



Logical Devices

- [About Logical Devices, on page 1](#)
- [Requirements and Prerequisites for Logical Devices, on page 2](#)
- [Guidelines and Limitations for Logical Devices, on page 4](#)
- [Add a Standalone Logical Device, on page 8](#)
- [Add a High Availability Pair, on page 22](#)
- [Add a Cluster, on page 23](#)
- [Configure Radware DefensePro, on page 47](#)
- [Manage Logical Devices, on page 54](#)
- [Monitoring Logical Devices, on page 61](#)
- [Examples for Inter-Site Clustering, on page 63](#)
- [History for Logical Devices, on page 66](#)

About Logical Devices

A logical device lets you run one application instance (either ASA or Firepower Threat Defense) and also one optional decorator application (Radware DefensePro) to form a service chain .

When you add a logical device, you also define the application instance type and version, assign interfaces, and configure bootstrap settings that are pushed to the application configuration.



Note

For the Firepower 9300, you must install the same application instance type (ASA or FTD) on all modules in the chassis; different types are not supported at this time. Note that modules can run different versions of an application instance type.

Standalone and Clustered Logical Devices

You can add the following logical device types:

- **Standalone**—A standalone logical device operates as a standalone unit or as a unit in a High Availability pair.
- **Cluster**—A clustered logical device lets you group multiple units together, providing all the convenience of a single device (management, integration into a network) while achieving the increased throughput

and redundancy of multiple devices. Multiple module devices, like the Firepower 9300, support intra-chassis clustering. For the Firepower 9300, all three modules must participate in the cluster.

Requirements and Prerequisites for Logical Devices

See the following sections for requirements and prerequisites.

Requirements and Prerequisites for Hardware and Software Combinations

The Firepower 4100/9300 supports multiple models, security modules, application types, and high availability and scalability features. See the following requirements for allowed combinations.

Firepower 9300 Requirements

The Firepower 9300 includes 3 security module slots and multiple types of security modules. See the following requirements:

- Security Module Types—
- Clustering—All security modules in the cluster, whether it is intra-chassis or inter-chassis, must be the same type. 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. For example, you can install 2 SM-36s in chassis 1, and 3 SM-36s in chassis 2.
- High Availability—High Availability is only supported between same-type modules on the Firepower 9300.
- ASA and FTD application types—
- ASA or FTD versions—You can run different versions of an application instance type on separate modules. For example, you can install FTD 6.3 on module 1, FTD 6.4 on module 2, and FTD 6.5 on module 3.

Firepower 4100 Requirements

The Firepower 4100 comes in multiple models. See the following requirements:

- Clustering—All chassis in the cluster must be the same model.
- High Availability—High Availability is only supported between same-type models.
- ASA and FTD application types—The Firepower 4100 can only run a single application type.

Requirements and Prerequisites for Clustering

Cluster Model Support

- ASA on the Firepower 9300—Maximum 16 modules. For example, you can use 1 module in 16 chassis, or 2 modules in 8 chassis, or any combination that provides a maximum of 16 modules. Note that all modules in a chassis must belong to the cluster. Supported for intra-chassis, inter-chassis, and inter-site clustering.

- ASA on the Firepower 4100 series—Maximum 16 chassis. Supported for inter-chassis and inter-site clustering.
- FTD on the Firepower 9300—Maximum 3 modules in 1 chassis. Supported for intra-chassis clustering.
- Radware DefensePro—Supported for intra-chassis clustering with the ASA.

Clustering Hardware and Software Requirements

All chassis in a cluster:

- 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.
- 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 units, and ending with the control unit.
- Must use the same NTP server. Do not set the time manually.
- ASA: Each FXOS chassis must be registered with the License Authority or satellite server. There is no extra cost for data units. For permanent license reservation, you must purchase separate licenses for each chassis. For Firepower Threat Defense, all licensing is handled by the Firepower Management Center.

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](#).

Sizing the Data Center Interconnect for Inter-Site Clustering

You should reserve bandwidth on the data center interconnect (DCI) for cluster control link traffic equivalent to the following calculation:

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

If the number of members differs at each site, use the larger number for your calculation. The minimum bandwidth for the DCI should not be less than the size of the cluster control link for one member.

For example:

- For 4 members at 2 sites:
 - 4 cluster members total

- 2 members at each site
- 5 Gbps cluster control link per member

Reserved DCI bandwidth = 5 Gbps ($2/2 \times 5$ Gbps).

- For 6 members at 3 sites, the size increases:
 - 6 cluster members total
 - 3 members at site 1, 2 members at site 2, and 1 member at site 3
 - 10 Gbps cluster control link per member

Reserved DCI bandwidth = 15 Gbps ($3/2 \times 10$ Gbps).

- For 2 members at 2 sites:
 - 2 cluster members total
 - 1 member at each site
 - 10 Gbps cluster control link per member

Reserved DCI bandwidth = 10 Gbps ($1/2 \times 10$ Gbps = 5 Gbps; but the minimum bandwidth should not be less than the size of the cluster control link (10 Gbps)).

Requirements and Prerequisites for High Availability

- The two units in a High Availability Failover configuration must:
 - Be on a separate chassis; intra-chassis High Availability for the Firepower 9300 is not supported.
 - Be the same model.
 - Have the same interfaces assigned to the High Availability logical devices.
 - Have the same number and types of interfaces. All interfaces must be preconfigured in FXOS identically before you enable High Availability.
- For High Availability system requirements, see.

Guidelines and Limitations for Logical Devices

See the following sections for guidelines and limitations.

General Guidelines and Limitations

Firewall Mode

You can set the firewall mode to routed or transparent in the bootstrap configuration for the FTD.

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links.

Context Mode

- Multiple context mode is only supported on the ASA.

Clustering Guidelines and Limitations

Switches for Inter-Chassis Clustering

- For the ASR 9006, if you want to set a non-default MTU, set the ASR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the **mtu-ignore** option is used. Note that the cluster device MTU should match the ASR *IPv4* MTU.
- On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.
- 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:

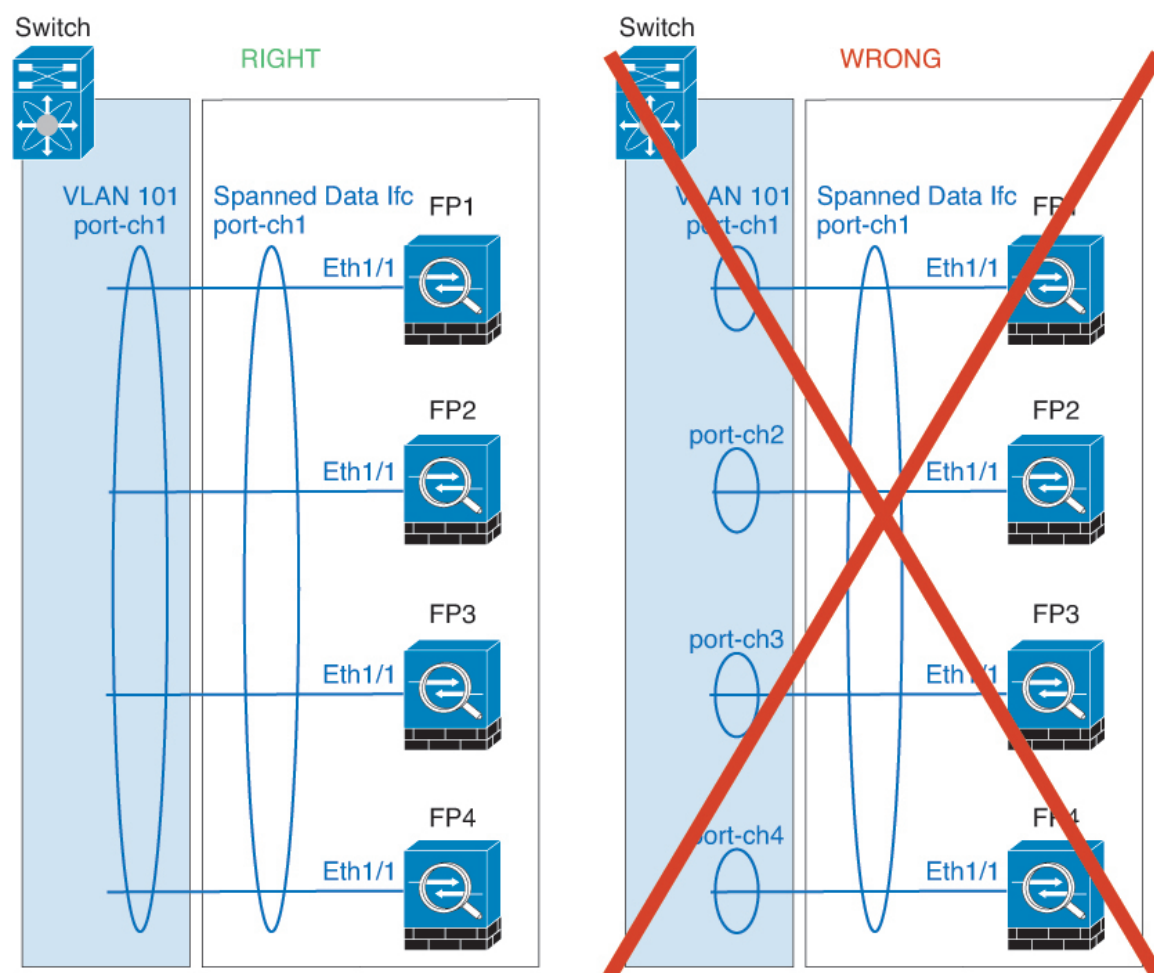
```
router(config)# port-channel id hash-distribution fixed
```

