSH.
- Back up your configurations in case you later want to leave the cluster, and need to restore your configuration.
• For multiple context mode, complete this procedure in the system execution space. To change from the context to the system execution space, enter the `change-to system` command.

• We recommend enabling jumbo frame reservation for use with the cluster control link.

• If you have any interfaces in your configuration that have not been configured for clustering (for example, the default configuration Management 0/0 interface), you can join the cluster as a slave unit (with no possibility of becoming the master in a current election).

• When you add a unit to a running cluster, you may see temporary, limited packet/connection drops; this is expected behavior.

**Procedure**

**Step 1** Configure the same cluster control link interface as you configured for the master unit.

**Example:**

```
ciscoasa(config)# interface tengigabitethernet 0/6
```
```
ciscoasa(config-if)# channel-group 1 mode on
```
```
ciscoasa(config-if)# no shutdown
```
```
ciscoasa(config)# interface tengigabitethernet 0/7
```
```
ciscoasa(config-if)# channel-group 1 mode on
```
```
ciscoasa(config-if)# no shutdown
```

**Step 2** Specify the same MTU that you configured for the master unit:

**Example:**

```
ciscoasa(config)# mtu cluster 9000
```

**Step 3** Identify the same cluster name that you configured for the master unit:

**Example:**

```
ciscoasa(config)# cluster group pod1
```

**Step 4** Name this member of the cluster with a unique string:

`local-unit unit_name`

**Example:**

```
ciscoasa(cfg-cluster)# local-unit unit2
```

Specify an ASCII string from 1 to 38 characters.

Each unit must have a unique name. A unit with a duplicated name will be not be allowed in the cluster.

**Step 5** Specify the same cluster control link interface that you configured for the master unit, but specify a different IP address on the same network for each unit:

`cluster-interface interface_id ip ip_address mask`

**Example:**

```
ciscoasa(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

Specify an IPv4 address for the IP address; IPv6 is not supported for this interface. This interface cannot have a nameif configured.

Each unit must have a unique name. A unit with a duplicated name will not be allowed in the cluster.

**Step 6** If you use inter-site clustering, set the site ID for this unit so it uses a site-specific MAC address:

```
site-id number
```

**Example:**

```
ciscoasa(cfg-cluster)# site-id 1
```

The **number** is between 1 and 8.

**Step 7** Set the priority of this unit for master unit elections, typically to a higher value than the master unit:

```
priority priority_number
```

**Example:**

```
ciscoasa(cfg-cluster)# priority 2
```

Set the priority between 1 and 100, where 1 is the highest priority.

**Step 8** Set the same authentication key that you set for the master unit:

**Example:**

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

**Step 9** Enable clustering:

```
enable as-slave
```

You can avoid any configuration incompatibilities (primarily the existence of any interfaces not yet configured for clustering) by using the `enable as-slave` command. This command ensures the slave joins the cluster with no possibility of becoming the master in any current election. Its configuration is overwritten with the one synced from the master unit.

To disable clustering, enter the `no enable` command.

**Note** If you disable clustering, all data interfaces are shut down, and only the management interface is active.

**Examples**

The following example includes the configuration for a slave unit, unit2:

```
interface tengigabitethernet 0/6
channel-group 1 mode on
no shutdown

interface tengigabitethernet 0/7
channel-group 1 mode on
no shutdown
```
cluster group pod1
local-unit unit2
customize cluster Interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave

Customize the Clustering Operation

You can customize clustering health monitoring, TCP connection replication delay, flow mobility and other optimizations.

Perform these procedures on the master unit.

Configure Basic ASA Cluster Parameters

You can customize cluster settings on the master unit.

Before You Begin

• For multiple context mode, complete this procedure in the system execution space on the master unit. To change from the context to the system execution space, enter the change to system command.

Procedure

Step 1 Enter cluster configuration mode:
cluster group name

Step 2 (Optional) Enable console replication from slave units to the master unit:
console-replicate

This feature is disabled by default. The ASA prints out some messages directly to the console for certain critical events. If you enable console replication, slave units send the console messages to the master unit so that you only need to monitor one console port for the cluster.

Step 3 Set the minimum trace level for clustering events:
trace-level level

Set the minimum level as desired:

• critical—Critical events (severity=1)
• warning—Warnings (severity=2)
• informational—Informational events (severity=3)
• debug—Debugging events (severity=4)
Configure Health Monitoring and Auto-Rejoin Settings

This procedure configures unit and interface health monitoring.

You might want to disable health monitoring of non-essential interfaces, for example, the management interface. You can monitor any port-channel ID, redundant ID, or single physical interface ID, or the software or hardware module, such as the ASA Firepower module. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored.

Procedure

Step 1  Enter cluster configuration mode.
    `cluster group name`

Example:
    `ciscoasa(config)# cluster group test`
    `ciscoasa(cfg-cluster)#`

Step 2  Customize the cluster unit health check feature.

    `health-check [holdtime timeout] [vss-enabled]`

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.

- **holdtime timeout**—Determines the amount of time between unit keepalive status messages, between .8 and 45 seconds; The default is 3 seconds.

- **vss-enabled**—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. If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, then you might need to enable the **vss-enabled** option. For some switches, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces.

When 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 and also disable interface monitoring for the disabled interfaces (**no health-check monitor-interface**). When the topology change is complete, and the configuration change is synced to all units, you can re-enable the health check feature.

Example:
    `ciscoasa(cfg-cluster)# health-check holdtime 5`

Step 3  Disable the interface health check on an interface.

    `no health-check monitor-interface [interface_id | service-module]`
The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular unit, but there are active ports under the same logical interface on other units, then the unit is removed from the cluster. The amount of time before the ASA removes a member from the cluster depends on the type of interface and whether the unit is an established member or is joining the cluster. Health check is enabled by default for all interfaces. You can disable it per interface using the `no` form of this command. You might want to disable health monitoring of non-essential interfaces, for example, the management interface.

- `interface_id`—Disables monitoring of any port-channel ID, redundant ID, or single physical interface ID. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored.

- `service-module`—Disables monitoring of a hardware or software module, such as the ASA FirePOWER module. Note that for the ASA 5585-X, if you disable monitoring of the service module, you may also want to disable monitoring of the interfaces on the module, which are monitored separately.

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 (`no health-check`) and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all units, you can re-enable the health check feature.

**Example:**

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
```

**Step 4** Customize the auto-rejoin cluster settings after a health check failure.

\[
\text{health-check \{data-interface | cluster-interface\} auto-rejoin \{unlimited | auto_rejoin_max\} \\
\quad \left[ \text{auto_rejoin_interval} \left| \text{auto_rejoin_interval_variation} \right. \right]
\]

- `unlimited`—(Default for the `cluster-interface`) Does not limit the number of rejoin attempts.

