



## Clustering for the Firepower Threat Defense

Clustering lets you group multiple FTD units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.



### Note

Some features are not supported when using clustering. See [Unsupported Features with Clustering, on page 38](#).

- [About Clustering on the Firepower 4100/9300 Chassis, on page 1](#)
- [Licenses for Clustering, on page 6](#)
- [Requirements and Prerequisites for Clustering, on page 7](#)
- [Clustering Guidelines and Limitations, on page 10](#)
- [Configure Clustering, on page 14](#)
- [FXOS: Remove a Cluster Unit, on page 32](#)
- [FMC: Manage Cluster Members, on page 33](#)
- [FMC: Monitoring the Cluster, on page 37](#)
- [Examples for Clustering, on page 37](#)
- [Reference for Clustering, on page 38](#)
- [History for Clustering, on page 48](#)

## About Clustering on the Firepower 4100/9300 Chassis

When you deploy a cluster on the Firepower 4100/9300 chassis, it does the following:

- For native instance clustering: Creates a *cluster-control link* (by default, port-channel 48) for unit-to-unit communication.

For multi-instance clustering: You should pre-configure subinterfaces on one or more cluster-type EtherChannels; each instance needs its own cluster control link.

For intra-chassis clustering (Firepower 9300 only), this link utilizes the Firepower 9300 backplane for cluster communications.

For inter-chassis clustering, you need to manually assign physical interface(s) to this EtherChannel for communications between chassis.

- Creates the cluster bootstrap configuration within the application.

When you deploy the cluster, the chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings.

- Assigns data interfaces to the cluster as *Spanned* interfaces.

For intra-chassis clustering, spanned interfaces are not limited to EtherChannels, like it is for inter-chassis clustering. The Firepower 9300 supervisor uses EtherChannel technology internally to load-balance traffic to multiple modules on a shared interface, so any data interface type works for Spanned mode. For inter-chassis clustering, you must use Spanned EtherChannels for all data interfaces.

**Note**

Individual interfaces are not supported, with the exception of a management interface.

- Assigns a management interface to all units in the cluster.

## Bootstrap Configuration

When you deploy the cluster, the Firepower 9300 chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings.

## Cluster Members

Cluster members work together to accomplish the sharing of the security policy and traffic flows.

One member of the cluster is the **control** unit. The control unit is determined automatically. All other members are **data** units.

You must perform all configuration on the control unit only; the configuration is then replicated to the data units.

Some features do not scale in a cluster, and the control unit handles all traffic for those features. See [Centralized Features for Clustering, on page 38](#).

## Cluster Control Link

For native instance clustering: The cluster control link is automatically created using the Port-channel 48 interface.

For multi-instance clustering: You should pre-configure subinterfaces on one or more cluster-type EtherChannels; each instance needs its own cluster control link.

For intra-chassis clustering, this interface has no member interfaces. This Cluster type EtherChannel utilizes the Firepower 9300 backplane for cluster communications for intra-chassis clustering. For inter-chassis clustering, you must add one or more interfaces to the EtherChannel.

For a 2-member inter-chassis cluster, do not directly connect the cluster control link from one chassis to the other chassis. 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.

Cluster control link traffic includes both control and data traffic.

## Size the Cluster Control Link for Inter-Chassis Clustering

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.

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.
- 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.



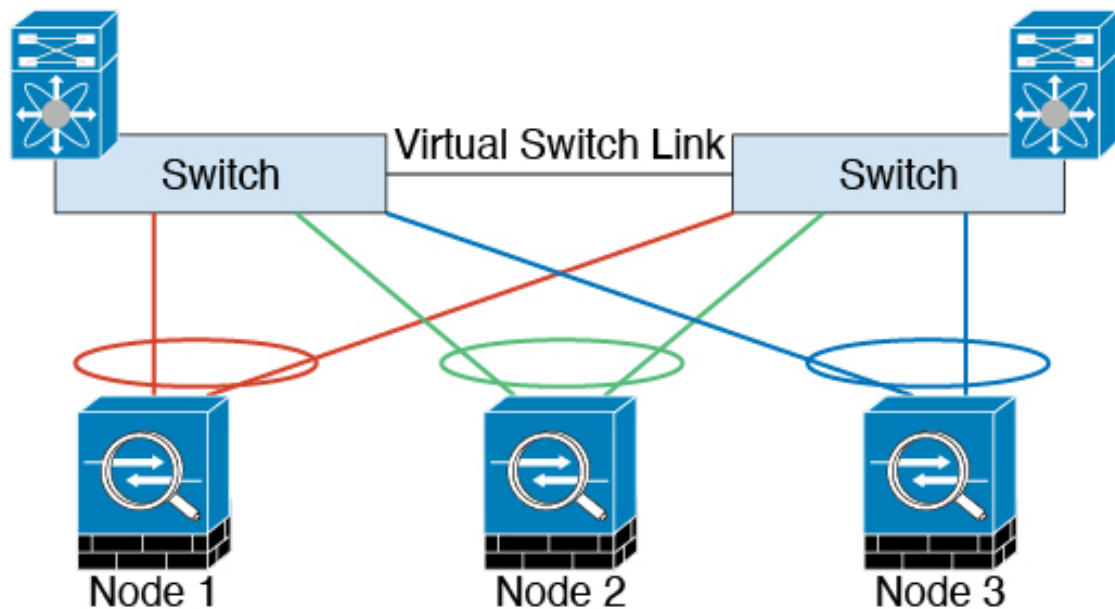
---

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

---

## Cluster Control Link Redundancy for Inter-Chassis Clustering

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 firewall 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 for Inter-Chassis Clustering

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 Network

The Firepower 4100/9300 chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: `127.2.chassis_id.slot_id`. For multi-instance clusters, which typically use different VLAN subinterfaces of the same EtherChannel, the same IP address can be used for different clusters because of VLAN separation. The cluster control link network cannot include any routers between units; only Layer 2 switching is allowed.

## Management Network

We recommend connecting all units to a single management network. This network is separate from the cluster control link.

## Management Interface

You must assign a Management type interface to the cluster. This interface is a special individual interface as opposed to a Spanned interface. The management interface lets you connect directly to each unit. This Management logical interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firepower Management Center. It uses its own local authentication, IP address, and static routing. Each cluster member uses a separate IP address on the management network that you set as part of the bootstrap configuration.



The management interface is shared between the Management logical interface and the *Diagnostic* logical interface. The Diagnostic logical interface is optional and is not configured as part of the bootstrap configuration. The Diagnostic interface can be configured along with the rest of the data interfaces. If you choose to configure the Diagnostic interface, configure a Main cluster IP address as a fixed address for the cluster that always belongs to the current control unit. You also configure a range of addresses so that each unit, including the current control unit, can use a Local address from the range. The Main cluster IP address provides consistent diagnostic access to an address; when a control unit changes, the Main cluster IP address moves to the new control unit, so access to the cluster continues seamlessly. For outbound management traffic such as TFTP or syslog, each unit, including the control unit, uses the Local IP address to connect to the server.

## Cluster Interfaces

For intra-chassis clustering, you can assign both physical interfaces or EtherChannels (also known as port channels) to the cluster. Interfaces assigned to the cluster are Spanned interfaces that load-balance traffic across all members of the cluster.

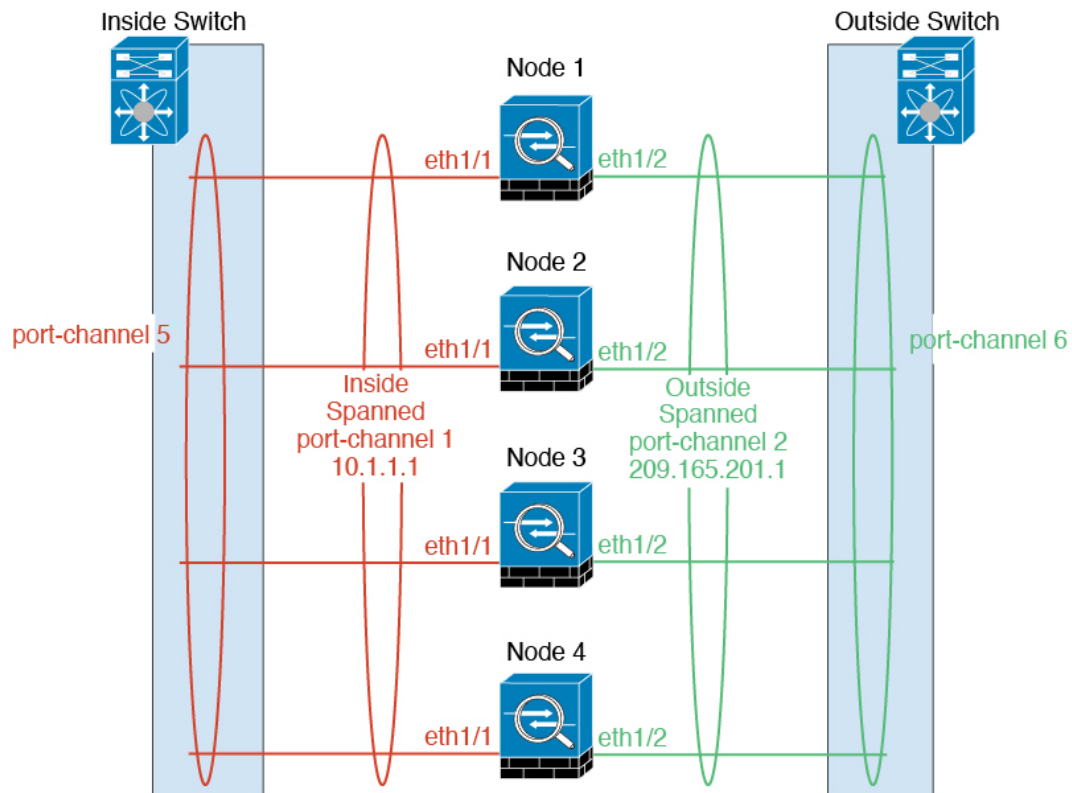
For inter-chassis clustering, you can only assign data EtherChannels to the cluster. These Spanned EtherChannels include the same member interfaces on each chassis; on the upstream switch, all of these interfaces are included in a single EtherChannel, so the switch does not know that it is connected to multiple devices.

Individual interfaces are not supported, with the exception of a management interface.

## Spanned EtherChannels

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.

For multi-instance clusters, each cluster requires dedicated data EtherChannels; you cannot use shared interfaces or VLAN subinterfaces.



## Connecting to a VSS or vPC

We recommend connecting EtherChannels to a VSS or vPC to provide redundancy for your interfaces.

## Configuration Replication

All nodes in the cluster share a single configuration. You can only make configuration changes on the control node (with the exception of the bootstrap configuration), and changes are automatically synced to all other nodes in the cluster.

## Licenses for Clustering

The FTD uses Smart Licensing. You assign licenses to the cluster as a whole, not to individual units. However, each unit of the cluster consumes a separate license for each feature. The clustering feature itself does not require any licenses.

When you add a cluster member to the FMC, you can specify the feature licenses you want to use for the cluster. You can modify licenses for the cluster in the **Devices > Device Management > Cluster > License** area.



**Note** If you add the cluster before the FMC is licensed (and running in Evaluation mode), then when you license the FMC, you can experience traffic disruption when you deploy policy changes to the cluster. Changing to licensed mode causes all data units to leave the cluster and then rejoin.

# Requirements and Prerequisites for Clustering

## Cluster Model Support

The FTD supports clustering on the following models:

- Firepower 9300—You can include up to 6 units in the cluster. For example, you can use 1 module in 6 chassis, or 2 modules in 3 chassis, or any combination that provides a maximum of 6 modules. Supports intra-chassis and inter-chassis clustering.
- Firepower 4100 series—Supported for up to 6 units using inter-chassis clustering.

