Configure Manager Access on FTD from Management to Data Interface

Contents

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
- Firepower Management Center

Components Used

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

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

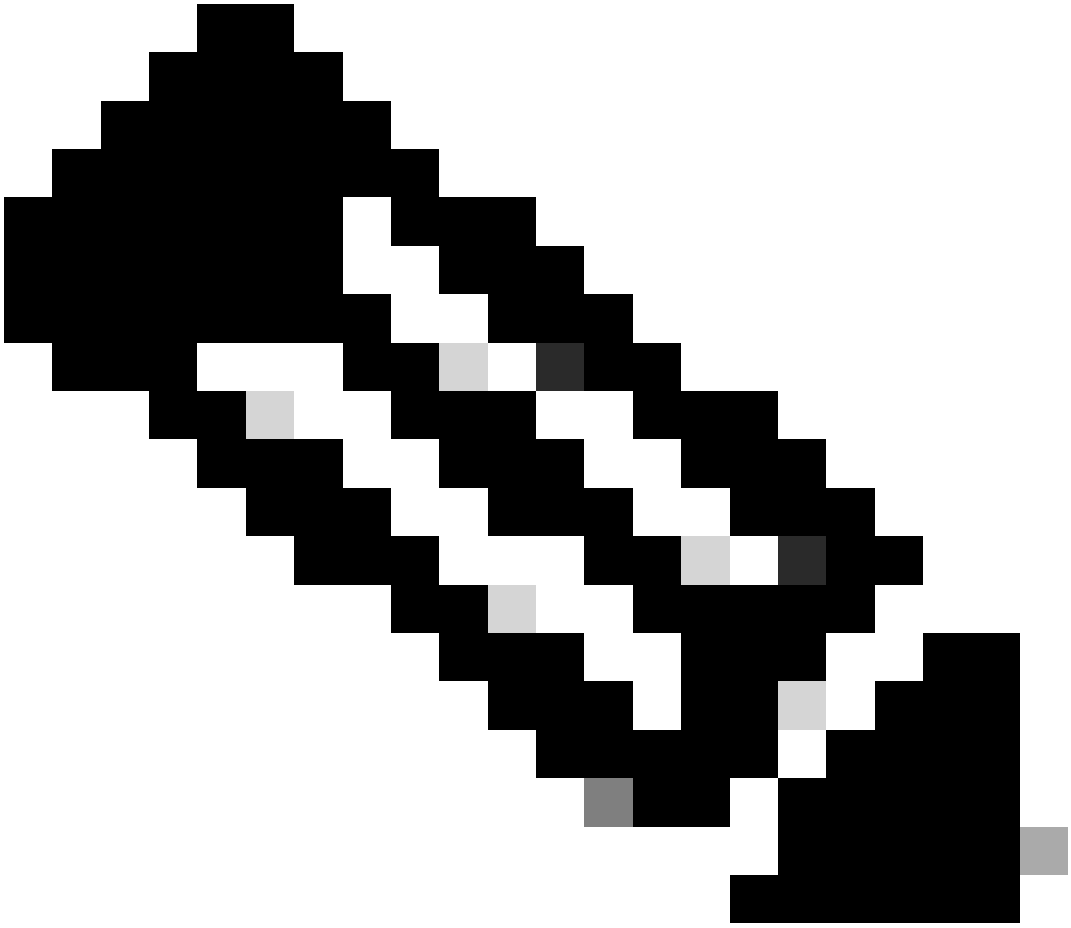
Each device includes a single dedicated Management interface for communicating with the FMC. You can optionally configure the device to use a data interface for management instead of the dedicated Management interface, The FMC access on a data interface is useful if you want to manage the Firepower Threat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

The FMC access from a data interface has the 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 have to put a router with PPPoE support between the Firepower Threat Defense and the WAN modem.
- You cannot use separate management and event only interfaces.