- `auto-rejoin-max`—Sets the number of rejoin attempts, between 0 and 65535. 0 disables auto-rejoining. The default for the `data-interface` is 3.

- `auto_rejoin_interval`—Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is 5 minutes. The maximum total time that the unit attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.

- `auto_rejoin_interval_variation`—Defines if the interval duration increases. Set the value between 1 and 3: 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration). For example, if you set the interval duration to 5 minutes, and set the variation to 2, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is 1 for the cluster-interface and 2 for the data-interface.

**Example:**

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```
Example

The following example configures the health-check holdtime to .3 seconds; enables VSS; disables monitoring on the Ethernet 1/2 interface, which is used for management; sets the auto-rejoin for data interfaces to 4 attempts starting at 2 minutes, increasing the duration by 3 x the previous interval; and sets the auto-rejoin for the cluster control link to 6 attempts every 2 minutes.

ciscoasa(config)# cluster group test
  ciscoasa(cfg-cluster)# health-check holdtime .3 vss-enabled
  ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/2
  ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
  ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1

Configure Connection Rebalancing and the Cluster TCP Replication Delay

You can configure connection rebalancing. For more information, see Rebalancing New TCP Connections Across the Cluster, on page 10

Enable the cluster replication delay for TCP connections to help eliminate the “unnecessary work” related to short-lived flows by delaying the director/backup flow creation. Note that if a unit fails before the director/backup flow is created, then those flows cannot be recovered. Similarly, if traffic is rebalanced to a different unit before the flow is created, then the flow cannot be recovered. You should not enable the TCP replication delay for traffic on which you disable TCP randomization.

Procedure

Step 1 Enable the cluster replication delay for TCP connections:
```
cluster replication delay seconds [http | match tcp {host ip_address | ip_address mask | any | any4 | any6} [{eq | lt | gt} port] {host ip_address | ip_address mask | any | any4 | any6} [{eq | lt | gt} port}]
```

Example:

ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http

Set the seconds between 1 and 15. The http delay is enabled by default for 5 seconds.

In multiple context mode, configure this setting within the context.

Step 2 Enter cluster configuration mode:
```
cluster group name
```

Step 3 (Optional) Enable connection rebalancing for TCP traffic:
```
conn-rebalance [frequency seconds]
```

Example:

ciscoasa(cfg-cluster)# conn-rebalance frequency 60

This command is disabled by default. If enabled, ASAs exchange load information periodically, and offload new connections from more loaded devices to less loaded devices. The frequency, between 1 and 360 seconds, specifies how often the load information is exchanged. The default is 5 seconds.
Do not configure connection rebalancing for inter-site topologies; you do not want connections rebalanced to cluster members at a different site.

Configure Cluster Flow Mobility

You can inspect LISP traffic to enable flow mobility when a server moves between sites.

About LISP Inspection

You can inspect LISP traffic to enable flow mobility between sites.

About LISP

Data center virtual machine mobility such as VMware VMotion enables servers to migrate between data centers while maintaining connections to clients. To support such data center server mobility, routers need to be able to update the ingress route towards the server when it moves. Cisco Locator/ID Separation Protocol (LISP) architecture separates the device identity, or endpoint identifier (EID), from its location, or routing locator (RLOC), into two different numbering spaces, making server migration transparent to clients. For example, when a server moves to a new site and a client sends traffic to the server, the router redirects traffic to the new location.

LISP requires routers and servers in certain roles, such as the LISP egress tunnel router (ETR), ingress tunnel router (ITR), first hop routers, map resolver (MR), and map server (MS). When the first hop router for the server senses that the server is connected to a different router, it updates all of the other routers and databases so that the ITR connected to the client can intercept, encapsulate, and send traffic to the new server location.

ASA LISP Support

The ASA does not run LISP itself; it can, however, inspect LISP traffic for location changes and then use this information for seamless clustering operation. Without LISP integration, when a server moves to a new site, traffic comes to an ASA cluster member at the new site instead of to the original flow owner. The new ASA forwards traffic to the ASA at the old site, and then the old ASA has to send traffic back to the new site to reach the server. This traffic flow is sub-optimal and is known as "tromboning" or "hair-pinning."

With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

LISP Guidelines

- The ASA cluster members must reside between the first hop router and the ITR or ETR for the site. The ASA cluster itself cannot be the first hop router for an extended segment.
- Only fully-distributed flows are supported; centralized flows, semi-distributed flows, or flows belonging to individual units are not moved to new owners. Semi-distributed flows include applications, such as SIP, where all child flows are owned by the same ASA that owns the parent flow.
- The cluster only moves Layer 3 and 4 flow states; some application data might be lost.
- For short-lived flows or non-business-critical flows, moving the owner may not be worthwhile. You can control the types of traffic that are supported with this feature when you configure the inspection policy, and should limit flow mobility to essential traffic.

ASA LISP Implementation

This feature includes several inter-related configurations (all of which are described in this chapter):
1 (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster.

2 LISP traffic inspection—The ASA inspects LISP traffic on UDP port 4342 for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. Note that LISP traffic is not assigned a director, and LISP traffic itself does not participate in cluster state sharing.

3 Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers.

4 Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner.

5 Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications.

Configure LISP Inspection

You can inspect LISP traffic to enable flow mobility when a server moves between sites.