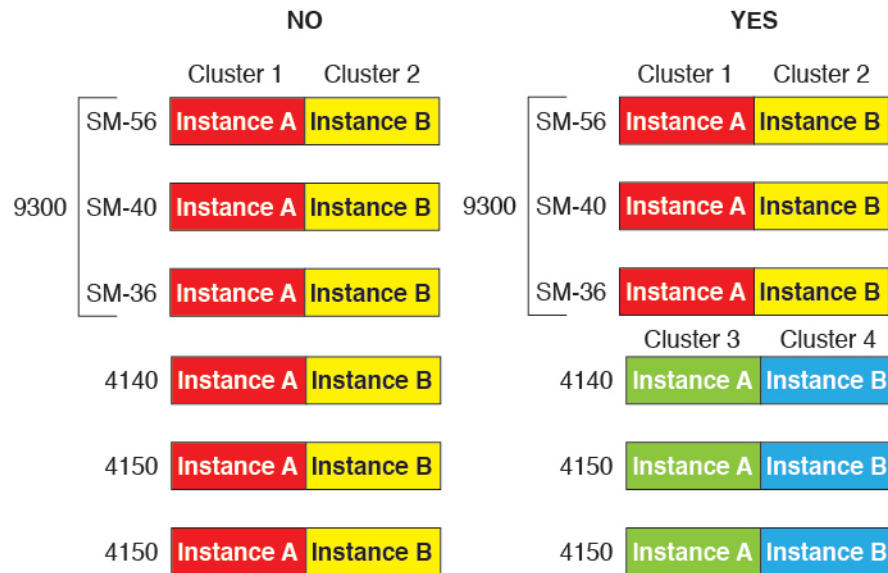
## User Roles

- Admin
- Access Admin
- Network Admin

## Inter-Chassis Clustering Hardware and Software Requirements

All chassis in a cluster:

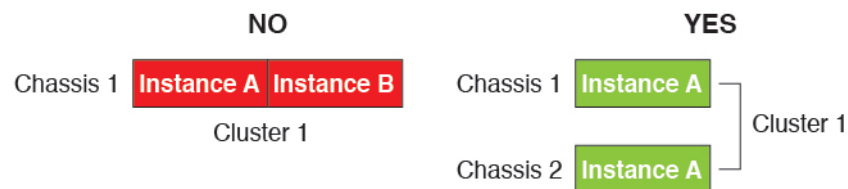
- Native instance clustering—For the Firepower 4100 series: All chassis must be the same model. For the Firepower 9300: All security modules must be the same type. For example, if you use clustering, all modules in the Firepower 9300 must be SM-40s. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots.
- Container instance clustering—We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. For example, you can create a cluster using an instance on a Firepower 9300 SM-56, SM-40, and SM-36. Or you can create a cluster on a Firepower 4140 and a 4150.



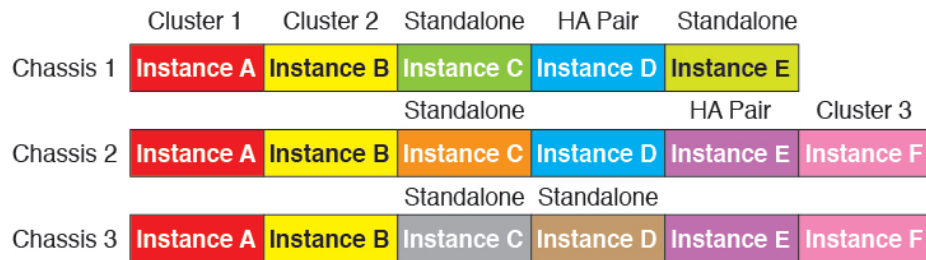
- Must run the identical FXOS software except at the time of an image upgrade.
- Must include the same interface configuration for interfaces you assign to the cluster, such as the same Management interface, EtherChannels, active interfaces, speed and duplex, and so on. You can use different network module types on the chassis as long as the capacity matches for the same interface IDs and interfaces can successfully bundle in the same spanned EtherChannel. Note that all data interfaces must be EtherChannels in inter-chassis clustering. If you change the interfaces in FXOS after you enable clustering (by adding or removing interface modules, or configuring EtherChannels, for example), then perform the same changes on each chassis, starting with the data nodes, and ending with the control node.
- Must use the same NTP server. For Firepower Threat Defense, the Firepower Management Center must also use the same NTP server. Do not set the time manually.

### Multi-Instance Clustering Requirements

- No intra-security-module/engine clustering—For a given cluster, you can only use a single container instance per security module/engine. You cannot add 2 container instances to the same cluster if they are running on the same module.



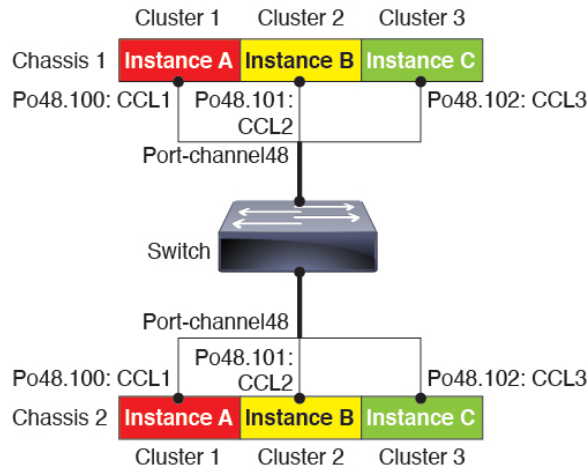
- Mix and match clusters and standalone instances—Not all container instances on a security module/engine need to belong to a cluster. You can use some instances as standalone or High Availability nodes. You can also create multiple clusters using separate instances on the same security module/engine.



- All 3 modules in a Firepower 9300 must belong to the cluster—For the Firepower 9300, a cluster requires a single container instance on all 3 modules. You cannot create a cluster using instances on module 1 and 2, and then use a native instance on module 3, or example.

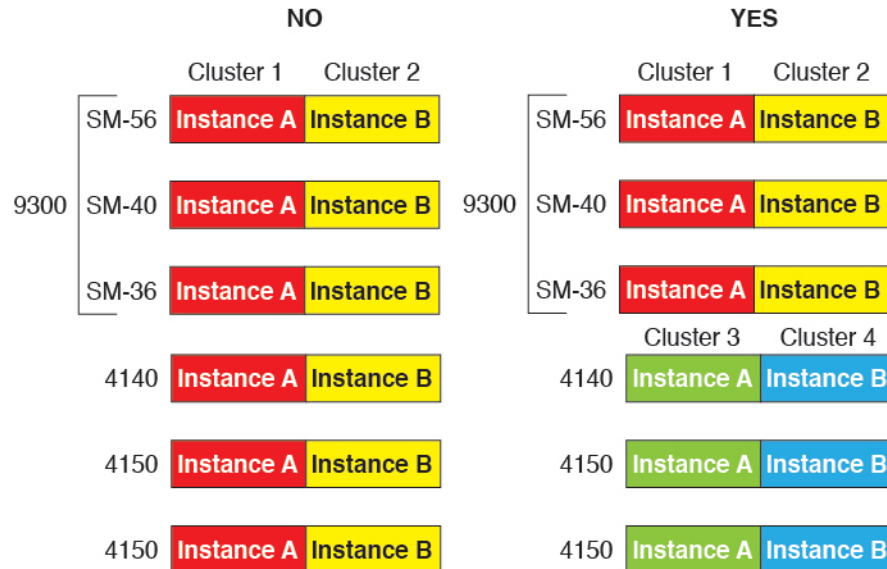


- Match resource profiles—We recommend that each node in the cluster use the same resource profile attributes; however, mismatched resources are allowed when changing cluster nodes to a different resource profile, or when using different models.
- Dedicated cluster control link—For inter-chassis clustering, each cluster needs a dedicated cluster control link. For example, each cluster can use a separate subinterface on the same cluster-type EtherChannel, or use separate EtherChannels.



- No shared interfaces—Shared-type interfaces are not supported with clustering. However, the same Management and Eventing interfaces can be used by multiple clusters.
- No subinterfaces—A multi-instance cluster cannot use FXOS-defined VLAN subinterfaces. An exception is made for the cluster control link, which can use a subinterface of the Cluster EtherChannel.
- Mix chassis models—We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300.

security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. For example, you can create a cluster using an instance on a Firepower 9300 SM-56, SM-40, and SM-36. Or you can create a cluster on a Firepower 4140 and a 4150.



- Maximum 6 nodes—You can use up to six container instances in a cluster.

### Switch Requirements for Inter-Chassis Clustering

- Be sure to complete the switch configuration and successfully connect all the EtherChannels from the chassis to the switch(es) before you configure clustering on the Firepower 4100/9300 chassis.
- For supported switch characteristics, see [Cisco FXOS Compatibility](#).

## Clustering Guidelines and Limitations

### Switches for Inter-Chassis Clustering

- Make sure connected switches match the MTU for both cluster data interfaces and the cluster control link interface. You should configure the cluster control link interface MTU to be at least 100 bytes higher than the data interface MTU, so make sure to configure the cluster control link connecting switch appropriately. Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead.
- For Cisco IOS XR systems, if you want to set a non-default MTU, set the IOS 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 IOS *IPv4* MTU. This adjustment is not required for Cisco Catalyst and Cisco Nexus switches.
- On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.

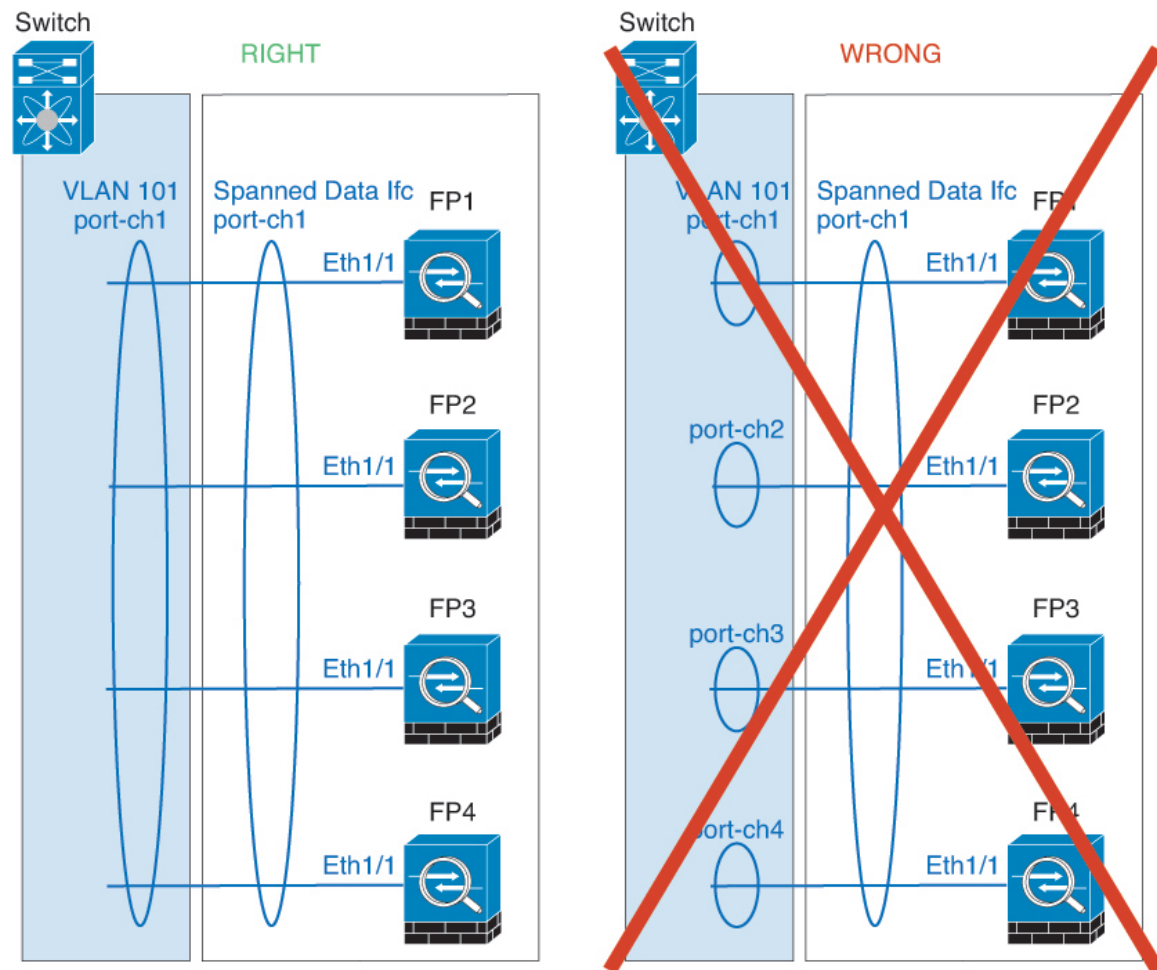
- On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: **source-dest-ip** or **source-dest-ip-port** (see the Cisco Nexus OS and Cisco IOS **port-channel load-balance** command). Do not use a **vlan** keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster.
- 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.
- Firepower 4100/9300 clusters support LACP graceful convergence. So you can leave LACP graceful convergence enabled on connected Cisco Nexus switches.
- 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. FXOS EtherChannels have the LACP rate set to fast by default. 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.