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

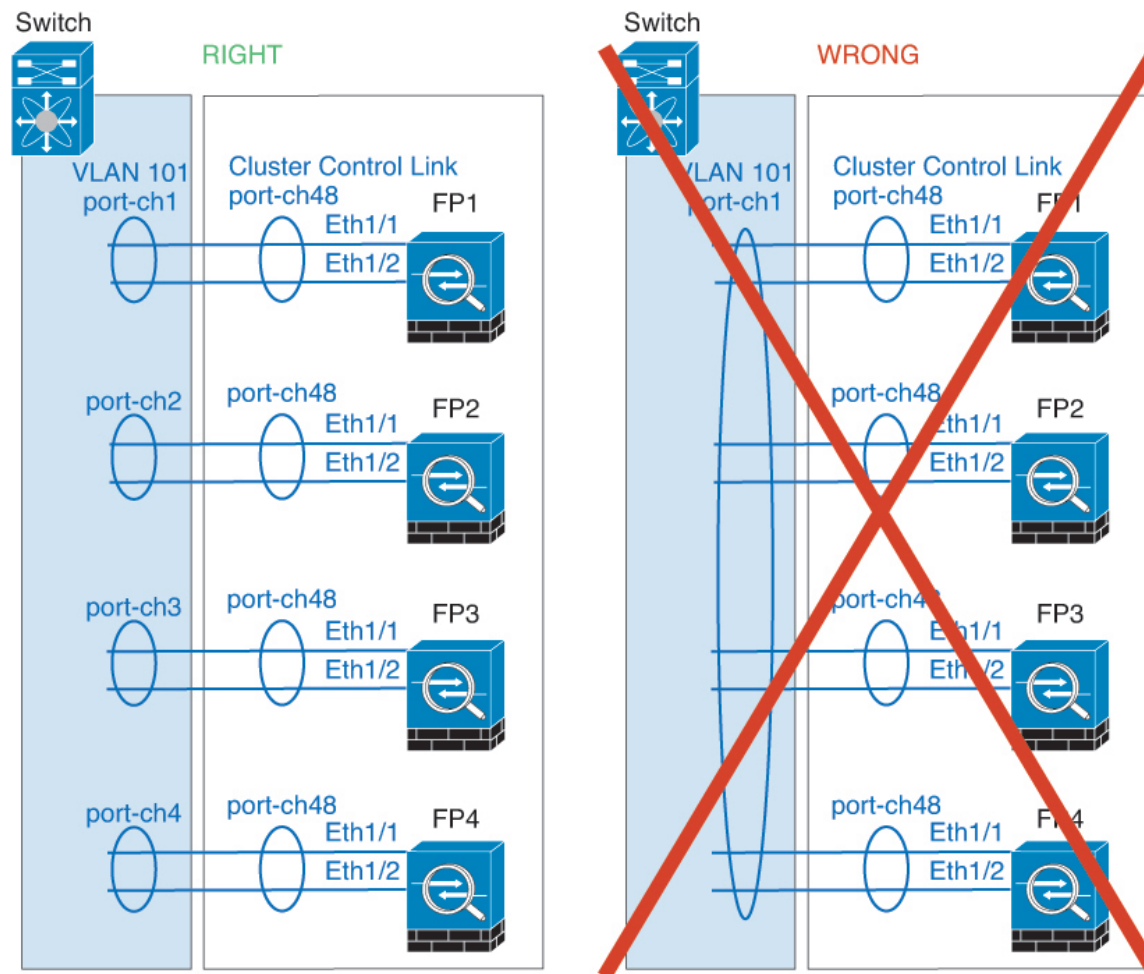
- Firepower 4100/9300 clusters support LACP graceful convergence. So you can leave LACP graceful convergence enabled on connected Cisco Nexus switches.
- When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an individual interface on the switch. FXOS EtherChannels 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.



Inter-Site Clustering

See the following guidelines for inter-site clustering:

- The cluster control link latency must be less than 20 ms round-trip time (RTT).
- The cluster control link must be reliable, with no out-of-order or dropped packets; for example, you should use a dedicated link.
- Do not configure connection rebalancing; you do not want connections rebalanced to cluster members at a different site.
- The cluster implementation does not differentiate between members at multiple sites for incoming connections; therefore, connection roles for a given connection may span across sites. This is expected behavior.
- For transparent mode, if the cluster is placed between a pair of inside and outside routers (AKA North-South insertion), you must ensure that both inside routers share a MAC address, and also that both outside routers share a MAC address. When a cluster member at site 1 forwards a connection to a member at site 2, the destination MAC address is preserved. The packet will only reach the router at site 2 if the MAC address is the same as the router at site 1.

- For transparent mode, if the cluster is placed between data networks and the gateway router at each site for firewalling between internal networks (AKA East-West insertion), then each gateway router should use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide identical virtual IP and MAC address destinations at each site. The data VLANs are extended across the sites using Overlay Transport Virtualization (OTV), or something similar. You need to create filters to prevent traffic that is destined to the local gateway router from being sent over the DCI to the other site. If the gateway router becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site's gateway.
- For routed mode using Spanned EtherChannel, configure site-specific MAC addresses. Extend the data VLANs across the sites using OTV, or something similar. You need to create filters to prevent traffic that is destined to the global MAC address from being sent over the DCI to the other site. If the cluster becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site's cluster units. Dynamic routing is not supported when an inter-site cluster acts as the first hop router for an extended segment.

Additional Guidelines

- When 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.

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.

Add a Standalone Logical Device

Standalone logical devices can be used alone or as high availability units. For more information about high availability usage, see [Add a High Availability Pair, on page 22](#).

Add a Standalone ASA

Standalone logical devices work either alone or in a High Availability pair. On the Firepower 9300 with multiple security modules, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

You can deploy a routed firewall mode ASA from the Firepower 4100/9300 chassis.

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then download that image to the Firepower 4100/9300 chassis.



Note For the Firepower 9300, you must install the same application instance type (ASA or FTD) on all modules in the chassis; different types are not supported at this time. Note that modules can run different versions of an application instance type.

- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (in FXOS, you might see it displayed as MGMT, management0, or other similar names).
- Gather the following information:
 - Interface IDs for this device
 - Management interface IP address and network mask
 - Gateway IP address

Procedure

Step 1 Enter security services mode.

scope ssa

Example:

```
Firepower# scope ssa
Firepower /ssa #
```

Step 2 Set the application instance image version.

a) View available images. Note the Version number that you want to use.

show app

Example:

Firepower /ssa # show app							
Name	Version	Author	Supported Deploy Types	CSP Type	Is Default		
App							
-----	-----	-----	-----	-----	-----		
asa	9.9.1	cisco	Native		Application	No	
asa	9.10.1	cisco	Native		Application	Yes	
ftd	6.2.3	cisco	Native		Application	Yes	

- b) Set the scope to the security module/engine slot.

scope slot *slot_id*

The *slot_id* is always 1 for the Firepower 4100, and 1, 2, or 3 for the Firepower 9300.

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

- c) Create the application instance.

enter app-instance asa

Example:

```
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* #
```

- d) Set the ASA image version.

set startup-version *version*

Example:

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

- e) Exit to slot mode.

exit

Example:

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

- f) Exit to ssa mode.

exit

Example:

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Step 3 Create the logical device.

enter logical-device *device_name* **asa** *slot_id* **standalone**

Example:

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

Step 4 Assign the management and data interfaces to the logical device. Repeat for each interface.

create external-port-link *name* *interface_id* **asa**

set description *description*

exit

- *name*—The name is used by the Firepower 4100/9300 chassis supervisor; it is not the interface name used in the ASA configuration.
- *description*—Use quotes (") around phrases with spaces.

The management interface is not the same as the chassis management port. You will later enable and configure the data interfaces on the ASA, including setting the IP addresses.

Example:

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

Step 5 Configure the management bootstrap information.

a) Create the bootstrap object.

create mgmt-bootstrap **asa**

Example:

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) Specify the admin password.

create bootstrap-key-secret PASSWORD**set value**

Enter a value: *password*

Confirm the value: *password*

exit**Example:**

The pre-configured ASA admin user is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Configure the IPv4 management interface settings.

create ipv4 slot_id default**set ip ip_address mask network_mask****set gateway gateway_address****exit****Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Configure the IPv6 management interface settings.

create ipv6 slot_id default**set ip ip_address prefix-length prefix****set gateway gateway_address****exit****Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) Exit the management bootstrap mode.

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Step 6 Save the configuration.

commit-buffer

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 status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State is Enabled** and the **Oper State is Online**.

Example:

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Profile Name	Cluster	State	Cluster Role		
asa	asa1	2	Disabled	Not Installed		9.12.1
Native			Not Applicable	None		
ftd	ftd1	1	Enabled	Online	6.4.0.49	6.4.0.49
Container	Default-Small		Not Applicable	None		

Step 7 See the ASA configuration guide to start configuring your security policy.

Example

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

Add a Standalone Firepower Threat Defense

Standalone logical devices work either alone or in a High Availability pair. On the Firepower 9300 with multiple security modules, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then download that image to the Firepower 4100/9300 chassis.



Note

For the Firepower 9300, you must install the same application instance type (ASA or FTD) on all modules in the chassis; different types are not supported at this time. Note that modules can run different versions of an application instance type.

- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (in FXOS, you might see it displayed as MGMT, management0, or other similar names).
- You must also configure at least one Data type interface. Optionally, you can also create a firepower-eventing interface to carry all event traffic (such as web events). See [Interface Types](#) for more information.
- Gather the following information:
 - Interface IDs for this device
 - Management interface IP address 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

Procedure

- Step 1** Enter security services mode.
- ```
scope ssa
```

**Example:**

```
Firepower# scope ssa
Firepower /ssa #
```

- Step 2** Accept the end-user license agreement for the Firepower Threat Defense version you want to use. You only need to perform this step if you have not already accepted the EULA for this version.

- a) View available images. Note the Version number that you want to use.

**show app****Example:**

```
Firepower /ssa # show app
```

| Name  | Version | Author | Supported Deploy Types | CSP Type    | Is Default |
|-------|---------|--------|------------------------|-------------|------------|
| App   |         |        |                        |             |            |
| ----- | -----   | -----  | -----                  | -----       | -----      |
| asa   | 9.9.1   | cisco  | Native                 | Application | No         |
| asa   | 9.10.1  | cisco  | Native                 | Application | Yes        |
| ftd   | 6.2.3   | cisco  | Native                 | Application | Yes        |

- b) Set the scope to the image version.

**scope app ftd *application\_version*****Example:**

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

- c) Accept the license agreement.

**accept-license-agreement****Example:**

```
Firepower /ssa/app # accept-license-agreement
```

```
End User License Agreement: End User License Agreement
```

```
Effective: May 22, 2017
```

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

```
[...]
```

```
Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".
```

```
Firepower /ssa/app* #
```

- d) Save the configuration.

**commit-buffer**

**Example:**

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

- e) Exit to security services mode.

**exit**

**Example:**

```
Firepower /ssa/app # exit
Firepower /ssa #
```

### Step 3 Set the application instance image version.

- a) Set the scope to the security module/engine slot.

**scope slot *slot\_id***

The *slot\_id* is always 1 for the Firepower 4100, and 1, 2, or 3 for the Firepower 9300.

**Example:**

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

- b) Create the application instance.

