Configure Manager Access on FTD from Management to Data Interface

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Proceed with Interface Migration
- Enable SSH on Platform Settings

Verify

- Verify from FMC Graphical User Interface (GUI)
- Verify from FTD Command Line Interface (CLI)

Troubleshoot

- Management Connection Status
  - Working Scenario
  - Non-Working Scenario
- Validate the Network Information
- Validate the Manager State
- Validate Network Connectivity
  - Ping the Management Center
  - Check Interface Status, Statistics, and Packet Count
  - Validate Route on FTD to Reach FMC
  - Check Sftunnel and Connection Statistics

Related Information

Introduction

This document describes the process for modifying the Manager Access on the Firepower Threat Defense (FTD) from a Management to a Data interface.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)

Components Used

- Firepower Threat Defense Virtual 7.2.5
- Firepower Management Center Virtual 7.4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Each device includes a single dedicated Management interface for communicating with the FMC. You can optionally configure the device to use a data interface for management instead of the dedicated Management interface. The FMC access on a data interface is useful if you want to manage the Firepower Threat Defense remotely from the outside interface, or you do not have a separate management network. This change must be performed on the Firepower Management Center for FTD managed by FMC.

The FMC access from a data interface has a few limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you must include a router with PPPoE support between the Firepower Threat Defense and the WAN modem.
- You cannot use separate management and event only interfaces.

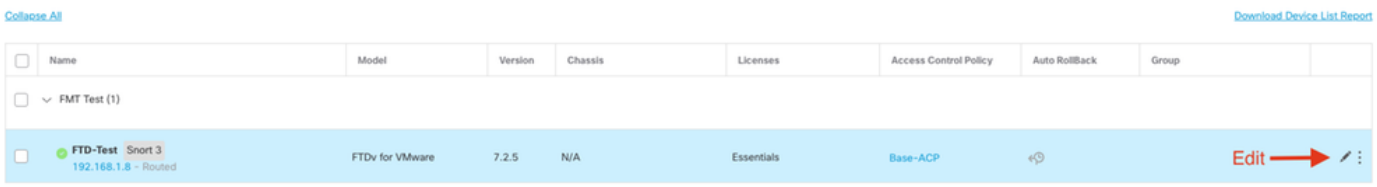
Configure

Proceed with Interface Migration

Note: It is strongly recommended to have the latest backup of both FTD and FMC before proceeding with any changes.