Before You Begin

- Assign each cluster unit to a site ID according to Configure the Master Unit Bootstrap Settings, on page 45 and Configure Slave Unit Bootstrap Settings, on page 49.

- LISP traffic is not included in the default-inspection-traffic class, so you must configure a separate class for LISP traffic as part of this procedure.

Procedure

Step 1 (Optional) Configure a LISP inspection map to limit inspected EIDs based on IP address, and to configure the LISP pre-shared key:

a) Create an extended ACL; only the destination IP address is matched to the EID embedded address:

   access list eid_acl_name extended permit ip source_address mask destination_address mask

   Both IPv4 and IPv6 ACLs are accepted. See the command reference for exact access-list extended syntax.

b) Create the LISP inspection map, and enter parameters mode:

   policy-map type inspect lisp inspect_map_name

   parameters

c) Define the allowed EIDs by identifying the ACL you created:

   allowed-eid access-list eid_acl_name

   The first hop router or ITR/ETR might send EID-notify messages for hosts or networks that the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your
cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster.

d) If necessary, enter the pre-shared key:

```
validate-key key
```

**Example:**

ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0

ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP

ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome

### Step 2

Configure LISP inspection for UDP traffic between the first hop router and the ITR or ETR on port 4342:

a) Configure the extended ACL to identify LISP traffic:

```
access-list inspect_acl_name extended permit udp source_address mask destination_address mask eq 4342
```

You must specify UDP port 4342. Both IPv4 and IPv6 ACLs are accepted. See the command reference for exact `access-list extended` syntax.

b) Create a class map for the ACL:

```
class-map inspect_class_name
```

```
motion access-list inspect_acl_name
```

c) Specify the policy map, the class map, enable inspection using the optional LISP inspection map, and apply the service policy to an interface (if new):

```
policy-map policy_map_name

class inspect_class_name

inspect lisp [inspect_map_name]

service-policy policy_map_name {global | interface ifc_name}
```

If you have an existing service policy, specify the existing policy map name. By default, the ASA includes a global policy called `global_policy`, so for a global policy, specify that name. You can also create one service policy per interface if you do not want to apply the policy globally. LISP inspection is applied to traffic bidirectionally so you do not need to apply the service policy on both the source and destination interfaces; all traffic that enters or exits the interface to which you apply the policy map is affected if the traffic matches the class map for both directions.

**Example:**

ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342

ciscoasa(config)# class-map LISP_CLASS

ciscoasa(config-cmap)# match access-list LISP_ACL

ciscoasa(config-cmap)# policy-map INSIDE_POLICY

ciscoasa(config-pmap)# class LISP_CLASS

ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT

ciscoasa(config)# service-policy INSIDE_POLICY interface inside

The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID.

### Step 3

Enable Flow Mobility for a traffic class:
a) Configure the extended ACL to identify business critical traffic that you want to re-assign to the most optimal site when servers change sites:

```
access-list flow_acl_name extended permit udp source_address mask destination_address mask eq port
```

Both IPv4 and IPv6 ACLs are accepted. See the command reference for exact `access-list extended` syntax. You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers.

b) Create a class map for the ACL:

```
class-map flow_map_name
match access-list flow_acl_name
```

c) Specify the same policy map on which you enabled LISP inspection, the flow class map, and enable flow mobility:

```
policy-map policy_map_name
class flow_map_name
cluster flow-mobility lisp
```

Example:

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
```

```
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
```

```
ciscoasa(config)# match access-list IMPORTANT-FLOWS
```

```
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
```

```
ciscoasa(config-pmap-c)# class IMPORTANT-FLOWS-MAP
```

```
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

**Step 4** Enter cluster group configuration mode, and enable flow mobility for the cluster:

```
cluster group name
flow-mobility lisp
```

This on/off toggle lets you easily enable or disable flow mobility.

**Examples**

The following example:

- Limits EIDs to those on the 10.10.10.0/24 network
- Inspects LISP traffic (UDP 4342) between a LISP router at 192.168.50.89 (on inside) and an ITR or ETR router (on another ASA interface) at 192.168.10.8
- Enables flow mobility for all inside traffic going to a server on 10.10.10.0/24 using HTTPS.
- Enables flow mobility for the cluster.

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
parameters
  allowed-eid access-list TRACKED_EID_LISP
  validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
```
Manage ASA Cluster Members

After you deploy the cluster, you can change the configuration and manage cluster members.

Become 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. 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 (for example, you saved the configuration with clustering disabled), then the management interface is disabled. You must use the console port for any further configuration.

Before You Begin

- You must use the console port; you cannot enable or disable clustering from a remote CLI connection.
- For multiple context mode, perform this procedure in the system execution space. If you are not already in the System configuration mode, enter the `chargeto system` command.

Procedure

Step 1 Enter cluster configuration mode:
```
cluster group name
```

Example:
```
ciscoasa(config)# cluster group pod1
```

Step 2 Disable clustering:
```
no enable
```
If this unit was the master unit, a new master election takes place, and a different member becomes the master unit.

The cluster configuration is maintained, so that you can enable clustering again later.

## Deactivate a Member

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

\[\text{Procedure}\]

Remove the unit from the cluster:

\[\text{cluster remove unit} \ \text{unit\_name}\]

\[\text{Example}:\]

\[\text{ciscoasa(config)}\# \text{cluster remove unit} \ ?\]

Current active units in the cluster:

asa2

\[\text{ciscoasa(config)}\# \text{cluster remove unit} \ \text{asa2}\]

\[\text{WARNING: Clustering will be disabled on unit asa2. To bring it back to the cluster please logon to that unit and re-enable clustering}\]

The bootstrap configuration remains intact, as well as the last configuration synched from the master unit, so that you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master unit is elected.

To view member names, enter \text{cluster remove unit} \ ?, or enter the \text{show cluster info} command.

## Rejoin the Cluster

If a unit was removed from the cluster, for example for a failed interface or if you manually deactivated a member, you must manually rejoin the cluster.
Before You Begin

- You must use the console port to reenable clustering. Other interfaces are shut down.
- 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.
- Make sure the failure is resolved before you try to rejoin the cluster.

Procedure

**Step 1**
At the console, enter cluster configuration mode:

```
cluster group name
```

**Example:**

```
ciscoasa(config)# cluster group pod1
```

**Step 2**
Enable clustering.