**enter app-instance ftd**

**Example:**

```
Firepower /ssa/slot # enter app-instance ftd
Firepower /ssa/slot/app-instance* #
```

- c) Set the Firepower Threat Defense image version.

**set startup-version *version***

Enter the version number that you noted earlier in this procedure when you accepted the EULA.

**Example:**

```
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

- d) Exit to slot mode.

**exit**



**Example:**

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

e) Exit to ssa mode.

**exit**

**Example:**

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

**Example:**

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

**Step 4** Create the logical device.

**enter logical-device** *device\_name* **ftd** *slot\_id* **standalone**

**Example:**

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

**Step 5** Assign the management and data interfaces to the logical device. Repeat for each interface.

**create external-port-link** *name* *interface\_id* **ftd**

**set description** *description*

**exit**

- *name*—The name is used by the Firepower 4100/9300 chassis supervisor; it is not the interface name used in the Firepower Threat Defense configuration.
- *description*—Use quotes (") around phrases with spaces.

The management interface is not the same as the chassis management port. You will later enable and configure the data interfaces in FMC, including setting the IP addresses.

**Example:**

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
```

```
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

### Step 6 Configure the management bootstrap parameters.

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.

- a) Create the bootstrap object.

**create mgmt-bootstrap ftd**

**Example:**

```
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the IP address or hostname of the managing Firepower Management Center:

Set one of the following:

- **enter bootstrap-key FIREPOWER\_MANAGER\_IP**

**set value** *IP\_address*

**exit**

- **enter bootstrap-key FQDN**

**set value** *fmc\_hostname*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Specify the firewall mode, routed or transparent.

**create bootstrap-key FIREWALL\_MODE**

**set value** {*routed* | *transparent*}

**exit**

In routed mode, the device 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.

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Specify the key to be shared between the device and the Firepower Management Center. You can choose any passphrase for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.

**create bootstrap-key-secret REGISTRATION\_KEY**

**set value**

Enter a value: *registration\_key*

Confirm the value: *registration\_key*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) Specify the admin password. This password is used for the admin user for CLI access.

**create bootstrap-key-secret PASSWORD**

**set value**

Enter a value: *password*

Confirm the value: *password*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- f) Specify the fully qualified hostname.

**create bootstrap-key FQDN**

**set value fqdn**

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftdl.cisco.com
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- g) Specify a comma-separated list of DNS servers.

**create bootstrap-key DNS\_SERVERS**

**set value** *dns\_servers*

**exit**

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

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- h) Specify a comma-separated list of search domains.

**create bootstrap-key SEARCH\_DOMAINS**

**set value** *search\_domains*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- i) Configure the IPv4 management interface settings.

**create ipv4 slot\_id firepower**

**set ip** *ip\_address* **mask** *network\_mask*

**set gateway** *gateway\_address*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- j) Configure the IPv6 management interface settings.

**create ipv6 slot\_id firepower**

**set ip** *ip\_address* **prefix-length** *prefix*

**set gateway** *gateway\_address*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

k) Exit the management bootstrap mode.

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

**Step 7** Save the configuration.

**commit-buffer**

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 status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State is Enabled** and the **Oper State is Online**.

**Example:**

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

| App Name    | Identifier    | Slot ID | Admin State    | Oper State    | Running Version | Startup Version |
|-------------|---------------|---------|----------------|---------------|-----------------|-----------------|
| Deploy Type | Profile Name  | Cluster | State          | Role          |                 |                 |
| asa         | asal          | 2       | Disabled       | Not Installed |                 | 9.12.1          |
| Native      |               |         | Not Applicable | None          |                 |                 |
| ftd         | ftd1          | 1       | Enabled        | Online        | 6.4.0.49        | 6.4.0.49        |
| Container   | Default-Small |         | Not Applicable | None          |                 |                 |

**Step 8** See the FMC configuration guide to add the FTD as a managed device and start configuring your security policy.

**Example**

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.3.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd
```

```

Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: juniorwindowpane
Confirm the value: juniorwindowpane
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #

```

## Add a High Availability Pair

or High Availability (also known as failover) is configured within the application, not in FXOS. However, to prepare your chassis for high availability, see the following steps.

### Before you begin

See .

### Procedure

- 
- Step 1** Allocate the same interfaces to each logical device.
- Step 2** Allocate 1 or 2 data interfaces for the failover and state link(s).
- These interfaces exchange high availability traffic between the 2 chassis. We recommend that you use a 10 GB data interface for a combined failover and state link. If you have available interfaces, you can use separate failover and state links; the state link requires the most bandwidth. You cannot use the management-type interface for the failover or state link. We recommend that you use a switch between the chassis, with no other device on the same network segment as the failover interfaces.
- Step 3** Enable High Availability on the logical devices.
- Step 4** If you need to make interface changes after you enable High Availability, perform the changes on the standby unit first, and then perform the changes on the active unit.
- 

## Add a Cluster

Clustering lets you group multiple devices together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. The Firepower 9300, which includes multiple modules, supports intra-chassis clustering where you group all modules within a single chassis into a cluster. You can also use inter-chassis clustering, where multiple chassis are grouped together; inter-chassis clustering is the only option for single module devices like the Firepower 4100 series.



---

**Note** The FTD does not support a cluster across multiple chassis (inter-chassis); only intra-chassis clustering is supported.

---

## About Clustering on the Firepower 4100/9300 Chassis

The cluster consists of multiple devices acting as a single logical unit. When you deploy a cluster on the Firepower 4100/9300 chassis, it does the following:

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

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. Some parts of the bootstrap configuration may be user-configurable within the application if you want to customize your clustering environment.

- 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.

The following sections provide more detail about clustering concepts and implementation.

## Primary and Secondary Unit Roles

One member of the cluster is the primary unit. The primary unit is determined automatically. All other members are secondary units.

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

## Cluster Control Link

The cluster control link is automatically created using the Port-channel 48 interface.

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.

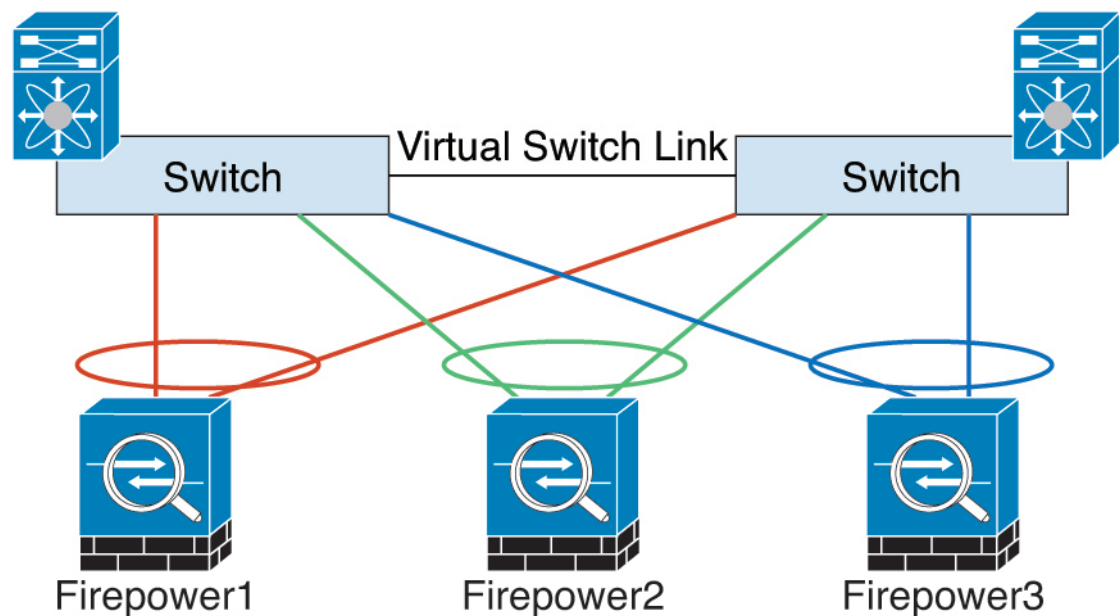




**Note** If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

### 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 Firepower 4100/9300 chassis 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`. The cluster control link network cannot include any routers between units; only Layer 2 switching is allowed. For inter-site traffic, Cisco recommends using Overlay Transport Virtualization (OTV).

## 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.

For the ASA, the Main cluster IP address is a fixed address for the cluster that always belongs to the current primary unit. You must configure a range of addresses so that each unit, including the current primary unit, can use a Local address from the range. The Main cluster IP address provides consistent management access to an address; when a primary unit changes, the Main cluster IP address moves to the new primary unit, so management of the cluster continues seamlessly. The Local IP address is used for routing, and is also useful for troubleshooting. For example, you can manage the cluster by connecting to the Main cluster IP address, which is always attached to the current primary unit. To manage an individual member, you can connect to the Local IP address. For outbound management traffic such as TFTP or syslog, each unit, including the primary unit, uses the Local IP address to connect to the server.

For the Firepower Threat Defense, assign a management IP address to each unit on the same network. Use these IP addresses when you add each unit to the FMC.

## 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.

## Inter-Site Clustering

For inter-site installations, you can take advantage of clustering as long as you follow the recommended guidelines.

You can configure each cluster chassis to belong to a separate site ID.

Site IDs work with site-specific MAC addresses and IP addresses. Packets sourced from the cluster use a site-specific MAC address and IP address, while packets received by the cluster use a global MAC address and IP address. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address. Site-specific MAC addresses and IP address are supported for routed mode using Spanned EtherChannels only.

Site IDs are also used to enable flow mobility using LISP inspection.

See the following sections for more information about inter-site clustering:

- Sizing the Data Center Interconnect—[Requirements and Prerequisites for Clustering, on page 2](#)
- Inter-Site Guidelines—[Clustering Guidelines and Limitations, on page 5](#)
- Inter-Site Examples—[Examples for Inter-Site Clustering, on page 63](#)

## Add an ASA Cluster

You can add a single Firepower 9300 chassis as an intra-chassis cluster, or add 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 enter most of the same settings on the next chassis.

### Create an ASA Cluster

Set the scope to the image version.

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, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

#### 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.
- Gather the following information:
  - Management interface ID, IP address, and network mask
  - Gateway IP address

#### Procedure

##### 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 5](#) for more information about EtherChannels for inter-chassis clustering.

- 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.

- 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.

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 5](#) for more information about EtherChannels for inter-chassis clustering.

**Step 2** Enter security services mode.

**scope ssa**

**Example:**

```
Firepower# scope ssa
Firepower /ssa #
```

**Step 3** Set the application instance image version.

a) View available images. Note the Version number that you want to use.

**show app**

**Example:**