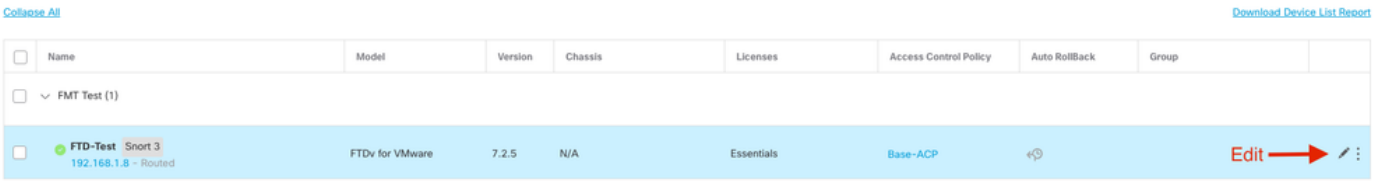
Configure

Proceed with Interface Migration



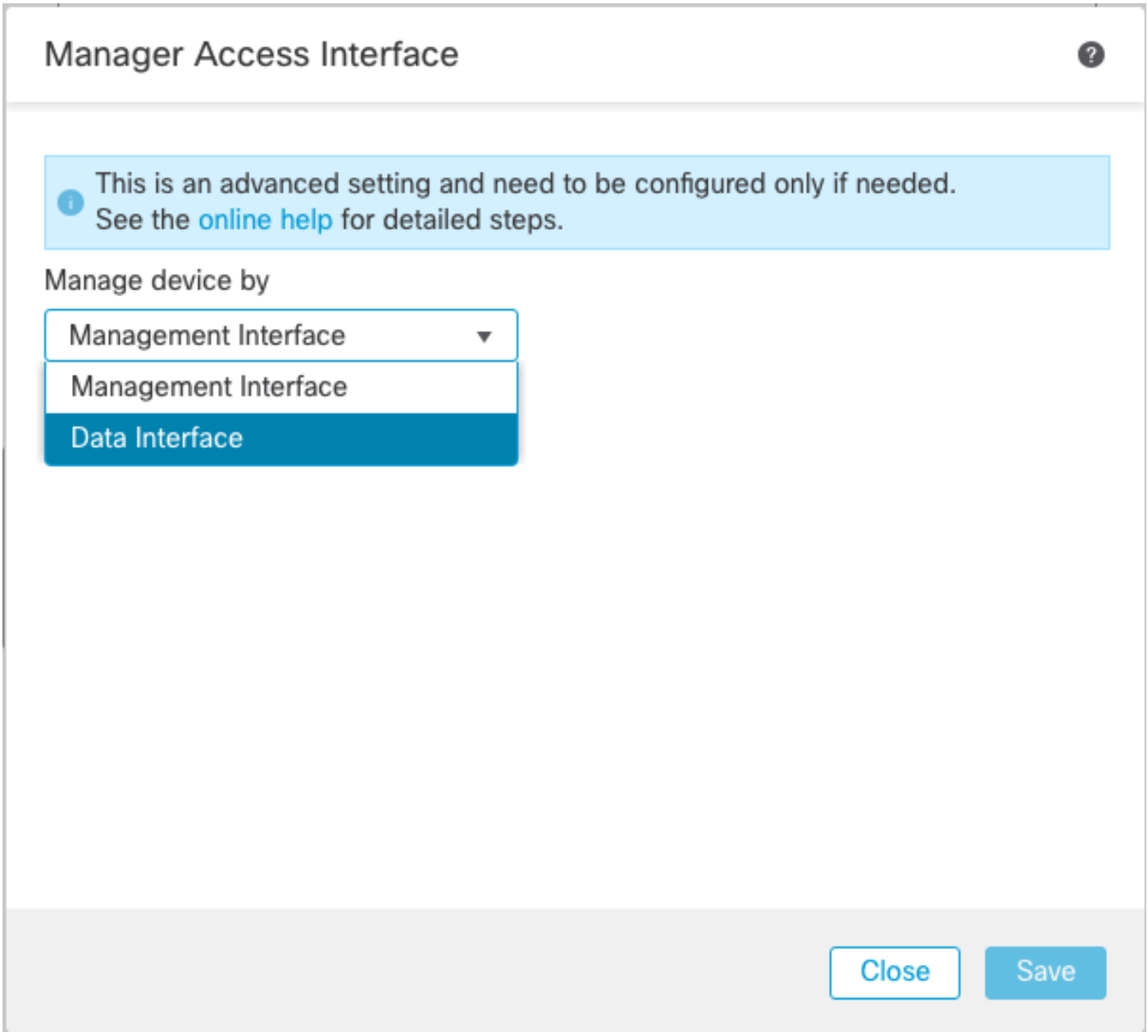
Note: It is strongly recommended to have the latest backup of both FTD and FMC before proceeding with any changes.