---

1. Navigate to **Devices > Device Management** page, click **Edit** for the device you are making changes.



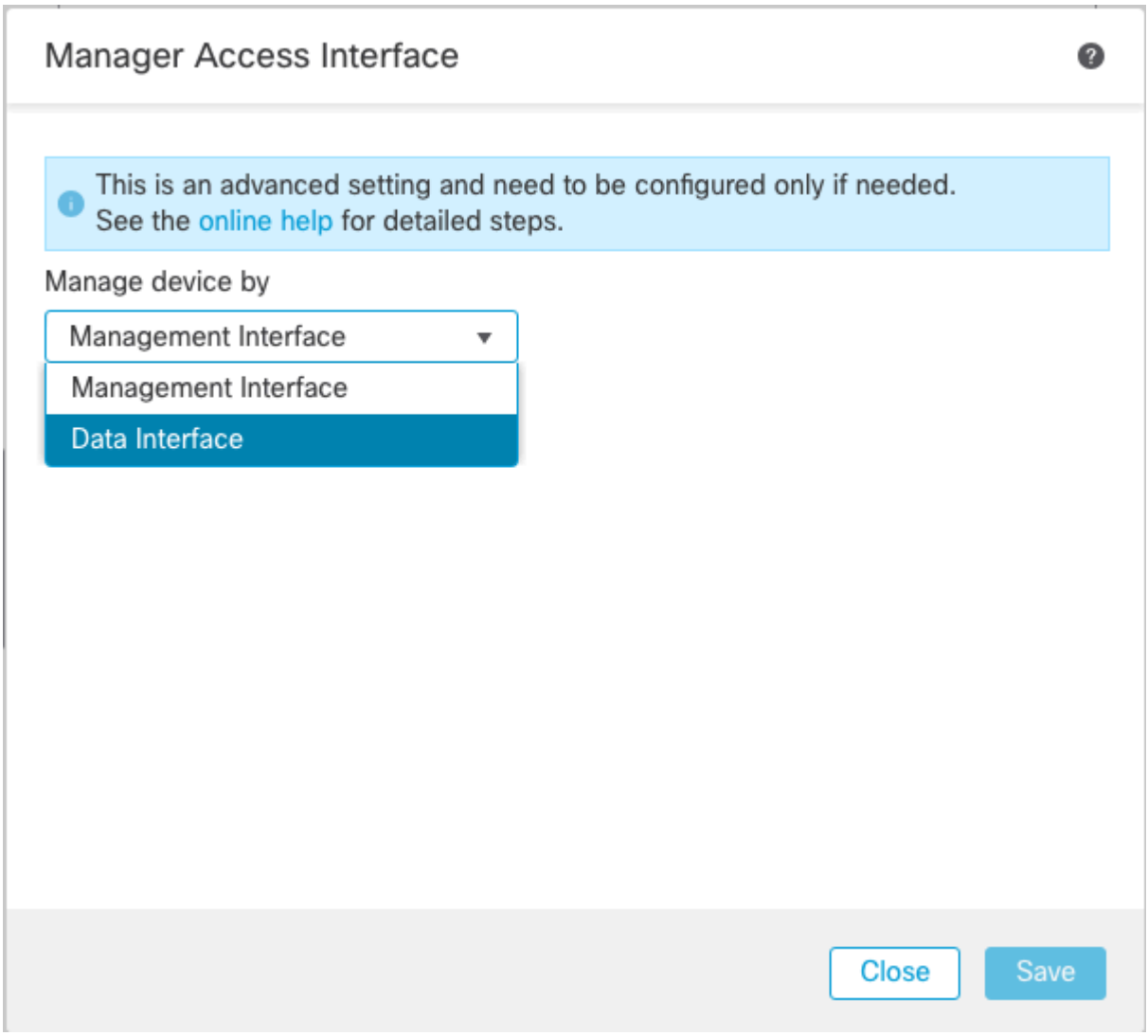
---

2. Go to the **Device > Management** section, and click the link for **Manager Access Interface**.



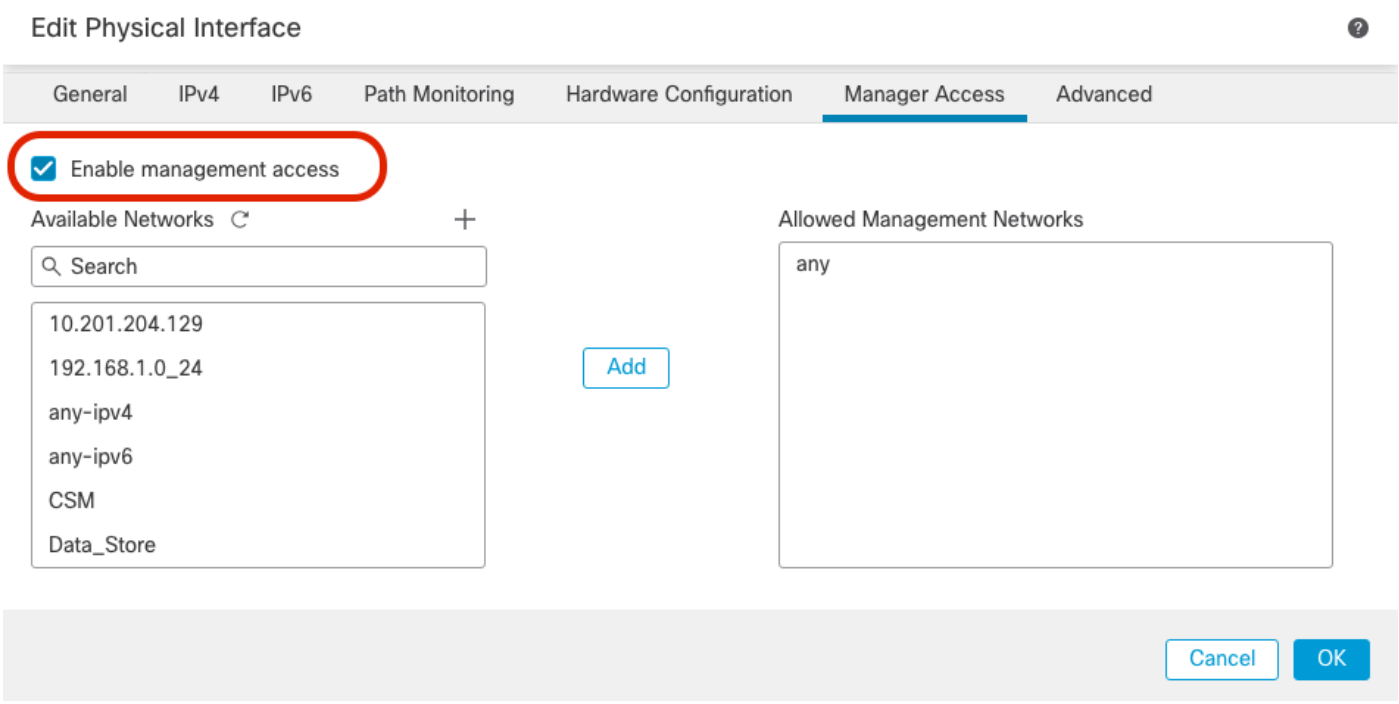
---

3. The Manager Access Interface field displays the existing Management interface. Click the **link** to select the new interface type, which is the **Data Interface** option in the **Manage device by** drop-down list and click **Save**.



---

4. You must now proceed to **Enable management access** on a data interface, navigate to **Devices > Device Management > Interfaces > Edit Physical Interface > Manager Access**.



Optional: If you use a secondary interface for redundancy, ensure you enable the management access on the interface used for redundancy purpose. If you use DHCP for the interface, enable the web type DDNS method on the **Devices > Device Management > DHCP > DDNS** dialog. You can Configure DNS in a Platform Settings policy, and apply it to this device under **Devices > Platform Settings > DNS**.

---

5. Ensure the threat defense can route to the management center through the data interface; add a static route if necessary on **Devices > Device Management > Routing > Static Route**.