```
Firepower /ssa # show app
```

| Name  | Version | Author | Supported Deploy Types | CSP Type    | Is Default |
|-------|---------|--------|------------------------|-------------|------------|
| App   |         |        |                        |             |            |
| ----- | -----   | -----  | -----                  | -----       | -----      |
| asa   | 9.9.1   | cisco  | Native                 | Application | No         |
| asa   | 9.10.1  | cisco  | Native                 | Application | Yes        |
| ftd   | 6.2.3   | cisco  | Native                 | Application | Yes        |

b) Set the scope to the image version.

**scope app asa application\_version**

**Example:**

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

c) Set this version as the default.

**set-default**

**Example:**

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) Exit to ssa mode.

**exit**

**Example:**

```
Firepower /ssa/app* # exit
```

```
Firepower /ssa* #
```

### Example:

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

## Step 4 Create the cluster.

### enter logical-device *device\_name* asa slots clustered

- *device\_name*—Used by the Firepower 4100/9300 chassis supervisor to configure clustering settings and assign interfaces; it is not the cluster name used in the security module configuration. You must specify all three security modules, even if you have not yet installed the hardware.
- *slots*—Assigns the chassis modules to the cluster. For the Firepower 4100, specify **1**. For the Firepower 9300, specify **1,2,3**. You must enable clustering for all 3 module slots in a Firepower 9300 chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

### Example:

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

## Step 5 Configure the cluster bootstrap parameters.

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.

- Create the cluster bootstrap object.

### enter cluster-bootstrap

#### Example:

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- Configure an authentication key for control traffic on the cluster control link.

### set key

#### Example:

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

You are prompted to enter the shared secret.

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.

- c) Set the cluster interface mode.

**set mode spanned-etherchannel**

Spanned EtherChannel mode is the only supported mode.

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- d) Set the cluster group name in the security module configuration.

**set service-type** *cluster\_name*

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

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- e) Configure the management IP address information.

This information is used to configure a management interface in the security module configuration.

1. Configure a pool of Local IP addresses, one of which will be assigned to each cluster unit for the interface.

**set ipv4 pool** *start\_ip end\_ip*

**set ipv6 pool** *start\_ip end\_ip*

Include at least as many addresses as there are units in the cluster. Note that for the Firepower 9300, you must include 3 addresses per chassis, even if you do not have all module slots filled. If you plan to expand the cluster, include additional addresses. The Virtual IP address (known as the Main cluster IP address) that belongs to the current control unit is *not* a part of this pool; be sure to reserve an IP address on the same network for the Main cluster IP address. You can use IPv4 and/or IPv6 addresses.

2. Configure the Main cluster IP address for the management interface.

**set virtual ipv4** *ip\_address mask mask*

**set virtual ipv6** *ip\_address prefix-length prefix*

This IP address must be on the same network as the cluster pool addresses, but not be part of the pool.

3. Enter the network gateway address.

**set ipv4 gateway** *ip\_address*

**set ipv6 gateway** *ip\_address*

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
```

```
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

- f) Exit the cluster bootstrap mode.

**exit**

**Example:**

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

**Step 6** Configure the management bootstrap parameters.

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.

- a) Create the management bootstrap object.

**enter mgmt-bootstrap asa**

**Example:**

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the admin password.

**create bootstrap-key-secret PASSWORD**

**set value**

Enter a value: *password*

Confirm the value: *password*

**exit**

**Example:**

The pre-configured ASA admin user is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Exit the management bootstrap mode.

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

**Step 7** Save the configuration.

**commit-buffer**

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 status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State** is **Enabled** and the **Oper State** is **Online**.

**Example:**

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

| App Name    | Identifier   | Slot ID | Admin State    | Oper State    | Running Version | Startup Version |
|-------------|--------------|---------|----------------|---------------|-----------------|-----------------|
| Deploy Type | Profile Name | Cluster | State          | Cluster Role  |                 |                 |
| ftd         | cluster1     | 1       | Enabled        | Online        | 6.4.0.49        | 6.4.0.49        |
| Native      |              |         | In Cluster     | Slave         |                 |                 |
| ftd         | cluster1     | 2       | Enabled        | Online        | 6.4.0.49        | 6.4.0.49        |
| Native      |              |         | In Cluster     | Master        |                 |                 |
| ftd         | cluster1     | 3       | Disabled       | Not Available |                 | 6.4.0.49        |
| Native      |              |         | Not Applicable | None          |                 |                 |

**Step 8** To add another chassis to the cluster, repeat this procedure except you must configure a unique **chassis-id**; otherwise, use the same configuration for both chassis.

Make sure the interface configuration is the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.

**Step 9** Connect to the control unit ASA to customize your clustering configuration.

**Example**

For chassis 1:

```
scope eth-uplink
 scope fabric a
 enter port-channel 1
 set port-type data
 enable
 enter member-port Ethernet1/1
 exit
 enter member-port Ethernet1/2
 exit
 exit
 enter port-channel 2
 set port-type data
```



```

 enable
 enter member-port Ethernet1/3
 exit
 enter member-port Ethernet1/4
 exit
 exit
 enter port-channel 3
 set port-type data
 enable
 enter member-port Ethernet1/5
 exit
 enter member-port Ethernet1/6
 exit
 exit
 enter port-channel 4
 set port-type mgmt
 enable
 enter member-port Ethernet2/1
 exit
 enter member-port Ethernet2/2
 exit
 exit
 enter port-channel 48
 set port-type cluster
 enable
 enter member-port Ethernet2/3
 exit
 exit
 exit
exit
commit-buffer

scope ssa
 enter logical-device ASA1 asa "1,2,3" clustered
 enter cluster-bootstrap
 set chassis-id 1
 set ipv4 gateway 10.1.1.254
 set ipv4 pool 10.1.1.11 10.1.1.27
 set ipv6 gateway 2001:DB8::AA
 set ipv6 pool 2001:DB8::11 2001:DB8::27
 set key
 Key: f@arscape
 set mode spanned-etherchannel
 set service-type cluster1
 set virtual ipv4 10.1.1.1 mask 255.255.255.0
 set virtual ipv6 2001:DB8::1 prefix-length 64
 exit
 exit
 scope app asa 9.5.2.1
 set-default
 exit
 commit-buffer

```

For chassis 2:

```

scope eth-uplink
 scope fabric a
 create port-channel 1
 set port-type data
 enable
 create member-port Ethernet1/1
 exit
 create member-port Ethernet1/2

```

```

 exit
 exit
create port-channel 2
 set port-type data
 enable
 create member-port Ethernet1/3
 exit
 create member-port Ethernet1/4
 exit
 exit
create port-channel 3
 set port-type data
 enable
 create member-port Ethernet1/5
 exit
 create member-port Ethernet1/6
 exit
 exit
create port-channel 4
 set port-type mgmt
 enable
 create member-port Ethernet2/1
 exit
 create member-port Ethernet2/2
 exit
 exit
create port-channel 48
 set port-type cluster
 enable
 create member-port Ethernet2/3
 exit
 exit
exit
exit
commit-buffer

scope ssa
 enter logical-device ASA1 asa "1,2,3" clustered
 enter cluster-bootstrap
 set chassis-id 2
 set ipv4 gateway 10.1.1.254
 set ipv4 pool 10.1.1.11 10.1.1.15
 set ipv6 gateway 2001:DB8::AA
 set ipv6 pool 2001:DB8::11 2001:DB8::19
 set key
 Key: f@rscape
 set mode spanned-etherchannel
 set service-type cluster1
 set virtual ipv4 10.1.1.1 mask 255.255.255.0
 set virtual ipv6 2001:DB8::1 prefix-length 64
 exit
 exit
scope app asa 9.5.2.1
 set-default
 exit
commit-buffer

```

## Add More Cluster Members

Add or replace an ASA cluster member.



**Note** This procedure only applies to adding or replacing a *chassis*; if you are adding or replacing a module to a Firepower 9300 where clustering is already enabled, the module will be added automatically.

#### Before you begin

- Make sure your existing cluster has enough IP addresses in the management IP address pool for this new member. If not, you need to edit the existing cluster bootstrap configuration on each chassis before you add this new member. This change causes a restart of the logical device.
- The interface configuration must be the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.
- For multiple context mode, enable multiple context mode in the ASA application on the first cluster member; additional cluster members will inherit the multiple context mode configuration automatically.

#### Procedure

- Step 1**      Click **OK**.
- Step 2**      To add another chassis to the cluster, repeat the procedure in [Create an ASA Cluster, on page 27](#) except you must configure a unique **chassis-id**; otherwise, use the same configuration for the new chassis.

## Add a Firepower Threat Defense Cluster

You can add a single Firepower 9300 chassis as an intra-chassis cluster.

### 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.

In a Firepower 9300 chassis, you must enable clustering for all 3 module slots, 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.
- 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

## Procedure

### 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 5](#) for more information about EtherChannels for inter-chassis clustering.

- 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.

- c) (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.

### Step 2

Enter security services mode.

**scope ssa**

**Example:**

```
Firepower# scope ssa
Firepower /ssa #
```

### Step 3

Set the default image version.

- a) View available images. Note the Version number that you want to use.

**show app**

**Example:**

```
Firepower /ssa # show app
```

| Name | Version | Author | Supported Deploy Types | CSP Type    | Is Default |
|------|---------|--------|------------------------|-------------|------------|
| App  |         |        |                        |             |            |
| asa  | 9.9.1   | cisco  | Native                 | Application | No         |
| asa  | 9.10.1  | cisco  | Native                 | Application | Yes        |
| ftd  | 6.2.3   | cisco  | Native                 | Application | Yes        |

- b) Set the scope to the image version.

**scope app ftd application\_version**

**Example:**

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

- c) Accept the license agreement.

**accept-license-agreement****Example:**

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017
```

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

```
Firepower /ssa/app* #
```

- d) Set this version as the default.

**set-default****Example:**

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

- e) Save the configuration.

**commit-buffer****Example:**

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

- f) Exit to ssa mode.

**exit**

**Example:**

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

**Example:**

```
Firepower /ssa # scope app ftd 6.3.0.21
Firepower /ssa/app # set-default
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # exit
Firepower /ssa* #
```

**Step 4** Create the cluster:**enter logical-device *device\_name* ftd slots clustered**

- *device\_name*—Used by the Firepower 4100/9300 chassis supervisor to configure clustering settings and assign interfaces; it is not the cluster name used in the security module configuration.
- *slots*—Assigns the chassis modules to the cluster. For the Firepower 4100, specify **1**. For the Firepower 9300, specify **1,2,3**. You must enable clustering for all 3 module slots in a Firepower 9300 chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

**Example:**

```
Firepower /ssa # enter logical-device FTD1 ftd 1,2,3 clustered
Firepower /ssa/logical-device* #
```

**Step 5** Configure the cluster bootstrap parameters.

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.