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

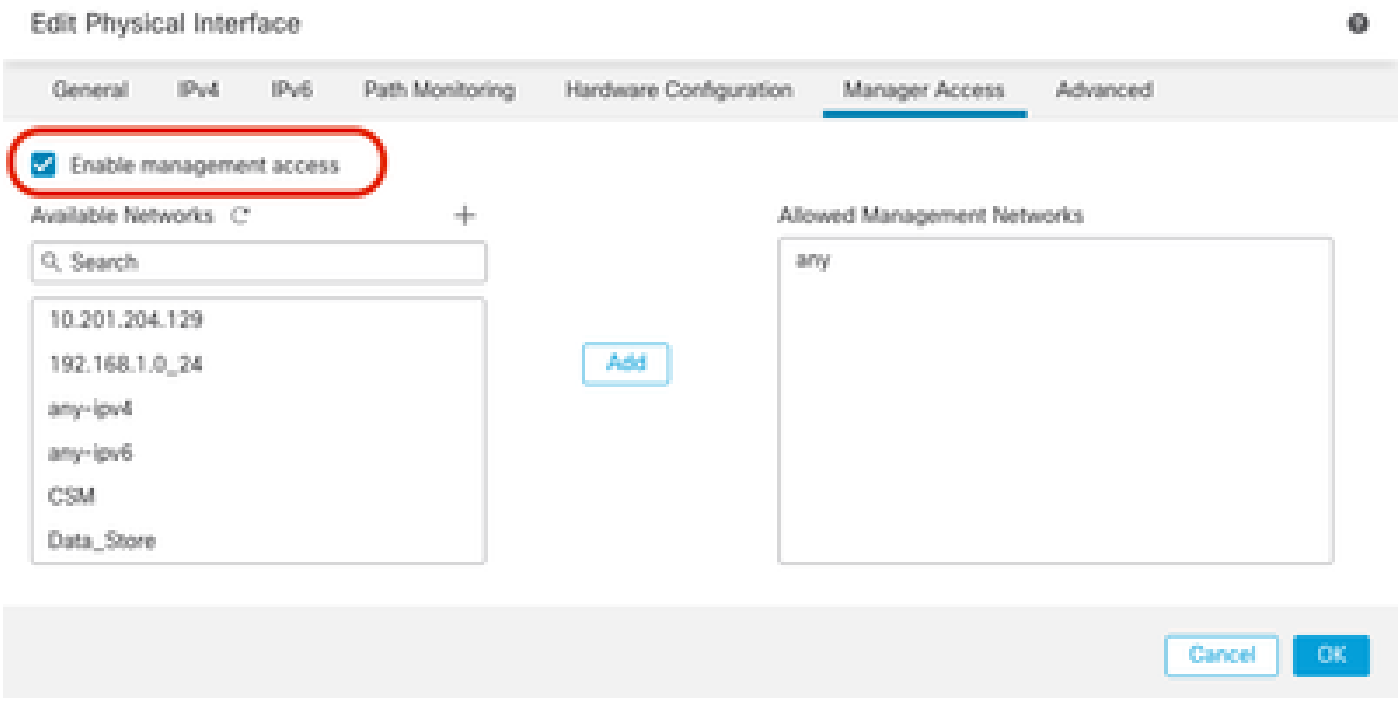


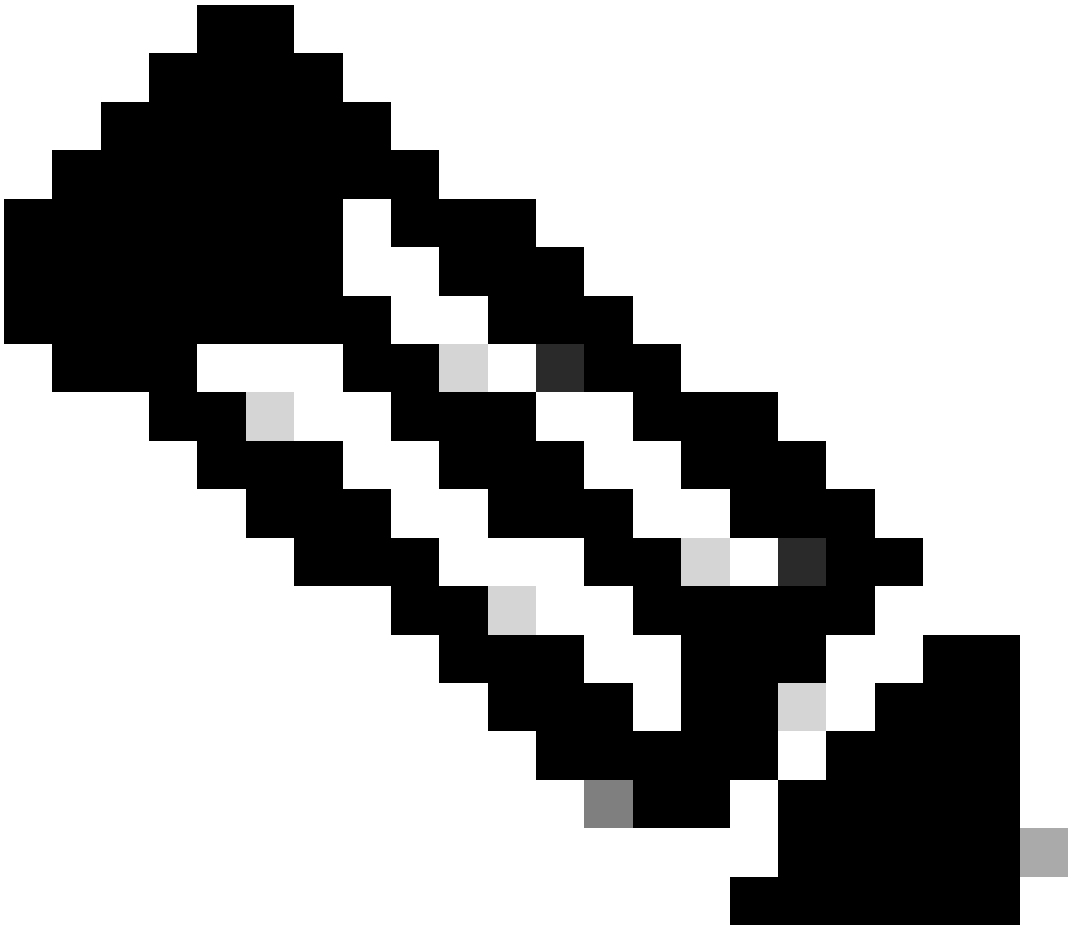
2. Go to the **Device > Management** section, and click the link for **Manager Access Interface**.