```
enable
```

---

Leave the Cluster

If you want to leave the cluster altogether, you need to remove the entire cluster bootstrap configuration. Because the current configuration on each member is the same (synced from the primary unit), leaving the cluster also means either restoring a pre-clustering configuration from backup, or clearing your configuration and starting over to avoid IP address conflicts.

**Before You Begin**

You must use the console port; when you remove the cluster configuration, all interfaces are shut down, including the management interface and cluster control link. Moreover, you cannot enable or disable clustering from a remote CLI connection.

**Procedure**

**Step 1**
For a secondary unit, disable clustering:

```
cluster group cluster_name no enable
```

**Example:**

```
ciscoasa(config)# cluster group cluster1
ciscoasa(config)# no enable
```

You cannot make configuration changes while clustering is enabled on a secondary unit.

**Step 2**
Clear the cluster configuration:

```
clear configure cluster
```
The ASA shuts down all interfaces including the management interface and cluster control link.

**Step 3**  
Disable cluster interface mode:  
`no cluster interface-mode`  
The mode is not stored in the configuration and must be reset manually.

**Step 4**  
If you have a backup configuration, copy the backup configuration to the running configuration:  
`copy backup_cfg running-config`

**Example:**

```
ciscoasa(config)# copy backup_cluster.cfg running-config
```

**Step 5**  
Save the configuration to startup:  
`write memory`

**Step 6**  
If you do not have a backup configuration, reconfigure management access. Be sure to change the interface IP addresses, and restore the correct hostname, for example.

---

### Change the Primary Unit

**Caution**

The best method to change the master unit is to disable clustering on the master unit, waiting for a new master election, and then re-enabling clustering. If you must specify the exact unit you want to become the master, use the procedure in this section. Note, however, that for centralized features, if you force a master unit change using this procedure, then all connections are dropped, and you have to re-establish the connections on the new master unit.

To change the master unit, perform the following steps.

**Before You Begin**

For multiple context mode, perform this procedure in the system execution space. If you are not already in the System configuration mode, enter the `changeto system` command.

**Procedure**

Set a new unit as the master unit:  
`cluster master unit unit_name`

**Example:**

```
ciscoasa(config)# cluster master unit asa2
```

You will need to reconnect to the Main cluster IP address.
Execute a Command Cluster-Wide

To view member names, enter `cluster master unit ?` (to see all names except the current unit), or enter the `show cluster info` command.

**Execute a Command Cluster-Wide**

To send a command to all members in the cluster, or to a specific member, perform the following steps. Sending a `show` command to all members collects all output and displays it on the console of the current unit. Other commands, such as `capture` and `copy`, can also take advantage of cluster-wide execution.

**Procedure**

Send a command to all members, or if you specify the unit name, a specific member:

```
cluster exec [unit unit_name] command
```

**Example:**

```
ciscoasa# cluster exec show xlate
```

To view member names, enter `cluster exec unit ?` (to see all names except the current unit), or enter the `show cluster info` command.

**Examples**

To copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the following command on the master unit:

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as capture1_asa1.pcap, capture1_asa2.pcap, and so on. In this example, asa1 and asa2 are cluster unit names.

The following sample output for the `cluster exec show port-channel summary` command shows EtherChannel information for each member in the cluster:

```
ciscoasa# cluster exec show port-channel summary
master:(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)
slave:******************************************************************
  Number of channel-groups in use: 2
  Group  Port-channel  Protocol  Span-cluster  Ports
---------------------------------------------------------------
1       Po1          LACP      Yes      Gi0/0(P)
2       Po2          LACP      Yes      Gi0/1(P)
```

**Monitoring the ASA Cluster**

You can monitor and troubleshoot cluster status and connections.
Monitoring Cluster Status

See the following commands for monitoring cluster status:

- **show cluster info [health]**

  With no keywords, the `show cluster info` command shows the status of all members of the cluster.

  The `show cluster info health` command shows the current health of interfaces, units, and the cluster overall.

  See the following output for the `show cluster info` command:

  ```
ciscoasa# show cluster info
  Cluster stbu: On
  This is "C" in state SLAVE
  ID : 0
  Site ID : 1
  Version : 9.4(1)
  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
  Site ID : 1
  Version : 9.4(1)
  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
  Site ID : 2
  Version : 9.4(1)
  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
  Site ID : 2
  Version : 9.4(1)
  Serial No.: P3000000191
  CCL IP : 10.0.0.2
  CCL MAC : 000b.fcf8.c61e
  Last join : 19:13:50 UTC Sep 23 2011
  Last leave: 19:13:36 UTC Sep 23 2011
  ```

- **show cluster info transport {asp | cp}**

  Shows transport related statistics for the following:

  - **asp** — Data plane transport statistics.
  - **cp** — Control plane transport statistics.

- **show cluster history**

  Shows the cluster history.
Capturing Packets Cluster-Wide

See the following command for capturing packets in a cluster:

```
cluster exec capture
```

To support cluster-wide troubleshooting, you can enable capture of cluster-specific traffic on the master unit using the `cluster exec capture` command, which is then automatically enabled on all of the slave units in the cluster.

Monitoring Cluster Resources

See the following command for monitoring cluster resources:

```
show cluster {cpu | memory | resource} [options]
```

Displays aggregated data for the entire cluster. The options available depends on the data type.

Monitoring Cluster Traffic

See the following commands for monitoring cluster traffic:

```
• show conn [detail], cluster exec show conn
```

The `show conn` command shows whether a flow is a director, backup, or forwarder flow. Use the `cluster exec show conn` command on any unit to view all connections. This command can show how traffic for a single flow arrives at different ASAs in the cluster. The throughput of the cluster is dependent on the efficiency and configuration of load balancing. This command provides an easy way to view how traffic for a connection is flowing through the cluster, and can help you understand how a load balancer might affect the performance of a flow.

The `show conn detail` command also shows which flows are subject to flow mobility.

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,
 S - initial SYN from outside, b - TCP state-bypass or nailed,
 c - CTIQBE media, C - cluster centralized,
 D - DNS, d - dump, E - outside back connection, e - semi-distributed,
 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, L - LISP triggered flow owner mobility,
 M - SMTP data, m - SIP media, n - GUP
 o - outbound data, o - offloaded,
 P - inside back connection,
 Q - Diameter, 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, X - HAAS,
 w - secondary domain backup,
 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,
```
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, ASA 3 has the Y flag showing it is the director for the connection, and ASA 2 has no special flags showing it is the owner. In the outbound direction, the packets for this connection enter the inside interface on ASA 2 and exit the outside interface. In the inbound direction, the packets for this connection enter the outside interface on ASA 1 and ASA 3, are forwarded over the cluster control link to ASA 2, and then exit the inside interface on ASA 2.

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):*****************************************************
  18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:00, bytes 37240828, flags z

ASA2:*****************************************************
  12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:00, bytes 37240828, flags UIO

ASA3:*****************************************************
  10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside 172.18.124.187:22 inside 192.168.103.131:44727, idle 0:00:03, bytes 0, flags Y
```

**show cluster info [conn-distribution | packet-distribution | loadbalance | flow-mobility counters]**

The `show cluster info conn-distribution` and `show cluster info packet-distribution` commands show traffic distribution across all cluster units. These commands can help you to evaluate and adjust the external load balancer.

The `show cluster info loadbalance` command shows connection rebalance statistics.

The `show cluster info flow-mobility counters` command shows EID movement and flow owner movement information. See the following output for `show cluster info flow-mobility counters`:

```
ciscoasa# show cluster info flow-mobility counters
  EID movement notification received : 4
  EID movement notification processed : 4
  Flow owner moving requested : 2
```

**show cluster {access-list | conn | traffic | user-identity | xlate} [options]**

Displays aggregated data for the entire cluster. The `options` available depends on the data type.
See the following output for the `show cluster access-list` command:

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B, unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0, 0, 0, 0, 0) 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 192.168.1.177 host 192.168.43.132
(hitcnt=1, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 9 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104) 0xce4f281d
access-list 101 line 10 extended permit tcp host 192.168.1.1.122 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) 0x2797875d
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x4237da0d
```
• show lisp eid

Shows the ASA EID table showing EIDs and site IDs.

See the following output from the `cluster exec show lisp eid` command.

```
ciscoasa# cluster exec show lisp eid
L1 (LOCAL):*************************************************************
    LISP EID       Site ID
  33.44.33.105    2
  33.44.33.201    2
  11.22.11.1      4
  11.22.11.2      4
L2:*************************************************************
    LISP EID       Site ID
  33.44.33.105    2
  33.44.33.201    2
  11.22.11.1      4
  11.22.11.2      4
```

• show asp table classify domain inspect-lisp

This command is useful for troubleshooting.

Configuring Logging for Clustering

See the following command for configuring logging for clustering:

```
logging device-id
```

Each unit in the cluster generates syslog messages independently. You can use the `logging device-id` command to generate syslog messages with identical or different device IDs to make messages appear to come from the same or different units in the cluster.

Monitoring Cluster Interfaces

See the following commands for monitoring cluster interfaces:

• show cluster interface-mode
  Shows the cluster interface mode.

• show port-channel
  Includes information about whether a port-channel is spanned.

• show lacp cluster {system-mac | system-id}
  Shows the cLACP system ID and priority.

• debug lacp cluster {all | ccp | misc | protocol}
  Shows debug messages for cLACP.

• show interface
  Shows the use of the site MAC address when in use:

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
```
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped

Debugging Clustering

See the following commands for debugging clustering:

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**
  Shows debug messages for clustering.
- **debug cluster flow-mobility**
  Shows events related to clustering flow mobility.
- **debug lisp eid-notify-intercept**
  Shows events when the eid-notify message is intercepted.
- **show cluster info trace**
  The **show cluster info trace** command shows the debug information for further troubleshooting.

See the following output for the **show cluster info trace** command:

ciscoasa# show cluster info trace
Feb 02 14:19:47.456 [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

Examples for ASA Clustering

These examples include all cluster-related ASA configuration for typical deployments.

Sample ASA and Switch Configuration

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

<table>
<thead>
<tr>
<th>ASA Interface</th>
<th>Switch Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet 0/2</td>
<td>GigabitEthernet 1/0/15</td>
</tr>
<tr>
<td>GigabitEthernet 0/3</td>
<td>GigabitEthernet 1/0/16</td>
</tr>
<tr>
<td>GigabitEthernet 0/4</td>
<td>GigabitEthernet 1/0/17</td>
</tr>
<tr>
<td>GigabitEthernet 0/5</td>
<td>GigabitEthernet 1/0/18</td>
</tr>
</tbody>
</table>
ASA Configuration

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

Cisco IOS Switch Configuration

interface GigabitEthernet1/0/15
  switchport access vlan 201
  switchport mode access
  spanning-tree portfast
  channel-group 10 mode active

interface GigabitEthernet1/0/16
  switchport access vlan 201
  switchport mode access
  spanning-tree portfast
  channel-group 10 mode active

interface GigabitEthernet1/0/17
  switchport access vlan 401
  switchport mode access
  spanning-tree portfast
  channel-group 11 mode active

interface GigabitEthernet1/0/18
  switchport access vlan 401
  switchport mode access
  spanning-tree portfast
  channel-group 11 mode active

interface Port-channel10
  switchport access vlan 201
  switchport mode access

interface Port-channel11
  switchport access vlan 401
  switchport mode access
Firewall on a Stick

Data traffic from different security domains are associated with different VLANs, for example, VLAN 10 for the inside network and VLAN 20 for the outside network. Each ASA has a single physical port connected to the external switch or router. Trunking is enabled so that all packets on the physical link are 802.1q encapsulated. The ASA is the firewall between VLAN 10 and VLAN 20.

When using Spanned EtherChannels, all data links are grouped into one EtherChannel on the switch side. If an ASA becomes unavailable, the switch will rebalance traffic between the remaining units.

**Interface Mode on Each Unit**

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

**ASA1 Master Bootstrap Configuration**