- Create the cluster bootstrap object.

**enter cluster-bootstrap****Example:**

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- Configure an authentication key for control traffic on the cluster control link.

**set key****Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

You are prompted to enter the shared secret.

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.

- c) Set the cluster interface mode.

**set mode spanned-etherchannel**

Spanned EtherChannel mode is the only supported mode.

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- d) Set the cluster group name in the security module configuration.

**set service-type cluster\_name**

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

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- e) Exit the cluster bootstrap mode.

**exit**

**Example:**

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

**Step 6** Configure the management bootstrap parameters.

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.

- a) Create the management bootstrap object.

**enter mgmt-bootstrap ftd**

**Example:**

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the IP address or hostname of the managing Firepower Management Center.

Set one of the following:

- **enter bootstrap-key FIREPOWER\_MANAGER\_IP**

**set value** *IP\_address*

**exit**

- **enter bootstrap-key FQDN**

**set value** *fmc\_hostname*

**exit**

- c) Specify the firewall mode, routed or transparent.

**create bootstrap-key FIREWALL\_MODE**

**set value** {*routed* | *transparent*}

**exit**

In routed mode, the device 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.

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Specify the key to be shared between the device and the FMC.

**enter bootstrap-key-secret REGISTRATION\_KEY**

**set value**

Enter a value: *registration\_key*

Confirm the value: *registration\_key*

**exit**

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.

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- e) Specify a password for the FTD admin user for CLI access.



**enter bootstrap-key-secret PASSWORD**

**set value**

Enter a value: *password*

Confirm the value: *password*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- f) Specify the fully qualified hostname.

**enter bootstrap-key FQDN**

**set value** *fqdn*

**exit**

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.

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftdcluster1.example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- g) Specify a comma-separated list of DNS servers.

**enter bootstrap-key DNS\_SERVERS**

**set value** *dns\_servers*

**exit**

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

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- h) Specify a comma-separated list of search domains.

**enter bootstrap-key SEARCH\_DOMAINS**

**set value** *search\_domains*

**exit**

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- i) Configure the management IP addresses for each security module in the cluster.

**Note** For the Firepower 9300, 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.

To create an IPv4 management interface object:

1. Create the management interface object.  
**enter ipv4 slot\_id firepower**
2. Set the gateway address.  
**set gateway gateway\_address**
3. Set the IP address and mask.  
**set ip ip\_address mask network\_mask**
4. Exit the management IP mode.  
**exit**
5. Repeat for the remaining modules in the chassis.

To create an IPv6 management interface object:

1. Create the management interface object.  
**enter ipv6 slot\_id firepower**
2. Set the gateway address.  
**set gateway gateway\_address**
3. Set the IP address and prefix.  
**set ip ip\_address prefix-length prefix**
4. Exit the management IP mode.  
**exit**
5. Repeat for the remaining modules in the chassis.

**Example:**

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 2 firepower
```

```

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.35 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.36 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3211
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3212
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

j) Exit the management bootstrap mode.

**exit**

**Example:**

```

Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #

```

**Example:**

```

Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: ziggy$tar dust
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: $pidersfrommars
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit

```

```

Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.32 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.33 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #

```

### Step 7 Save the configuration.

#### commit-buffer

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 status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State** is **Enabled** and the **Oper State** is **Online**.

#### Example:

```

Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance

```

| App Name    | Identifier   | Slot ID | Admin State    | Oper State    | Running Version | Startup Version |
|-------------|--------------|---------|----------------|---------------|-----------------|-----------------|
| Deploy Type | Profile Name | Cluster | State          | Role          |                 |                 |
| ftd         | cluster1     | 1       | Enabled        | Online        | 6.4.0.49        | 6.4.0.49        |
| Native      |              |         | In Cluster     | Slave         |                 |                 |
| ftd         | cluster1     | 2       | Enabled        | Online        | 6.4.0.49        | 6.4.0.49        |
| Native      |              |         | In Cluster     | Master        |                 |                 |
| ftd         | cluster1     | 3       | Disabled       | Not Available |                 | 6.4.0.49        |
| Native      |              |         | Not Applicable | None          |                 |                 |

### Step 8 Add each unit to the Firepower Management Center using the management IP addresses, and then group them into a cluster at the web interface.

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

#### Example

```

scope eth-uplink
 scope fabric a
 enter port-channel 1
 set port-type data
 enable

```

```
 create member-port Ethernet1/1
 exit
 create member-port Ethernet1/2
 exit
 exit
 enter port-channel 2
 set port-type data
 enable
 create member-port Ethernet1/3
 exit
 create member-port Ethernet1/4
 exit
 exit
 enter port-channel 3
 set port-type firepower-eventing
 enable
 create member-port Ethernet1/5
 exit
 create member-port Ethernet1/6
 exit
 exit
 enter port-channel 4
 set port-type mgmt
 enable
 create member-port Ethernet2/1
 exit
 enter member-port Ethernet2/2
 exit
 exit

exit
exit
commit-buffer

scope ssa
 enter logical-device FTD1 ftd "1,2,3" clustered
 enter cluster-bootstrap
 set chassis-id 1
 set key cluster_key
 set mode spanned-etherchannel
 set service-type ftd-cluster
 exit
 enter mgmt-bootstrap ftd
 enter bootstrap-key FIREPOWER_MANAGER_IP
 set value 10.0.0.100
 exit
 enter bootstrap-key FIREWALL_MODE
 set value transparent
 exit
 enter bootstrap-key-secret REGISTRATION_KEY
 set value
 Value: alladinsane
 exit
 enter bootstrap-key-secret PASSWORD
 set value
 Value: widthofacircle
 exit
 enter bootstrap-key FQDN
 set value ftd.cisco.com
 exit
 enter bootstrap-key DNS_SERVERS
 set value 192.168.1.1
 exit
 enter bootstrap-key SEARCH_DOMAINS
```

```

 set value search.com
 exit
 enter ipv4 1 firepower
 set gateway 10.0.0.1
 set ip 10.0.0.31 mask 255.255.255.0
 exit
 enter ipv4 2 firepower
 set gateway 10.0.0.1
 set ip 10.0.0.32 mask 255.255.255.0
 exit
 enter ipv4 3 firepower
 set gateway 10.0.0.1
 set ip 10.0.0.33 mask 255.255.255.0
 exit
 exit
exit
scope app ftd 6.0.0.837
 accept-license-agreement
 set-default
 exit
commit-buffer

```

## Add More Cluster Units

Add or replace a FTD cluster unit in an existing cluster.



### 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. However, you must still add the new module to the Firepower Management Center; skip to the Firepower Management Center steps.

### 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.

### Procedure

To add another chassis to the cluster, repeat the procedure in [Create a Firepower Threat Defense Cluster, on page 35](#) except you must configure the following settings to be unique; otherwise, use the same configuration for both chassis.

- Chassis ID
- Management IP addresses

# Configure Radware DefensePro

The Cisco Firepower 4100/9300 chassis can support multiple services (for example, a firewall and a third-party DDoS application) on a single blade. These applications and services can be linked together to form a Service Chain.

## About Radware DefensePro

In the current supported Service Chaining configuration, the third-party Radware DefensePro virtual platform runs in front of the ASA firewall. Radware DefensePro is a KVM-based virtual platform that provides distributed denial-of-service (DDoS) detection and mitigation capabilities on the Firepower 4100/9300 chassis. When Service Chaining is enabled on your Firepower 4100/9300 chassis, traffic from the network must first pass through the DefensePro virtual platform before reaching the main ASA firewall.

**Note**

- The Radware DefensePro virtual platform may be referred to as *Radware vDP* (virtual DefensePro), or simply *vDP*.
- The Radware DefensePro virtual platform may occasionally be referred to as a Link Decorator.

## Prerequisites for Radware DefensePro

Prior to deploying Radware DefensePro on your Firepower 4100/9300 chassis, you must configure the Firepower 4100/9300 chassis to use an NTP Server with the **etc/UTC** Time Zone. For more information about setting the date and time in your Firepower 4100/9300 chassis, see [Setting the Date and Time](#).

## Guidelines for Service Chaining

### Models

- ASA—The Radware DefensePro (vDP) platform is supported with ASA on the following models:
  - Firepower 9300
  - Firepower 4120—You must use the CLI to deploy Radware DefensePro on this platform; the Firepower Chassis Manager does not yet support this functionality.
  - Firepower 4140—You must use the CLI to deploy Radware DefensePro on this platform; the Firepower Chassis Manager does not yet support this functionality.
  - Firepower 4150

**Note**

The Radware DefensePro platform is not currently supported with ASA on Firepower 4110 devices.

### Additional Guidelines

## Configure Radware DefensePro on a Standalone Logical Device

The following procedure shows how to install Radware DefensePro in a single Service Chain in front of a standalone ASA or Firepower Threat Defense logical device.

### Before you begin

- Download the vDP image from Cisco.com (see [Downloading Images from Cisco.com](#)) and then download that image to the Firepower 4100/9300 chassis (see [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis](#)).
- You can deploy the Radware DefensePro application in a standalone configuration on an intra-chassis cluster; for intra-chassis clustering, see [Configure Radware DefensePro on an Intra-Chassis Cluster](#), on page 49.