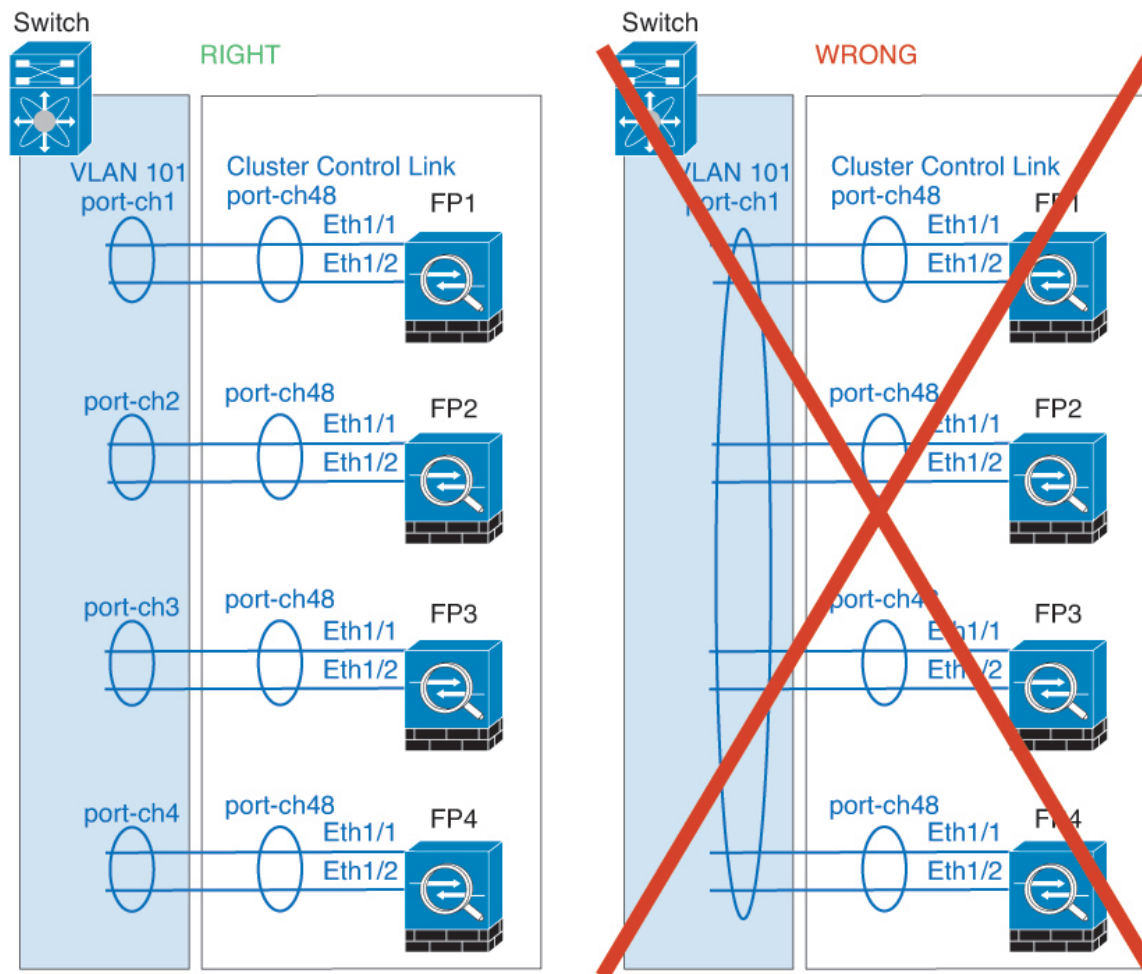
### EtherChannels for Inter-Chassis Clustering

- 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 control unit 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.





### Additional Guidelines

- 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 connections; 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 interface, 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 cluster. These messages can result in some units of the cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.
- We recommend connecting EtherChannels to a VSS or vPC for redundancy.
- Within a chassis, you cannot cluster some security modules and run other security modules in standalone mode; you must include all security modules in the cluster.
- For decrypted TLS/SSL connections, the decryption states are not synchronized, and if the connection owner fails, then decrypted connections will be reset. New connections will need to be established to a

new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.

### Defaults

- 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 set to unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is set to 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

## Configure Clustering

You can easily deploy the cluster from the Firepower 4100/9300 chassis supervisor. All initial configuration is automatically generated for each unit. You can then add the units to the FMC and group them into a cluster.

### FXOS: Add a Firepower Threat Defense Cluster

In native mode: You can add a single Firepower 9300 chassis as an intra-chassis cluster, or add multiple chassis for inter-chassis clustering.

In multi-instance mode: You can add one or more clusters on a single Firepower 9300 chassis as intra-chassis clusters (you must include an instance on each module), or add one or more clusters on multiple chassis for inter-chassis clustering.

For inter-chassis clustering, you must configure each chassis separately. Add the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

### Create a Firepower Threat Defense Cluster

You can easily deploy the cluster from the Firepower 4100/9300 chassis supervisor. All initial configuration is automatically generated for each unit.

For inter-chassis clustering, you must configure each chassis separately. Deploy the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

In a Firepower 9300 chassis, you must enable clustering for all 3 module slots, or for container instances, a container instance in each slot, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

#### Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 4100/9300 chassis.
- For container instances, if you do not want to use the default profile, add a resource profile according to [Add a Resource Profile for Container Instances](#).

- For container instances, before you can install a container instance for the first time, you must reinitialize the security module/engine so that the disk has the correct formatting. Choose **Security Modules** or **Security Engine**, and click the Reinitialize icon (🔄). An existing logical device will be deleted and then reinstalled as a new device, losing any local application configuration. If you are replacing a native instance with container instances, you will need to delete the native instance in any case. You cannot automatically migrate a native instance to a container instance.
- Gather the following information:
  - Management interface ID, IP addresses, and network mask
  - Gateway IP address
  - FMC IP address and/or NAT ID of your choosing
  - DNS server IP address
  - FTD hostname and domain name

## Step 1

Configure interfaces.

- a) Add at least one Data type interface or EtherChannel (also known as a port-channel) before you deploy the cluster. See [Add an EtherChannel \(Port Channel\)](#) or [Configure a Physical Interface](#).

For inter-chassis clustering, all data interfaces must be Spanned EtherChannels with at least one member interface. Add the same EtherChannels on each chassis. Combine the member interfaces from all cluster units into a single EtherChannel on the switch. See [Clustering Guidelines and Limitations, on page 10](#) for more information about EtherChannels for inter-chassis clustering.

For multi-instance clustering, you cannot use FXOS-defined VLAN subinterfaces or data-sharing interfaces in the cluster. Only application-defined subinterfaces are supported. See [FXOS Interfaces vs. Application Interfaces](#) for more information.

- b) Add a Management type interface or EtherChannel. See [Add an EtherChannel \(Port Channel\)](#) or [Configure a Physical Interface](#).

The management interface is required. Note that this management interface is not the same as the chassis management interface that is used only for chassis management (in FXOS, you might see the chassis management interface displayed as MGMT, management0, or other similar names).

For inter-chassis clustering, add the same Management interface on each chassis.

For multi-instance clustering, you can share the same management interface across multiple clusters on the same chassis, or with standalone instances.

- c) For inter-chassis clustering, add a member interface to the cluster control link EtherChannel (by default, port-channel 48). See [Add an EtherChannel \(Port Channel\)](#).

Do not add a member interface for intra-chassis clustering. If you add a member, the chassis assumes this cluster will be inter-chassis, and will only allow you to use Spanned EtherChannels, for example.

On the **Interfaces** tab, the port-channel 48 cluster type interface shows the **Operation State** as **failed** if it does not include any member interfaces. For intra-chassis clustering, this EtherChannel does not require any member interfaces, and you can ignore this Operational State.

Add the same member interfaces on each chassis. The cluster control link is a device-local EtherChannel on each chassis. Use separate EtherChannels on the switch per device. See [Clustering Guidelines and Limitations, on page 10](#) for more information about EtherChannels for inter-chassis clustering.

For multi-instance clustering, you can create additional Cluster type EtherChannels. Unlike the Management interface, the cluster control link is *not* sharable across multiple devices, so you will need a Cluster interface for each cluster. However, we recommend using VLAN subinterfaces instead of multiple EtherChannels; see the next step to add a VLAN subinterface to the Cluster interface.

- d) For multi-instance clustering, add VLAN subinterfaces to the cluster EtherChannel so you have a subinterface for each cluster. See [Add a VLAN Subinterface for Container Instances](#).

If you add subinterfaces to a Cluster interface, you cannot use that interface for a native cluster.

- e) (Optional) Add a Firepower-eventing interface. See [Add an EtherChannel \(Port Channel\)](#) or [Configure a Physical Interface](#).

This interface is a secondary management interface for FTD devices. To use this interface, you must configure its IP address and other parameters at the FTD CLI. For example, you can separate management traffic from events (such as web events). See the **configure network** commands in the Firepower Threat Defense command reference.

For inter-chassis clustering, add the same eventing interface on each chassis.

## Step 2 Choose Logical Devices.

## Step 3 Click **Add > Cluster**, and set the following parameters:

**Figure 1: Native Cluster**

**Add Cluster**

I want to: Create New Cluster

Device Name: cluster1

Template: Cisco Firepower Threat Defense

Image Version: 6.5.0.1159

Instance Type: Native

OK Cancel

**Figure 2: Multi-Instance Cluster**

**Add Cluster**

I want to: Create New Cluster

Device Name: cluster1

Template: Cisco Firepower Threat Defense

Image Version: 6.5.0.39

Instance Type: Container

Resource Profile: Default-Small

SM 1 - 46 Cores Available  
SM 2 - 46 Cores Available  
SM 3 - Module offline. No information available

**i** Before you add the first container instance, you must reinitialize the security module/engine so that the disk has the correct formatting. You only need to perform this action once.

OK Cancel

- a) Choose **I want to: > Create New Cluster**
- b) Provide a **Device Name**.

This name is used internally by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

- c) For the **Template**, choose **Cisco Firepower Threat Defense**.
- d) Choose the **Image Version**.
- e) For the **Instance Type**, choose either **Native** or **Container**.

A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance. A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances.

- f) (Container Instance only) For the **Resource Type**, choose one of the resource profiles from the drop-down list.

