在FTD上配置从管理到数据接口的管理器访问

目录

简介

本文档介绍将Firepower威胁防御(FTD)上的Manager访问从管理修改为数据接口的流程。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower威胁防御
- Firepower 管理中心

使用的组件

- Firepower管理中心虚拟7.4.1

- Firepower威胁防御虚拟7.2.5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

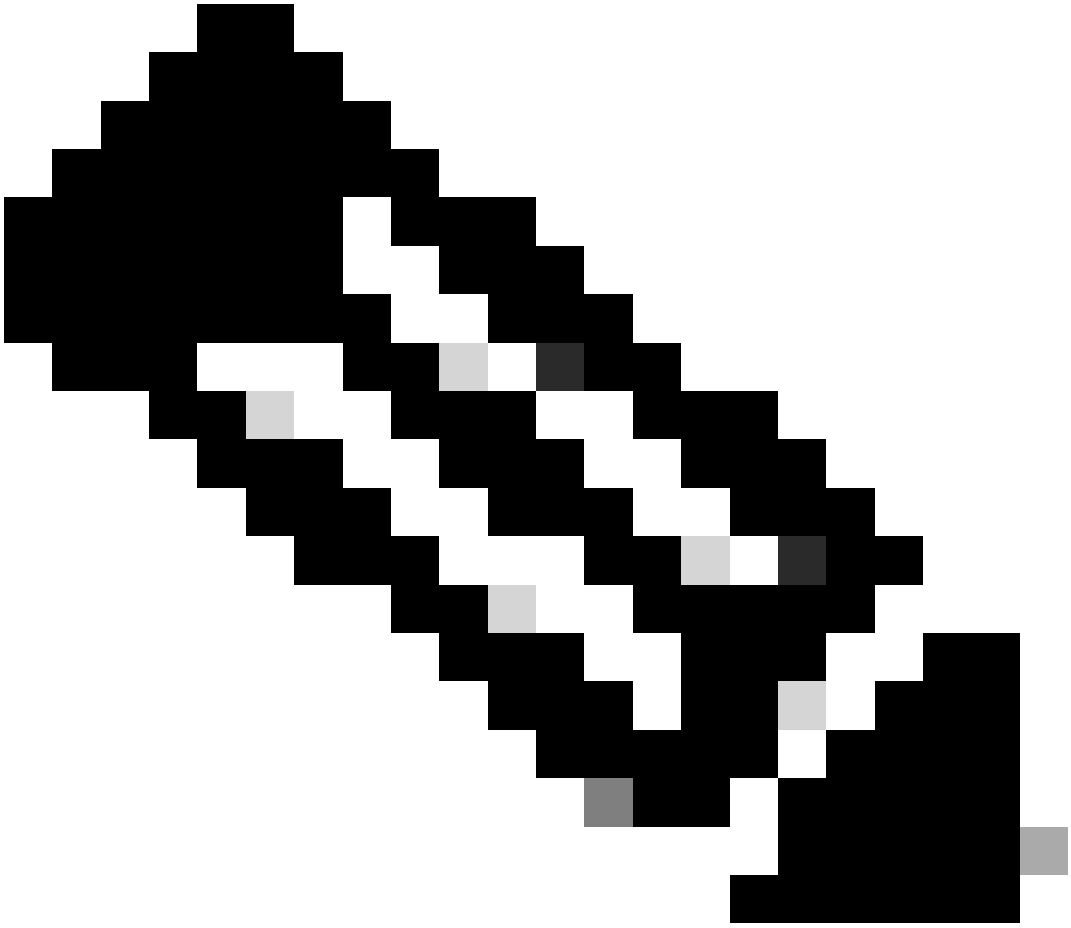
每个设备包括用于与FMC通信的单个专用管理接口。您可以选择将设备配置为使用数据接口而不是专用管理接口进行管理。如果要从外部接口远程管理Firepower威胁防御，或者没有单独的管理网络，则数据接口上的FMC访问非常有用。此更改必须在FMC管理的FTD的Firepower管理中心(FMC)上执行。

从数据接口进行FMC访问存在一些限制：

- 您只能在一个物理数据接口上启用管理器访问。不能使用子接口或EtherChannel。
- 仅路由防火墙模式，使用路由接口。
- 不支持PPPoE。如果您的ISP需要PPPoE，则必须在Firepower威胁防御和广域网调制解调器之间放置一台具有PPPoE支持的路由器。
- 不能使用单独的管理接口和仅事件接口。