### Procedure

- 
- Step 1** If you want to use a separate management interface for vDP, enable the interface and set it to be the mgmt type according to [Configure a Physical Interface](#). Otherwise, you can share the application management interface.
- Step 2** Create an ASA logical device in standalone configuration (see [Add a Standalone ASA](#), on page 9).
- Step 3** Enter security services mode:
- ```
Firepower# scope ssa
```
- Step 4** Create the Radware vDP instance:
- ```
Firepower /ssa # scope slot slot_id
Firepower /ssa/slot # create app-instance vdp logical_device_identifier
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot/* # exit
```
- Step 5** Commit the configuration:
- ```
commit-buffer
```
- Step 6** Verify the installation and provisioning of vDP on the security module:
- ```
Firepower /ssa # show app-instance
```
- Step 7** Once the vDP application is installed, access the logical device:
- ```
Firepower /ssa # scope logical-device device_name
```
- Step 8** Assign the management interface to vDP. You can use the same physical interface as for the logical device, or you can use a separate interface.
- ```
Firepower /ssa/logical-device # enter external-port-link name interface_id vdp
Firepower /ssa/logical-device/external-port-link* # exit
```



- Step 9** Configure the external management interface settings for vDP.
- Create the bootstrap object:  
Firepower /ssa/logical-device\* # **create mgmt-bootstrap vdp**
  - Configure the management IP address:  
Firepower /ssa/logical-device/mgmt-bootstrap\* #**create ipv4 slot\_id default**
  - Set the gateway address:  
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4\* #**set gateway gateway\_address**
  - Set the IP address and mask:  
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4\* #**set ip ip\_address mask network\_mask**
  - Exit the management IP configuration scope:  
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4\* #**exit**
  - Exit the management bootstrap configuration scope:  
Firepower /ssa/logical-device/mgmt-bootstrap\* #**exit**
- Step 10** Edit the data interface where you want to place the vDP in front of the ASA flow:  
Firepower /ssa/logical-device\* # **scope external-port-link name**  
Enter the **show external-port-link** command to view interface names.
- Step 11** Add the vDP to the logical device:  
Firepower /ssa/logical-device/external-port-link\* # **set decorator vdp**  
Repeat for each interface where you want to use vDP.
- Step 12** Commit the configuration:  
**commit-buffer**
- Step 13** Verify that the third-party app is set for the interface:  
Firepower /ssa/logical-device/external-port-link\* # **show detail**

**What to do next**

Set a password for the DefensePro application. Note that the application does not come online until you set a password. For more information, see the Radware DefensePro DDoS Mitigation User Guide on cisco.com.

## Configure Radware DefensePro on an Intra-Chassis Cluster



**Note** Service Chaining is not supported in an inter-chassis cluster configuration. However, the Radware DefensePro application can be deployed in a standalone configuration in an inter-chassis cluster scenario.

**Before you begin**

- Download the vDP image from Cisco.com (see [Downloading Images from Cisco.com](#)) and then download that image to the Firepower 4100/9300 chassis (see [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis](#)).

**Procedure**

- 
- Step 1** If you want to use a separate management interface for vDP, enable the interface and set it to be the mgmt type according to [Configure a Physical Interface](#). Otherwise, you can share the application management interface.
- Step 2** Configure an ASA intra-chassis cluster (see [Create an ASA Cluster, on page 27](#))
- Step 3** Decorate the external (client-facing) port with Radware DefensePro:
- ```

enter external-port-link name interface_name { asa }
set decorator vdp
set description ""
exit

```
- Step 4** Assign the external management port for the logical device:
- ```

enter external-port-link { mgmt_asa / mgmt_ftd } interface_id { asa / ftd }
set decorator ""
set description ""
exit

```
- Step 5** Assign the external management port for DefensePro:
- ```

enter external-port-link mgmt_vdp interface_name { asa / ftd }
set decorator ""
set description ""

```
- Step 6** Configure cluster port channel:
- ```

enter external-port-link port-channel48 Port-channel48 { asa / ftd }
set decorator ""
set description ""
exit

```
- Step 7** Configure management bootstrap for all three DefensePro instances:
- ```

enter mgmt-bootstrap vdp
enter ipv4 slot_id default
set gateway gateway_address
set ip ip_address mask network_mask

```

exit

Example:

```

enter mgmt-bootstrap vdp
  enter ipv4 1 default
    set gateway 172.16.0.1
    set ip 172.16.4.219 mask 255.255.0.0
  exit

  enter ipv4 2 default
    set gateway 172.16.0.1
    set ip 172.16.4.220 mask 255.255.0.0
  exit

  enter ipv4 3 default
    set gateway 172.16.0.1
    set ip 172.16.4.221 mask 255.255.0.0
  exit

```

Step 8 Exit management bootstrap configuration scope:

exit

Step 9 Enter the DefensePro application instance on the Control blade:

connect module slot console

connect vdp

Step 10 On the Control blade, set the management IP:

device clustering management-channel ip

Step 11 Using the IP found in the previous step, set the Control IP:

device clustering master set management-channel ip

Step 12 Enable the cluster:

device clustering state set enable

Step 13 Exit the application console and return to the FXOS module CLI:

Ctrl]

Step 14 Repeat steps 10, 12, 13, and 14 to set the Control blade IP found in step 11 and enable the cluster for each blade application instance.

Step 15 Commit the configuration:

commit-buffer

Note After completing this procedure, you must verify whether the DefensePro instances are configured in a cluster.

Step 16 Validate that all DefensePro applications have joined the cluster:

device cluster show

Step 17 Use either of the following methods to verify which DefensePro instance is primary, and which one is secondary.

a) Scope the DefensePro instance and show application attributes for DefensePro only:

scope ssa

scope slot *slot_number*

scope app-instance vdp

show app-attri

- b) Scope the slot and show the DefensePro instance in expanded detail. This approach displays information for both logical device and vDP application instances on the slot.

scope ssa

scope *slot_number*

show app-instance expand detail

If the DefensePro application is online but not yet formed in a cluster, the CLI displays:

```
App Attribute:
App Attribute Key: cluster-role
Value: unknown
```

If the system displays this "unknown" value, you must enter the DefensePro application and configure the Control blade IP address to create the vDP cluster.

If the DefensePro application is online and formed in a cluster, the CLI displays:

```
App Attribute:
App Attribute Key: cluster-role
Value: primary/secondary
```

Example

```
scope ssa
  enter logical-device ld asa "1,2,3" clustered
  enter cluster-bootstrap
    set chassis-id 1
    set ipv4 gateway 172.16.0.1
    set ipv4 pool 172.16.4.216 172.16.4.218
    set ipv6 gateway 2010::2
    set ipv6 pool 2010::21 2010::26
    set key secret
    set mode spanned-etherchannel
    set name cisco
    set virtual ipv4 172.16.4.222 mask 255.255.0.0
    set virtual ipv6 2010::134 prefix-length 64
  exit
  enter external-port-link Ethernet1-2 Ethernet1/2 asa
    set decorator vdp
    set description ""
  exit
  enter external-port-link Ethernet1-3_asa Ethernet1/3 asa
    set decorator ""
    set description ""
  exit
  enter external-port-link mgmt_asa Ethernet1/1 asa
    set decorator ""
    set description ""
  exit
```

```

enter external-port-link mgmt_vdp Ethernet1/1 vdp
    set decorator ""
    set description ""
exit
enter external-port-link port-channel48 Port-channel48 asa
    set decorator ""
    set description ""
exit
enter mgmt-bootstrap vdp
    enter ipv4 1 default
        set gateway 172.16.0.1
        set ip 172.16.4.219 mask 255.255.0.0
    exit

    enter ipv4 2 default
        set gateway 172.16.0.1
        set ip 172.16.4.220 mask 255.255.0.0
    exit

    enter ipv4 3 default
        set gateway 172.16.0.1
        set ip 172.16.4.221 mask 255.255.0.0
    exit
exit
commit-buffer
scope ssa
    scope slot 1
    scope app-instance vdp
    show app-attri
App Attribute:
App Attribute Key: cluster-role
Value: unknown

```

What to do next

Set a password for the DefensePro application. Note that the application does not come online until you set a password. For more information, see the Radware DefensePro DDoS Mitigation User Guide on [cisco.com](https://www.cisco.com).

Open UDP/TCP Ports and Enable vDP Web Services

The Radware APSolute Vision Manager interfaces communicate with the Radware vDP application using various UDP/TCP ports. In order for the vDP application to communicate with the APSolute Vision Manager, you must ensure that these ports are accessible and not blocked by your firewall. For more information on which specific ports to open, see the following tables in the APSolute Vision User Guide:

- **Ports for APSolute Vision Server-WBM Communication and Operating System**
- **Communication Ports for APSolute Vision Server with Radware Devices**

In order for Radware APSolute Vision to manage the Virtual DefensePro application deployed on the FXOS chassis, you must enable the vDP web service using the FXOS CLI.

Procedure

-
- Step 1** From the FXOS CLI, connect to the vDP application instance.

connect module *slot* console

connect vdp

Step 2 Enable vDP web services.

manage secure-web status set enable

Step 3 Exit the vDP application console and return to the FXOS module CLI.

Ctrl]

Manage Logical Devices

You can delete a logical device, convert an ASA to transparent mode, change the interface configuration, and perform other tasks on existing logical devices.

Connect to the Console of the Application

Use the following procedure to connect to the console of the application.

Procedure

Step 1 Connect to the module CLI.

connect module *slot_number* console

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

Step 2 Connect to the application console. Enter the appropriate command for your device.

connect ftd

connect vdp

Step 3 Exit the application console to the FXOS module CLI.

- FTD—Enter

- vDP—Enter **Ctrl-], .**

Step 4 Return to the supervisor level of the FXOS CLI.

a) Enter ~

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Delete a Logical Device

Procedure

Step 1 Enter security services mode:

Firepower# **scope ssa**

Step 2 View details for the logical devices on the chassis:

Firepower /ssa # **show logical-device**

Step 3 For each logical device that you want to delete, enter the following command:

Firepower /ssa # **delete logical-device** *device_name*

Step 4 View details for the applications installed on the logical devices:

Firepower /ssa # **show app-instance**

Step 5 For each application that you want to delete, enter the following commands:

a) Firepower /ssa # **scope slot** *slot_number*

b) Firepower /ssa/slot # **delete app-instance** *application_name*

c) Firepower /ssa/slot # **exit**

Step 6 Commit the configuration:

commit-buffer

Commits the transaction to the system configuration.