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.**



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


Edit Physical Interface
General
IPv4
IPv6
Path Monitoring
Hardware Configuration
Manager Access
Advanced
Enable management access
Available Networks
Search
10.201.204.129
192.168.1.0_24
any-ipv4
any-ipv6
CSM
Data_Store
Add
Allowed Management Networks
any
Cancel
OK



Note: (Optional) If you use a secondary interface for redundancy, Enable management access on the interface used for redundancy purpose.

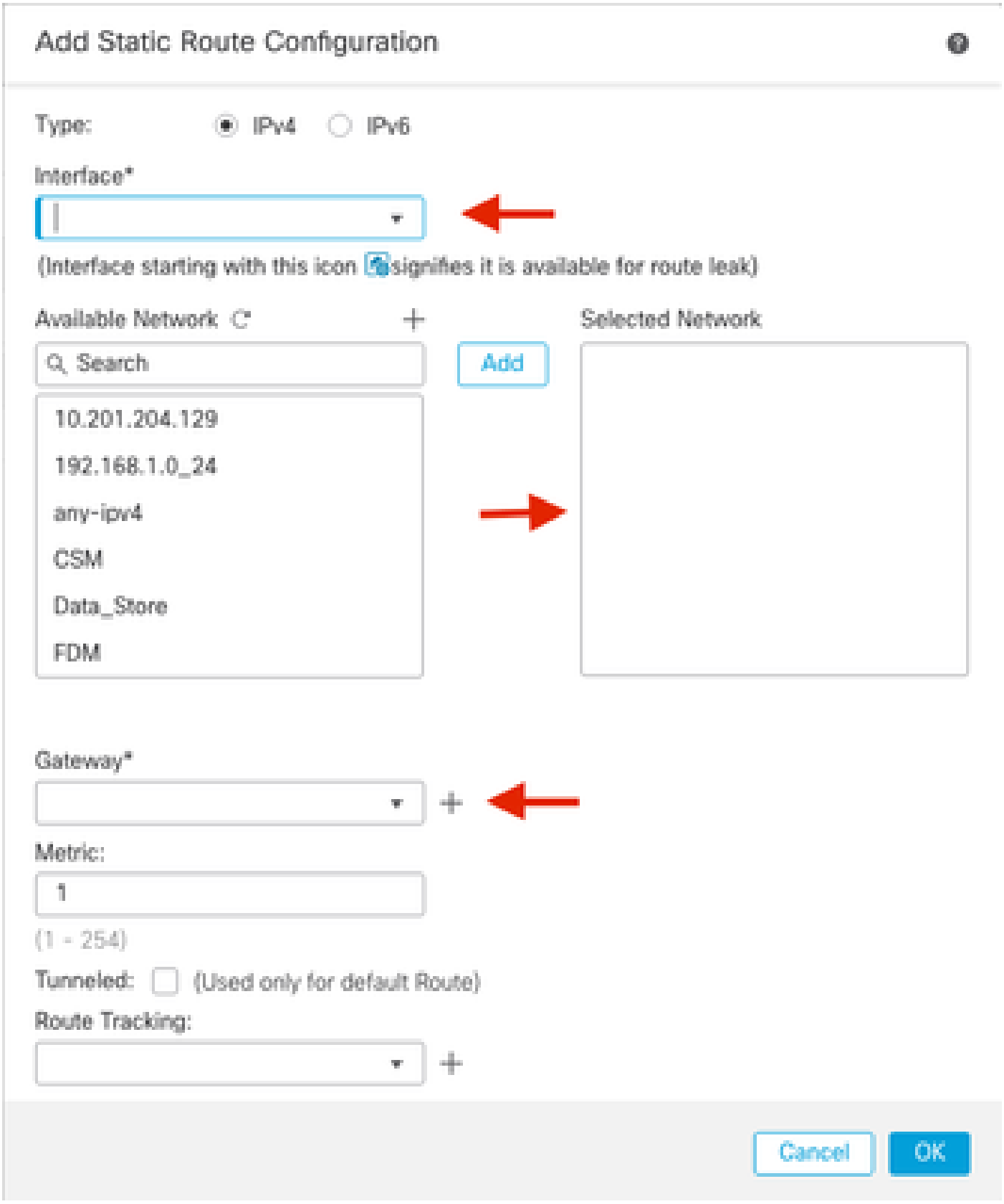
(Optional) If you use DHCP for the interface, enable the web type DDNS method on the **Devices > Device Management > DHCP > DDNS** dialog.

(Optional) Configure DNS in a Platform Settings policy, and apply it to this device at **Devices > Platform Settings > DNS**.

4. Make sure 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.**

1. Click **IPv4**or **IPv6** depending on the type of static route that you are adding.
2. Choose the **Interface** to which this static route applies.
3. In the **Available Network list**, choose the **destination network**.
4. 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 an **Service Level Agreement (SLA)** Monitor object that defines the monitoring policy, in the Route Tracking field.