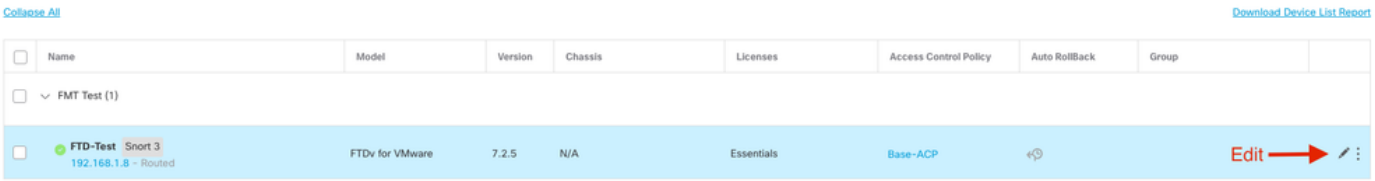
配置

继续接口迁移



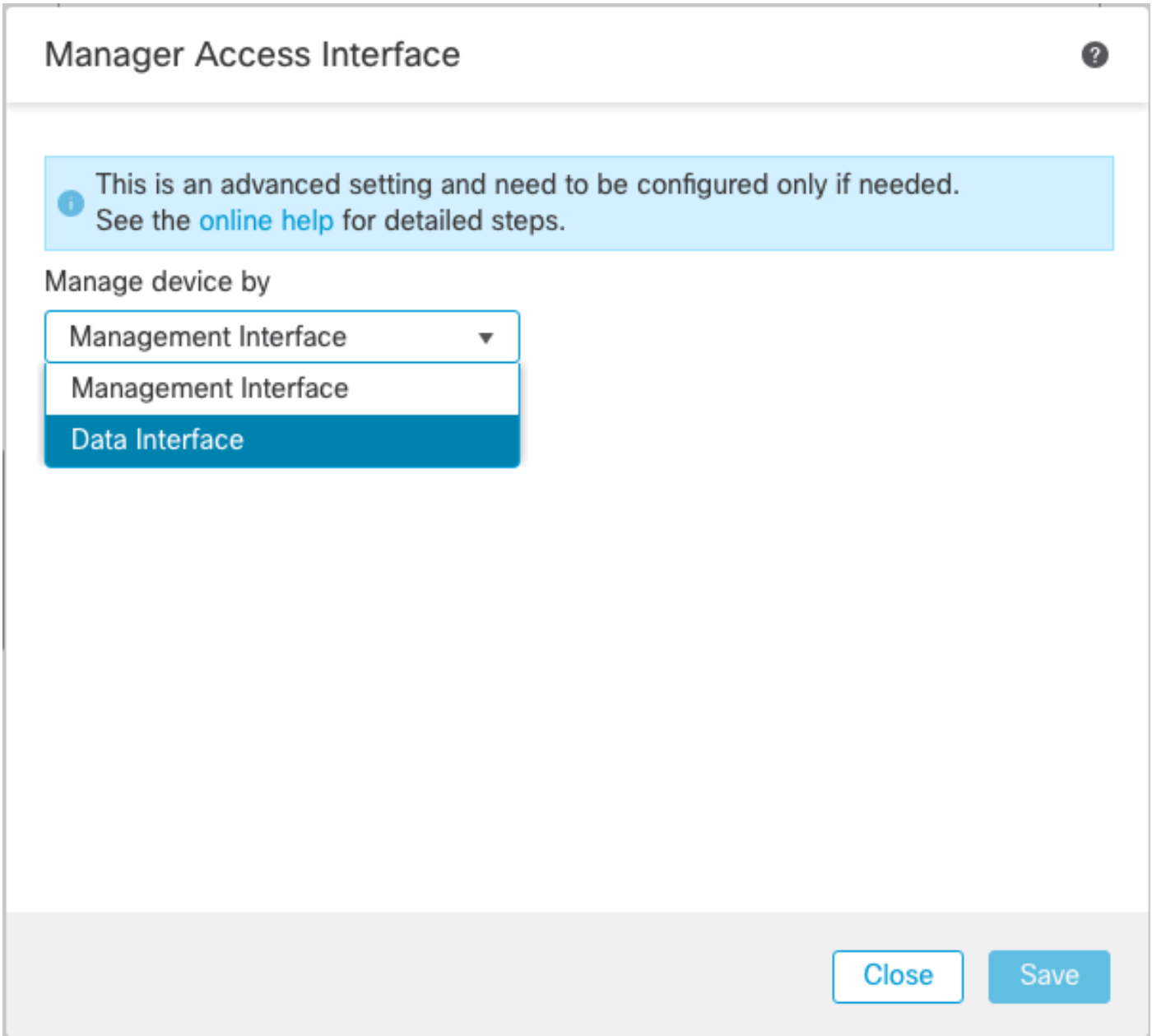
注意：强烈建议在继续进行任何更改之前同时备份FTD和FMC。

1. 导航到设备>设备管理页面，点击要更改的设备的编辑。

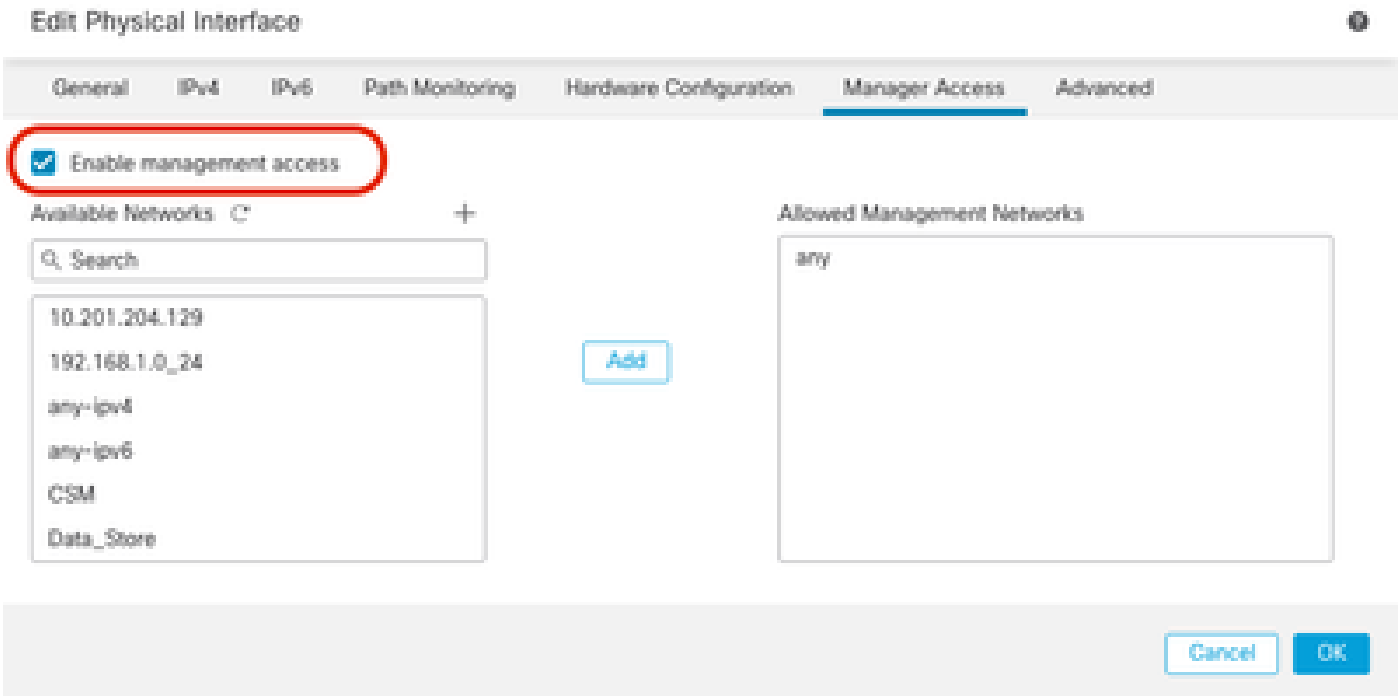


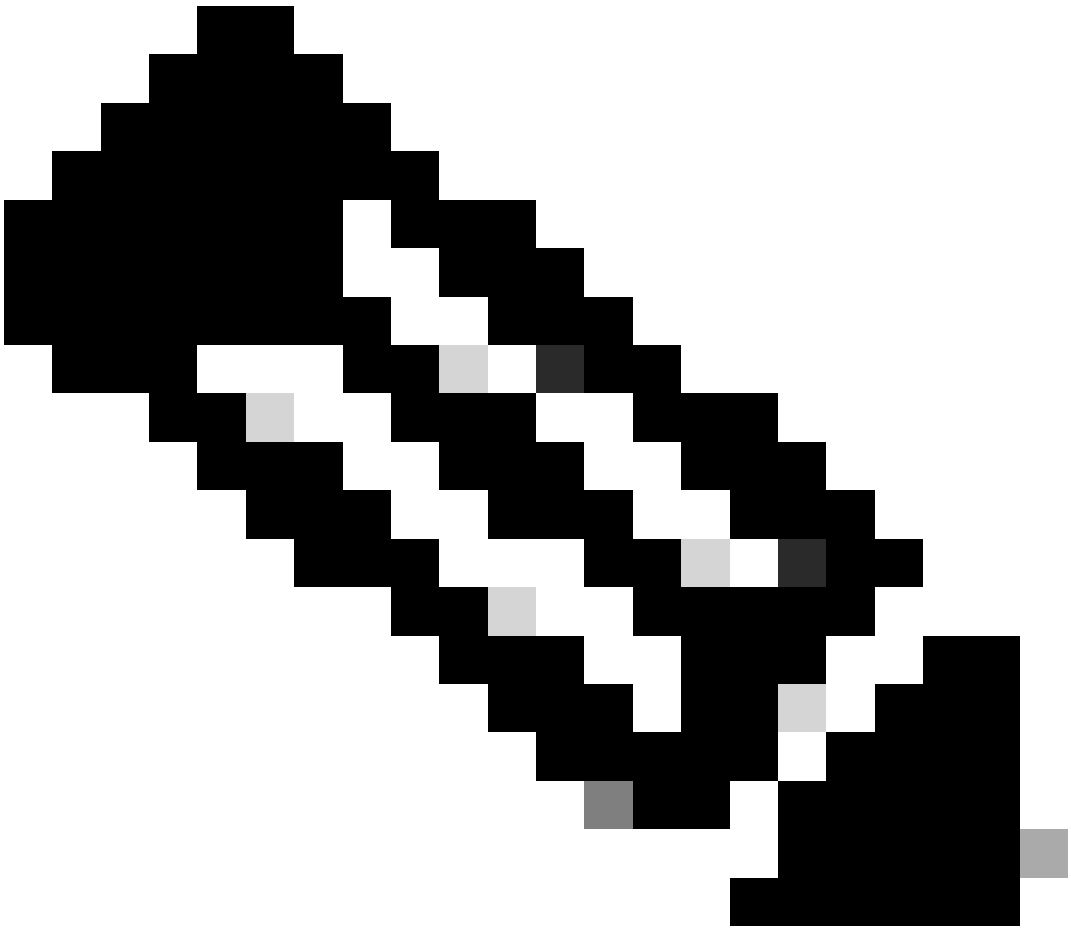
2.转至Device > Management部分，单击Manager Access Interface的链接。

Manager Access Interface字段显示现有管理接口。点击链接以选择新的接口类型，这是Manage device by下拉列表中的Data Interface选项，然后单击Save。



3. 现在，您必须继续在数据接口上启用管理访问，导航到“设备”(Devices) >“设备管理”(Device Management) >“接口”(Interfaces) >“编辑物理接口”(Edit Physical Interface) >“管理器访问”(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