Example

```
Firepower# scope ssa
```

```
Firepower /ssa # show logical-device
```

```
Logical Device:
```

Name	Description	Slot ID	Mode	Operational State	Template Name
FTD		1,2,3	Clustered	Ok	ftd

```

Firepower /ssa # delete logical-device FTD
Firepower /ssa* # show app-instance
Application Name      Slot ID      Admin State      Operational State      Running Version Startup
Version Cluster Oper State
-----
ftd                    1 Disabled      Stopping          6.0.0.837
6.0.0.837             Not Applicable
ftd                    2 Disabled      Offline           6.0.0.837
6.0.0.837             Not Applicable
ftd                    3 Disabled      Not Available
6.0.0.837             Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer

```

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 within the application using the **show cluster info** command:

```

ciscoasa# show cluster info
Clustering is not enabled

```

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**—At the FXOS CLI, see the following example:


```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asa1
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

To reenable:

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- Shut down the security module/engine—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

To power up:

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- Shut down the chassis—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

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—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- 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.

Change the ASA to Transparent Firewall Mode

You can only deploy a routed firewall mode ASA from the Firepower 4100/9300 chassis. To change the ASA to transparent firewall mode, complete the initial deployment, and then change the firewall mode within the ASA CLI. For standalone ASAs, because changing the firewall mode erases the configuration, you must then redeploy the configuration from the Firepower 4100/9300 chassis to regain the bootstrap configuration. The ASA then remains in transparent mode with a working bootstrap configuration. For clustered ASAs, the configuration is not erased, so you do not need to redeploy the bootstrap configuration from FXOS.

Procedure

Step 1 Connect to the ASA console according to [Connect to the Console of the Application, on page 54](#). For a cluster, connect to the primary unit. For a failover pair, connect to the active unit.

Step 2 Enter configuration mode:

enable

configure terminal

By default, the enable password is blank.

Step 3 Set the firewall mode to transparent:

firewall transparent

Step 4 Save the configuration:

write memory

For a cluster or failover pair, this configuration is replicated to secondary units:

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to unit-1-2
End Configuration Replication to data unit.

asa(config)#
```

Step 5 On the Firepower Chassis Manager **Logical Devices** page, click the **Edit** icon to edit the ASA.

The **Provisioning** page appears.

Step 6 Click the device icon to edit the bootstrap configuration. Change any value in your configuration, and click **OK**.

You must change the value of at least one field, for example, the **Password** field.

You see a warning about changing the bootstrap configuration; click **Yes**.

Step 7 For an inter-chassis cluster or for a failover pair, repeat steps 5 through 7 to redeploy the bootstrap configuration on each chassis.

Wait several minutes for the chassis/security modules to reload, and for the ASA to become operational again. The ASA now has an operational bootstrap configuration, but remains in transparent mode.

Change an Interface on a Firepower Threat Defense Logical Device

You can allocate or unallocate an interface on the FTD logical device. You can then sync the interface configuration in FMC.

Adding a new interface, or deleting an unused interface has minimal impact on the FTD configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the FTD configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the FMC.

Deleting an interface will delete any configuration associated with that interface.

Before you begin

- Configure your interfaces, and add any EtherChannels according to [Configure a Physical Interface](#) and [Add an EtherChannel \(Port Channel\)](#).
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- If you want to replace the management or firepower eventing interface, you must use the Firepower Chassis Manager; the CLI does not support this change.
- For clustering or High Availability, make sure you add or remove the interface on all units before you sync the configuration in the FMC. We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.

Procedure

- | | |
|---------------|---|
| Step 1 | Enter security services mode:

Firepower# scope ssa |
| Step 2 | Edit the logical device:

Firepower /ssa # scope logical-device device_name |
| Step 3 | Allocate a new interface to the logical device:

Firepower /ssa/logical-device* # create external-port-link name interface_id ftd

Do not delete any interfaces yet. |
| Step 4 | Commit the configuration: |

commit-buffer

Commits the transaction to the system configuration.

- Step 5** Sync the interfaces in FMC.
- Log into the FMC.
 - Select **Devices > Device Management** and click **Edit** (✎) for your FTD device. The **Interfaces** page is selected by default.
 - Click the **Sync Device** button on the top left of the **Interfaces** page.
 - After the changes are detected, you will see a red banner on the **Interfaces** page indicating that the interface configuration has changed. Click the **Click to know more** link to view the interface changes.
 - If you plan to delete an interface, manually transfer any interface configuration from the old interface to the new interface.

Because you have not yet deleted any interfaces, you can refer to the existing configuration. You will have additional opportunity to fix the configuration after you delete the old interface and re-run the validation. The validation will show you all locations in which the old interface is still used.

- Click **Save**.
- Select the devices and click **Deploy** to deploy the policy to the assigned devices. The changes are not active until you deploy them.

- Step 6** In FXOS, unallocate an interface from the logical device:
- Firepower /ssa/logical-device # **delete external-port-link** *name*
- Enter the **show external-port-link** command to view interface names.

- Step 7** Commit the configuration:

commit-buffer

Commits the transaction to the system configuration.

- Step 8** Sync the interfaces again in FMC.

Change an Interface on an ASA Logical Device

You can allocate, unallocate, or replace a management interface on an ASA logical device. ASDM discovers the new interfaces automatically.

Adding a new interface, or deleting an unused interface has minimal impact on the ASA configuration. However, if you remove an allocated interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an allocated interface to an EtherChannel), and the interface is used in your security policy, removal will impact the ASA configuration. In this case, the ASA configuration retains the original commands so that you can make any necessary adjustments. You can manually remove the old interface configuration in the ASA OS.



Note You can edit the membership of an allocated EtherChannel without impacting the logical device.

Before you begin

- Configure your interfaces and add any EtherChannels according to [Configure a Physical Interface](#) and [Add an EtherChannel \(Port Channel\)](#).
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- For clustering or failover, make sure you add or remove the interface on all units. We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. New interfaces are added in an administratively down state, so they do not affect interface monitoring.

Procedure

-
- Step 1** Enter security services mode:
Firepower# **scope ssa**
- Step 2** Edit the logical device:
Firepower /ssa # **scope logical-device** *device_name*
- Step 3** Unallocate an interface from the logical device:
Firepower /ssa/logical-device # **delete external-port-link** *name*
Enter the **show external-port-link** command to view interface names.
For a management interface, delete the current interface then commit your change using the **commit-buffer** command before you add the new management interface.
- Step 4** Allocate a new interface to the logical device:
Firepower /ssa/logical-device* # **create external-port-link** *name interface_id asa*
- Step 5** Commit the configuration:
commit-buffer
Commits the transaction to the system configuration.
-

Monitoring Logical Devices

- **show app**

View available images.

```
Firepower# scope ssa
Firepower /ssa # show app
```

Name	Version	Author	Supported Deploy Types	CSP Type	Is Default
App					

```

-----
asa          9.10.1          cisco      Native      Application Yes
ftd          6.2.3          cisco      Native      Application Yes
vdp          8.13.01.09-2    radware    Vm          Application Yes

```

• show app-instance

View the application instance status and information.

```

Firepower# scope ssa
Firepower /ssa # show app-instance
App Name    Slot ID    Admin State Oper State    Running Version Startup Version
Cluster State Cluster Role
-----
ftd         1          Enabled    Online        6.2.1.62      6.2.1.62      Not
Applicable  None
vdp         1          Disabled   Installing    8.10.01.16-5  Not
Applicable  None

```

• show logical-device

View details for logical devices.

```

Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
Name        Description Slot ID    Mode        Oper State    Template Name
-----
asa1        1          Standalone Ok          asa

```

• show app-resource-profile

Show resource profiles for vDP.

```

Firepower# scope ssa
Firepower /ssa # scope app vdp 8.13.01.09-2
Firepower /ssa/app # show app-resource-profile
Profile Name          Security Model  CPU Logical Core Count RAM Size (MB)  Default
Profile
-----
DEFAULT-4110-RESOURCE  FPR4K-SM-12          4          16384 Yes
DEFAULT-RESOURCE       FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44,
FPR4K-SM-36, FPR4K-SM-24          6          24576 Yes
VDP-10-CORES           FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44,
FPR4K-SM-36, FPR4K-SM-24          10         40960 No
VDP-2-CORES            all                  2          8192 No
VDP-4-CORES            all                  4          16384 No
VDP-8-CORES            FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44,
FPR4K-SM-36, FPR4K-SM-24          8          32768 No

```

Examples for Inter-Site Clustering

The following examples show supported cluster deployments.

Spanned EtherChannel Routed Mode Example with Site-Specific MAC Addresses

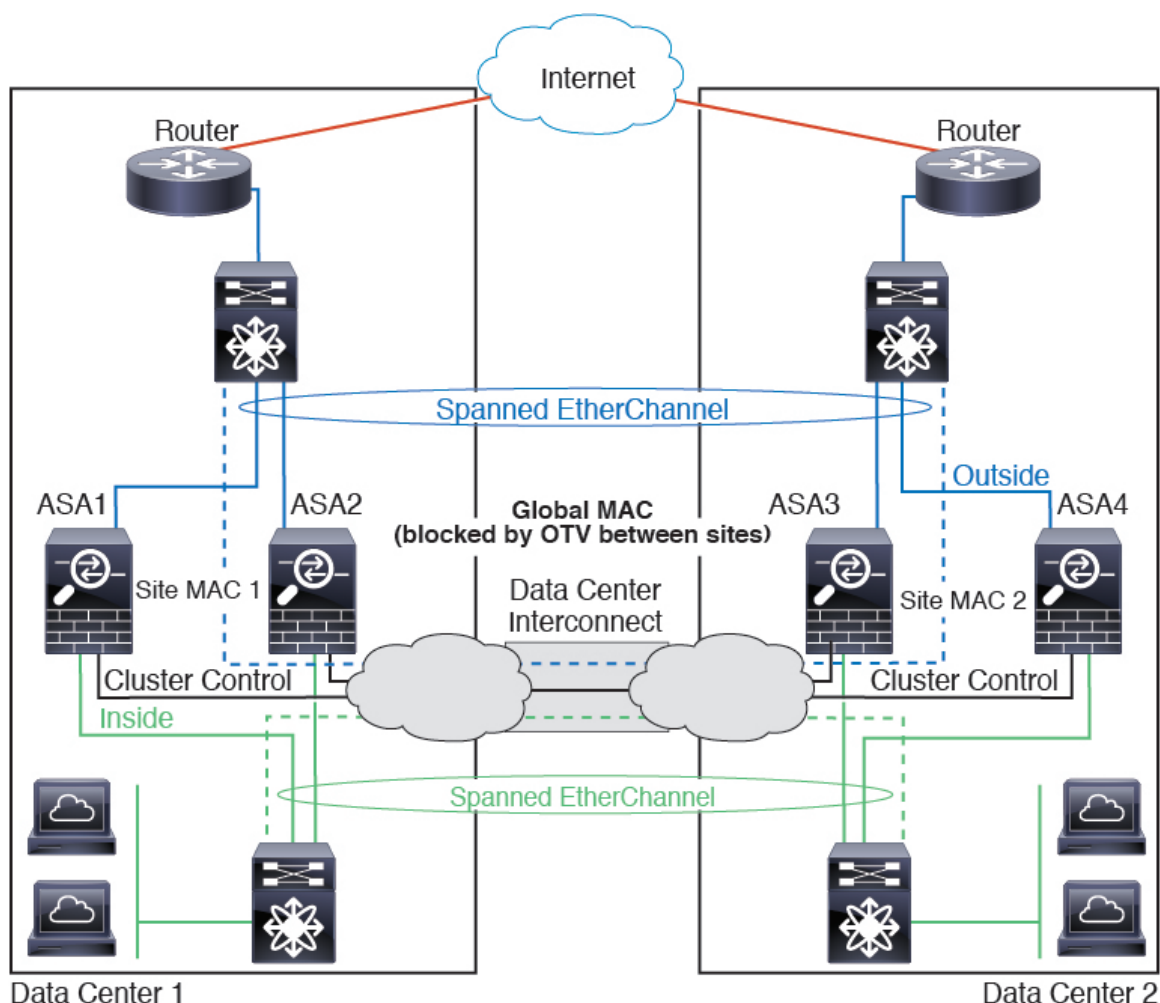
The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and an inside network at each site (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches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

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

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

In this scenario:

- All egress packets sent from the cluster use the site MAC address and are localized at the data center.
- All ingress packets to the cluster are sent using the global MAC address, so they can be received by any of the units at both sites; filters at the OTV localize the traffic within the data center.