```
interface tengigabitethernet 0/8
no shutdown
description CCL
```
cluster group cluster1
local-unit asa1
cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm

ASA2 Slave Bootstrap Configuration

interface tengigabitethernet 0/8
no shutdown
description CCL
cluster group cluster1
local-unit asa2
cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-slave

ASA3 Slave Bootstrap Configuration

interface tengigabitethernet 0/8
no shutdown
description CCL
cluster group cluster1
local-unit asa3
cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-slave

Master Interface Configuration

ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 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::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
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
Spanned EtherChannel with Backup Links (Traditional 8 Active/8 Standby)

The maximum number of active ports in a traditional EtherChannel is limited to 8 from the switch side. If you have an 8-ASA cluster, and you allocate 2 ports per unit to the EtherChannel, for a total of 16 ports total, then 8 of them have to be in standby mode. The ASA uses LACP to negotiate which links should be active or standby. If you enable multi-switch EtherChannel using 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 "master" port (for example, GigabitEthernet 0/0), and the other one is the "slave" port (for example, GigabitEthernet 0/1). You must guarantee symmetry in the hardware connection: all master links must terminate on one switch, and all slave 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 master ports and the number of active slave 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 master and slave 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
OTV Configuration for Routed Mode Inter-Site Clustering

The success of inter-site clustering for routed mode with Spanned EtherChannels depends on the proper configuration and monitoring of OTV. OTV plays a major role by forwarding the packets across the DCI. OTV forwards unicast packets across the DCI only when it learns the MAC address in its forwarding table. If the MAC address is not learned in the OTV forwarding table, it will drop the unicast packets.

Sample OTV Configuration

```
//Sample OTV config:
//3151 – Inside VLAN, 3152 – Outside VLAN, 202 – CCL VLAN
//aaaa.1111.1234 – ASA inside interface global vMAC
//0050.56A8.3D22 – Server MAC

feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000

vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop

vlan access-map Local 20
  match mac address ALL_MACs
  action forward

vlan filter Local vlan-list 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY
```
interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 230.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
  redistribute filter route-map stop-GMAC
  otv site-identifier 0x2
  otv flood mac 0050.56A8.3D22 vlan 3151

OTV Filter Modifications Required Because of Site Failure

If a site goes down, the filters need to be removed from OTV because you do not want to block the global MAC address anymore. There are some additional configurations required.

You need to add a static entry for the ASA global MAC address on the OTV switch in the site that is functional. This entry will let the OTV at the other end add these entries on the overlay interface. This step is required because if the server and client already have the ARP entry for the ASA, which is the case for existing connections, then they will not send the ARP again. Therefore, OTV will not get a chance to learn the ASA global MAC address in its forwarding table. Because OTV does not have the global MAC address in its forwarding table, and per OTV design it will not flood unicast packets over the overlay interface, then it will drop the unicast packets to the global MAC address from the server, and the existing connections will break.

//OTV filter configs when one of the sites is down
mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
  redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site

When the other site is restored, you need to add the filters back again and remove this static entry on the OTV. It is very important to clear the dynamic MAC address table on both the OTVs to clear the overlay entry for the global MAC address.
MAC Address Table Clearing

When a site goes down, and a static entry for the global MAC address is added to OTV, you need to let the other OTV learn the global MAC address on the overlay interface. After the other site comes up, these entries should be cleared. Make sure to clear the mac address table to make sure OTV does not have these entries in its forwarding table.

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen, + - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G   d867.d900.2e42 static  -  F  F  sup-eth1(R)
O   202 885a.92f6.44a5 dynamic  -  F  F  Overlay1
*  202 885a.92f6.4b8f dynamic 5  F  F  Eth8/3
O   3151 0050.5660.9412 dynamic  -  F  F  Overlay1
*  3151 aaaa.1111.1234 dynamic 50  F  F  Eth8/3
```

OTV ARP Cache Monitoring

OTV maintains an ARP cache to proxy ARP for IP addresses that it learned across the OTV interface.

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache
Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

Examples for Inter-Site Clustering

The following examples show supported cluster deployments.

Individual Interface Routed Mode North-South Inter-Site Example

The following example shows 2 ASA cluster members at each of 2 data centers placed between inside and outside routers (North-South insertion). The cluster members are connected by the cluster control link over the DCI. The inside and outside routers at each data center use OSPF and PBR or ECMP to load balance the traffic between cluster members. By assigning a higher cost route across the DCI, traffic stays within each data center unless all ASA cluster members at a given site go down. In the event of a failure of all cluster members at one site, traffic goes from each router over the DCI to the ASA cluster members at the other site.
Spanned EtherChannel Routed Mode Example with Site-Specific MAC Addresses

The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and an inside network at each site (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the inside and outside networks. Each EtherChannel is spanned across all chassis in the cluster.

The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters blocking the global MAC address to prevent traffic from traversing the DCI to the other site when the traffic is destined for the cluster. If the cluster units at one site become unreachable, you must remove the filters so traffic can be sent to the other site’s cluster units. You should use VACLs to filter the global MAC address. Be sure to disable ARP inspection. See OTV Configuration for Routed Mode Inter-Site Clustering, on page 83 for more information.

The cluster acts as the gateway for the inside networks. The global virtual MAC, which is shared across all cluster units, is used only to receive packets. Outgoing packets use a site-specific MAC address from each DC cluster. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address.

In this scenario:

- All egress packets sent from the cluster use the site MAC address and are localized at the data center.
- All ingress packets to the cluster are sent using the global MAC address, so they can be received by any of the units at both sites; filters at the OTV localize the traffic within the data center.
For a sample OTV configuration and best practices, see OTV Configuration for Routed Mode Inter-Site Clustering, on page 83.