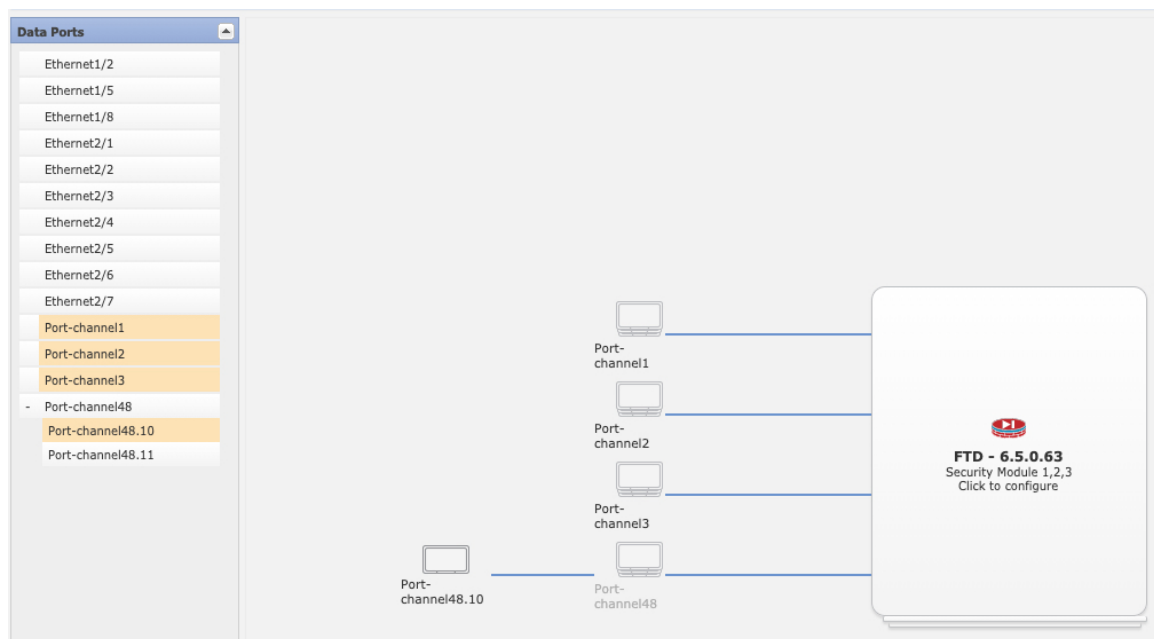
For the Firepower 9300, this profile will be applied to each instance on each security module. You can set different profiles per security module later in this procedure; for example, if you are using different security module types, and you want to use more CPUs on a lower-end model. We recommend choosing the correct profile before you create the cluster. If you need to create a new profile, cancel out of the cluster creation, and add one using [Add a Resource Profile for Container Instances](#).

- g) Click **OK**.

You see the Provisioning - *device name* window.

#### Step 4

Choose the interfaces you want to assign to this cluster.



For native mode clustering: All valid interfaces are assigned by default. If you defined multiple Cluster type interfaces, deselect all but one.

For multi-instance clustering: Choose each data interface you want to assign to the cluster, and also choose the Cluster type port-channel or port-channel subinterface.

#### Step 5

Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

**Step 6** On the **Cluster Information** page, complete the following.

**Figure 3: Native Cluster**

The image shows a screenshot of the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box. The 'Cluster Information' tab is selected, showing fields for Chassis ID, Site ID, Cluster Key, Confirm Cluster Key, Cluster Group Name, Management Interface, and CCL Subnet IP. The 'Security Module' section is also visible, showing 'Security Module-1, Security Module-2, Security Module-3'. The 'OK' and 'Cancel' buttons are at the bottom.

**Cisco Firepower Threat Defense - Bootstrap Configuration** ? X

**Cluster Information** Settings Interface Information Agreement

**Security Module**

Security Module-1, Security Module-2, Security Module-3

**Interface Information**

Chassis ID: 1

Site ID: 1

Cluster Key: \*\*\*\*

Confirm Cluster Key: \*\*\*\*

Cluster Group Name: cluster1

Management Interface: Ethernet1/4

CCL Subnet IP: Eg:x.x.0.0

OK Cancel

Figure 4: Multi-Instance Cluster

**Cisco Firepower Threat Defense - Bootstrap Configuration**

**Cluster Information** Settings Interface Information Agreement

**Security Module(SM) and Resource Profile Selection**

Security Module-1, Security Module-2, Security Module-3

**Resource Profile Selection**

Security Module 1: Default-Small

SM 1 - 46 Cores Available

Security Module 2: Default-Small

SM 2 - 46 Cores Available

Security Module 3: Default-Small

**Interface Information**

Chassis ID: 1

Site ID: 1

Cluster Key: ....

Confirm Cluster Key: ....

Cluster Group Name: mi-cluster-1

Management Interface: Ethernet1/4

CCL Subnet IP: Eg:x.x.0.0

OK Cancel

- (Container Instance for the Firepower 9300 only) In the **Security Module (SM) and Resource Profile Selection** area, you can set a different resource profile per module; for example, if you are using different security module types, and you want to use more CPUs on a lower-end model.
- For inter-chassis clustering, in the **Chassis ID** field, enter a chassis ID. Each chassis in the cluster must use a unique ID.

This field only appears if you added a member interface to cluster control link Port-Channel 48.

- For inter-site clustering, in the **Site ID** field, enter the site ID for this chassis between 1 and 8. FlexConfig feature. Additional inter-site cluster customizations to enhance redundancy and stability, such as director localization, site redundancy, and cluster flow mobility, are only configurable using the Firepower Management Center FlexConfig feature.
- In the **Cluster Key** field, configure an authentication key for control traffic on the cluster control link.

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

- Set the **Cluster Group Name**, which is the cluster group name in the logical device configuration.

The name must be an ASCII string from 1 to 38 characters.

- Choose the **Management Interface**.

This interface is used to manage the logical device. This interface is separate from the chassis management port.

If you assign a Hardware Bypass-capable interface as the Management interface, you see a warning message to make sure your assignment is intentional.

- g) (Optional) Set the **CCL Subnet IP** as *a.b.0.0*.

By default, the cluster control link uses the 127.2.0.0/16 network. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. In this case, specify any /16 network address on a unique network for the cluster, except for loopback (127.0.0.0/8), multicast (224.0.0.0/4), and internal (169.254.0.0/16) addresses. If you set the value to 0.0.0.0, then the default network is used.

The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: *a.b.chassis\_id.slot\_id*.

## Step 7

On the **Settings** page, complete the following.

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' dialog box with the 'Settings' tab selected. The fields and their values are as follows:

Field	Value
Registration Key:	****
Confirm Registration Key:	****
Password:	*****
Confirm Password:	*****
Firepower Management Center IP:	10.89.5.35
Permit Expert mode for FTD SSH sessions:	yes
Search domains:	cisco.com
Firewall Mode:	Routed
DNS Servers:	10.89.4.5
Firepower Management Center NAT ID:	test
Fully Qualified Hostname:	ftd1.cisco.com
Eventing Interface:	

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- a) In the **Registration Key** field, enter the key to be shared between the Firepower Management Center and the cluster members during registration.

You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.

- b) Enter a **Password** for the FTD admin user for CLI access.
- c) In the **Firepower Management Center IP** field, enter the IP address of the managing Firepower Management Center. If you do not know the FMC IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.
- d) (Optional) For a container instance, **Permit Expert mode from FTD SSH sessions: Yes or No**. Expert Mode provides FTD shell access for advanced troubleshooting.

If you choose **Yes** for this option, then users who access the container instance directly from an SSH session can enter Expert Mode. If you choose **No**, then only users who access the container instance from the FXOS CLI can enter Expert Mode. We recommend choosing **No** to increase isolation between instances.



Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the FTD CLI.

- e) (Optional) In the **Search Domains** field, enter a comma-separated list of search domains for the management network.
- f) (Optional) From the **Firewall Mode** drop-down list, choose **Transparent** or **Routed**.

In routed mode, the FTD is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

- g) (Optional) In the **DNS Servers** field, enter a comma-separated list of DNS servers.

The FTD uses DNS if you specify a hostname for the FMC, for example.

- h) (Optional) In the **Firepower Management Center NAT ID** field, enter a passphrase that you will also enter on the FMC when you add the cluster as a new device.

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. You can specify any text string as the NAT ID, from 1 to 37 characters. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

- i) (Optional) In the **Fully Qualified Hostname** field, enter a fully qualified name for the FTD device.

Valid characters are the letters from a to z, the digits from 0 to 9, the dot (.), and the hyphen (-); maximum number of characters is 253.

- j) (Optional) From the **Eventing Interface** drop-down list, choose the interface on which Firepower events should be sent. If not specified, the management interface will be used.

To specify a separate interface to use for Firepower events, you must configure an interface as a *firepower-eventing* interface. If you assign a Hardware Bypass-capable interface as the Eventing interface, you see a warning message to make sure your assignment is intentional.

## Step 8

On the **Interface Information** page, configure a management IP address for each security module in the cluster. Select the type of address from the **Address Type** drop-down list and then complete the following for each security module.

**Note** You must set the IP address for all 3 module slots in a chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

**Cisco Firepower Threat Defense - Bootstrap Configuration** ? X

Cluster Information Settings **Interface Information** Agreement

Address Type: IPv4 only

**Security Module 1**  
**IPv4**

Management IP: 10.89.5.20

Network Mask: 255.255.255.192

Gateway: 10.89.5.1

**Security Module 2**  
**IPv4**

Management IP: 10.89.5.21

Network Mask: 255.255.255.192

Gateway: 10.89.5.1

**Security Module 3**  
**IPv4**

Management IP: 10.89.5.22

Network Mask: 255.255.255.192

Gateway: 10.89.5.1

OK Cancel

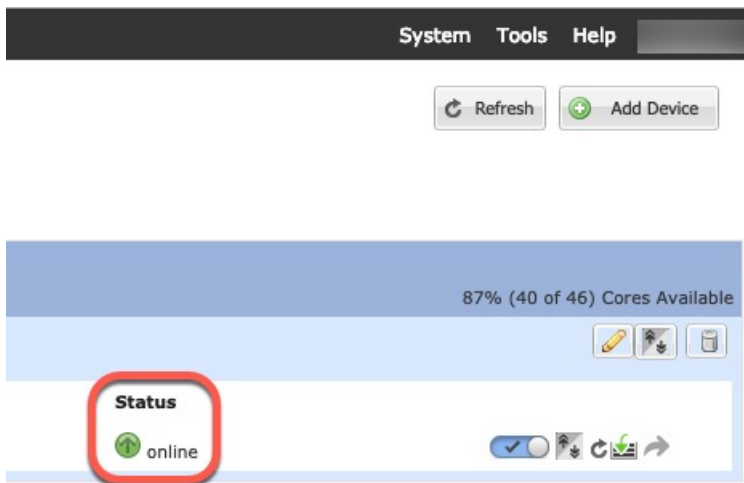
- a) In the **Management IP** field, configure an IP address.  
Specify a unique IP address on the same network for each module.
- b) Enter a **Network Mask** or **Prefix Length**.
- c) Enter a **Network Gateway** address.

**Step 9** On the **Agreement** tab, read and accept the end user license agreement (EULA).

**Step 10** Click **OK** to close the configuration dialog box.

**Step 11** Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can add the remaining cluster chassis, or for intra-chassis clustering start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.

**Step 12**

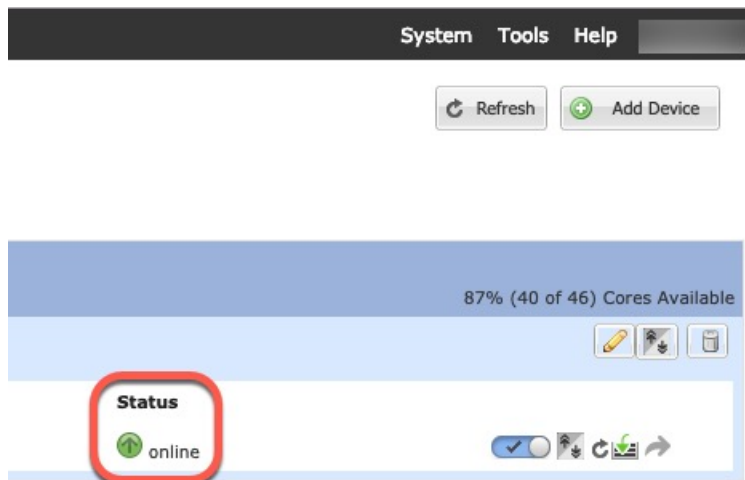
For inter-chassis clustering, add the next chassis to the cluster:

- On the first chassis Firepower Chassis Manager, click the **Show Configuration icon** at the top right; copy the displayed cluster configuration.
- Connect to the Firepower Chassis Manager on the next chassis, and add a logical device according to this procedure.
- Choose **I want to: > Join an Existing Cluster**.
- Click **OK**.
- In the **Copy Cluster Details** box, paste in the cluster configuration from the first chassis, and click **OK**.
- Click the device icon in the center of the screen. The cluster information is mostly pre-filled, but you must change the following settings:
  - **Chassis ID**—Enter a unique chassis ID.
  - **Site ID**—For inter-site clustering, enter the site ID for this chassis between 1 and 8. Additional inter-site cluster customizations to enhance redundancy and stability, such as director localization, site redundancy, and cluster flow mobility, are only configurable using the Firepower Management Center FlexConfig feature.
  - **Cluster Key**—(Not prefilled) Enter the same cluster key.
  - **Management IP**—Change the management address for each module to be a unique IP address on the same network as the other cluster members.