注意：（可选）如果使用辅助接口实现冗余，请在用于冗余目的的接口上启用管理访问。

（可选）如果对接口使用DHCP，请在Devices > Device Management > DHCP > DDNS对话框上启用Web类型“DDNS”方法。

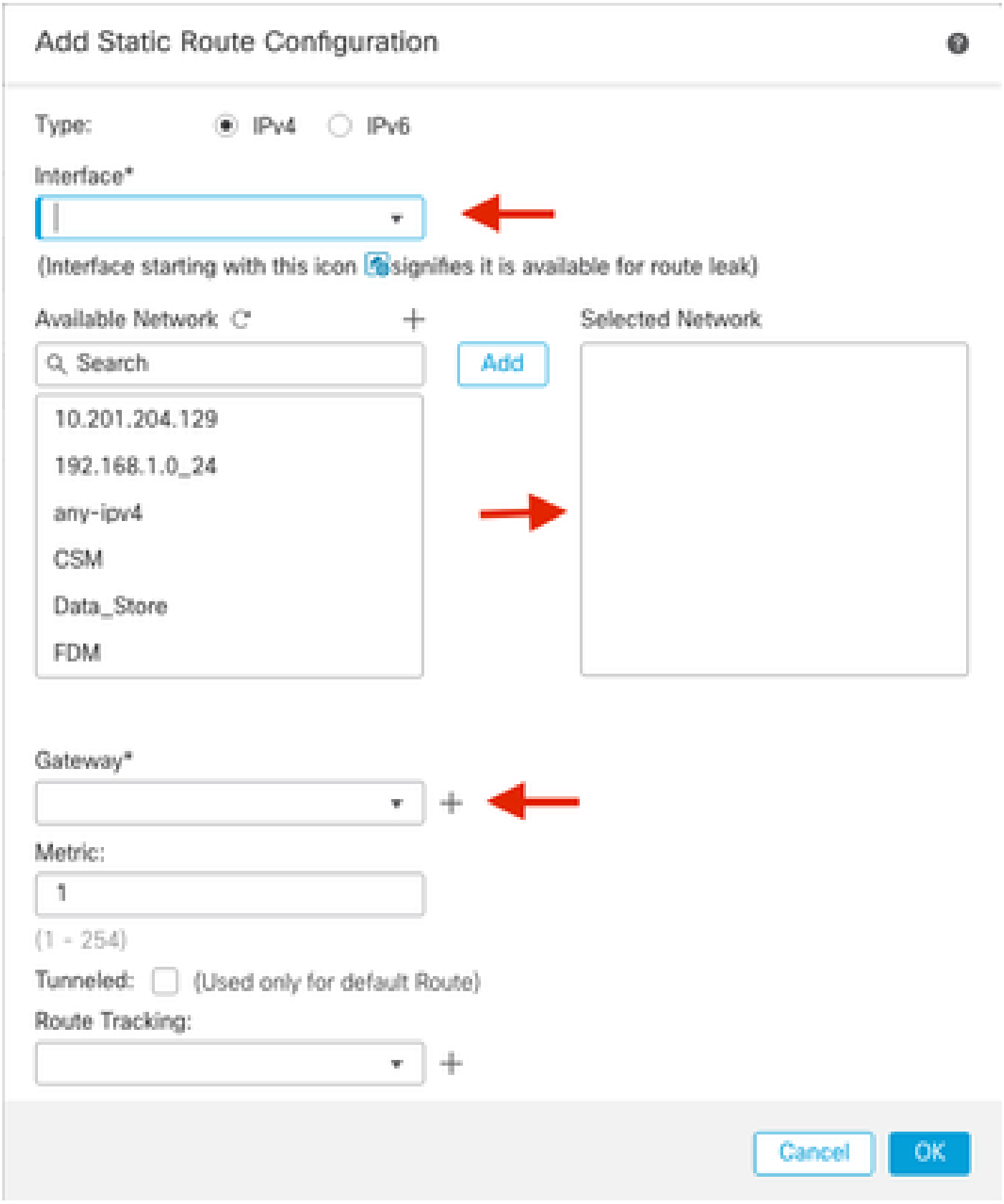
（可选）在平台设置策略中配置DNS，并将其应用于Devices > Platform Settings > DNS下的此设备。

---

4. 确保威胁防御可以通过数据接口路由到管理中心；如有必要，在Devices > Device Management > Routing > Static Route上添加静态路由。

1. 根据您要添加的静态路由类型，单击IPv4或IPv6。
2. 选择此静态路由所应用的Interface。
3. 在Available Network列表中，选择目标网络。
4. 在Gateway或IPv6 Gateway字段中，输入或选择作为此路由的下一跳的网关路由器。

