Interface Overview

The threat defense device includes data interfaces that you can configure in different modes, as well as a management/diagnostic interface.

Management/Diagnostic Interface

The physical management interface is shared between the Diagnostic logical interface and the Management logical interface.

Management Interface

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the management center. It uses its own IP address and static routing. You can configure its settings at the CLI using the **configure network** command. If you change the IP address at the CLI after you add it to the management center, you can match the IP address in the Secure Firewall Management Center in the **Devices** > **Device Management** > **Devices** > **Management** area.

You can alternatively manage the threat defense using a data interface instead of the Management interface.

Diagnostic Interface

The Diagnostic logical interface can be configured along with the rest of the data interfaces on the **Devices** > **Device Management** > **Interfaces** screen. Using the Diagnostic interface is optional (see the routed and transparent mode deployments for scenarios). The Diagnostic interface only allows management traffic, and does not allow through traffic. It does not support SSH; you can SSH to data interfaces or to the Management interface only. The Diagnostic interface is useful for SNMP or syslog monitoring.

Note Although the Diagnostic and Management interfaces share a physical port, you must assign different IP addresses to each interface on the same network.

Interface Mode and Types

You can deploy threat defense interfaces in two modes: Regular firewall mode and IPS-only mode. You can include both firewall and IPS-only interfaces on the same device.

Regular Firewall Mode

Firewall mode interfaces subject traffic to firewall functions such as maintaining flows, tracking flow states at both IP and TCP layers, IP defragmentation, and TCP normalization. You can also optionally configure IPS functions for this traffic according to your security policy.

The types of firewall interfaces you can configure depends on the firewall mode set for the device: routed or transparent mode. See Transparent or Routed Firewall Mode for more information.

- Routed mode interfaces (routed firewall mode only)—Each interface that you want to route between is on a different subnet.
- Bridge group interfaces (routed and transparent firewall mode)—You can group together multiple interfaces on a network, and the threat defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. In routed mode, the threat defense device routes between BVIs and regular routed interfaces. In transparent mode, each bridge group is separate and cannot communicate with each other.

IPS-Only Mode

IPS-only mode interfaces bypass many firewall checks and only support IPS security policy. You might want to implement IPS-only interfaces if you have a separate firewall protecting these interfaces and do not want the overhead of firewall functions.

Note The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes.

IPS-only interfaces can be deployed as the following types:

- Inline Set, with optional Tap mode—An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the threat defense to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

  With tap mode, the threat defense is deployed inline, but the network traffic flow is undisturbed. Instead, the threat defense makes a copy of each packet so that it can analyze the packets. Note that rules of these types do generate intrusion events when they are triggered, and the table view of intrusion events indicates that the triggering packets would have dropped in an inline deployment. There are benefits to using tap mode with FTDs that are deployed inline. For example, you can set up the cabling between the threat defense and the network as if the threat defense were inline and analyze the kinds of intrusion events the threat defense generates. Based on the results, you can modify your intrusion policy and add the drop rules that best protect your network without impacting its efficiency. When you are ready to deploy the threat defense inline, you can disable tap mode and begin dropping suspicious traffic without having to reconfigure the cabling between the threat defense and the network.

Note Tap mode *significantly* impacts threat defense performance, depending on the traffic.

Note Inline sets might be familiar to you as "transparent inline sets," but the inline interface type is unrelated to the transparent firewall mode or the firewall-type interfaces.

- Passive or ERSPAN Passive—Passive interfaces monitor traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When you configure the threat defense in a passive deployment, the threat defense cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally. and no traffic received on these interfaces is retransmitted. Encapsulated remote switched port analyzer (ERSPAN) interfaces allow you to monitor traffic from source ports distributed over multiple switches, and uses GRE to encapsulate the traffic. ERSPAN interfaces are only allowed when the threat defense is in routed firewall mode.

Note Using SR-IOV interfaces as passive interfaces on NGFWv is not supported on some Intel network adapters (such as Intel X710 or 82599) using SR-IOV drivers due to a promiscuous mode restriction. In such cases, use a network adapter that supports this functionality. See Intel Ethernet Products for more information on Intel network adapters.

Security Zones and Interface Groups

Each interface can be assigned to a *security zone* and/or *interface group*. You then apply your security policy based on zones or groups. For example, you can assign the "inside" interface on one or more devices to the "inside" zone; and the "outside" interfaces to the "outside" zone. You can then configure your access control policy to enable traffic to go from the inside zone to the outside zone for every device using the same zones.

To view the interfaces that belong to each object, choose **Objects** > **Object Management** and click **Interface**. This page lists the security zones and interface groups configured on your managed devices. You can expand each interface object to view the type of interfaces in each interface object.

Note Policies that apply to **any** zone (a global policy) apply to interfaces in zones as well as any interfaces that are not assigned to a zone.

Note The Diagnostic/Management interface does not belong to a zone or interface group.

Security Zones Vs. Interface Groups

There are two types of interface objects:

- Security zones—An interface can belong to only one security zone.
- Interface groups—An interface can belong to multiple interface groups (and to one security zone).

  You can use interface groups in NAT policies, prefilter policies, and QoS policies, as well as features that let you specify the interface name directly, such as Syslog servers or DNS servers.

Some policies only support security zones, while other policies support zones and groups. Unless you need the functionality an interface group provides, you should default to using security zones because security zones are supported for all features.

You cannot change an existing security zone to an interface group or vice-versa; instead you must create a new interface object.

Note Although tunnel zones are not interface objects, you can use them in place of security zones in certain configurations; see Tunnel Zones and Prefiltering.

Interface Object Types

See the following interface object types:

- Passive—For IPS-only passive or ERSPAN interfaces.
- Inline—For IPS-only inline set interfaces.
- Switched—For regular firewall bridge group interfaces.
- Routed—For regular firewall routed interfaces.
- ASA—(Security zones only) For legacy ASA FirePOWER device interfaces.

All interfaces in an interface object must be of the same type. After you create an interface object, you cannot change the type of interfaces it contains.

Interface Names

Note that the interface (or zone name) itself does not provide any default behavior in regards to the security policy. We recommend using names that are self-describing to avoid mistakes in future configuration. A good name signifies a logical segment or traffic specification, for example:

- Names of internal interfaces—InsideV110, InsideV160, InsideV195
- Names of DMZ interfaces—DMZV11, DMZV12, DMZV-TEST
- Names of external interfaces—Outside-ASN78, Outside-ASN91

Interface Objects and Multitenancy

In a multidomain deployment, you can create interface objects at any level. An interface object created in an ancestor domain can contain interfaces that reside on devices in different domains. In this situation, subdomain users viewing the ancestor interface object configuration in the object manager can see only the interfaces in their domain.

Unless restricted by role, subdomain users can view **and** edit interface objects created in ancestor domains. Subdomain users can add and delete interfaces from these interface objects. They cannot, however, delete or rename the interface objects. You can neither view nor edit interface objects created in descendant domains.

Auto-MDI/MDIX Feature

For RJ-45 interfaces, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. For Gigabit Ethernet, when the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

Default Settings for Interfaces

This section lists default settings for interfaces.

Default State of Interfaces

The default state of an interface depends on the type.

- Physical interfaces—Disabled. The exception is the Management interface that is enabled for initial setup.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- VLAN subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.
- EtherChannel port-channel interfaces (ISA 3000)—Enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.
- EtherChannel port-channel interfaces (Firepower and Secure Firewall models)—Disabled.

Note For the Firepower 4100/9300, you can administratively enable and disable interfaces in both the chassis and in the management center. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and management center.

Default Speed and Duplex

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

By default, the speed and duplex for fiber (SFP) interfaces are set to the maximum speed, with auto-negotiation enabled.

For the Secure Firewall 3100, the speed is set to detect the installed SFP speed.

Create Security Zone and Interface Group Objects

Add security zones and interface groups to which you can assign device interfaces.

Tip You can create empty interface objects and add interfaces to them later. To add an interface, the interface must have a name. You can also create security zones (but not interface groups) while configuring interfaces.

Before you begin

Understand the usage requirements and restrictions for each type of interface object. See Security Zones and Interface Groups, on page 3.

Procedure

Step 1 Choose **Objects** > **Object Management**.

Step 2 Choose **Interface** from the list of object types.

Step 3 Click **Add > Security Zone** or **Add > Interface Group**.

Step 4 Enter a **Name**.

Step 5 Choose an **Interface Type**.