**Spanned EtherChannel Transparent Mode North-South Inter-Site Example**

The following example shows 2 cluster members at each of 2 data centers placed between inside and outside routers (North-South insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

The inside and outside routers at each data center use OSPF, which is passed through the transparent ASAs. Unlike MACs, router IPs are unique on all routers. By assigning a higher cost route across the DCI, traffic stays within each data center unless all cluster members at a given site go down. The lower cost route through the ASAs must traverse the same bridge group at each site for the cluster to maintain asymmetric connections. In the event of a failure of all cluster members at one site, traffic goes from each router over the DCI to the cluster members at the other site.
The implementation of the switches at each site can include:

- Inter-site VSS/vPC—In this scenario, you install one switch at Data Center 1, and the other at Data Center 2. One option is for the cluster units at each Data Center to only connect to the local switch, while the VSS/vPC traffic goes across the DCI. In this case, connections are for the most part kept local to each datacenter. You can optionally connect each unit to both switches across the DCI if the DCI can handle the extra traffic. In this case, traffic is distributed across the data centers, so it is essential for the DCI to be very robust.

- Local VSS/vPC at each site—For better switch redundancy, you can install 2 separate VSS/vPC pairs at each site. In this case, although the cluster units still have a spanned EtherChannel with Data Center 1 chassis connected only to both local switches, and Data Center 2 chassis connected to those local switches, the spanned EtherChannel is essentially "split." Each local VSS/vPC sees the spanned EtherChannel as a site-local EtherChannel.

---

**Spanned EtherChannel Transparent Mode East-West Inter-Site Example**

The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and two inside networks at each site, the App network and the DB network (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the App and DB networks on the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

The gateway router at each site uses an FHRP such as HSRP to provide the same destination virtual MAC and IP addresses at each site. A good practice to avoid unintended MAC address flapping is to statically add the gateway routers real MAC addresses to the ASA MAC address table using the `mac-address-table static..."
outside_interface mac_address command. Without these entries, if the gateway at site 1 communicates with the gateway at site 2, that traffic might pass through the ASA and attempt to reach site 2 from the inside interface and cause problems. The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters to prevent traffic from traversing the DCI to the other site when the traffic is destined for the gateway router. If the gateway router at one site becomes unreachable, you must remove the filters so traffic can be sent to the other site’s gateway router.

See Spanned EtherChannel Transparent Mode North-South Inter-Site Example, on page 87 for information about vPC/VSS options.
# History for ASA Clustering