（可选）要监控路由可用性，请在路由跟踪(Route Tracking)字段中输入或选择定义监控策略的服务级别协议(SLA)监控对象的名称。

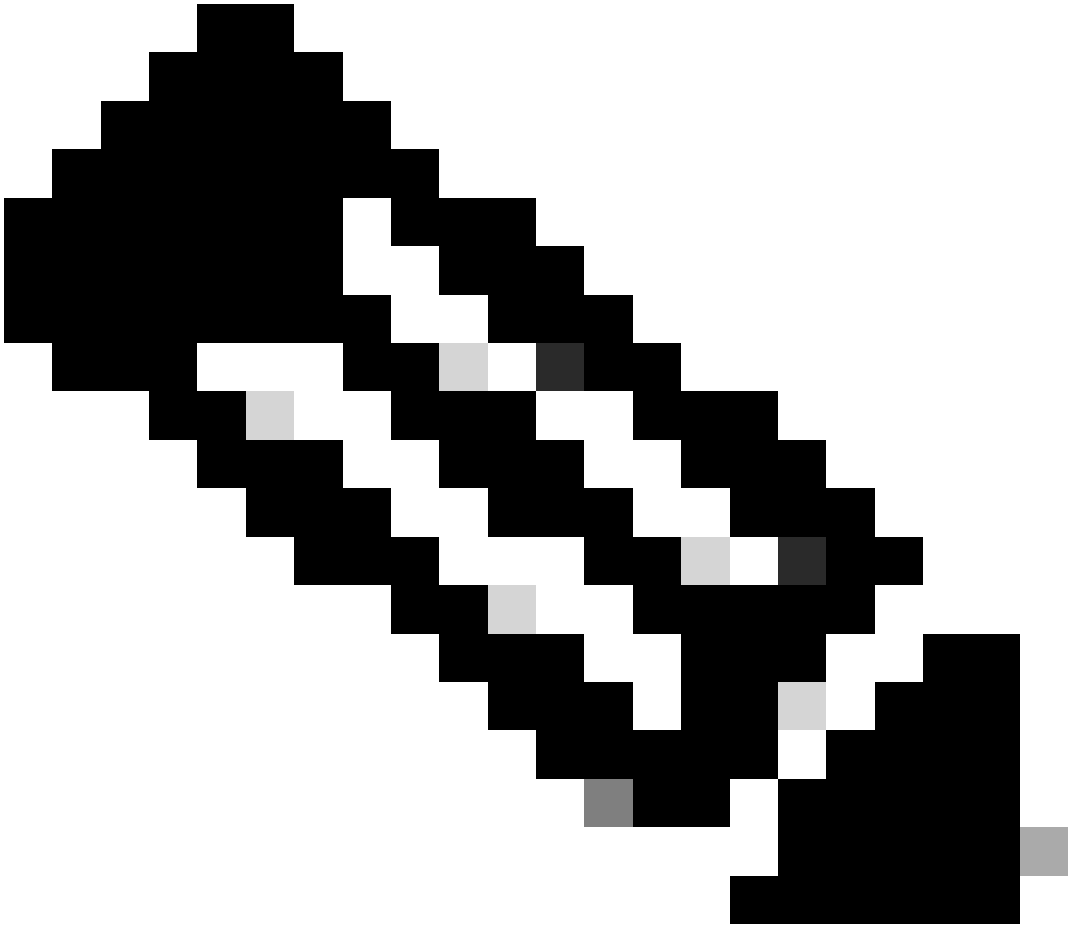


5.部署配置更改。配置更改现在通过当前管理接口进行部署。

6. 在FTD CLI中，将管理接口设置为使用静态IP地址，并将网关设置为数据接口。

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

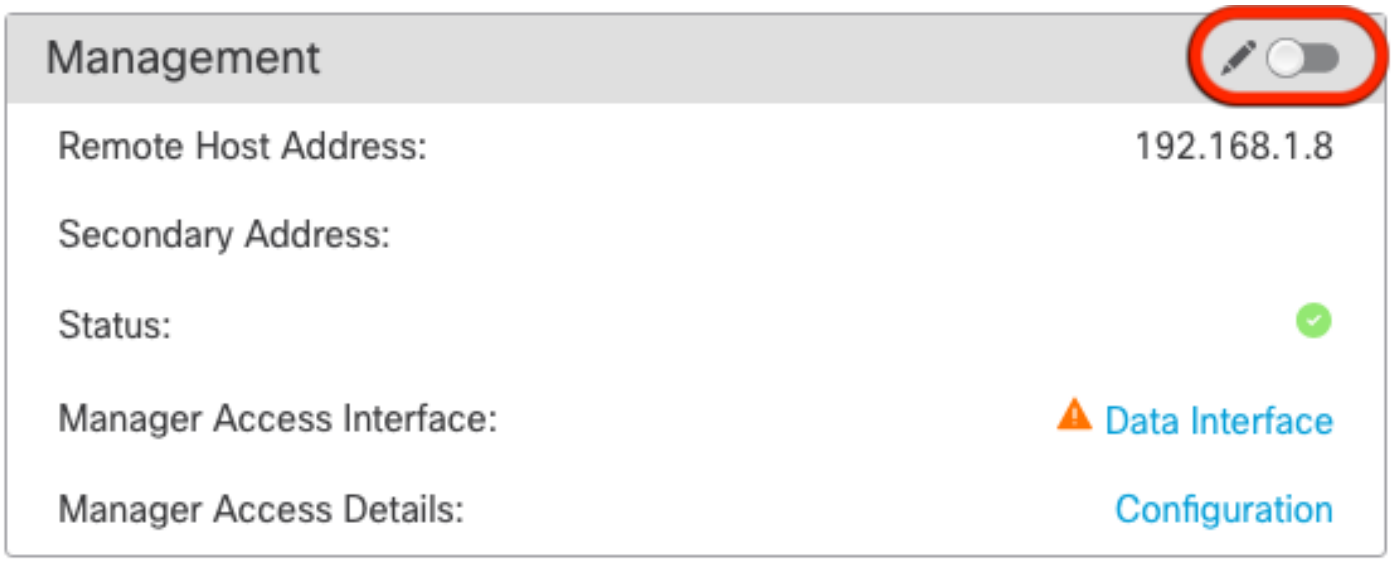
```
>
>                                    IP_ADDRESS      NETMASK         GATEWAY
> configure network ipv4 manual 192.168.1.8 255.255.255.0 data-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```