Step 6 (Optional) From the **Device** > **Interfaces** drop-down list, choose a device that contains interfaces you want to add.

You do not need to assign interfaces on this screen; you can instead assign interfaces to the zone or group when you configure the interface.

Step 7 Click **Save**.

What to do next

- If an active policy references your object, deploy configuration changes.

Enable the Physical Interface and Configure Ethernet Settings

This section describes how to:

- Enable the physical interface. By default, physical interfaces are disabled (with the exception of the Diagnostic interface).
- Set a specific speed and duplex. By default, speed and duplex are set to Auto.

This procedure only covers a small subset of Interface settings. Refrain from setting other parameters at this point. For example, you cannot name an interface that you want to use as part of an EtherChannel or redundant interface.

Note For the Firepower 4100/9300, you configure basic interface settings in FXOS. See Configure a Physical Interface for more information.

Note For Firepower 1010 switch ports, see Configure Firepower 1010 Switch Ports.

Threat Defense Feature History:

- 7.3—Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to Clause 108 RS-FEC from Clause 74 FC-FEC for 25 GB+ SR, CSR, and LR transceivers
- 7.2—LLDP support for the Firepower 2100, Secure Firewall 3100. Flow control support for the Secure Firewall 3100.
- 7.2—Support for Forward Error Correction for the Secure Firewall 3100
- 7.2—Support for setting the speed based on the SFP for the Secure Firewall 3100
- 7.2—LLDP support for the Firepower 1100
- 7.2—Interface auto-negotiation is now set independently from speed and duplex, interface sync improved

Before you begin

If you changed the physical interfaces on the device after you added it to the management center, you need to refresh the interface listing by clicking **Sync Interfaces from device** on the top left of **Interfaces**. For the Secure Firewall 3100, which supports hot swapping, see Manage the Network Module for the Secure Firewall 3100, on page 12 before you change interfaces on a device.

Procedure

Step 1 Select **Devices** > **Device Management** and click **Edit** (✎) for your threat defense device. The **Interfaces** page is selected by default.

Step 2 Click **Edit** (✎) for the interface you want to edit.

Step 3 Enable the interface by checking the **Enabled** check box.

Step 4 (Optional) Add a description in the **Description** field.

The description can be up to 200 characters on a single line, without carriage returns.

Step 5 (Optional) Set the duplex and speed by clicking **Hardware Configuration** > **Speed**.

- **Duplex**—Choose **Full** or **Half**. SFP interfaces only support **Full** duplex.
- **Speed**—Choose a speed (varies depending on the model). (Secure Firewall 3100 only) Choose **Detect SFP** to detect the speed of the installed SFP module and use the appropriate speed. Duplex is always Full, and auto-negotiation is always enabled. This option is useful if you later change the network module to a different model, and want the speed to update automatically.
- **Auto-negotiation**—Set the interface to negotiate the speed, link status, and flow control.
- **Forward Error Correction Mode**—(Secure Firewall 3100 only) For 25 Gbps and higher interfaces, enable Forward Error Correction (FEC). For an EtherChannel member interface, you must configure FEC before you add it to the EtherChannel. The setting chosen when you use **Auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 1: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC (Ethernet 1/9 through 1/16)	Network Module Default FEC
25G-SR	Clause 108 RS-FEC	Clause 108 RS-FEC
25G-LR	Clause 108 RS-FEC	Clause 108 RS-FEC
10/25G-CSR	Clause 108 RS-FEC	Clause 74 FC-FEC
25G-AOC*x*M	Clause 74 FC-FEC	Clause 74 FC-FEC
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate

Step 6 (Optional) (Firepower 1100, 2100, Secure Firewall 3100) Enable Link Layer Discovery Protocol (LLDP) by clicking **Hardware Configuration** > **Network Connectivity**.

- **Enable LLDP Receive**—Enables the firewall to receive LLDP packets from its peers.
- **Enable LLDP Transmit**—Enables the firewall to send LLDP packets to its peers.

Step 7 (Optional) (Secure Firewall 3100) Enable pause (XOFF) frames for flow control by clicking **Hardware Configuration** > **Network Connectivity**, and checking **Flow Control Send**.

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If the threat defense port experiences congestion (exhaustion of queuing resources on the internal switch) and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Note The threat defense supports transmitting pause frames so that the remote peer can rate-control the traffic.

However, receiving of pause frames is not supported.

The internal switch has a global pool of 8000 buffers of 250 bytes each, and the switch allocates buffers dynamically to each port. A pause frame is sent out every interface with flowcontrol enabled when the buffer usage exceeds the global high-water mark (2 MB (8000 buffers)); and a pause frame is sent out of a particular interface when its buffer exceeds the port high-water mark (.3125 MB (1250 buffers)). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark (1.25 MB globally (5000 buffers); .25 MB per port (1000 buffers)). The link partner can resume traffic after receiving an XON frame.

Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Step 8 In the **Mode** drop-down list, choose one of the following:.

- **None**—Choose this setting for regular firewall interfaces and inline sets. The mode will automatically be changed to Routed, Switched, or Inline based on futher configuration.
- **Passive**—Choose this setting for passive IPS-only interfaces.
- **Erspan**—Choose this setting for ERSPAN passive IPS-only interfaces.

Step 9 In the **Priority** field, enter a number ranging from 0–65535.

This value is used in the policy based routing configuration. The priority is used to determine how you want to distribute the traffic across multiple egress interfaces.

Step 10 Click **OK**.

Step 11 Click **Save**.

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

Step 12 Continue configuring interfaces.

- Regular Firewall Interfaces
- Inline Sets and Passive Interfaces

Sync Interface Changes with the Management Center

Interface configuration changes on the device can cause the management center and the device to get out of sync. The management center can detect interface changes by one of the following methods:

- Event sent from the device

- Sync when you deploy from the management center

  If the management center detects interface changes when it attempts to deploy, the deploy will fail. You must first accept the interface changes.

- Manual sync

There are two types of interface changes performed outside of management center that need to be synched:

- Addition or deletion of physical interfaces—Adding a new interface, or deleting an unused interface has minimal impact on the threat defense 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 threat defense configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. 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 management center.

  When the management center detects changes, the **Interface** page shows status (removed, changed, or added) to the left of each interface.

- Management Center access interface changes—If you configure a data interface for managing using the **configure network management-data-interface** command, you must manually make matching configuration changes in and then acknowledge the changes. These interface changes cannot be made automatically.

This procedure describes how to manually sync device changes if required and how to acknowledge the detected changes. If device changes are temporary, you should not save the changes in the management center; you should wait until the device is stable, and then re-sync.

Before you begin

Procedure

Step 1 Select **Devices** > **Device Management** and click **Edit** (✎) for your threat defense device. The **Interfaces** page is selected by default.

Step 2 If required, click **Sync Device** on the top left of **Interfaces**.

Step 3 After the changes are detected, see the following steps.

Addition or Deletion of Physical Interfaces

a) You will see a red banner on **Interfaces** indicating that the interface configuration has changed. Click the **Click to know more** link to view the interface changes.

b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

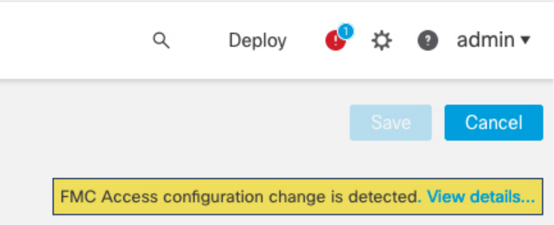
   If there are any errors, you need to change your policy and rerun the validation.

c) Click **Save**.

   You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices.

FMC Access Interface Changes

a) You will see a yellow banner in the top right of the **Device** page indicating that the management center access configuration has changed. Click the **View details** link to view the interface changes.