Click **OK**.

- Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for each cluster member for the status of the new logical device. When the logical device for each cluster member shows its **Status** as **online**, you can start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.



**Step 13** Add the control unit to the Firepower Management Center using the management IP address.

All cluster units must be in a successfully-formed cluster on FXOS prior to adding them to Firepower Management Center.

The Firepower Management Center then automatically detects the data units.

## Add More Cluster Units

Add or replace the FTD cluster unit in an existing cluster. When you add a new cluster unit in FXOS, the Firepower Management Center adds the unit automatically.



**Note** The FXOS steps in this procedure only apply to adding a new *chassis*; if you are adding a new module to a Firepower 9300 where clustering is already enabled, the module will be added automatically.

### Before you begin

- In the case of a replacement, you must delete the old cluster unit from the Firepower Management Center. When you replace it with a new unit, it is considered to be a new device on the Firepower Management Center.
- The interface configuration must be the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.

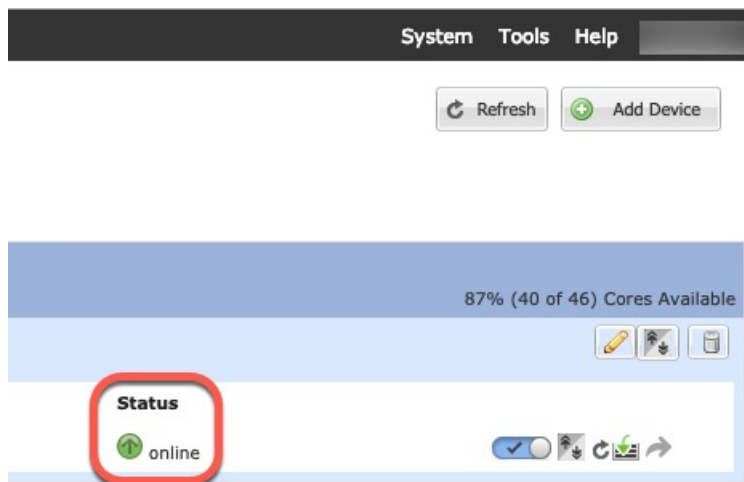
- Step 1** On an existing cluster chassis Firepower Chassis Manager, choose **Logical Devices** to open the **Logical Devices** page.
- Step 2** Click the **Show Configuration icon** at the top right; copy the displayed cluster configuration.
- Step 3** Connect to the Firepower Chassis Manager on the new chassis, and click **Add > Cluster**.
- Step 4** For the **Device Name**, provide a name for the logical device.
- Step 5** Click **OK**.
- Step 6** In the **Copy Cluster Details** box, paste in the cluster configuration from the first chassis, and click **OK**.

- Step 7** Click the device icon in the center of the screen. The cluster information is mostly pre-filled, but you must change the following settings:
- **Chassis ID**—Enter a unique chassis ID.
  - **Site ID**—For inter-site clustering, enter the site ID for this chassis between 1 and 8. This feature is only configurable using the Firepower Management Center FlexConfig feature.
  - **Cluster Key**—(Not prefilled) Enter the same cluster key.
  - **Management IP**—Change the management address for each module to be a unique IP address on the same network as the other cluster members.

Click **OK**.

- Step 8** Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for each cluster member for the status of the new logical device. When the logical device for each cluster member shows its **Status** as **online**, you can start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.



## FMC: Add a Cluster

Add one of the cluster units as a new device to the Firepower Management Center; the FMC auto-detects all other cluster members.

### Before you begin

- This method for adding a cluster requires Firepower Threat Defense Version 6.2 or later. If you need to manage an earlier version device, then refer to the Firepower Management Center configuration guide for that version.

- All cluster units must be in a successfully-formed cluster on FXOS prior to adding the cluster to the Management Center. You should also check which unit is the control unit. Refer to the Firepower Chassis Manager **Logical Devices** screen or use the Firepower Threat Defense **show cluster info** command.

**Step 1**

In the FMC, choose **Devices > Device Management**, and then choose **Add > Add Device** to add the control unit using the unit's management IP address you assigned when you deployed the cluster.

**Add Device**

Host:†

Display Name:

Registration Key:†

Group:

Access Control Policy:†

Smart Licensing

☒ Malware

☒ Threat

☒ URL Filtering

Advanced Settings

Unique NAT ID:†

☒ Transfer Packets

- In the **Host** field, enter the IP address or hostname of the control unit.  
 We recommend adding the control unit for the best performance, but you can add any unit of the cluster.  
 If you used a NAT ID during device setup, you may not need to enter this field. For more information, see [NAT Environments](#).
- In the **Display Name** field, enter a name for the control unit as you want it to display in the FMC.  
 This display name is not for the cluster; it is only for the control unit you are adding. You can later change the name of other cluster members and the cluster display name.
- In the **Registration Key** field, enter the same registration key that you used when you deployed the cluster in FXOS.  
 The registration key is a one-time-use shared secret.
- In a multidomain deployment, regardless of your current domain, assign the device to a leaf **Domain**.

If your current domain is a leaf domain, the device is automatically added to the current domain. If your current domain is not a leaf domain, post-registration, you must switch to the leaf domain to configure the device.

- e) (Optional) Add the device to a device **Group**.
- f) Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If you create a new policy, you create a basic policy only. You can later customize the policy as needed.

### New Policy

Name:

Description:

Select Base Policy:

Default Action:  
☒ Block all traffic  
☐ Intrusion Prevention  
☐ Network Discovery

Snort3: ☐

- g) Choose licenses to apply to the device.
- h) If you used a NAT ID during device setup, expand the **Advanced** section and enter the same NAT ID in the **Unique NAT ID** field.
- i) Check the **Transfer Packets** check box to allow the device to transfer packets to the FMC.

This option is enabled by default. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the FMC for inspection. If you disable it, only event information will be sent to the FMC but packet data is not sent.

- j) Click **Register**.

The FMC identifies and registers the control unit, and then registers all data units. If the control unit does not successfully register, then the cluster is not added. A registration failure can occur if the cluster was not up on the chassis, or because of other connectivity issues. In this case, we recommend that you try re-adding the cluster unit.

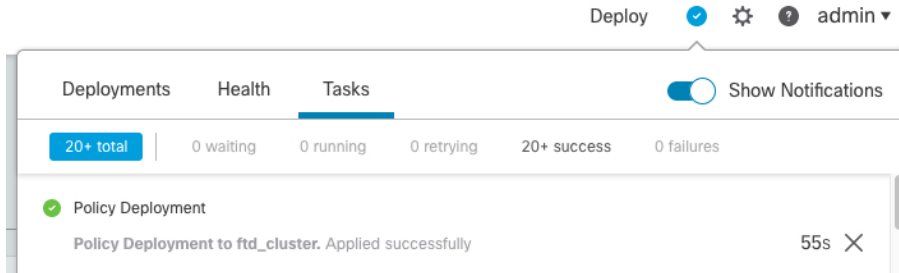
The cluster name shows on the **Devices > Device Management** page; expand the cluster to see the cluster units.

Name	Model	Version	Chassis	Licenses	Access Control Policy	
Ungrouped (1)						
ftd_cluster						
Cluster						
10.89.5.21 10.89.5.21 - Routed	FTD on Firepower 9300 SM-24	6.6.0	firepower-9300.cisco.com:443	Base, Threat (2 more...)	None	🗑️ ⚙️
FTD1(Master) 10.89.5.20 - Routed	FTD on Firepower 9300 SM-24	6.6.0	firepower-9300.cisco.com:443 Security Module - 1	Base, Threat (2 more...)	None	⚙️

A unit that is currently registering shows the loading icon.

ftd_cluster	
Cluster	
10.89.5.21 10.89.5.21 - Routed	
FTD1(Master) 10.89.5.20 - Routed	

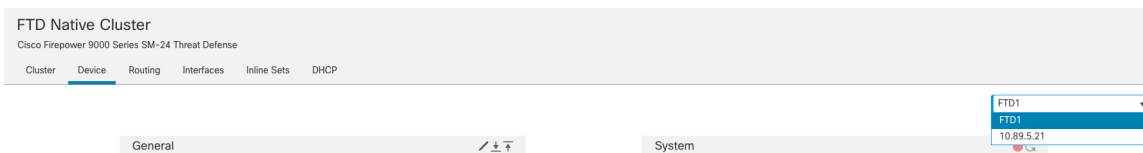
You can monitor cluster unit registration by clicking the **Notifications** icon and choosing **Tasks**. The FMC updates the Cluster Registration task as each unit registers. If any units fail to register, see [Reconcile Cluster Members, on page 36](#).



**Step 2** Configure device-specific settings by clicking the **Edit** (✎) for the cluster.

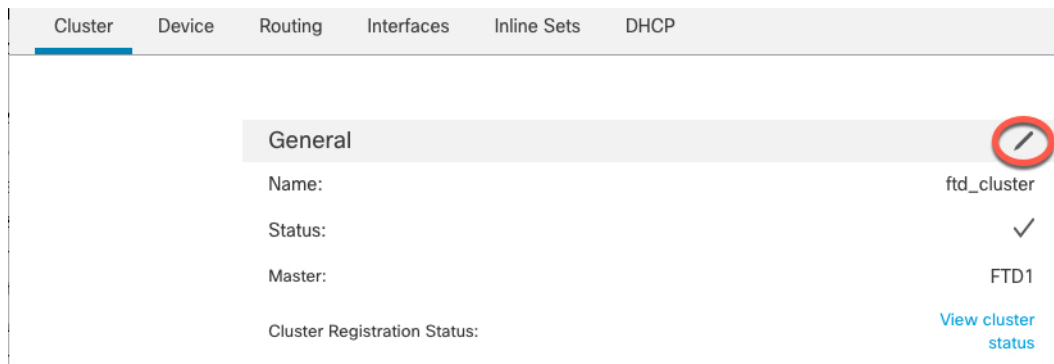
Most configuration can be applied to the cluster as a whole, and not member units in the cluster. For example, you can change the display name per unit, but you can only configure interfaces for the whole cluster.

**Step 3** On the **Devices > Device Management > Cluster** screen, you see **General**, **License**, **System**, and **Health** settings.



See the following cluster-specific items:

- **General > Name**—Change the cluster display name by clicking the **Edit** (✎).



Then set the **Name** field.



**General**

Name::

Transfer Packets: ☐

Compliance Mode:

Force Deploy: →

- **General > View cluster status**—Click the **View cluster status** link to open the **Cluster Status** dialog box.

Cluster Device Routing Interfaces Inline Sets DHCP

**General**

Name: ftd\_cluster

Status: ✓

Master: FTD1

Cluster Registration Status: [View cluster status](#)

The **Cluster Status** dialog box also lets you retry data unit registration by clicking **Reconcile**.

**Cluster Status (2 Nodes)**

Status	Device Name	Unit Name	Chassis URL
In Sync.	10.89.5.20	unit-1-1	<a href="https://firepower-9300.c...">https://firepower-9300.c...</a>
In Sync.	10.89.5.21	unit-1-2	<a href="https://firepower-9300.c...">https://firepower-9300.c...</a>

Dated: 14 Jan 2020 | 01:51:51

- **License**—Click **Edit** (✎) to set license entitlements.

**Step 4** On the **Devices > Device Management > Devices**, you can choose each member in the cluster from the top right drop-down menu and configure the following settings.

- **General > Name**—Change the cluster member display name by clicking the **Edit** (✎).

General	
Name:	10.89.5.21
Transfer Packets:	Yes
Mode:	routed
Compliance Mode:	None
TLS Crypto Acceleration:	Enabled

Then set the **Name** field.

General	
Name:	<input type="text" value="FTD2"/>
Transfer Packets:	<input checked="" type="checkbox"/>
Mode:	routed
Compliance Mode:	None
Force Deploy:	→
<div> <div>Cancel</div> <div>Save</div> </div>	

- **Management > Host**—If you change the management IP address in the device configuration, you must match the new address in the FMC so that it can reach the device on the network; edit the **Host** address in the **Management** area.