注意：虽然不计划使用管理接口，但必须设置静态IP地址。例如，提供私有地址，以便您可以将网关设置为**data-interfaces**。此管理用于使用tap_nlp接口将管理流量转发到数据接口。

---

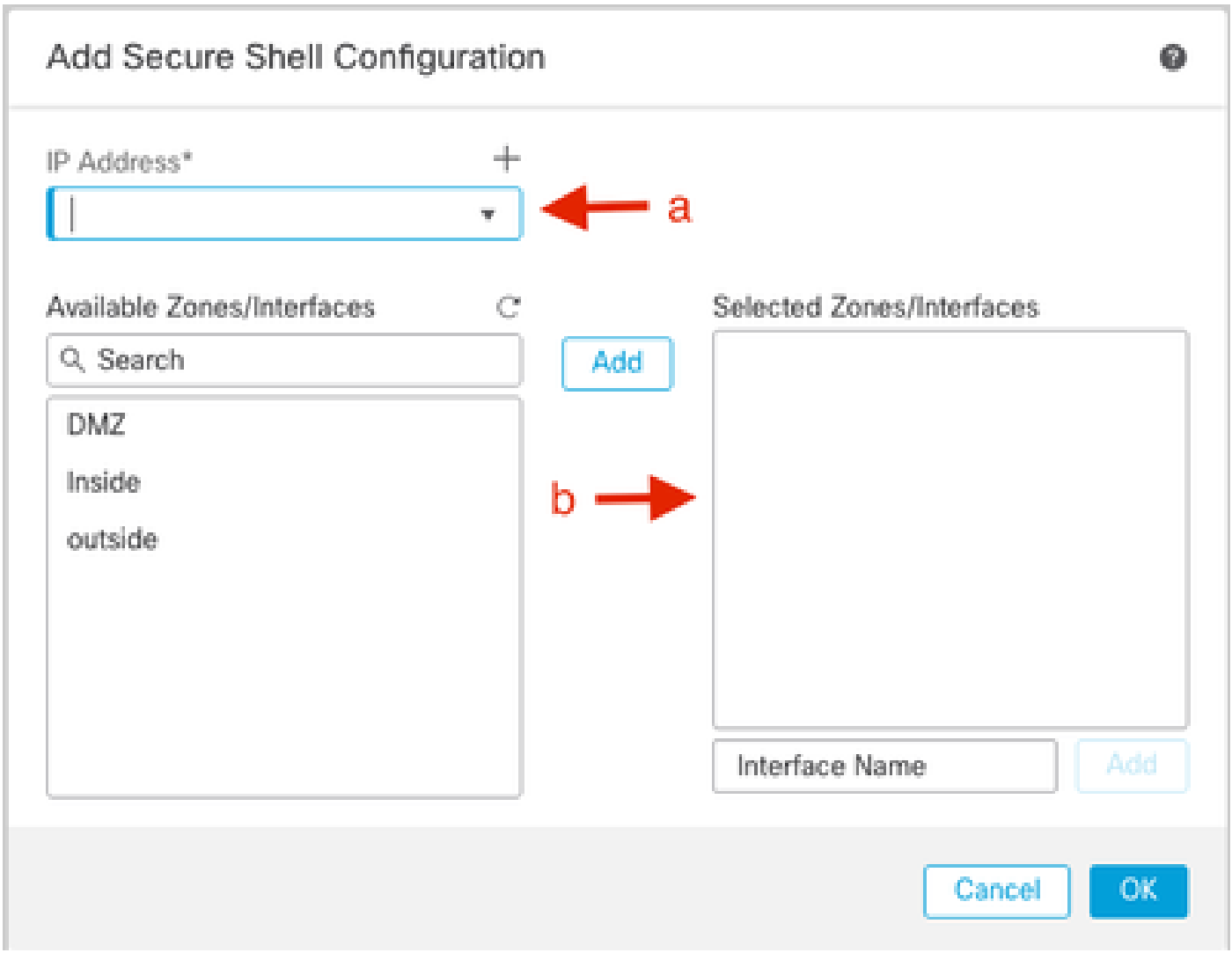
7. 禁用管理中心中的管理，在Devices > **Device Management** > **Device** > **Management部分**单击Edit并更新威胁防御的远程主机地址**IP地址和**（**可**选）辅助地址，**然后启用**连接。

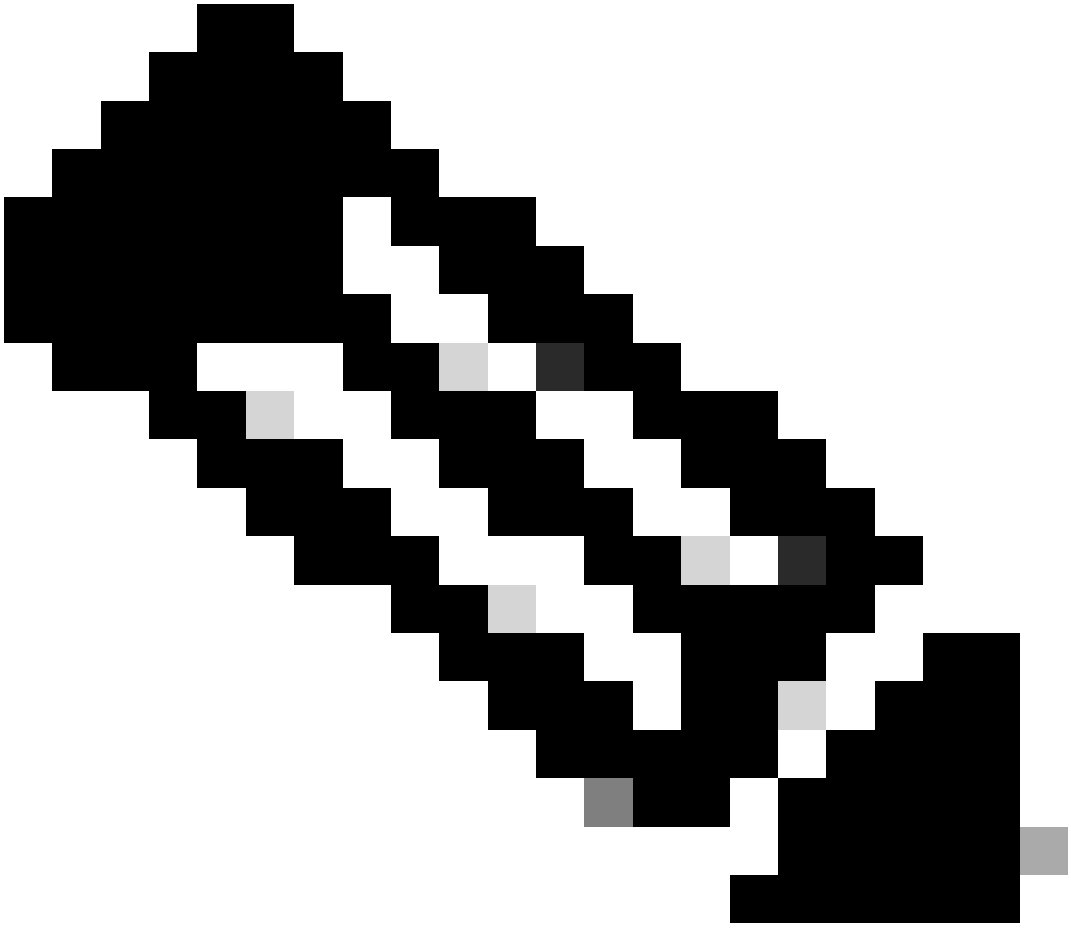


在平台设置中启用SSH

在“平台设置”策略中为数据接口启用SSH，然后在“设备”(Devices) >**“平台设置”(Platform Settings)**>“SSH访问”(**SSH Access)**处将SSH应用于此设备。单击“添加”(**Add)**。

- 允许进行SSH连接的主机或网络。