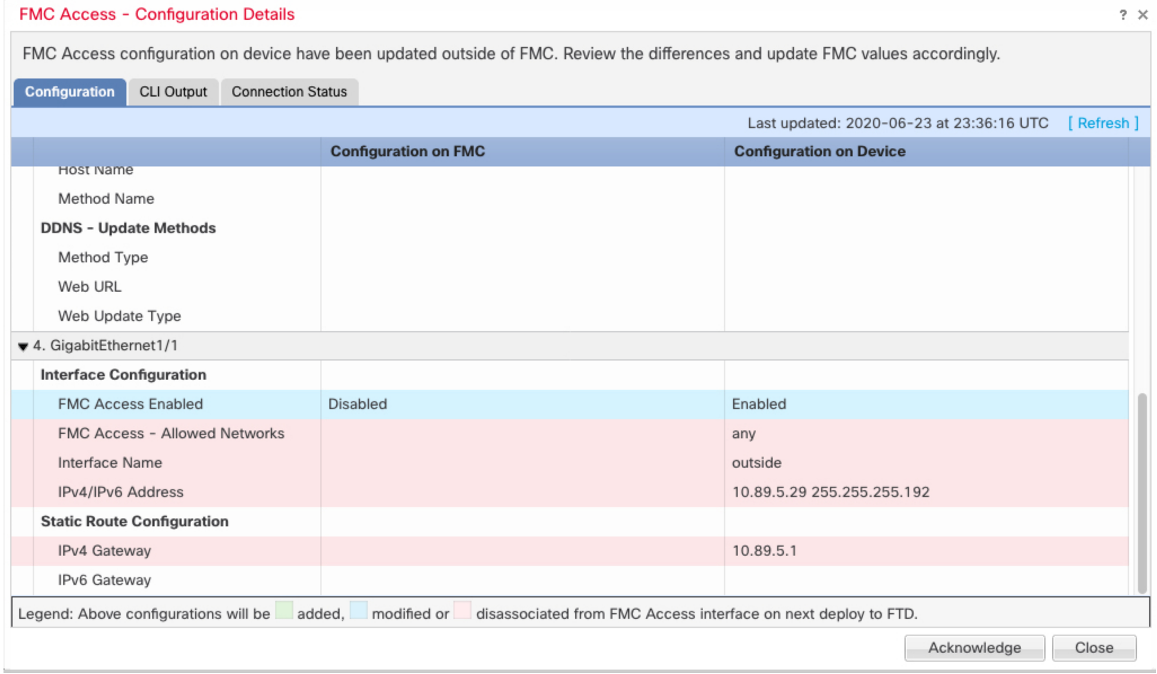


FMC Access configuration change is detected. View details...

The **FMC Access - Configuration Details** dialog box opens.

b) Take note of all highlighted configurations, especially the pink highlighted ones. You need to match any values on the threat defense by manually configuring them on the management center.

For example, the pink highlights below show configuration that exists on the threat defense but not yet on the management center.



FMC Access - Configuration Details

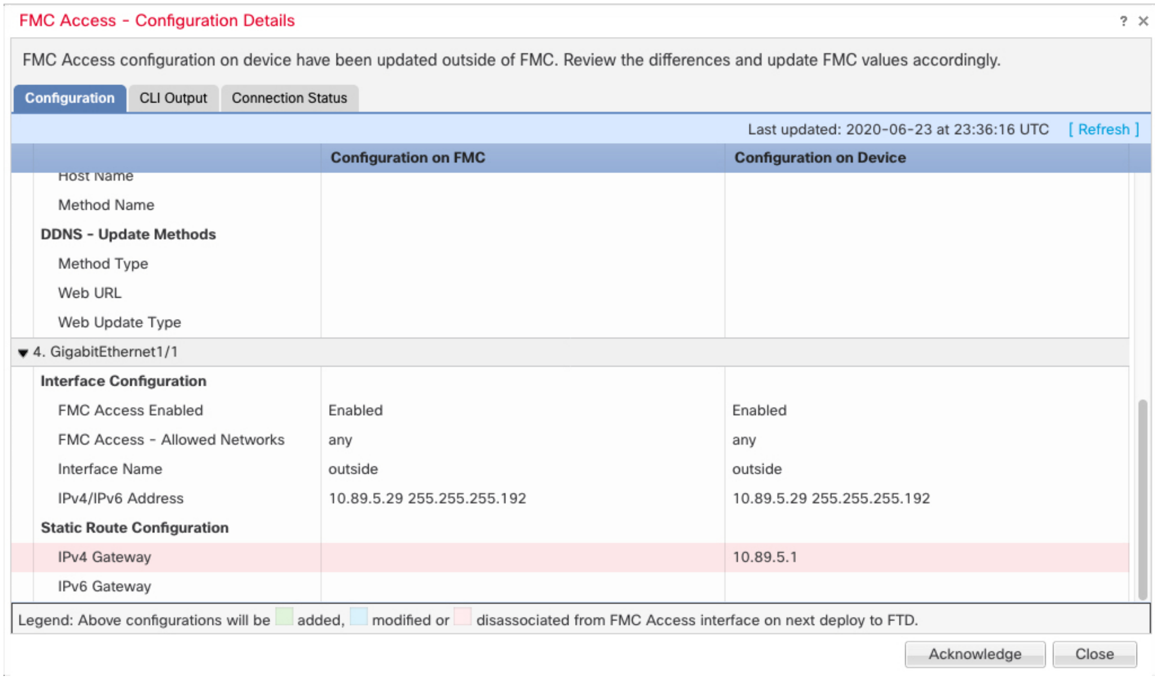
FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Last updated: 2020-06-23 at 23:36:16 UTC

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
DDNS - Update Methods		
Method Type		
Web URL		
Web Update Type		
▾ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Disabled	Enabled
FMC Access - Allowed Networks		any
Interface Name		outside
IPv4/IPv6 Address		10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be 🟩 added, 🟦 modified or 🟥 disassociated from FMC Access interface on next deploy to FTD.

The following example shows this page after configuring the interface in management center; the interface settings match, and the pink highlight was removed.



FMC Access - Configuration Details

FMC Access configuration on device have been updated outside of FMC. Review the differences and update FMC values accordingly.

Last updated: 2020-06-23 at 23:36:16 UTC [Refresh]

	Configuration on FMC	Configuration on Device
Host Name		
Method Name		
DDNS - Update Methods		
Method Type		
Web URL		
Web Update Type		
▼ 4. GigabitEthernet1/1		
Interface Configuration		
FMC Access Enabled	Enabled	Enabled
FMC Access - Allowed Networks	any	any
Interface Name	outside	outside
IPv4/IPv6 Address	10.89.5.29 255.255.255.192	10.89.5.29 255.255.255.192
Static Route Configuration		
IPv4 Gateway		10.89.5.1
IPv6 Gateway		

Legend: Above configurations will be 🟩 added, 🟦 modified or 🟥 disassociated from FMC Access interface on next deploy to FTD.

c) Click **Acknowledge**.

We recommend that you do not click **Acknowledge** until you have finished the management center configuration, and are ready to deploy. Clicking **Acknowledge** removes the block on deployment. The next time you deploy, the management center configuration will overwrite any remaining conflicting settings on the threat defense. It is your responsibility to manually fix the configuration in the management center before you re-deploy.

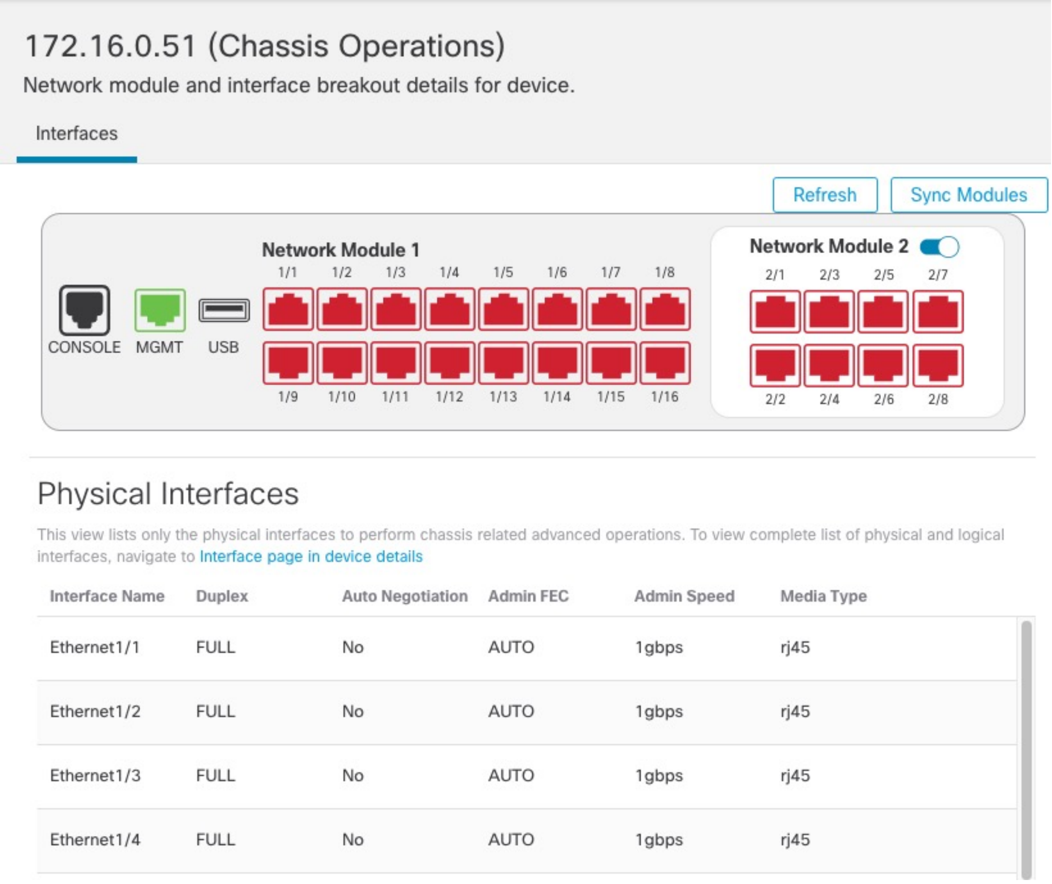
d) You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices.