Management	
Host:	10.89.5.20
Status:	✓

## FMC: Configure Cluster, Data, and Diagnostic Interfaces

This procedure configures basic parameters for each data interface that you assigned to the cluster when you deployed it in FXOS. For inter-chassis clustering, data interfaces are always Spanned EtherChannel interfaces. For the cluster control link interface for inter-chassis clustering, you must increase the MTU from the default. You can also configure the Diagnostic interface, which is the only interface that can run as an individual interface.



**Note** When using Spanned EtherChannels for inter-chassis clustering, 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.

**Step 1** Choose **Devices > Device Management**, and click **Edit** (✎) next to the cluster.

**Step 2** Click **Interfaces**.

**Step 3** Configure the cluster control link.

For inter-chassis clustering, set the cluster control link MTU to be at least 100 bytes higher than the highest MTU of the data interfaces. Because the cluster control link traffic includes data packet forwarding, the cluster control link needs to accommodate the entire size of a data packet plus cluster traffic overhead. We suggest setting the MTU to the maximum of 9184; the minimum value is 1400 bytes. For example, because the maximum MTU is 9184, then the highest data interface MTU can be 9084, while the cluster control link can be set to 9184.

For native clusters: The cluster control link interface is Port-Channel48 by default.

- a) Click **Edit** (✎) for the cluster control link interface.
- b) On the **General** page, in the **MTU** field, enter a value between 1400 and 9184. We suggest using the maximum, 9184.
- c) Click **OK**.

**Step 4** Configure data interfaces.

- a) (Optional) Configure VLAN subinterfaces on the data interface. The rest of this procedure applies to the subinterfaces. See [Add a Subinterface](#).
- b) Click **Edit** (✎) for the data interface.
- c) Configure the name, IP address, and other parameters according to [Configure Routed Mode Interfaces](#) or [Configure Bridge Group Interfaces](#).

**Note** If the cluster control link interface MTU is not at least 100 bytes higher than the data interface MTU, you will see an error that you must reduce the MTU of the data interface. See step [Step 3, on page 31](#) to increase the cluster control link MTU, after which you can continue configuring the data interfaces.

- d) For inter-chassis clusters, set a manual global MAC address for the EtherChannel. Click **Advanced**, and in the **Active Mac Address** field, enter a MAC address in H.H.H format, where H is a 16-bit hexadecimal digit.

For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.

Do not set the **Standby Mac Address**; it is ignored.

You must configure a MAC address for a Spanned EtherChannel to avoid potential network connectivity problems. With a manually-configured MAC address, the MAC address stays with the current control unit. If you do not configure a MAC address, then if the control unit changes, the new control unit uses a new MAC address for the interface, which can cause a temporary network outage.

- e) Click **OK**. Repeat the above steps for other data interfaces.

**Step 5** (Optional) Configure the Diagnostic interface.

The Diagnostic interface is the only interface that can run in Individual interface mode. You can use this interface for syslog messages or SNMP, for example.

- a) Choose **Objects > Object Management > Address Pools** to add an IPv4 and/or IPv6 address pool. See [Address Pools](#).

Include at least as many addresses as there are units in the cluster. The Virtual IP address is not a part of this pool, but needs to be on the same network. You cannot determine the exact Local address assigned to each unit in advance.

- b) On **Devices > Device Management > Interfaces**, click **Edit** (✎) for the Diagnostic interface.
- c) On the **IPv4**, enter the **IP Address** and mask. This IP address is a fixed address for the cluster, and always belongs to the current control unit.
- d) From the **IPv4 Address Pool** drop-down list, choose the address pool you created.
- e) On **IPv6 > Basic**, from the **IPv6 Address Pool** drop-down list, choose the address pool you created.
- f) Configure other interface settings as normal.

#### Step 6 Click Save.

You can now go to **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

## FXOS: Remove a Cluster Unit

The following sections describe how to remove units temporarily or permanently from the cluster.

### Temporary Removal

A cluster unit will be automatically removed from the cluster due to a hardware or network failure, for example. This removal is temporary until the conditions are rectified, and it can rejoin the cluster. You can also manually disable clustering.

To check whether a device is currently in the cluster, check the cluster status on the Firepower Chassis Manager **Logical Devices** page:



The screenshot shows the 'Logical Devices' page in the Firepower Chassis Manager. At the top, there are icons for edit, refresh, delete, and a back arrow. Below this is a table with two columns: 'Management Port' and 'Status'. The first row shows 'Ethernet1/4' under 'Management Port' and 'online' under 'Status'. To the right of the 'Status' column, there are several icons: a checkmark, a refresh icon, a green checkmark, and a right arrow. Below the table, there is a section titled 'Attributes' which lists the following information:



- Cluster Operational Status : not-in-cluster
- FIREPOWER-MGMT-IP : 10.89.5.20
- CLUSTER-ROLE : none
- CLUSTER-IP : 127.2.1.1
- MGMT-URL : https://10.89.5.35/
- UUID : 8e459170-451d-11e9-8475-f22f06c32630

For FTD using FMC, you should leave the device in the FMC device list so that it can resume full functionality after you reenable clustering.

- Disable clustering in the application—You can disable clustering using the application CLI. Enter the **cluster remove unit** *name* command to remove any unit other than the one you are logged into. The bootstrap configuration remains intact, as well as the last configuration synced from the control unit, so you can later re-add the unit without losing your configuration. If you enter this command on a data unit to remove the control unit, a new control unit is elected.

When a device becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, re-enable clustering. The Management interface remains up using the IP address the unit received from the bootstrap configuration. However if you reload, and the unit is still inactive in the cluster, the Management interface is disabled.


To reenable clustering, on the FTD enter **cluster enable**.

- Disable the application instance—In Firepower Chassis Manager on the **Logical Devices** page, click the **Slider enabled** (). You can later reenable it using the **Slider disabled** (.
- Shut down the security module/engine—In Firepower Chassis Manager on the **Security Module/Engine** page, click the **Power Off icon**.
- Shut down the chassis—In Firepower Chassis Manager on the **Overview** page, click the **Shut Down icon**.

### Permanent Removal

You can permanently remove a cluster member using the following methods.

For FTD using FMC, be sure to remove the unit from the FMC device list after you disable clustering on the chassis.

- Delete the logical device—In Firepower Chassis Manager on the **Logical Devices** page, click the **Delete** (). You can then deploy a standalone logical device, a new cluster, or even add a new logical device to the same cluster.
- Remove the chassis or security module from service—If you remove a device from service, you can add replacement hardware as a new member of the cluster.

## FMC: Manage Cluster Members

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

### Add a New Cluster Member

When you add a new cluster member in FXOS, the Firepower Management Center adds the member automatically.

#### Before you begin

- Make sure the interface configuration is the same on the replacement unit as for the other chassis.

- 
- Step 1** Add the new unit to the cluster in FXOS. See the [FXOS configuration guide](#).
- Wait for the new unit to be added to the cluster. Refer to the Firepower Chassis Manager **Logical Devices** screen or use the Firepower Threat Defense **show cluster info** command to view cluster status.
- Step 2** The new cluster member is added automatically. To monitor the registration of the replacement unit, view the following:
- **Cluster Status** dialog box (which is available from the **Devices > Device Management > Cluster** tab > **General** area > **View Cluster Status** link)—A unit that is joining the cluster on the chassis shows "Joining cluster..." After it joins the cluster, the FMC attempts to register it, and the status changes to "Available for Registration". After it completes registration, the status changes to "In Sync." If the registration fails, the unit will stay at "Available for Registration". In this case, force a re-registration by clicking **Reconcile**.

- **System status > Tasks**—The FMC shows all registration events and failures.
- **Devices > Device Management**—When you expand the cluster on the devices listing page, you can see when a unit is registering when it has the loading icon to the left.

## Replace a Cluster Member

You can replace a cluster member in an existing cluster. The FMC auto-detects the replacement unit. However, you must manually delete the old cluster member in the FMC. This procedure also applies to a unit that was reinitialized; in this case, although the hardware remains the same, it appears to be a new member.

### Before you begin

- Make sure the interface configuration is the same on the replacement unit as for other chassis.

**Step 1** For a new chassis, if possible, backup and restore the configuration from the old chassis in FXOS.

If you are replacing a module in a Firepower 9300, you do not need to perform these steps.

If you do not have a backup FXOS configuration from the old chassis, first perform the steps in [Add a New Cluster Member, on page 33](#).

For information about all of the below steps, see the [FXOS configuration guide](#).


- Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis.
- Import the configuration file to the replacement chassis.
- Accept the license agreement.
- If necessary, upgrade the logical device application instance version to match the rest of the cluster.

**Step 2** In the FMC for the old unit, choose **Devices > Device Management**, and click **Delete** (  ).

**Step 3** Confirm that you want to delete the unit.

The unit is removed from the cluster and from the FMC devices list.

**Step 4** The new or reinitialized cluster member is added automatically. To monitor the registration of the replacement unit, view the following:

- **Cluster Status** dialog box (**Devices > Device Management > Cluster** page > **General** area > **View Cluster Status** link)—A unit that is joining the cluster on the chassis shows "Joining cluster..." After it joins the cluster, the FMC attempts to register it, and the status changes to "Available for Registration". After it completes registration, the status changes to "In Sync." If the registration fails, the unit will stay at "Available for Registration". In this case, force a re-registration by clicking **Reconcile**.
- **System** (  ) > **Tasks**—The FMC shows all registration events and failures.
- **Devices > Device Management**—When you expand the cluster on the devices listing page, you can see when a unit is registering when it has the loading icon to the left.

## Deactivate a Member

You may want to deactivate a member in preparation for deleting the unit, or temporarily for maintenance. This procedure is meant to temporarily deactivate a member; the unit will still appear in the FMC device list.

To deactivate a member other than the unit you are logged into, perform the following steps at the FTD CLI.



**Note** When a unit becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, reenabling clustering. The Management interface remains up using the IP address the unit received from the bootstrap configuration. However if you reload, and the unit is still inactive in the cluster, the management interface is disabled. You must use the console for any further configuration.

**Step 1** Access the FTD CLI.

**Step 2** Remove the unit from the cluster:

**cluster remove unit** *unit\_name*

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

To view member names, enter **cluster remove unit ?**, or enter the **show cluster info** command.