- 添加包含允许SSH连接的接口的区域。对于不在区域中的接口，您可以将**接口名称**键入字段**Selected Zones/Interfaces**列表并单击**Add**。
- Click **OK**. **部署**更改


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



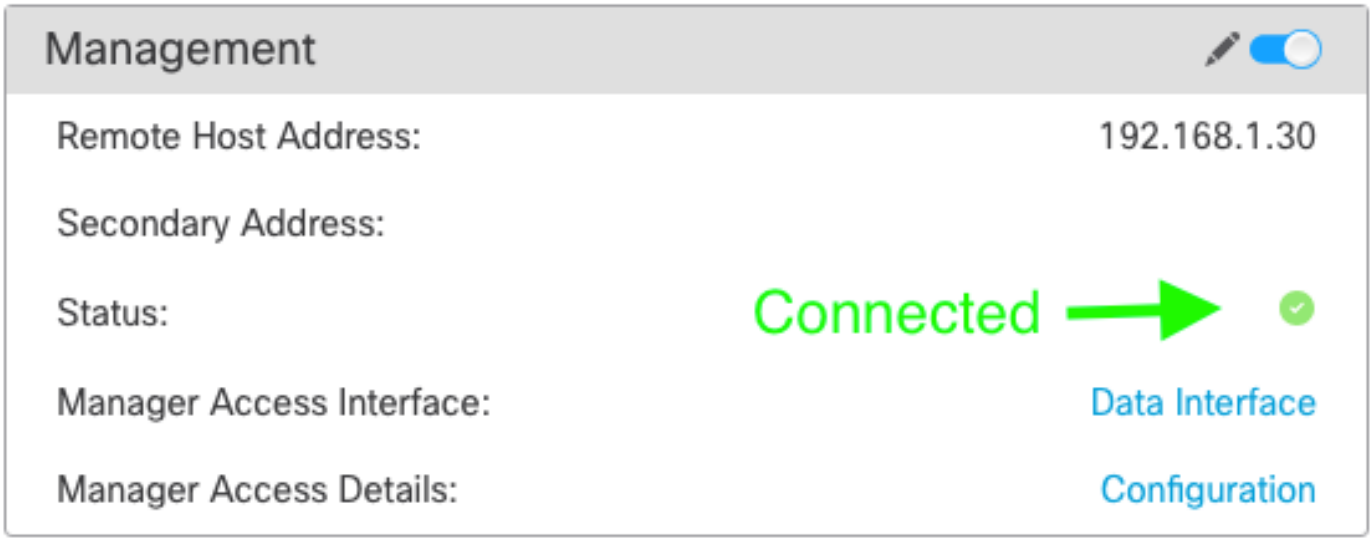
注意：默认情况下，SSH在数据接口上未启用，因此，如果您希望使用SSH管理威胁防御，则需要明确允许它。

验证

确保已在数据接口上建立管理连接。

从FMC图形用户界面(GUI)进行验证

在管理中心，在Devices > **Device Management > Device > Management > Manager Access - Configuration Details > Connection Status**页面上检查管理连接状态。



从FTD命令行界面(CLI)进行验证

在威胁防御CLI中，输入**thesftunnel-status**-briefcommand以查看管理连接状态。