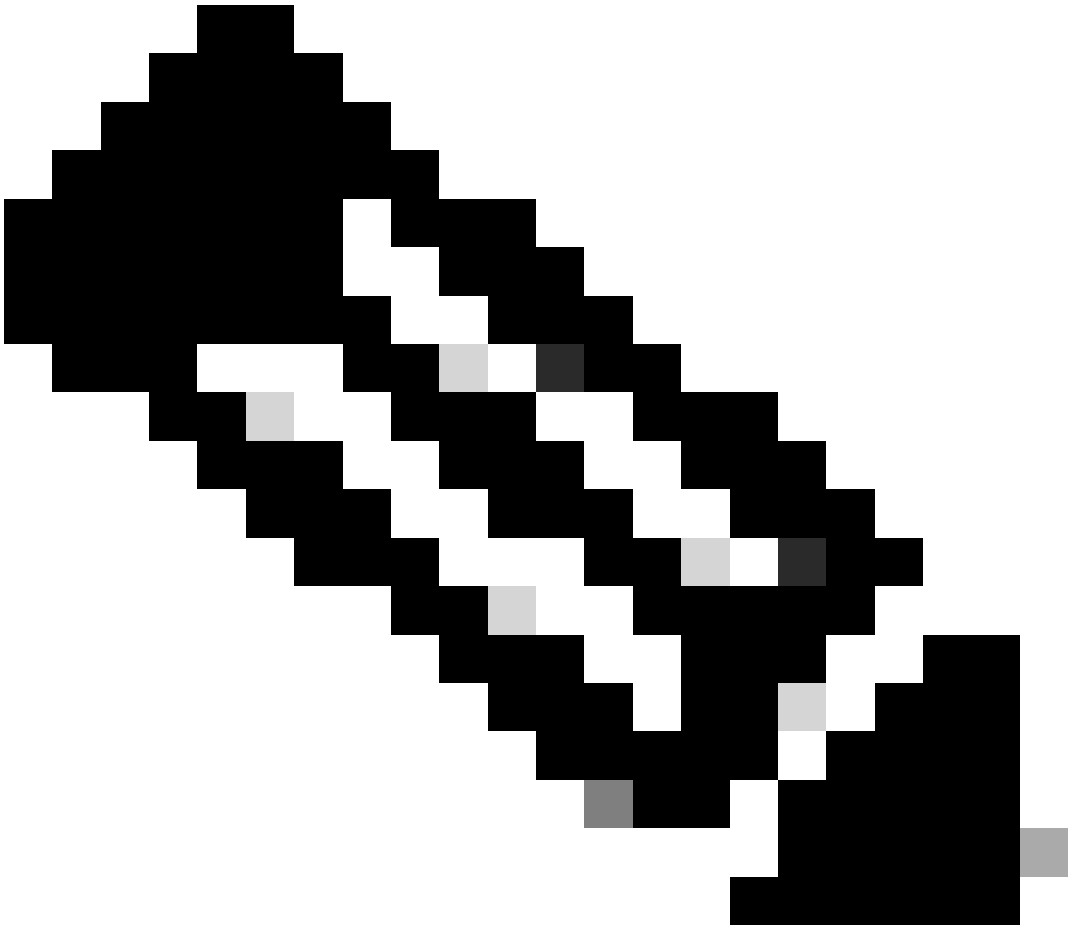


5. **Deploy** configuration changes. The configuration changes are now deployed over the current Management interface.