Manage the Network Module for the Secure Firewall 3100

If you install a network module before you first power on the device, no action is required; the network module is enabled and ready for use.

To view physical interface details for the device, and to manage the network module, open the **Chassis Operations** page. From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit. The **Chassis Operations** page opens for the device.

Figure 1: Chassis Operations



172.16.0.51 (Chassis Operations)

Network module and interface breakout details for device.

Physical Interfaces

This view lists only the physical interfaces to perform chassis related advanced operations. To view complete list of physical and logical interfaces, navigate to Interface page in device details

Interface Name	Duplex	Auto Negotiation	Admin FEC	Admin Speed	Media Type
Ethernet1/1	FULL	No	AUTO	1gbps	rj45
Ethernet1/2	FULL	No	AUTO	1gbps	rj45
Ethernet1/3	FULL	No	AUTO	1gbps	rj45
Ethernet1/4	FULL	No	AUTO	1gbps	rj45

Click **Refresh** to refresh interface status. Click **Sync Modules** if you made a hardware change on the device that you need to detect.

If you need to make changes to your network module installation after initial bootup, then see the following procedures.

Configure Breakout Ports

You can configure 10GB breakout ports for each 40GB or higher interface. This procedure tells you how to break out and rejoin the ports. breakout ports can be used just like any other physical Ethernet port, including being added to EtherChannels.

Changes are immediate; you do not need to deploy to the device. After you break or rejoin, you cannot roll back to the previous interface state.

Before you begin

- You must use a supported breakout cable. See the hardware installation guide for more information.
- The interface cannot be in use for the following before breaking or rejoining:
    - Failover link

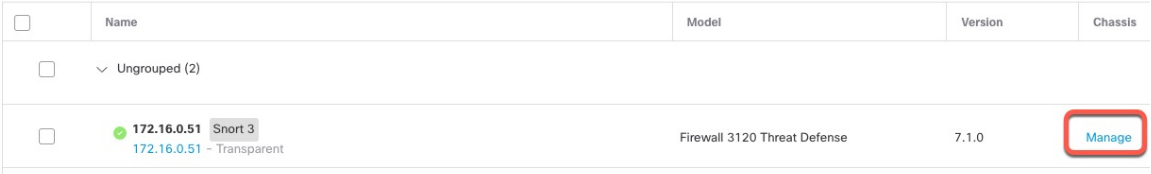
  - Cluster control link
  - Have a subinterface
  - EtherChannel member
  - BVI member
  - Manager access interface

- Breaking or rejoining and interface that is used directly in your security policy can impact the configuration; however, the action is not blocked.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 2: Manage Chassis



□	Name	Model	Version	Chassis
□	⌄ Ungrouped (2)			
□	● 172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 2 Break out 10GB ports from a 40GB or higher interface.

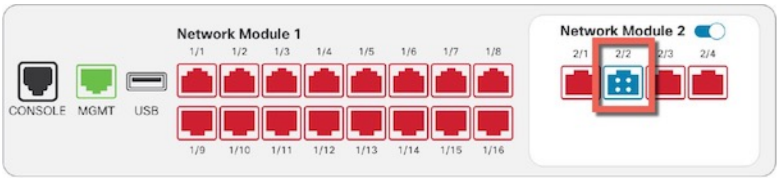
a) click **Break** (⤵) to the right of the interface.

Click **Yes** on the confirmation dialog box. If the interface is in use, you will see an error message. You must resolve any use cases before you can retry the breakout.

For example, to break out the Ethernet2/1 40GB interface, the resulting child interfaces will be identified as Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3, and Ethernet2/1/4.

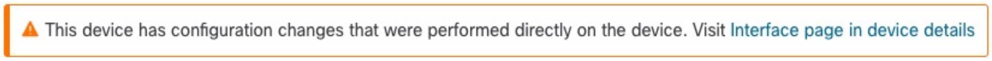
On the interfaces graphic, a port that is broken out has this appearance:

Figure 3: Breakout Ports



b) Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

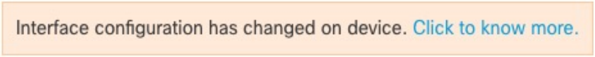
Figure 4: Go to Interface Page



⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

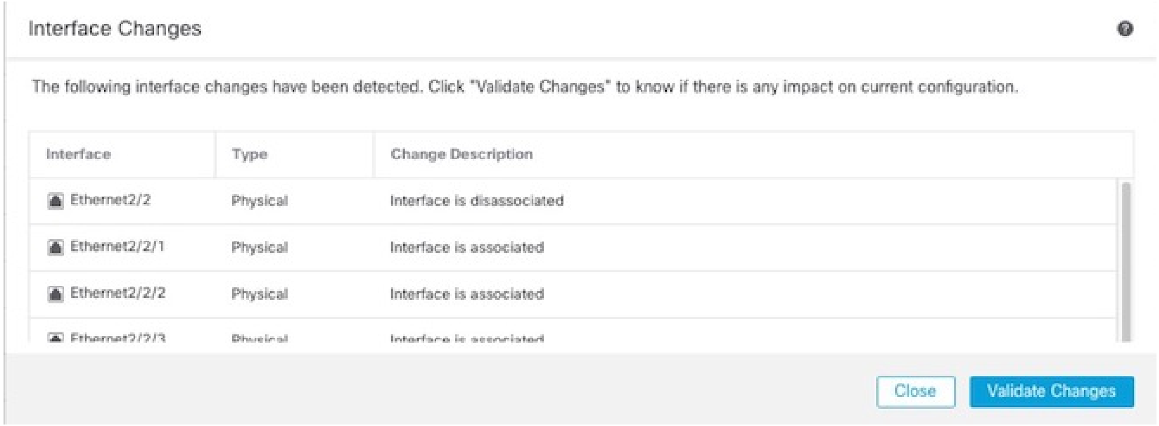
c) At the top of the **Interfaces** page, click **Click to know more**. The **Interface Changes** dialog box opens.

Figure 5: View Interface Changes



Interface configuration has changed on device. Click to know more.

Figure 6: Interface Changes



Interface Changes

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/2	Physical	Interface is disassociated
Ethernet2/2/1	Physical	Interface is associated
Ethernet2/2/2	Physical	Interface is associated
Ethernet2/2/3	Physical	Interface is associated

d) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Replacing the parent interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

e) Click **Close** to return to the **Interfaces** page.

f) Click **Save** to save the interface changes to the firewall.

g) If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the breakout port changes.

Step 3 Rejoin breakout ports.

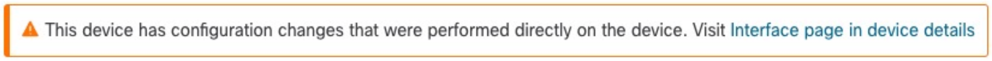
You must rejoin all child ports for the interface.

a) Click **Join** (↪) to the right of the interface.