Spanned EtherChannel Transparent Mode North-South Inter-Site Example

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

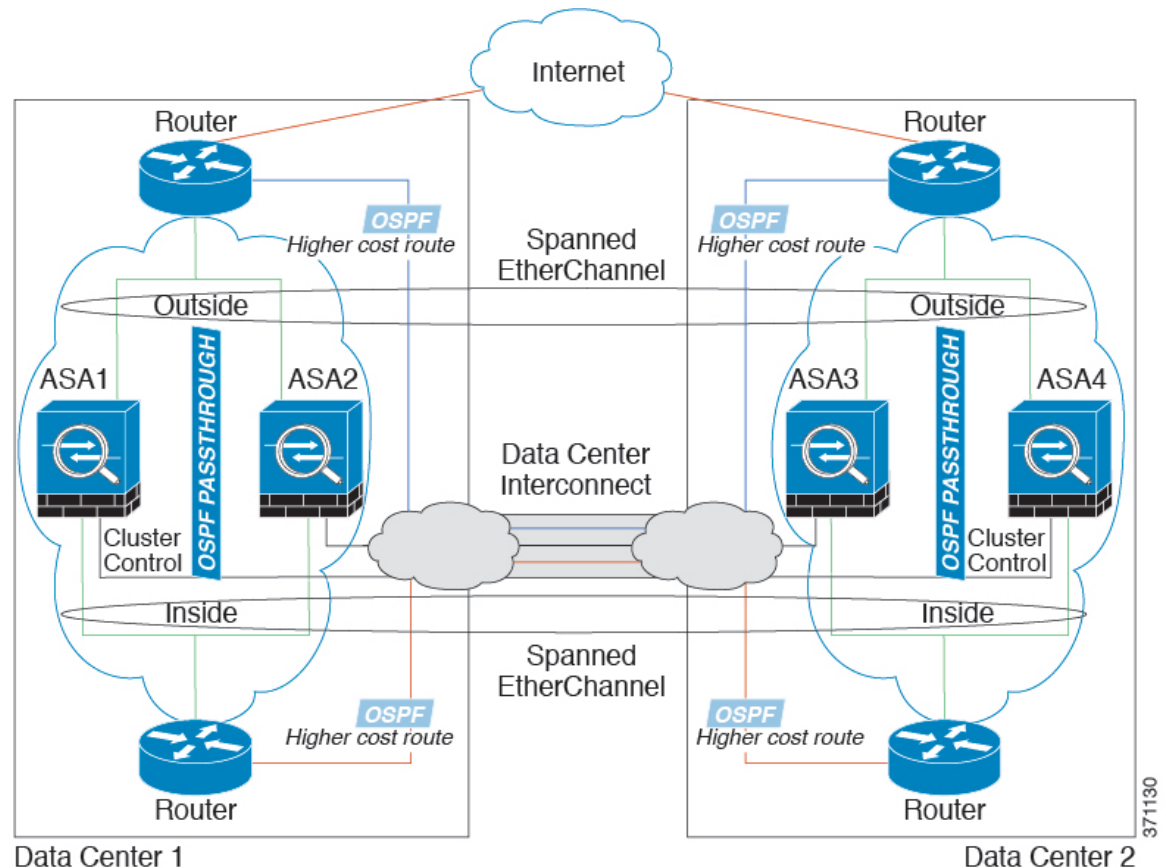
The inside and outside routers at each data center use OSPF, which is passed through the transparent ASAs. Unlike MACs, router IPs are unique on all routers. By assigning a higher cost route across the DCI, traffic stays within each data center unless all cluster members at a given site go down. The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

The implementation of the switches at each site can include:

- Inter-site VSS/vPC—In this scenario, you install one switch at Data Center 1, and the other at Data Center 2. One option is for the cluster units at each Data Center to only connect to the local switch, while the VSS/vPC traffic goes across the DCI. In this case, connections are for the most part kept local to each

datacenter. You can optionally connect each unit to both switches across the DCI if the DCI can handle the extra traffic. In this case, traffic is distributed across the data centers, so it is essential for the DCI to be very robust.

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

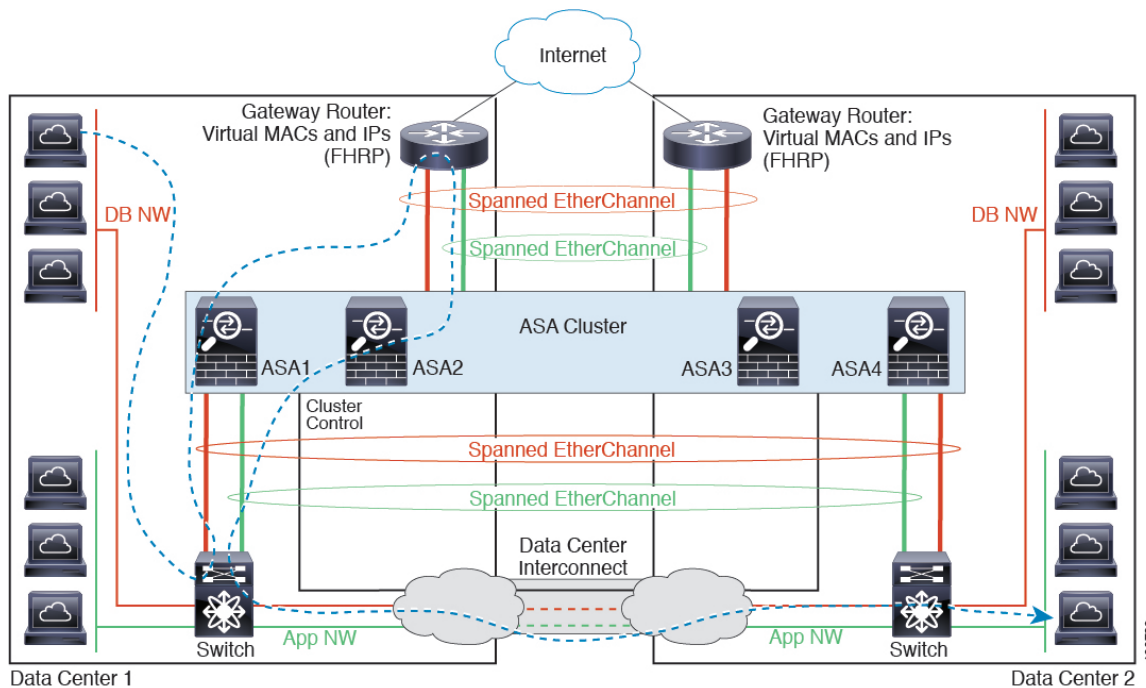


Spanned EtherChannel Transparent Mode East-West Inter-Site Example

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

The gateway router at each site uses an FHRP such as HSRP to provide the same destination virtual MAC and IP addresses at each site. A good practice to avoid unintended MAC address flapping is to statically add the gateway routers real MAC addresses to the ASA MAC address table using the **mac-address-table static *outside_interface* *mac_address*** command. Without these entries, if the gateway at site 1 communicates with the gateway at site 2, that traffic might pass through the ASA and attempt to reach site 2 from the inside

interface and cause problems. The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters to prevent traffic from traversing the DCI to the other site when the traffic is destined for the gateway router. If the gateway router at one site becomes unreachable, you must remove the filters so traffic can be sent to the other site's gateway router.



See [Spanned EtherChannel Transparent Mode North-South Inter-Site Example, on page 64](#) for information about vPC/VSS options.

History for Logical Devices

Feature Name	Platform Releases	Feature Information
Support for FTD clustering on the Firepower 4100	2.1.1	You can cluster up to 6 chassis in an FTD cluster.
Support for 16 Firepower 4100 chassis in an ASA cluster	2.0.1	You can cluster up to 16 chassis in an ASA cluster.
Support for ASA clustering on the Firepower 4100	1.1.4	You can cluster up to 6 chassis in an ASA cluster.

Feature Name	Platform Releases	Feature Information
Support for intra-chassis clustering on the FTD on the Firepower 9300	1.1.4	<p>The Firepower 9300 supports intra-chassis clustering with the FTD application.</p> <p>We introduced the following commands: enter mgmt-bootstrap ftd, enter bootstrap-key FIREPOWER_MANAGER_IP, enter bootstrap-key FIREWALL_MODE, enter bootstrap-key-secret REGISTRATION_KEY, enter bootstrap-key-secret PASSWORD, enter bootstrap-key FQDN, enter bootstrap-key DNS_SERVERS, enter bootstrap-key SEARCH_DOMAINS, enter ipv4 firepower, enter ipv6 firepower, set value, set gateway, set ip, accept-license-agreement</p>
Inter-chassis clustering for 16 ASA modules on the Firepower 9300	1.1.3	<p>You can now enable inter-chassis clustering for the ASA. You can include up to 16 modules. For example, you can use 1 module in 16 chassis, or 2 modules in 8 chassis, or any combination that provides a maximum of 16 modules.</p>
Intra-chassis Clustering for the ASA on the Firepower 9300	1.1.1	<p>You can cluster all ASA security modules within the Firepower 9300 chassis.</p> <p>We introduced the following commands: enter cluster-bootstrap, enter logical-device clustered, set chassis-id, set ipv4 gateway, set ipv4 pool, set ipv6 gateway, set ipv6 pool, set key, set mode spanned-etherchannel, set port-type cluster, set service-type, set virtual ipv4, set virtual ipv6</p>