**Example:**

```
> cluster remove unit ?
```

```
Current active units in the cluster:
```

```
ftd1
ftd2
ftd3
```

```
> cluster remove unit ftd2
```

```
WARNING: Clustering will be disabled on unit ftd2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

**Step 3** To reenabling clustering, see [Rejoin the Cluster, on page 35](#).

## Rejoin the Cluster

If a unit was removed from the cluster, for example for a failed interface or if you manually disabled clustering, you must manually rejoin the cluster by accessing the unit CLI. Make sure the failure is resolved before you try to rejoin the cluster. See [Rejoining the Cluster, on page 44](#) for more information about why a unit can be removed from a cluster.

**Step 1** Access the CLI of the unit that needs to rejoin the cluster, either from the console port or using SSH to the Management interface. Log in with the username **admin** and the password you set during initial setup.

- Step 2** Enable clustering:  
**cluster enable**
- 

## Delete a Data Unit

If you need to permanently remove a cluster member (for example, if you remove a module on the Firepower 9300, or remove a chassis), then you should delete it from the FMC.

Do not delete the member if it is still a healthy part of the cluster, or if you only want to disable the member temporarily. To delete it permanently from the cluster in FXOS, see [FXOS: Remove a Cluster Unit, on page 32](#). If you remove it from the FMC, and it is still part of the cluster, it will continue to pass traffic, and could even become the control unit—a control unit that the FMC can no longer manage.

### Before you begin

To manually deactivate the unit, see [Deactivate a Member, on page 35](#). Before you delete a unit, the unit must be inactive, either manually or because of a health failure.

---

- Step 1** Make sure the unit is ready to be deleted from the FMC.
- Choose **Devices > Device Management**, and click **Edit** (✎) for the cluster.
  - On the **Devices > Device Management > Cluster > General** area, click the **Current Cluster Summary** link to open the **Cluster Status** dialog box.
  - Ensure that the devices you want to delete are in the Available for Deletion state.
- If the status is stale, click **Reconcile** to force an update.

- Step 2** In the FMC for the data unit you want to delete, choose **Devices > Device Management**, and click **Delete** (🗑).

- Step 3** Confirm that you want to delete the unit.

The unit is removed from the cluster and from the FMC devices list.

---

## Reconcile Cluster Members

If a cluster member fails to register, you can reconcile the cluster membership from the chassis to the Firepower Management Center. For example, a data unit might fail to register if the FMC is occupied with certain processes, or if there is a network issue.

---

- Step 1** Choose **Devices > Device Management**, and click **Edit** (✎) for the cluster.
- Step 2** On the **Cluster > General** area, click the **Current Cluster Summary** link to open the **Cluster Status** dialog box.
- Step 3** Click **Reconcile**.
- For more information about the cluster status, see [FMC: Monitoring the Cluster, on page 37](#).
-



# FMC: Monitoring the Cluster

You can monitor the cluster in Firepower Management Center and at the FTD CLI.

- **Cluster Status** dialog box, which is available from the **Devices > Device Management > Cluster** page > **General** area > **View Cluster Status** link.

Cluster member **Status** includes the following states:

- **In Sync.**—The unit is registered with the FMC.
- **Available for Registration**—The unit is part of the cluster, but has not yet registered with the FMC. If a unit fails to register, you can retry registration by clicking **Reconcile**.
- **Available for Deletion**—The unit is registered with the FMC, but is an inactive member of the cluster. The clustering configuration remains intact if you intend to later re-enable it, or you can delete the unit from the cluster.
- **Joining cluster...**—The unit is joining the cluster on the chassis, but has not completed joining. After it joins, it will register with the FMC.

To refresh this dialog box, close and reopen it.

- **System** (⚙️) > **Tasks** page.

The **Tasks** page shows updates of the Cluster Registration task as each unit registers.

- **Devices > Device Management > *cluster\_name***.

When you expand the cluster on the devices listing page, you can see all member units, including the control unit shown with its role next to the IP address. For units that are still registering, you can see the loading icon.

- **show cluster** {**access-list** [*acl\_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

To view aggregated data for the entire cluster or other information, use the **show cluster** command.

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp** }]

To view cluster information, use the **show cluster info** command.

## Examples for Clustering

These examples include typical deployments.

### Firewall on a Stick

.

## Traffic Segregation

•

## Spanned EtherChannel with Backup Links (Traditional 8 Active/8 Standby)

•

## Reference for Clustering

This section includes more information about how clustering operates.

## Firepower Threat Defense Features and Clustering

Some FTD features are not supported with clustering, and some are only supported on the control 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.

**Note**

To view FlexConfig features that are also not supported with clustering, for example WCCP inspection, see the [ASA general operations configuration guide](#). FlexConfig lets you configure many ASA features that are not present in the FMC GUI. See [FlexConfig Policies for Firepower Threat Defense](#).

- Remote access VPN (SSL VPN and IPsec VPN)
- DHCP client, server, and proxy. DHCP relay is supported.
- High Availability
- Integrated Routing and Bridging
- FMC UCAPL/CC mode

### Centralized Features for Clustering

The following features are only supported on the control unit, and are not scaled for the cluster.

**Note**

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

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

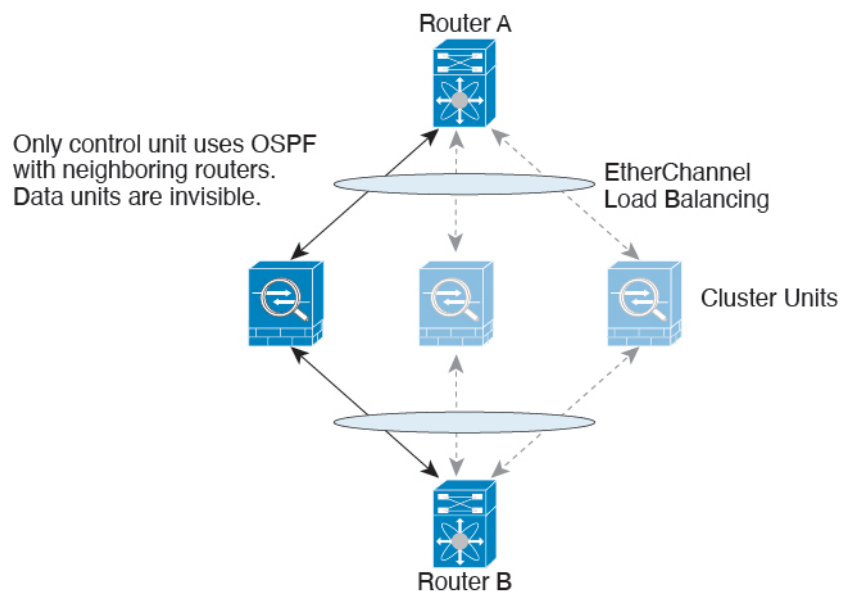
For centralized features, if the control unit fails, all connections are dropped, and you have to re-establish the connections on the new control unit.

- The following application inspections:
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- Dynamic routing
- Static route monitoring

## Dynamic Routing and Clustering

The routing process only runs on the control unit, and routes are learned through the control unit and replicated to secondaries. If a routing packet arrives at a data unit, it is redirected to the control unit.

**Figure 5: Dynamic Routing**



After the data units learn the routes from the control unit, each unit makes forwarding decisions independently.

The OSPF LSA database is not synchronized from the control unit to data units. If there is a control 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.

## Connection Settings

Connection limits are enforced cluster-wide. Each node has an estimate of the cluster-wide counter values based on broadcast messages. Due to efficiency considerations, the configured connection limit across the cluster might not be enforced exactly at the limit number. Each node may overestimate or underestimate the cluster-wide counter value at any given time. However, the information will get updated over time in a load-balanced cluster.

## 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 reloaded, and the control flow is re-hosted, the parent/child flow relationship will not longer be maintained; the control flow idle timeout will not be updated.

## NAT and Clustering

NAT can affect the overall throughput of the cluster. Inbound and outbound NAT packets can be sent to different FTDs 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 FTD that is not the NAT owner, it is forwarded over the cluster control link to the owner, causing large amounts of traffic on the cluster control link. Note that the receiving node does not create a forwarding flow to the owner, because the NAT owner may not end up creating a connection for the packet depending on the results of security and policy checks.

If you still want to use NAT in clustering, then consider the following guidelines:

- 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 node 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 nodes, then it can get allocated 3 blocks with 1 in each node.
  - Port blocks created on the backup node 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 node will own the PAT IP address, corresponding port blocks, and xlates. If it runs out of ports on its normal PAT address, it can use the address that it took over 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 nodes.
- NAT pool address distribution for dynamic PAT—The control node evenly pre-distributes addresses across the cluster. If a member receives a connection and they have no addresses assigned, then the connection is forwarded to the control node for PAT. If a cluster member leaves the cluster (due to failure), a backup member will get the PAT IP address, and if the backup exhausts its normal PAT IP address, it can make use of the new address. Make sure to include at least as many NAT addresses as there are nodes in the cluster, plus at least one extra address, to ensure that each node receives an address,

and that a failed node can get a new address if its old address is in use by the member that took over the address. Use the **show nat pool cluster** command in the device CLI to see the address allocations.

- Reusing a PAT pool in multiple rules—To use the same PAT pool in multiple rules, you must be careful about the interface selection in the rules. You must either use specific interfaces in all rules, or "any" in all rules. You cannot mix specific interfaces and "any" across the rules, or the system might not be able to match return traffic to the right node in the cluster. Using unique PAT pools per rule is the most reliable option.
- No round-robin—Round-robin for a PAT pool is not supported with clustering.
- Dynamic NAT xlates managed by the control node—The control node maintains and replicates the xlate table to data nodes. When a data node receives a connection that requires dynamic NAT, and the xlate is not in the table, it requests the xlate from the control node. The data node owns the connection.
- Stale xlates—The xlate idle time on the connection owner does not get updated. Thus, the idle time might exceed the idle timeout. An idle timer value higher than the configured timeout with a refcnt of 0 is an indication of a stale xlate.
- No static PAT for the following inspections—
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- If you have an extremely large number of NAT rules, over ten thousand, you should enable the transactional commit model using the **asp rule-engine transactional-commit nat** command in the device CLI. Otherwise, the node might not be able to join the cluster.

## SIP Inspection and Clustering

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

## SNMP and Clustering

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

When using SNMPv3 with clustering, if you add a new cluster node after the initial cluster formation, then SNMPv3 users are not replicated to the new node. You must remove the users, and re-add them, and then redeploy your configuration to force the users to replicate to the new node.

## Syslog and Clustering

- Each node in the cluster generates its own syslog messages. You can configure logging so that each node 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 nodes in the cluster. If you configure logging to use the

hostname as the device ID, syslog messages generated by all nodes look as if they come from a single node. If you configure logging to use the local-node name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different nodes.

## TLS/SSL Connections and Clustering

The decryption states of TLS/SSL connections are not synchronized, and if the connection owner fails, then the decrypted connections will be reset. New connections will need to be established to a new unit. Connections that are not decrypted (they match a do-not-decrypt rule) are not affected and are replicated correctly.

## Cisco TrustSec and Clustering

Only the control node learns security group tag (SGT) information. The control node then populates the SGT to data nodes, and data nodes 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 control unit supports VPN connections.



### Note

Remote access VPN is not supported with clustering.

VPN functionality is limited to the control unit and does not take advantage of the cluster high availability capabilities. If the control unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control unit is elected, you must reestablish the VPN connections.

When you connect a VPN tunnel to a Spanned interface address, connections are automatically forwarded to the control unit.

VPN-related keys and certificates are replicated to all units.

## Performance Scaling Factor

When you combine multiple units into a cluster, you can expect the total cluster performance to be approximately:

- 80% of the combined TCP or CPS throughput
- 90% of the combined UDP throughput
- 60% of the combined Ethernet MIX (EMIX) throughput, depending on the traffic mix.

For example, for TCP throughput, the Firepower 9300 with 3 SM-44 modules can handle approximately 135 Gbps of real world firewall traffic when running alone. For 2 chassis, the maximum combined throughput will be approximately 80% of 270 Gbps (2 chassis x 135 Gbps): 216 Gbps.

## Control Unit Election

Members of the cluster communicate over the cluster control link to elect a control unit as follows:

1. When you deploy the cluster, each unit broadcasts an election request every 3 seconds.

2. Any other units with a higher priority respond to the election request; the priority is set when you deploy the cluster and is not configurable.
3. If after 45 seconds, a unit does not receive a response from another unit with a higher priority, then it becomes the control unit.



---

**Note** If multiple units tie for the highest priority, the cluster unit name and then the serial number is used to determine the control unit.

---

4. If a unit later joins the cluster with a higher priority, it does not automatically become the control unit; the existing control unit always remains as the control unit unless it stops responding, at which point a new control unit is elected.