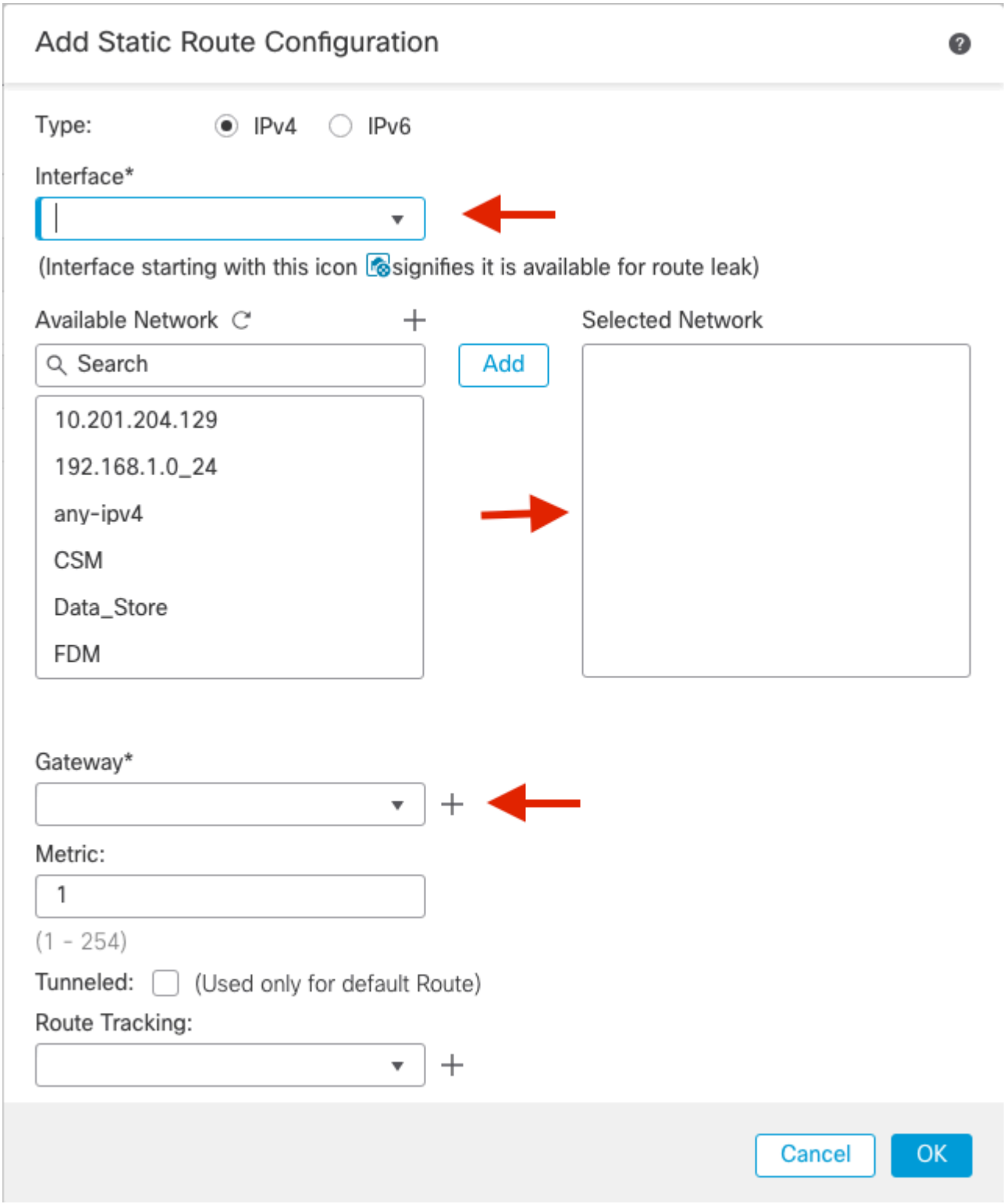
a. Click **IPv4** or **IPv6** depending on the type of static route you are adding.

b. Choose the **Interface** where this static route applies.

c. In the **Available Network list**, choose the **destination network**.

d. In the **Gateway or IPv6 Gateway field**, enter or choose the **gateway router** which is the next hop for this route.

Optional: To monitor route availability, enter or choose the name of a **Service Level Agreement (SLA)** Monitor object that defines the monitoring policy in the Route Tracking field.



---

6. **Deploy** the configuration changes, as these updates are now deployed over the current Management interface.