Click **Yes** on the confirmation dialog box. If any child ports are in use, you will see an error message. You must resolve any use cases before you can retry the rejoin.

b) Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

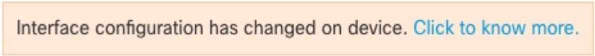
Figure 7: Go to Interface Page



⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

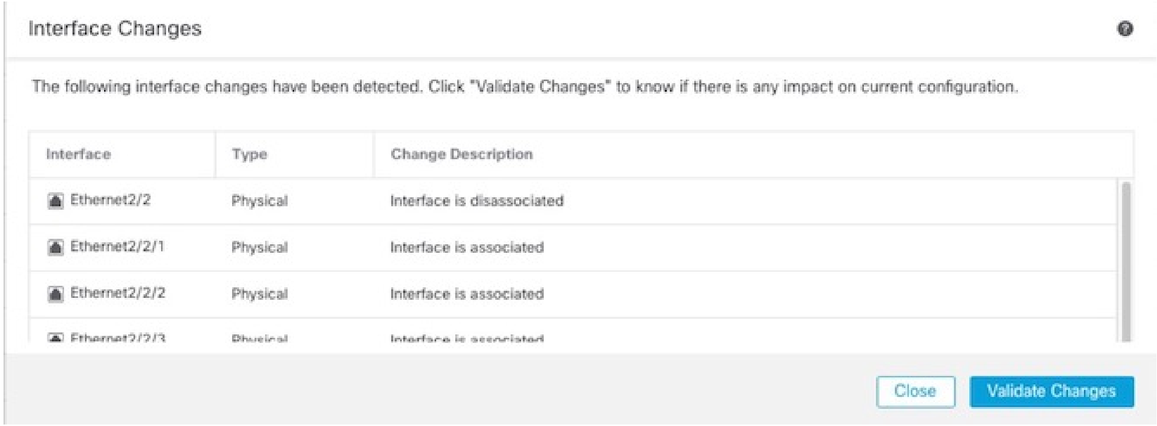
c) At the top of the **Interfaces** page, click **Click to know more**. The **Interface Changes** dialog box opens.

Figure 8: View Interface Changes



Interface configuration has changed on device. Click to know more.

Figure 9: Interface Changes



Interface Changes

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/2	Physical	Interface is disassociated
Ethernet2/2/1	Physical	Interface is associated
Ethernet2/2/2	Physical	Interface is associated
Ethernet2/2/3	Physical	Interface is associated

d) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Replacing the child interfaces that are used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

e) Click **Close** to return to the **Interfaces** page.

f) Click **Save** to save the interface changes to the firewall.

g) If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the breakout port changes.

Add a Network Module

To add a network module to a firewall after initial bootup, perform the following steps. Adding a new module requires a reboot.

Procedure

Step 1 Install the network module according to the hardware installation guide.

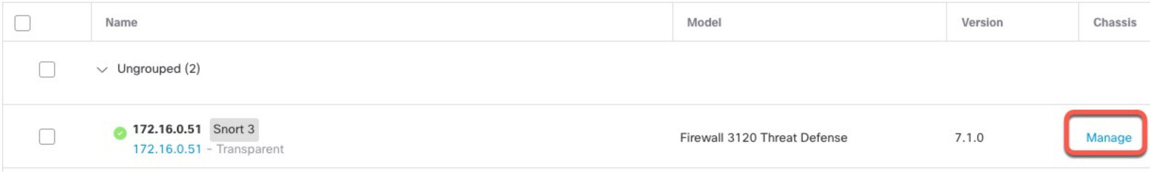
For clustering or High Availability, install the network module on all nodes.

Step 2 Reboot the firewall; see Shut Down or Restart the Device.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control nodeor active unit (see Switch the Active Peer in the Threat Defense High Availability Pair), and reboot the former control node/active unit.

Step 3 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 10: Manage Chassis



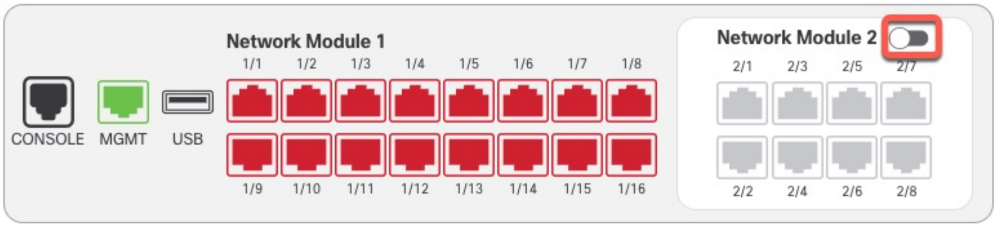
☐	Name	Model	Version	Chassis
☐	⌄ Ungrouped (2)			
☐	● 172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 4 Click **Sync Modules** to update the page with the new network module details.

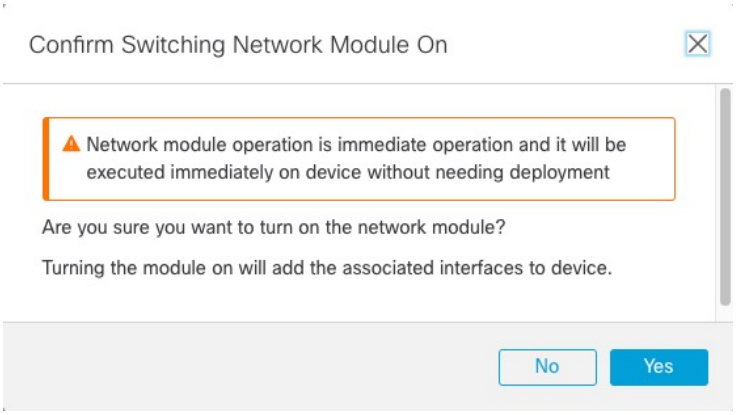
Step 5 On the interfaces graphic, click the slider ( ) to enable the network module.

Figure 11: Enable the Network Module



Step 6 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 12: Confirm Enable



Confirm Switching Network Module On

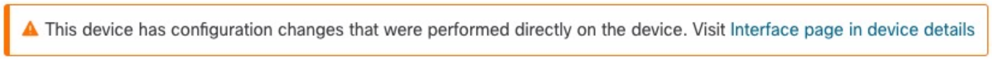
⚠ Network module operation is immediate operation and it will be executed immediately on device without needing deployment

Are you sure you want to turn on the network module?

Turning the module on will add the associated interfaces to device.

Step 7 You see a message at the top of the screen; click the link to go to the **Interfaces** page to save the interface changes.

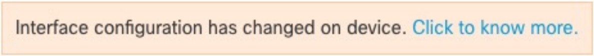
Figure 13: Go to Interface Page



⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

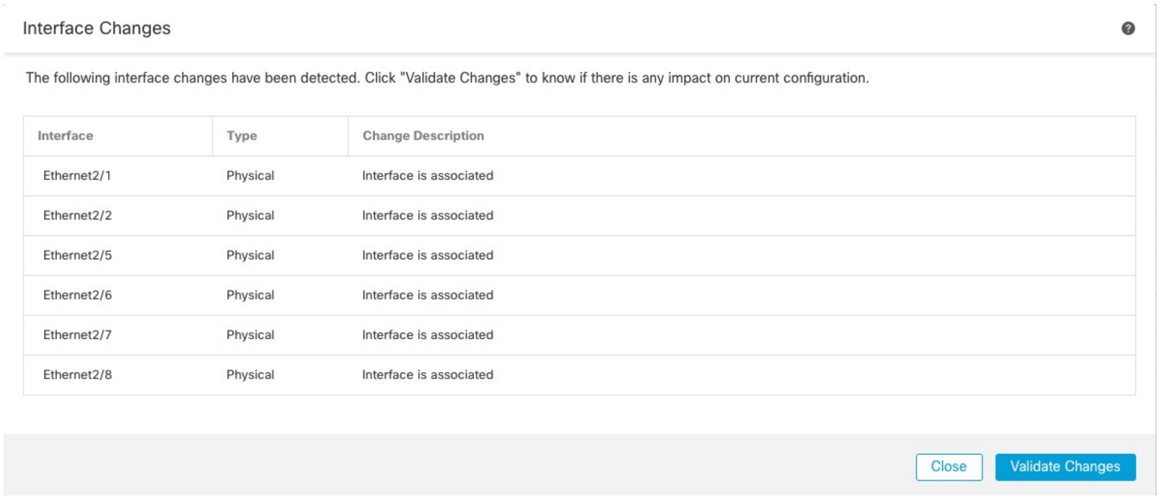
Step 8 (Optional) At the top of the **Interfaces** page, you see a message that the interface configuration has changed. You can click **Click to know more** to open the **Interface Changes** dialog box to view the changes.