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

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

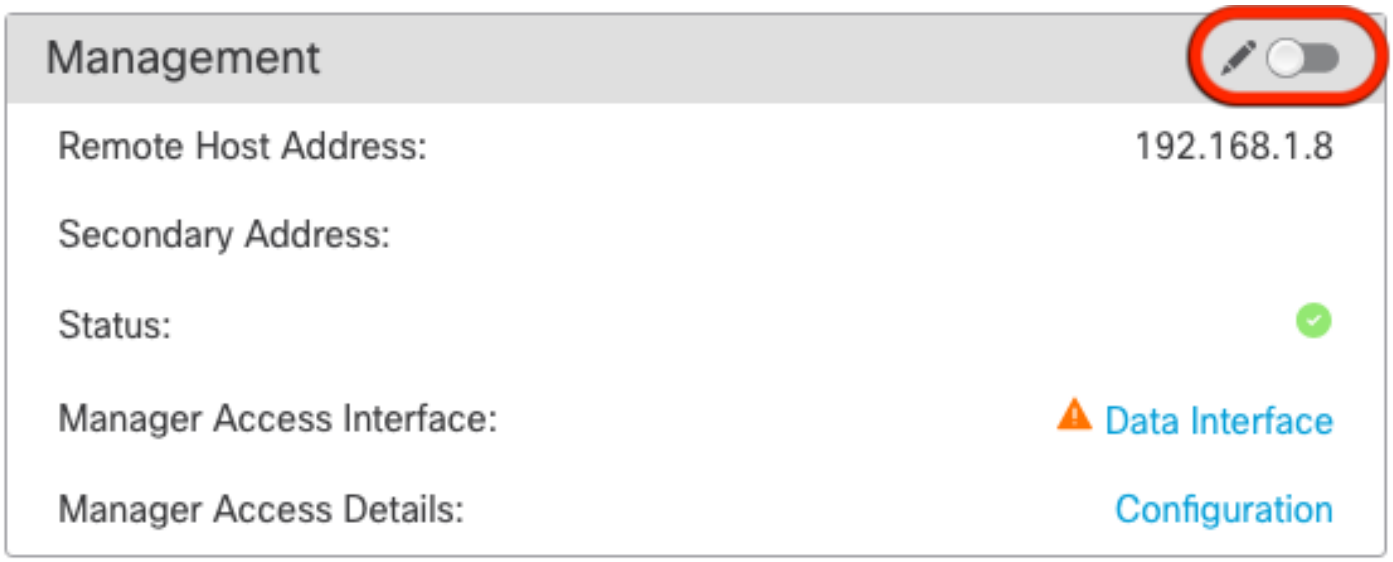
```
>
>                                    IP_ADDRESS      NETMASK         GATEWAY
> configure network ipv4 manual 192.168.1.8 255.255.255.0 data-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```



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

---

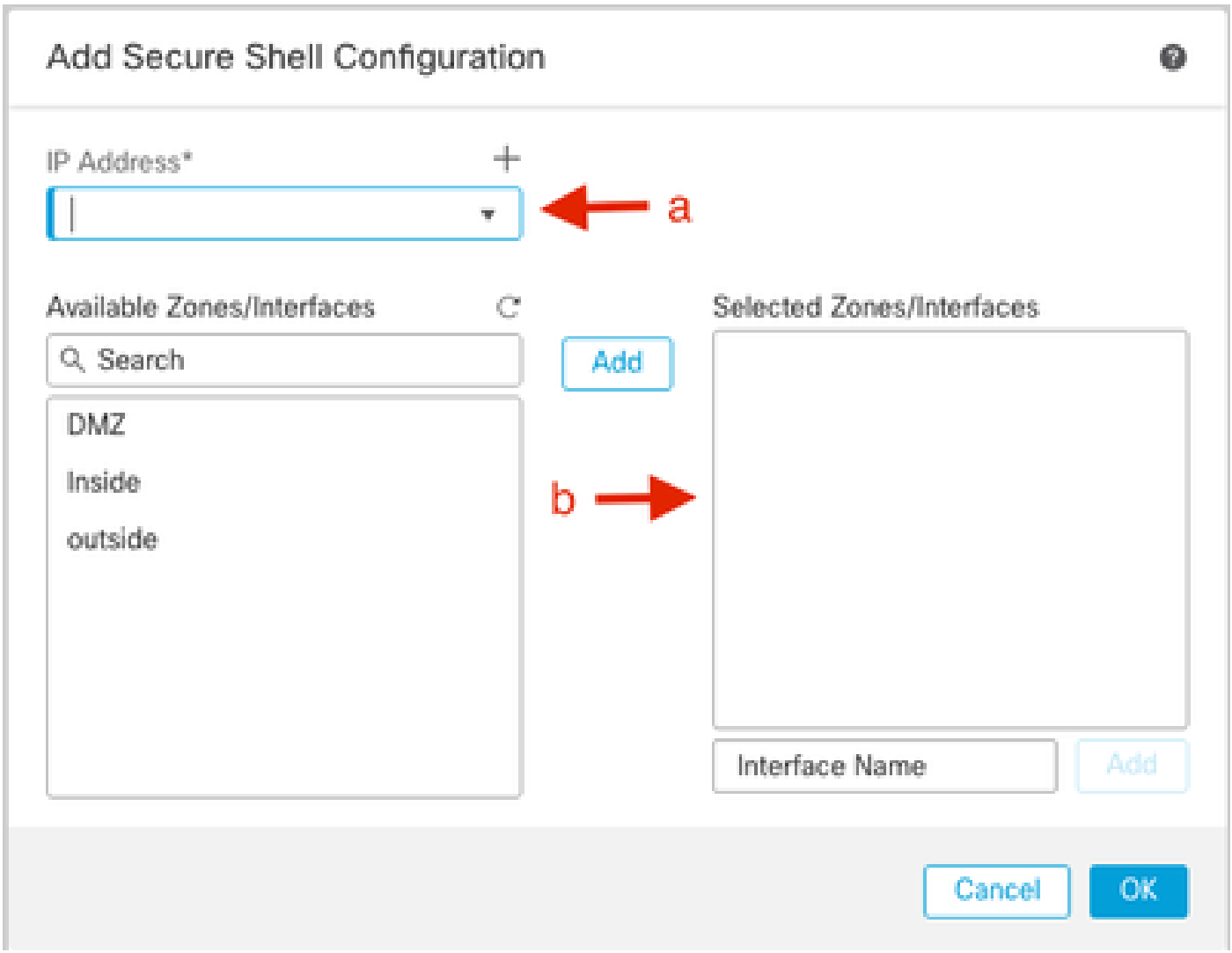
7. Disable the **Management** in the Management Center, Click **Edit** and update the **Remote Host Address IP** addressand **(Optional)Secondary Address** for the threat defense in the **Devices > Device Management > Device > Management** section, and enable the **connection**.

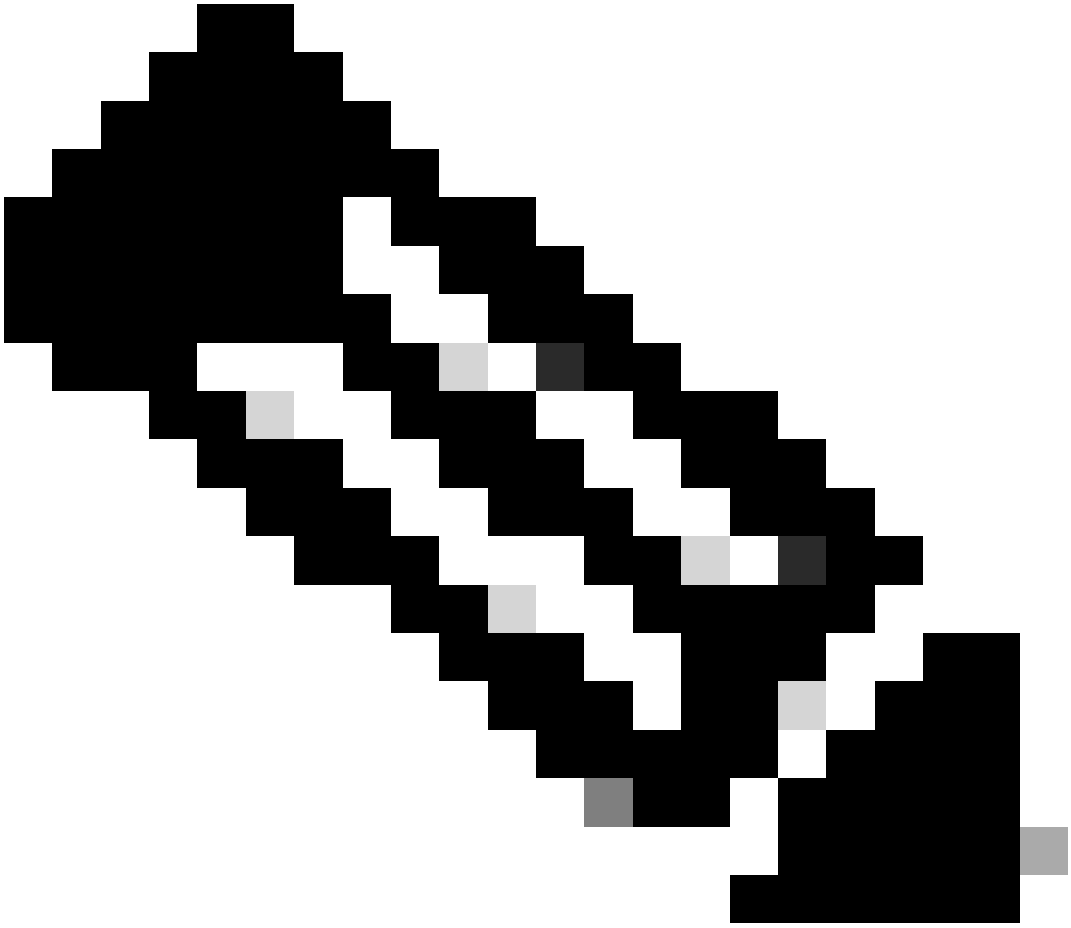


Enable SSH on Platform Settings

Enable **SSH** for the data interface in **Platform Settings policy**, and apply it to this device at **Devices > Platform Settings > SSH Access**.Click **Add .**

1. The hosts or networks you are allowing to make SSH connections.