---

7. At the FTD CLI, set the Management interface to use a static IP address and the gateway to be data-interfaces.

a. configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

---

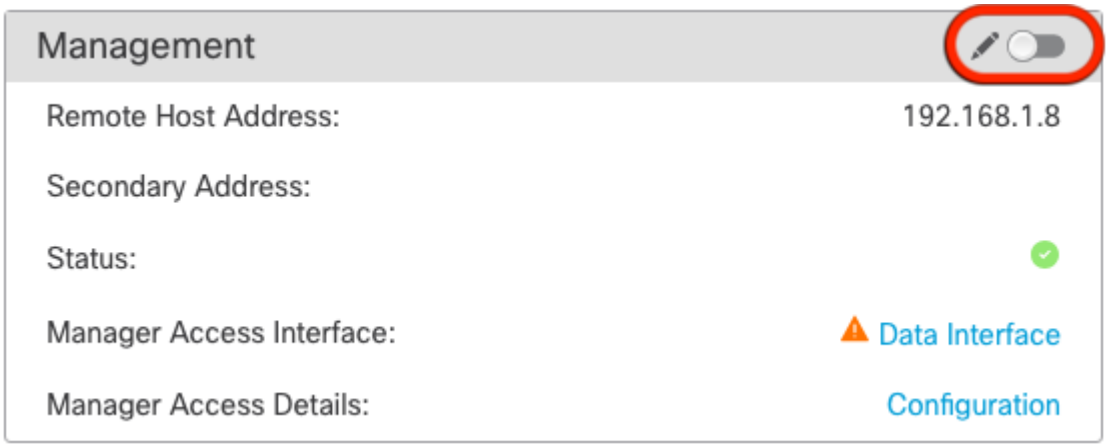
```
>
>
> configure network ipv4 manual 192.168.1.8 255.255.255.0 data-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```

IP_ADDRESS NETMASK GATEWAY

Note: Although you do not plan to use the Management interface, you must set a static IP address. For example, a private address so you can set the gateway to data-interfaces. This management is used to forward the management traffic to data interface using tap_nlp interface.

---

8. Disable the **Management** in the **Management Center**. Click **Edit** and update the **Remote Host Address IP** address and **(Optional) Secondary Address** for the threat defense in the **Devices > Device Management > Device > Management** section, and enable the **Connection**.



Enable SSH on Platform Settings

1. Enable **SSH** for the data interface in the **Platform Settings Policy** and apply it to the device at **Devices > Platform Settings > SSH Access**.