Figure 14: View Interface Changes



Interface configuration has changed on device. Click to know more.

Figure 15: Interface Changes



Interface Changes

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/1	Physical	Interface is associated
Ethernet2/2	Physical	Interface is associated
Ethernet2/5	Physical	Interface is associated
Ethernet2/6	Physical	Interface is associated
Ethernet2/7	Physical	Interface is associated
Ethernet2/8	Physical	Interface is associated

Click **Close** to return to the **Interfaces** page. (Because you are adding a new module, there shouldn't be any configuration impact, so you do not need to click **Validate Changes**.)

Step 9 Click **Save** to save the interface changes to the firewall.

Hot Swap the Network Module

You can hot swap a network module for a new module of the same type without having to reboot. However, you must shut down the current module to remove it safely. This procedure describes how to shut down the old module, install a new module, and enable it.

For clustering or High Availability, you can only perform chassis operations on the control node/active unit. You cannot disable a network module if the cluster control link/failover link is on the module.

Before you begin

Procedure

Step 1 For clustering or High Availability, perform the following steps.

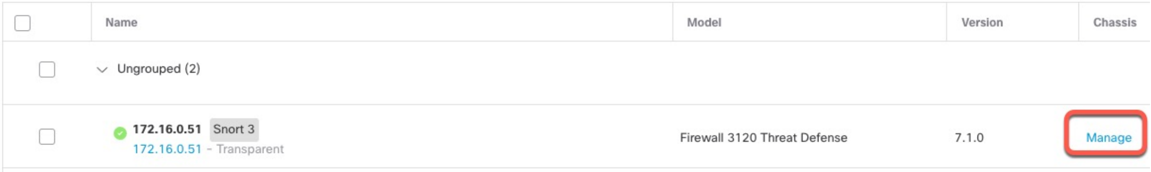
- **Clustering**—Ensure the unit you want to perform the hot swap on is a data node; then break the node so it is no longer in the cluster.

  You will add the node back to the cluster after you perform the hot swap. Alternatively, you can perform all operations on the control node, and the network module changes will sync to all data nodes. However, you will lose use of those interfaces on all nodes during the hot swap.

- **High Availability**—To avoid failing over when you disable the network module:
  - If the failover link is on the network module, you must break High Availability. See Break a High Availability Pair. Disabling the network module with an active failover link is not allowed.
  - Disable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Step 2 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 16: Manage Chassis

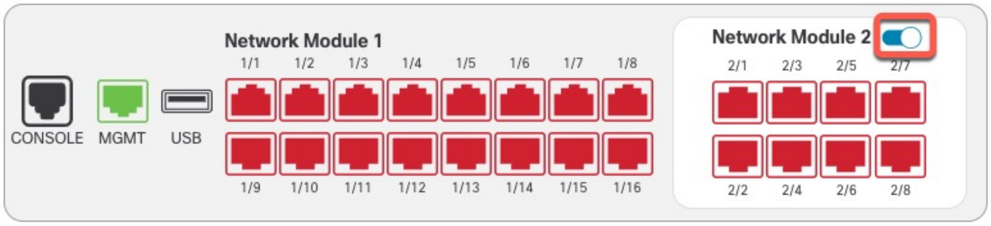


☐	Name	Model	Version	Chassis
☐	Ungrouped (2)			
☐	● 172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 3 On the interfaces graphic, click the slider (●) to disable the network module.

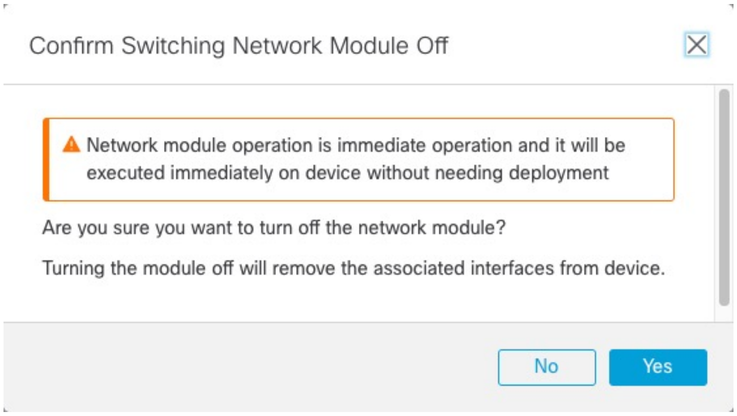
Figure 17: Disable the Network Module



Do not save any changes on the **Interfaces** page. Because you are replacing the network module, you do not want to disrupt any existing configuration.

Step 4 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 18: Confirm Disable



Confirm Switching Network Module Off

⚠ Network module operation is immediate operation and it will be executed immediately on device without needing deployment

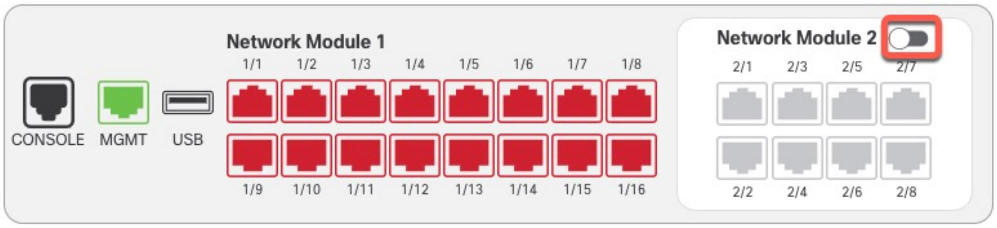
Are you sure you want to turn off the network module?

Turning the module off will remove the associated interfaces from device.

Step 5 On the device, remove the old network module and replace it with the new network module according to the hardware installation guide.

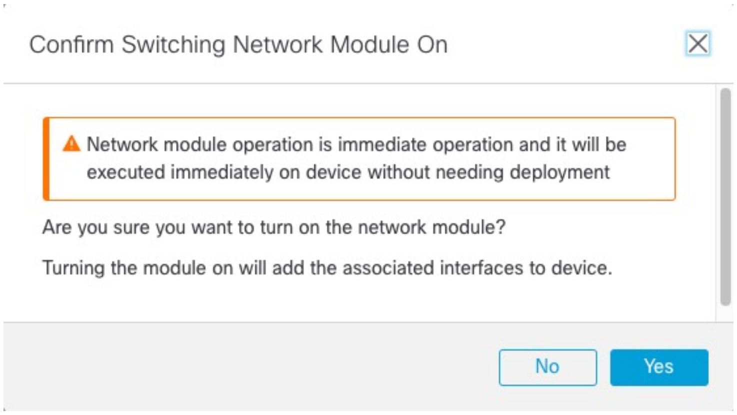
Step 6 In the management center, enable the new module by clicking the slider (○).

Figure 19: Enable the Network Module



Step 7 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 20: Confirm Enable



Confirm Switching Network Module On

⚠ Network module operation is immediate operation and it will be executed immediately on device without needing deployment

Are you sure you want to turn on the network module?

Turning the module on will add the associated interfaces to device.

Step 8 For clustering or High Availability, perform the following steps.

- **Clustering**—Add the node back to the cluster.
- **High Availability**—
  - If you broke High Availability, then reform High Availability. See Add a High Availability Pair.
  - Reenable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Replace the Network Module with a Different Type

If you replace a network module with a different type, then a reboot is required. If the new module has fewer interfaces than the old module, you will have to manually remove any configuration related to interfaces that will no longer be present.

For clustering or High Availability, you can only perform chassis operations on the control node/active unit.

Before you begin

For High Availability, you cannot disable a network module if the failover link is on the module. You will have to break High Availability (see Break a High Availability Pair), which means you will have downtime when you reboot the active unit. After the units finish rebooting, you can reform High Availability.

Procedure

Step 1 For clustering or High Availability, perform the following steps.

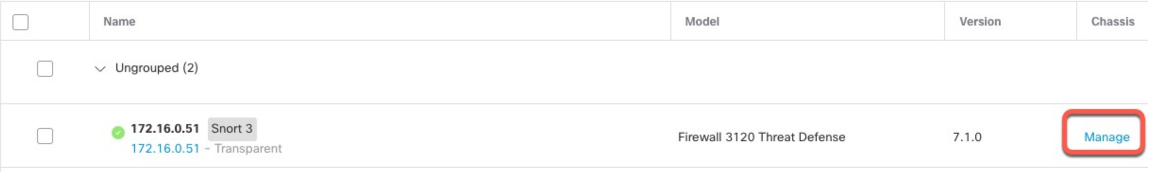
- **Clustering**—To avoid downtime, you can break each node one at a time so it is no longer in the cluster while you perform the network module replacement.