2. Add the zones that contain the interfaces to which 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**.
3. Click **OK**. **Deploy** the changes


Add Secure Shell Configuration
IP Address*
a
Available Zones/Interfaces
Search
DMZ
Inside
outside
Add
b
Selected Zones/Interfaces
Interface Name
Add
Cancel
OK



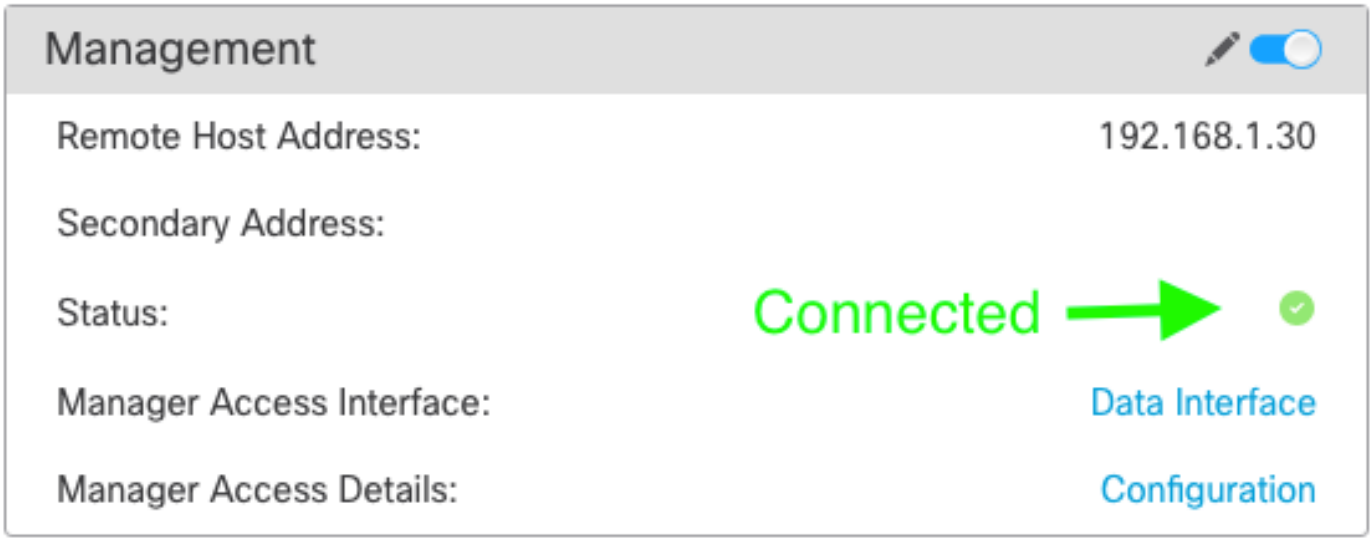
Note: SSH is not enabled by default on the data interfaces, so if you want to manage the threat defense using SSH, you need to explicitly allow it.

Verify

Ensure that 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 the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.



Verify from FTD Command Line Interface (CLI)

At thethreat defenseCLI, enter 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 thethreat defenseCLI, enter the**sftunnel-status-brief**command to view the management connection status. You can also use**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 thethreat defenseCLI, 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
```