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA Clustering for the ASA 5580 and 5585-X</td>
<td>9.0(1)</td>
<td>ASA Clustering lets you group multiple ASAs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. ASA clustering is supported for the ASA 5580 and the ASA 5585-X; all units in a cluster must be the same model with the same hardware specifications. See the configuration guide for a list of unsupported features when clustering is enabled. We introduced or modified the following commands: <code>channel-group</code>, <code>clacp system-mac</code>, <code>clear cluster info</code>, <code>clear configure cluster</code>, <code>cluster exec</code>, <code>cluster group</code>, <code>cluster interface-mode</code>, <code>cluster-interface</code>, <code>conn-rebalance</code>, <code>console-replicate</code>, <code>cluster master unit</code>, <code>cluster remove unit</code>, <code>debug cluster</code>, <code>debug lacp cluster</code>, <code>enable</code> (cluster group), <code>health-check</code>, <code>ip address</code>, <code>ipv6 address</code>, <code>key</code> (cluster group), <code>local-unit</code>, <code>mac-address</code> (interface), <code>mac-address pool</code>, <code>mtu cluster</code>, <code>port-channel span-cluster</code>, <code>priority</code> (cluster group), <code>prompt cluster-unit</code>, <code>show asp cluster counter</code>, <code>show asp table cluster chash-table</code>, <code>show cluster</code>, <code>show cluster info</code>, <code>show cluster user-identity</code>, <code>show lacp cluster</code>, and <code>show running-config cluster</code>.</td>
</tr>
<tr>
<td>ASA 5500-X support for clustering</td>
<td>9.1(4)</td>
<td>The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now support 2-unit clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 5512-X, you need the Security Plus license. We did not modify any commands.</td>
</tr>
<tr>
<td>Improved VSS and vPC support for health check monitoring</td>
<td>9.1(4)</td>
<td>If you configure the cluster control link as an EtherChannel (recommended), and it is connected to a VSS or vPC pair, you can now increase stability with health check monitoring. For some switches, such as the Cisco Nexus 5000, when one unit in the VSS/vPC is shutting down or booting up, EtherChannel member interfaces connected to that switch may appear to be Up to the ASA, but they are not passing traffic on the switch side. The ASA can be erroneously removed from the cluster if you set the ASA holdtime timeout to a low value (such as .8 seconds), and the ASA sends keepalive messages on one of these EtherChannel interfaces. When you enable the VSS/vPC health check feature, the ASA floods the keepalive messages on all EtherChannel interfaces in the cluster control link to ensure that at least one of the switches can receive them. We modified the following command: <code>health-check [vss-enabled]</code>.</td>
</tr>
<tr>
<td>Support for cluster members at different geographical locations (inter-site); Individual Interface mode only</td>
<td>9.1(4)</td>
<td>You can now place cluster members at different geographical locations when using Individual Interface mode. We did not modify any commands.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Support for cluster members at different geographical locations (inter-site) for transparent mode</td>
<td>9.2(1)</td>
<td>You can now place cluster members at different geographical locations when using Spanned EtherChannel mode in transparent firewall mode. Inter-site clustering with spanned EtherChannels in routed firewall mode is not supported. We did not modify any commands.</td>
</tr>
</tbody>
</table>
| Static LACP port priority support for clustering | 9.2(1) | Some switches do not support dynamic port priority with LACP (active and standby links). You can now disable dynamic port priority to provide better compatibility with spanned EtherChannels. You should also follow these guidelines:  
• Network elements on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.  
• Port-channel bundling downtime should not exceed the configured keepalive interval. We introduced the following command: `clacp static-port-priority`. |
| Support for 32 active links in a spanned EtherChannel | 9.2(1) | ASA EtherChannels now support up to 16 active links. With *spanned* EtherChannels, that functionality is extended to support up to 32 active links across the cluster when used with two switches in a vPC and when you disable dynamic port priority. The switches must support EtherChannels with 16 active links, for example, the Cisco Nexus 7000 with F2-Series 10 Gigabit Ethernet Module. For switches in a VSS or vPC that support 8 active links, you can now configure 16 active links in the spanned EtherChannel (8 connected to each switch). Previously, the spanned EtherChannel only supported 8 active links and 8 standby links, even for use with a VSS/vPC.  
**Note** If you want to use more than 8 active links in a spanned EtherChannel, you cannot also have standby links; the support for 9 to 32 active links requires you to disable cLACP dynamic port priority that allows the use of standby links. We introduced the following command: `clacp static-port-priority`. |
<p>| Support for 16 cluster members for the ASA 5585-X | 9.2(1) | The ASA 5585-X now supports 16-unit clusters. We did not modify any commands. |
| BGP support for ASA clustering | 9.3(1) | We added support for BGP with ASA clustering. We introduced the following command: <code>bgp router-id clusterpool</code>. |
| Inter-site deployment in transparent mode with the ASA cluster firewalling between inside networks | 9.3(2) | You can now deploy a cluster in transparent mode between inside networks and the gateway router at each site (AKA East-West insertion), and extend the inside VLANs between sites. We recommend using Overlay Transport Virtualization (OTV), but you can use any method that ensures that the overlapping MAC Addresses and IP addresses of the gateway router do not leak between sites. Use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide the same virtual MAC and IP addresses to the gateway routers. |</p>
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable and disable ASA cluster health monitoring per interface</td>
<td>9.4(1)</td>
<td>You can now enable or disable health monitoring per interface. Health monitoring is enabled by default on all port-channel, redundant, and single physical interfaces. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored. You might want to disable health monitoring of non-essential interfaces, for example, the management interface. We introduced the following command: <code>health-check monitor-interface</code>.</td>
</tr>
<tr>
<td>ASA clustering support for DHCP relay</td>
<td>9.4(1)</td>
<td>You can now configure DHCP relay on the ASA cluster. Client DHCP requests are load-balanced to the cluster members using a hash of the client MAC address. DHCP client and server functions are still not supported. We did not modify any commands.</td>
</tr>
<tr>
<td>SIP inspection support in ASA clustering</td>
<td>9.4(1)</td>
<td>You can now configure SIP inspection on the ASA cluster. A control flow can be created on any unit (due to load balancing), but its child data flows must reside on the same unit. TLS Proxy configuration is not supported. We introduced the following command: <code>show cluster service-policy</code>.</td>
</tr>
<tr>
<td>Site-specific MAC addresses for inter-site clustering support forSpanned EtherChannel in Routed firewall mode</td>
<td>9.5(1)</td>
<td>You can now use inter-site clustering for Spanned EtherChannels in routed mode. To avoid MAC address flapping, configure a site ID for each cluster member so that a site-specific MAC address for each interface can be shared among a site’s units. We introduced or modified the following commands: <code>site-id</code>, <code>mac-address site-id</code>, <code>show cluster info</code>, <code>show interface</code></td>
</tr>
<tr>
<td>ASA cluster customization of the auto-rejoin behavior when an interface or the cluster control link fails</td>
<td>9.5(1)</td>
<td>You can now customize the auto-rejoin behavior when an interface or the cluster control link fails. We introduced the following command: <code>health-check auto-rejoin</code>.</td>
</tr>
<tr>
<td>The ASA cluster supports GTPv1 and GTPv2</td>
<td>9.5(1)</td>
<td>The ASA cluster now supports GTPv1 and GTPv2 inspection. We did not modify any commands.</td>
</tr>
<tr>
<td>Disable health monitoring of a hardware module in ASA clustering</td>
<td>9.5(1)</td>
<td>By default when using clustering, the ASA monitors the health of an installed hardware module such as the ASA FirePOWER module. If you do not want a hardware module failure to trigger failover, you can disable module monitoring. We modified the following command: <code>health-check monitor-interface service-module</code></td>
</tr>
<tr>
<td>Cluster replication delay for TCP connections</td>
<td>9.5(1)</td>
<td>This feature helps eliminate the &quot;unnecessary work&quot; related to short-lived flows by delaying the director/backup flow creation. We introduced the following command: <code>cluster replication delay</code></td>
</tr>
<tr>
<td>ASA 5516-X support for clustering</td>
<td>9.5(2)</td>
<td>The ASA 5516-X now supports 2-unit clusters. Clustering for 2 units is enabled by default in the base license. We did not modify any commands.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LISP Inspection for Inter-Site Flow Mobility</td>
<td>9.5(2)</td>
<td>Cisco Locator/ID Separation Protocol (LISP) architecture separates the device identity from its location into two different numbering spaces, making server migration transparent to clients. The ASA can inspect LISP traffic for location changes and then use this information for seamless clustering operation; the ASA cluster members inspect LISP traffic passing between the first hop router and the egress tunnel router (ETR) or ingress tunnel router (ITR), and then change the flow owner to be at the new site. We introduced or modified the following commands: allowed-eid, clear cluster info flow-mobility counters, clear lisp eid, cluster flow-mobility lisp, debug cluster flow-mobility, debug lisp eid-notify-intercept, flow-mobility lisp, inspect lisp, policy-map type inspect lisp, site-id, show asp table classify domain inspect-lisp, show cluster info flow-mobility counters, show conn, show lisp eid, show service-policy, validate-key</td>
</tr>
<tr>
<td>Carrier Grade NAT enhancements now supported in failover and ASA clustering</td>
<td>9.5(2)</td>
<td>For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). This feature is now supported in failover and ASA cluster deployments. We modified the following command: show local-host</td>
</tr>
<tr>
<td>Configurable level for clustering trace entries</td>
<td>9.5(2)</td>
<td>By default, all levels of clustering events are included in the trace buffer, including many low level events. To limit the trace to higher level events, you can set the minimum trace level for the cluster. We introduced the following command: trace-level</td>
</tr>
</tbody>
</table>