  You will add the node back to the cluster after you perform the replacement.

- **High Availability**—To avoid failing over when you replace the network module, disable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Step 2 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 21: Manage Chassis

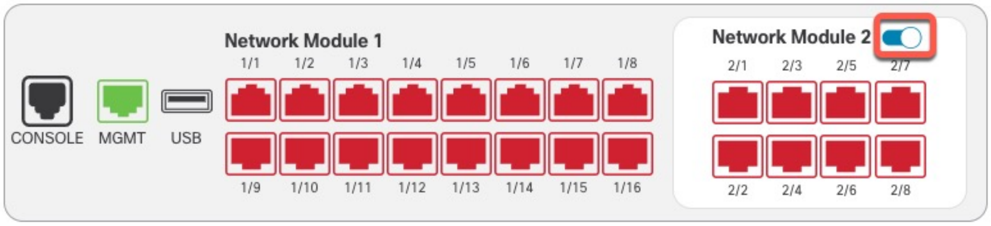


□	Name	Model	Version	Chassis
□	Ungrouped (2)			
□	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

Step 3 On the interfaces graphic, click the slider (●) to disable the network module.

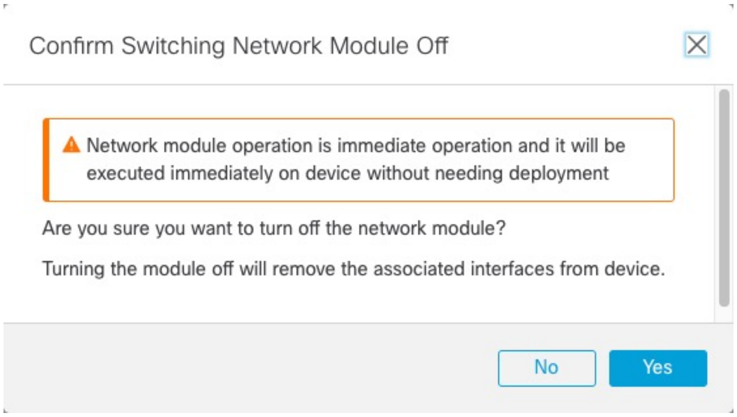
Figure 22: Disable the Network Module



Do not save any changes on the **Interfaces** page. Because you are replacing the network module, you do not want to disrupt any existing configuration.

Step 4 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 23: Confirm Disable



Confirm Switching Network Module Off

Network module operation is immediate operation and it will be executed immediately on device without needing deployment

Are you sure you want to turn off the network module?

Turning the module off will remove the associated interfaces from device.

Step 5 On the device, remove the old network module and replace it with the new network module according to the hardware installation guide.

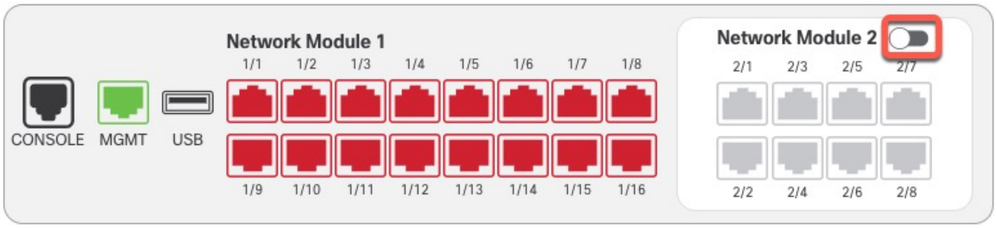
Step 6 Reboot the firewall; see Shut Down or Restart the Device.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control nodeor active unit (see Switch the Active Peer in the Threat Defense High Availability Pair), and reboot the former control node/active unit.

Step 7 In the management center, click **Sync Modules** to update the page with the new network module details.

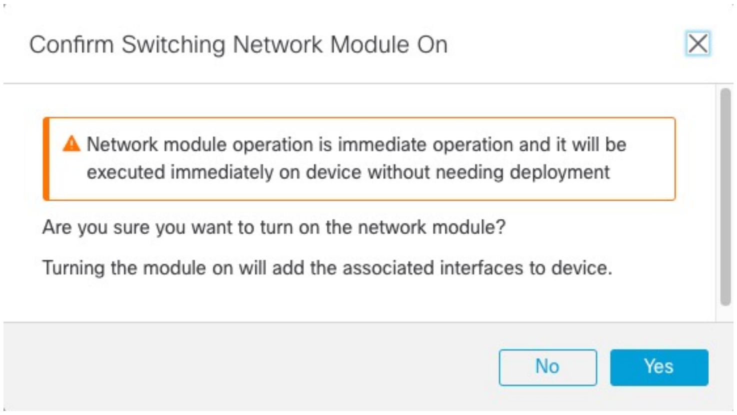
Step 8 Enable the new module by clicking the slider ().

Figure 24: Enable the Network Module



Step 9 You are prompted to confirm that you want to turn the network module on. Click **Yes**.

Figure 25: Confirm Enable



Confirm Switching Network Module On

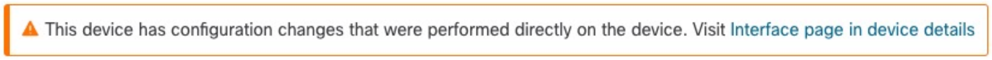
Network module operation is immediate operation and it will be executed immediately on device without needing deployment

Are you sure you want to turn on the network module?

Turning the module on will add the associated interfaces to device.

Step 10 Click the link in the message at the top of the screen to go to the **Interfaces** page to save the interface changes.

Figure 26: Go to Interface Page

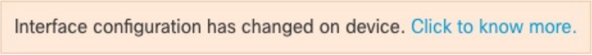


This device has configuration changes that were performed directly on the device. Visit Interface page in device details

Step 11 If the network module has *fewer* interfaces:

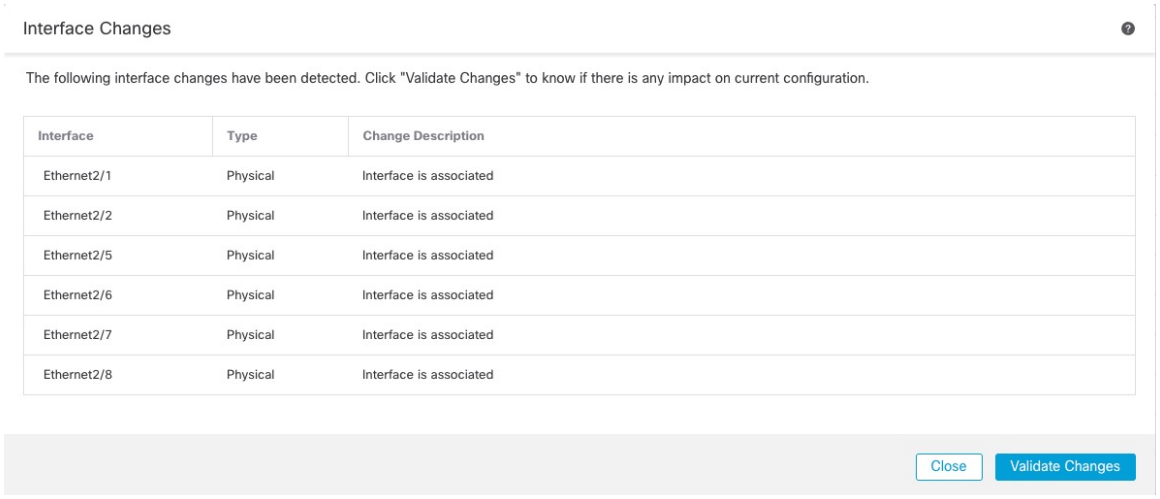
a) At the top of the **Interfaces** page, click **Click to know more**. The **Interface Changes** dialog box opens.

Figure 27: View Interface Changes



Interface configuration has changed on device. Click to know more.