CLI, check that the default route (S*) was added and that 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
```

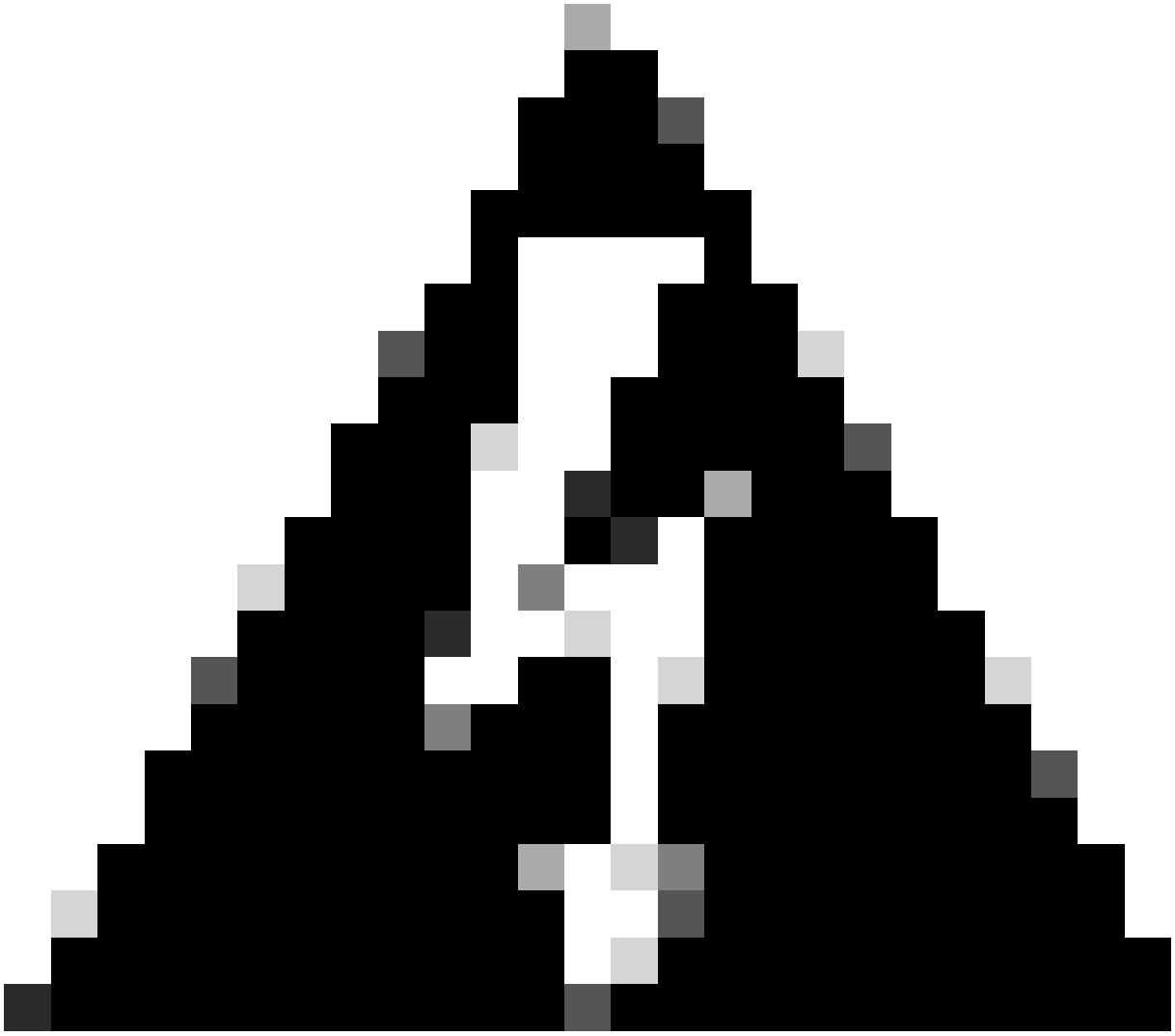
> show nat

```
> 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