```
>
> 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
```

状态显示数据接口的连接成功，显示内部tap_nlp接口。

故障排除

在管理中心，在Devices > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** > **Connection Status**页面上检查管理连接状态。

在威胁防御CLI中，输入**thesftunnel-status**-briefcommand以查看管理连接状态。还可以使用**ftunnel-statusto**查看更完整的信息。

管理连接状态

工作场景

```
> 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
```

非工作场景

```
> 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
```

验证网络信息

在威胁防御CLI中，查看管理和管理器访问数据接口网络设置：

> 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
```

注意：此命令不显示管理连接的当前状态。

验证网络连接

Ping管理中心

在威胁防御CLI中，使用命令从数据接口对管理中心执行ping操作：

> 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
```

在威胁防御CLI中，使用命令从管理接口对管理中心执行ping操作，该管理接口通过背板路由到数据接口：

> 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
```

检查接口状态、统计信息和数据包计数

在threat defenseCLI中，请参阅有关内部背板接口的信息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
```

验证FTD上的路由以到达FMC

在threat defenseCLI中，检查是否已添加默认路由(S*)以及管理接口(nlp_int_tap)是否存在内部NAT规则。

> **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
```

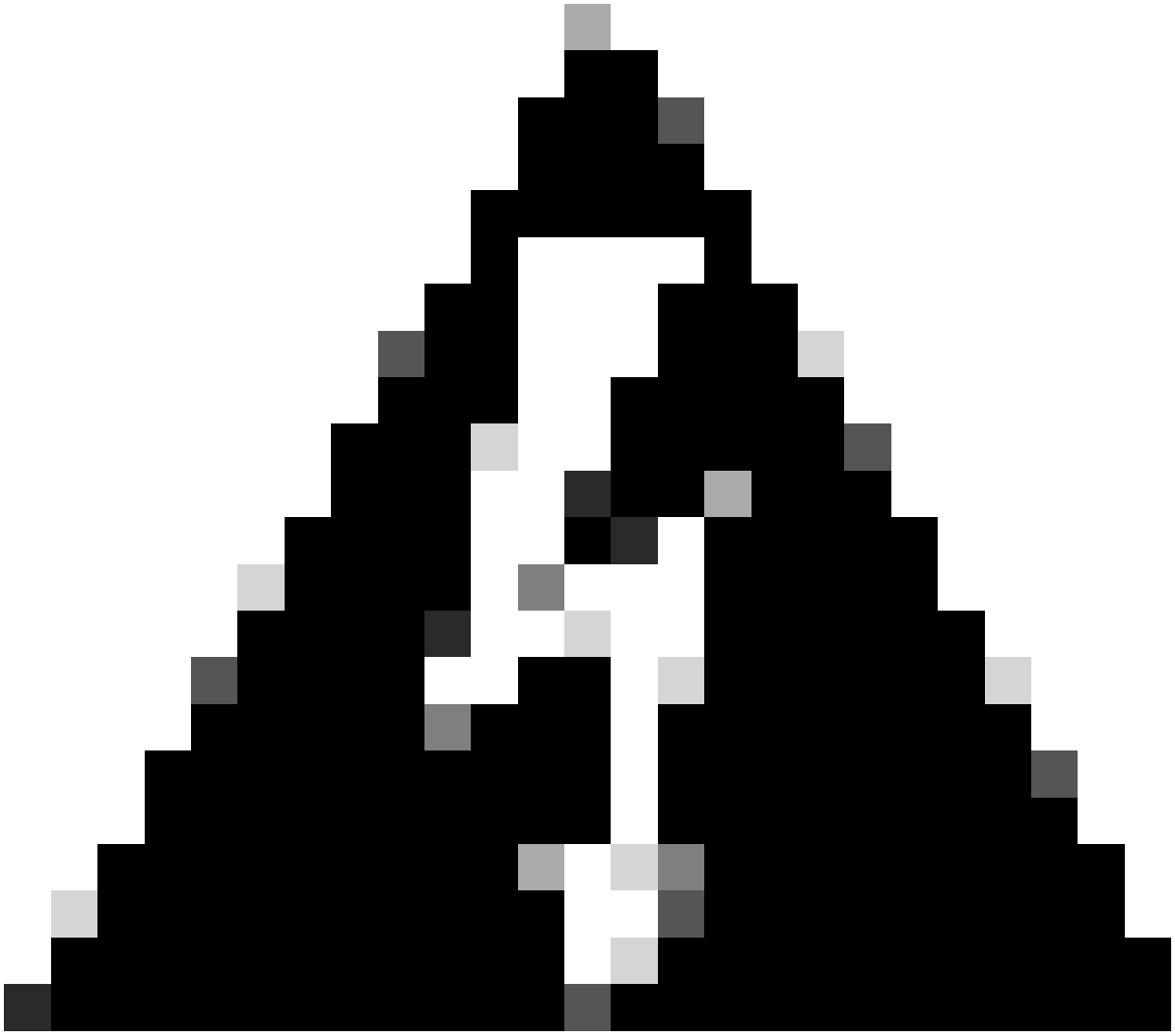
> show nat

```
> 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
```

检查Sftunnel和连接统计信息

> show running-config sftunnel

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



警告：在更改管理员访问权限的整个过程中，请勿在FTD上删除管理员，或取消注册/强制从FMC中删除FTD。

相关信息

- 通过平台设置配置DNS
- 通过FMC配置对FTD（HTTPS和SSH）的管理访问

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。