Figure 28: Interface Changes



Interface Changes

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/1	Physical	Interface is associated
Ethernet2/2	Physical	Interface is associated
Ethernet2/5	Physical	Interface is associated
Ethernet2/6	Physical	Interface is associated
Ethernet2/7	Physical	Interface is associated
Ethernet2/8	Physical	Interface is associated

b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Deleting an interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

c) Click **Close** to return to the **Interfaces** page.

Step 12 To change the interface speed, see Enable the Physical Interface and Configure Ethernet Settings, on page 7.

The default speed is set to Detect SFP, which detects the correct speed from the SFP installed. You only need to fix the speed if you manually set the speed to a particular value and you now need a new speed.

Step 13 Click **Save** to save the interface changes to the firewall.

Step 14 If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

You do not need to deploy just to save the network module changes.

Step 15 For clustering or High Availability, perform the following steps.

- **Clustering**—Add the node back to the cluster.
- **High Availability**—Reenable interface monitoring for interfaces on the network module. See Configure Standby IP Addresses and Interface Monitoring.

Remove the Network Module

If you want to permanently remove the network module, follow these steps. Removing a network module requires a reboot.

For clustering or High Availability, you can only perform chassis operations on the control node/active unit.

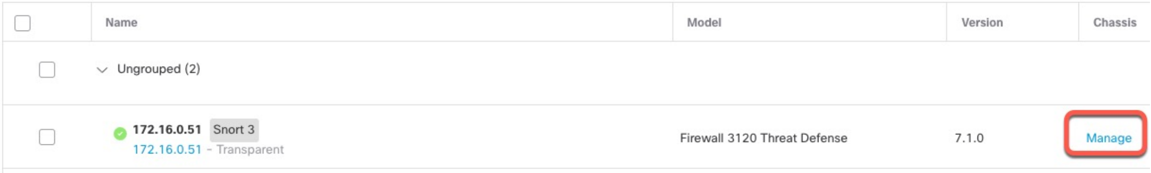
Before you begin

For clustering or High Availability, make sure the cluster/failover link is not on the network module.

Procedure

Step 1 From **Devices** > **Device Management**, click **Manage** in the **Chassis** column. For clustering or High Availability, this option is only available for the control node/active unit; network module changes are replicated to all nodes.

Figure 29: Manage Chassis

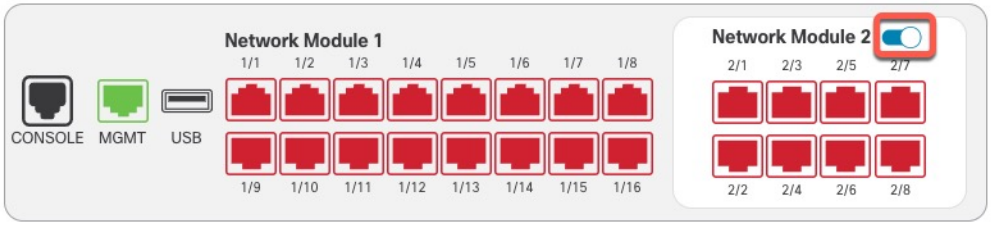


□	Name	Model	Version	Chassis
□	Ungrouped (2)			
□	172.16.0.51 Snort 3 172.16.0.51 - Transparent	Firewall 3120 Threat Defense	7.1.0	Manage

The **Chassis Operations** page opens for the device. This page shows physical interface details for the device.

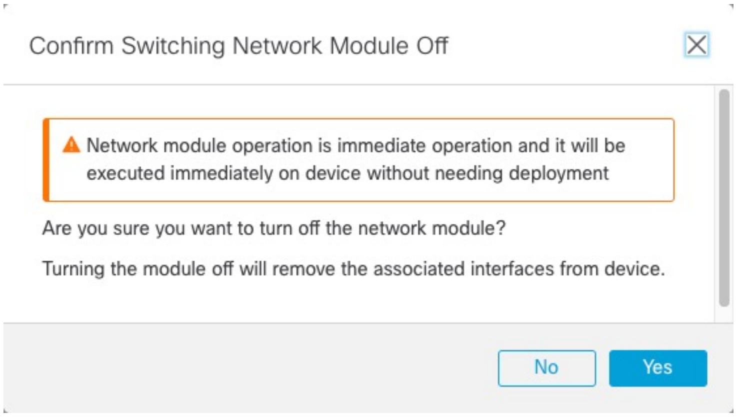
Step 2 On the interfaces graphic, click the slider (●) to disable the network module.

Figure 30: Disable the Network Module



Step 3 You are prompted to confirm that you want to turn the network module off. Click **Yes**.

Figure 31: Confirm Disable



Confirm Switching Network Module Off

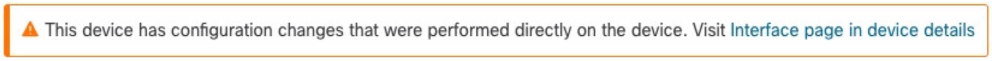
⚠ Network module operation is immediate operation and it will be executed immediately on device without needing deployment

Are you sure you want to turn off the network module?

Turning the module off will remove the associated interfaces from device.

Step 4 You see a message at the top of the screen; click the link to go to the **Interfaces** page to save the interface changes.

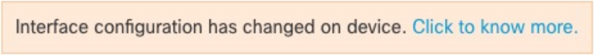
Figure 32: Go to Interface Page



⚠ This device has configuration changes that were performed directly on the device. Visit Interface page in device details

Step 5 At the top of the **Interfaces** page, you see a message that the interface configuration has changed.

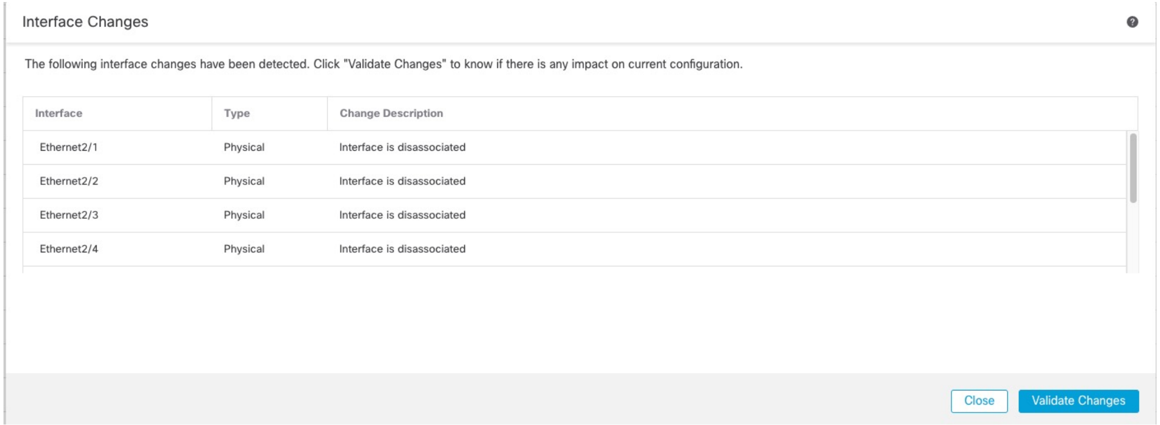
Figure 33: View Interface Changes



Interface configuration has changed on device. Click to know more.

a) Click **Click to know more** to open the **Interface Changes** dialog box to view the changes.

Figure 34: Interface Changes



Interface Changes

The following interface changes have been detected. Click "Validate Changes" to know if there is any impact on current configuration.

Interface	Type	Change Description
Ethernet2/1	Physical	Interface is disassociated
Ethernet2/2	Physical	Interface is disassociated
Ethernet2/3	Physical	Interface is disassociated
Ethernet2/4	Physical	Interface is disassociated

b) Click **Validate Changes** to make sure your policy will still work with the interface changes.

If there are any errors, you need to change your policy and rerun the validation.

Deleting an interface that is used in your security policy can impact the configuration. Interfaces can be referenced directly in many places in the configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Deleting an interface will delete any configuration associated with that interface. Policies that refer to security zones are not affected.

c) Click **Close** to return to the **Interfaces** page.

Step 6 Click **Save** to save the interface changes to the firewall.

Step 7 If you had to change any configuration, go to **Deploy** > **Deployment** and deploy the policy.

Step 8 Reboot the firewall; see Shut Down or Restart the Device.

For clustering or High Availability, reboot the data nodes/standby unit first, and wait for them to come back up. Then you can change the control nodeor active unit (see Switch the Active Peer in the Threat Defense High Availability Pair), and reboot the former control node/active unit.