---

2. Click **Add**.

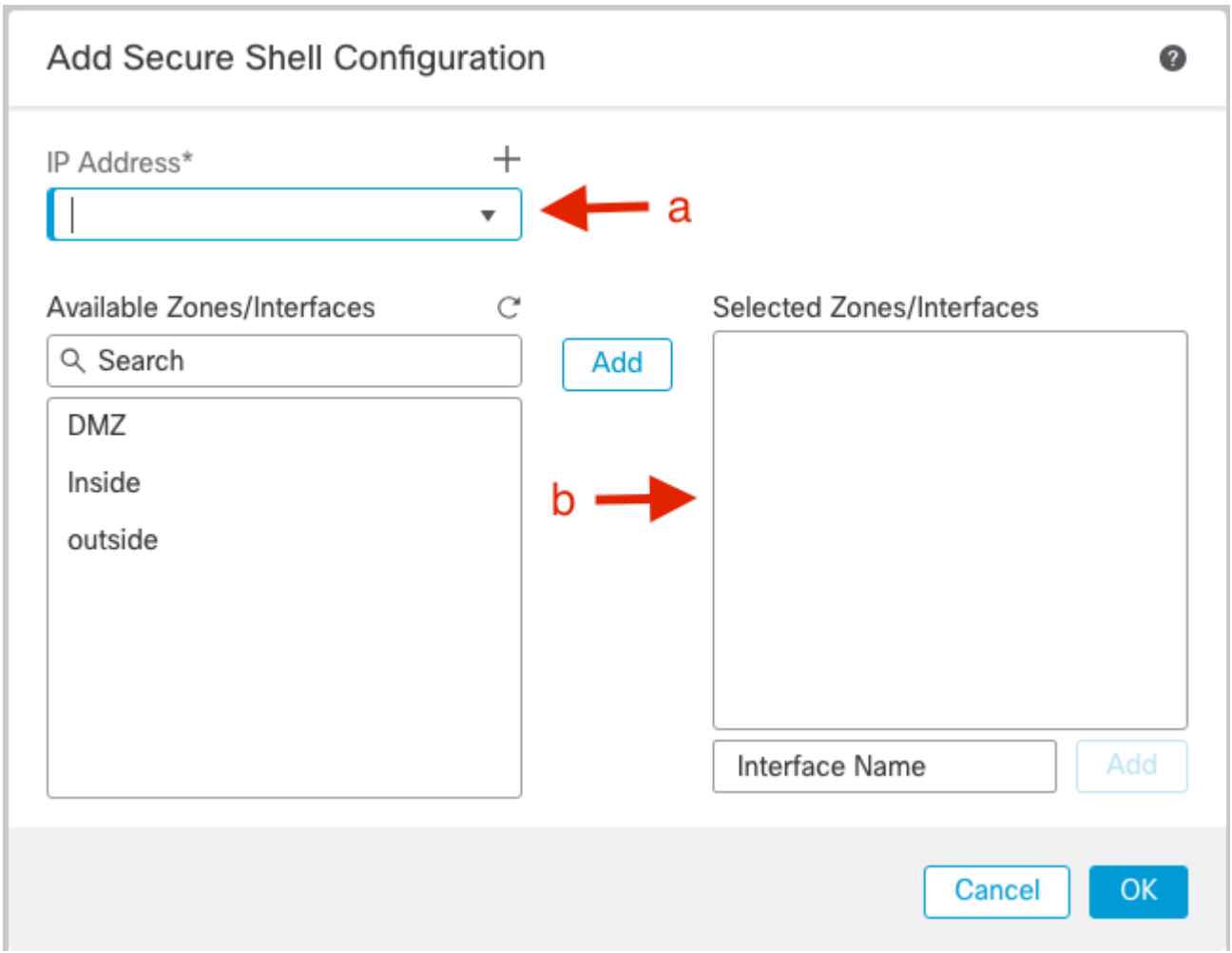
---

3. The hosts or networks you are allowing to make SSH connections. Add the zones that contain the

interfaces to allow SSH connections. For interfaces not in a zone, you can type the **interface name** into the field **Selected Zones/Interfaces** list and click **Add**.

---

4. Click **OK**. **Deploy** the changes.



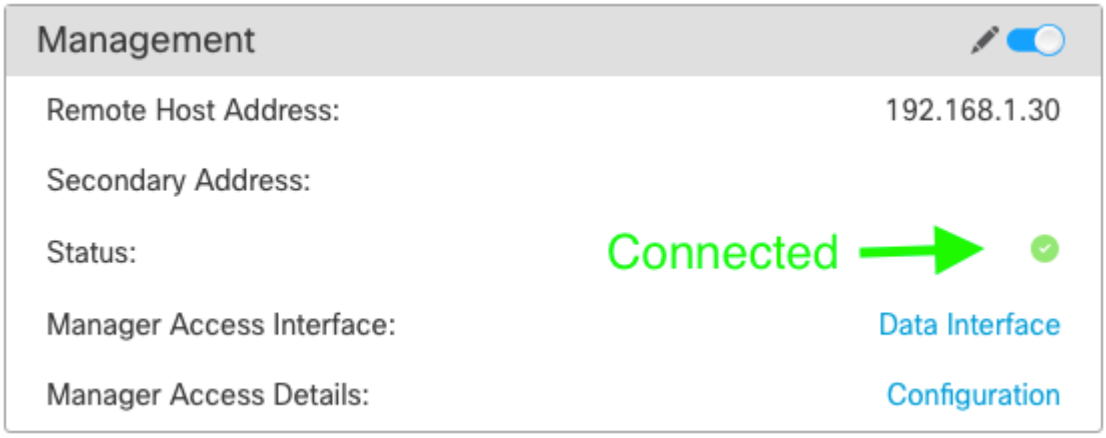
Note: SSH is not enabled by default on the data interfaces, so if you want to manage the threat defense using SSH, you need to explicitly allow it.

Verify

Ensure the management connection is established over the data interface.

Verify from FMC Graphical User Interface (GUI)

In the Management Center, check the management connection status on **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.



Verify from FTD Command Line Interface (CLI)

At the threat defense CLI, run the **sftunnel-status-brief** command to view the management connection status.