5. In a "split brain" scenario when there are temporarily multiple control units, then the unit with highest priority retains the role while the other units return to data unit roles.



---

**Note** You can manually force a unit to become the control unit. For centralized features, if you force a control unit change, then all connections are dropped, and you have to re-establish the connections on the new control unit.

---

## High Availability Within the Cluster

Clustering provides high availability by monitoring chassis, unit, and interface health and by replicating connection states between units.

### Chassis-Application Monitoring

Chassis-application health monitoring is always enabled. The Firepower 4100/9300 chassis supervisor checks the Firepower Threat Defense application periodically (every second). If the Firepower Threat Defense device is up and cannot communicate with the Firepower 4100/9300 chassis supervisor for 3 seconds, the Firepower Threat Defense device generates a syslog message and leaves the cluster.

If the Firepower 4100/9300 chassis supervisor cannot communicate with the application after 45 seconds, it reloads the Firepower Threat Defense device. If the Firepower Threat Defense device cannot communicate with the supervisor, it removes itself from the cluster.

### Unit Health Monitoring

Each unit periodically sends a broadcast keepaliveheartbeat packet over the cluster control link. If the control unit does not receive any keepaliveheartbeat packets or other packets from a data unit within the timeout period, then the control unit removes the data unit from the cluster. If the data units do not receive packets from the control unit, then a new control unit is elected from the remaining members.

If units cannot reach each other over the cluster control link because of a network failure and not because a unit has actually failed, then the cluster may go into a "split brain" scenario where isolated data units will elect their own control units. For example, if a router fails between two cluster locations, then the original control unit at location 1 will remove the location 2 data units from the cluster. Meanwhile, the units at location 2 will elect their own control unit and form their own cluster. Note that asymmetric traffic may fail in this

scenario. After the cluster control link is restored, then the control unit that has the higher priority will keep the control unit's role. See [Control Unit Election, on page 42](#) for more information.

## Interface Monitoring

Each unit monitors the link status of all hardware interfaces in use, and reports status changes to the control unit. For inter-chassis clustering, Spanned EtherChannels use the cluster Link Aggregation Control Protocol (cLACP). Each chassis monitors the link status and the cLACP protocol messages to determine if the port is still active in the EtherChannel, and informs the Firepower Threat Defense application if the interface is down. All physical interfaces are monitored by default (including the main EtherChannel for EtherChannel interfaces). Only named interfaces that are in an Up state can be monitored. For example, all member ports of an EtherChannel must fail before a *named* EtherChannel is removed from the cluster.

If a monitored interface fails on a particular unit, but it is active on other units, then the unit is removed from the cluster. The amount of time before the Firepower Threat Defense device removes a member from the cluster depends on whether the unit is an established member or is joining the cluster. The Firepower Threat Defense device 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 Firepower Threat Defense device to be removed from the cluster. For an established member, the unit is removed after 500 ms.

For inter-chassis clustering, if you add or delete an EtherChannel from the cluster, interface health-monitoring is suspended for 95 seconds to ensure that you have time to make the changes on each chassis.

## Decorator Application Monitoring

When you install a decorator application on an interface, such as the Radware DefensePro application, then both the Firepower Threat Defense device and the decorator application must be operational to remain in the cluster. The unit does not join the cluster until both applications are operational. Once in the cluster, the unit monitors the decorator application health every 3 seconds. If the decorator application is down, the unit is removed from the cluster.

## Status After Failure

When a node in the cluster fails, the connections hosted by that node are seamlessly transferred to other nodes; state information for traffic flows is shared over the control node's cluster control link.

If the control node fails, then another member of the cluster with the highest priority (lowest number) becomes the control node.

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



### Note

When the FTD becomes inactive and fails to automatically rejoin the cluster, all data interfaces are shut down; only the Management/Diagnostic interface can send and receive traffic.

## 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.



- Failed cluster control link after joining the cluster—The FTD automatically tries to rejoin every 5 minutes, indefinitely.
- Failed data interface—The FTD 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 FTD application disables clustering. After you resolve the problem with the data interface, you have to manually enable clustering.
- 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. The FTD application attempts to rejoin the cluster every 5 seconds.
- Failed Chassis-Application Communication—When the FTD application detects that the chassis-application health has recovered, it tries to rejoin the cluster automatically.
- Internal error—Internal failures include: application sync timeout; inconsistent application statuses; and so on.
- Failed configuration deployment—If you deploy a new configuration from FMC, and the deployment fails on some cluster members but succeeds on others, then the units that failed are removed from the cluster. You must manually rejoin the cluster by re-enabling clustering. If the deployment fails on the control unit, then the deployment is rolled back, and no members are removed.

## 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 1: Features Replicated Across the Cluster**

Traffic	State Support	Notes
Up time	Yes	Keeps track of the system up time.
ARP Table	Yes	—
MAC address table	Yes	—
User Identity	Yes	—
IPv6 Neighbor database	Yes	—
Dynamic routing	Yes	—
SNMP Engine ID	No	—

## How the 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 node 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 nodes receive packets from the connection, the director chooses a new owner from those nodes.
- **Backup owner**—The node 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 node 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 node 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 clustering on the Firepower 9300, which can include up to 3 cluster nodes 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 node 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 (see below for ICMP hash details), and sends a message to the director to register the new connection. If packets arrive at any node other than the owner, the node queries the director about which node 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 node 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.

ICMP/ICMPv6 hash details:

- For Echo packets, the source port is the ICMP identifier, and the destination port is 0.
- For Reply packets, the source port is 0, and the destination port is the ICMP identifier.
- For other packets, both source and destination ports are 0.
- **Forwarder**—A node 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.



**Note** We do not recommend disabling TCP sequence randomization when using clustering. There is a small chance that some TCP sessions won't be established, because the SYN/ACK packet might be dropped.

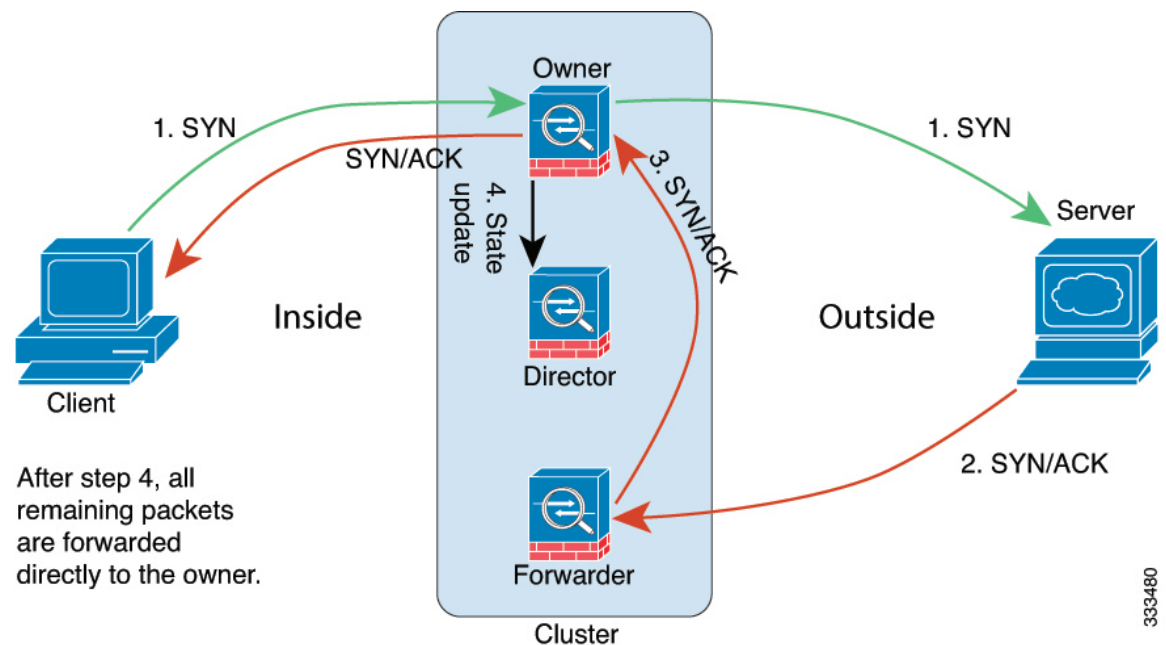
- **Fragment Owner**—For fragmented packets, cluster nodes that receive a fragment determine a fragment owner using a hash of the fragment source IP address, destination IP address, and the packet ID. All fragments are then forwarded to the fragment owner over the cluster control link. Fragments may be load-balanced to different cluster nodes, because only the first fragment includes the 5-tuple used in the switch load balance hash. Other fragments do not contain the source and destination ports and may be load-balanced to other cluster nodes. The fragment owner temporarily reassembles the packet so it can determine the director based on a hash of the source/destination IP address and ports. If it is a new connection, the fragment owner will register to be the connection owner. If it is an existing connection, the fragment owner forwards all fragments to the provided connection owner over the cluster control link. The connection owner will then reassemble all fragments.

## 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. If a reverse flow arrives at a different unit, it is redirected back to the original unit.

## Sample Data Flow for TCP

The following example shows the establishment of a new connection.



1. The SYN packet originates from the client and is delivered to one FTD (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 FTD (based on the load balancing method). This FTD 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 nodes, 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.

## History for Clustering

Feature	Version	Details
Multi-instance clustering	6.6	<p>You can now create a cluster using container instances. On the Firepower 9300, you must include one container instance on each module in the cluster. You cannot add more than one container instance to the cluster per security engine/module. We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster.</p> <p>New/Modified FXOS commands: <b>set port-type cluster</b></p> <p>New/modified Firepower Chassis Manager screens:</p> <ul style="list-style-type: none"> <li>• <b>Logical Devices &gt; Add Cluster</b></li> <li>• <b>Interfaces &gt; All Interfaces &gt; Add New</b> drop-down menu &gt; <b>Subinterface &gt; Type</b> field</li> </ul> <p>Supported platforms: Firepower Threat Defense on the Firepower 4100/9300</p>
Configuration sync to data units in parallel	6.6	<p>The control unit now syncs configuration changes with data units in parallel by default. Formerly, synching occurred sequentially.</p> <p>New/Modified screens: none.</p>

Feature	Version	Details
Messages for cluster join failure or eviction added to <b>show cluster history</b>	6.6	<p>New messages were added to the <b>show cluster history</b> command for when a cluster unit either fails to join the cluster or leaves the cluster.</p> <p>New/Modified commands: <b>show cluster history</b></p> <p>New/Modified screens: none.</p>
Initiator and responder information for Dead Connection Detection (DCD), and DCD support in a cluster.	6.5	<p>If you enable Dead Connection Detection (DCD), you can use the <b>show conn detail</b> command to get information about the initiator and responder. Dead Connection Detection allows you to maintain an inactive connection, and the <b>show conn</b> output tells you how often the endpoints have been probed. In addition, DCD is now supported in a cluster.</p> <p>New/Modified commands: <b>show conn</b> (output only).</p> <p>Supported platforms: Firepower Threat Defense on the Firepower 4100/9300</p>
Improved Firepower Threat Defense cluster addition to the Firepower Management Center	6.3	<p>You can now add any unit of a cluster to the Firepower Management Center, and the other cluster units are detected automatically. Formerly, you had to add each cluster unit as a separate device, and then group them into a cluster in the Management Center. Adding a cluster unit is also now automatic. Note that you must delete a unit manually.</p> <p>New/Modified screens:</p> <p><b>Devices &gt; Device Management &gt; Add</b> drop-down menu &gt; <b>Device &gt; Add Device</b> dialog box</p> <p><b>Devices &gt; Device Management &gt; Cluster</b> tab &gt; <b>General</b> area &gt; <b>Cluster Registration Status &gt; Current Cluster Summary</b> link &gt; <b>Cluster Status</b> dialog box</p> <p>Supported platforms: Firepower Threat Defense on the Firepower 4100/9300</p>
Support for Site-to-Site VPN with clustering as a centralized feature	6.2.3.3	<p>You can now configure site-to-site VPN with clustering. Site-to-site VPN is a centralized feature; only the control unit supports VPN connections.</p> <p>Supported platforms: Firepower Threat Defense on the Firepower 4100/9300</p>

Feature	Version	Details
Automatically rejoin the cluster after an internal failure	6.2.3	<p>Formerly, many internal error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals: 5 minutes, 10 minutes, and then 20 minutes. Internal failures include: application sync timeout; inconsistent application statuses; and so on.</p> <p>New/Modified command: <b>show cluster info auto-join</b></p> <p>No modified screens.</p> <p>Supported platforms: Firepower Threat Defense on the Firepower 4100/9300</p>
Inter-chassis clustering for 6 modules; Firepower 4100 support	6.2	<p>With FXOS 2.1.1, you can now enable inter-chassis clustering on the Firepower 9300 and 4100. For the Firepower 9300, you can include up to 6 modules. For example, you can use 1 module in 6 chassis, or 2 modules in 3 chassis, or any combination that provides a maximum of 6 modules. For the Firepower 4100, you can include up to 6 chassis.</p> <p><b>Note</b> Inter-site clustering is also supported. However, customizations to enhance redundancy and stability, such as site-specific MAC and IP addresses, director localization, site redundancy, and cluster flow mobility, are only configurable using the FlexConfig feature.</p> <p>No modified screens.</p> <p>Supported platforms: Firepower Threat Defense on the Firepower 4100/9300</p>
Intra-chassis Clustering for the Firepower 9300	6.0.1	<p>You can cluster up to 3 security modules within the Firepower 9300 chassis. All modules in the chassis must belong to the cluster.</p> <p>New/Modified screens:</p> <p><b>Devices &gt; Device Management &gt; Add &gt; Add Cluster</b></p> <p><b>Devices &gt; Device Management &gt; Cluster</b></p> <p>Supported platforms: Firepower Threat Defense on the Firepower 9300</p>