```
>
> sftunnel-status-brief

PEER:192.168.1.2
        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Registration: Completed.
        IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC
        Heartbeat Send Time:     Tue Jul 16 22:39:52 2024 UTC
        Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC
        Last disconnect time   : Tue Jul 16 22:17:42 2024 UTC
        Last disconnect reason : Both control and event channel connections with peer went down
```

The status shows a successful connection for a data interface, showing the internal tap_nlp interface.

Troubleshoot

In the Management Center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the threat defense CLI, run the **sftunnel-status-brief** command to view the management connection status. You can also run **sftunnel-status** to view more complete information.

Management Connection Status

Working Scenario

```
> sftunnel-status-brief

PEER:192.168.1.2
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
        Registration: Completed.
        IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC
        Heartbeat Send Time:     Wed Jul 17 17:15:20 2024 UTC
        Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC
        Last disconnect time   : Wed Jul 17 06:21:12 2024 UTC
        Last disconnect reason : Process shutdown due to stop request from PM
```

Non-Working Scenario

```
> sftunnel-status-brief

PEER:192.168.1.2
        Registration: Completed.
        Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC
        Last disconnect time   : Wed Jul 17 17:20:26 2024 UTC
        Last disconnect reason : Both control and event channel connections with peer went down
```

Validate the Network Information

At the threat defense CLI, view the Management and Manager access data interface network settings:

> show network

```
> show network
==============[ System Information ]==============
Hostname                  : ftdcdo.breakstuff.com
Domains                   : breakstuff.com
DNS Servers               : 192.168.1.103
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ eth0 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:0C:29:54:D4:47
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.168.1.8
Netmask                   : 255.255.255.0
Gateway                   : 192.168.1.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

==============[ Proxy Information ]===============
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet0/0

==============[ GigabitEthernet0/0 ]==============
State                     : Enabled
Link                      : Up
Name                      : Outside
MTU                       : 1500
MAC Address               : 00:0C:29:54:D4:5B
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.168.1.30
Netmask                   : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

Validate the Manager State

At the threat defense CLI, validate that the management center registration was completed.

> show managers

```
> show managers
Type                      : Manager
Host                      : 192.168.1.2
Display name              : 192.168.1.2
Identifier                : d4cd32d6-da7f-11ee-840e-b88231b3fd47
Registration              : Completed
Management type           : Configuration and analytics
```

Note: This command does not show the current status of the management connection.

Validate Network Connectivity

Ping the Management Center

At the threat defense CLI, run the command to ping the management center from the data interfaces:

> ping fmc_ip

```
> ping 192.168.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

At the threat defense CLI, run the command to ping the management center from the Management Interface, which routes over the backplane to the data interfaces:

> ping system fmc_ip

```
> ping system 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.282 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 132ms
rtt min/avg/max/mdev = 0.282/0.311/0.340/0.030 ms
```

Check Interface Status, Statistics, and Packet Count

At the threat defense CLI, review the information on the internal backplane interface, nlp_int_tap:

> **show interface detail**

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0000.0100.0001, MTU 1500
        IP address 169.254.1.1, subnet mask 255.255.255.248
        311553 packets input, 41414494 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        232599 packets output, 165049822 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
        311553 packets input, 37052752 bytes
        232599 packets output, 161793436 bytes
        167463 packets dropped
      1 minute input rate 0 pkts/sec,  3 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  3 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 14
        Interface config status is active
        Interface state is active
```

Validate Route on FTD to Reach FMC

At the threat defense CLI, check that the default route (S*) was added and the internal NAT rules exist for the Management Interface (nlp_int_tap).

> show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        192.168.1.0 255.255.255.0 is directly connected, Outside
L        192.168.1.30 255.255.255.255 is directly connected, Outside
```

> show nat

```
> show nat
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface  destination static 0_0.0.0.0_5 0_0.0.0.0_5 service tcp 8305 8305
    translate_hits = 5, untranslate_hits = 6
2 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_::_intf3 interface ipv6  destination static 0_::_6 0_::_6 service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
3 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 10, untranslate_hits = 0
4 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
```

Check Sftunnel and Connection Statistics

> show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface Outside
sftunnel port 8305
```

Warning: Throughout the process of changing manager access, refrain from deleting the manager on the FTD or unregistering/force deleting the FTD from FMC.

Related Information

- Configure DNS over Platform Settings
- Configure Management Access to FTD (HTTPS and SSH) via FMC