在FTD上配置从管理到数据接口的管理器访问

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 继续接口迁移
- 在平台设置上启用SSH

验证

- 从FMC图形用户界面(GUI)进行验证
- 从FTD命令行界面(CLI)进行验证

故障排除

- 管理连接状态
  - 工作场景
  - 非工作场景
- 验证网络信息
- 验证管理器状态
- 验证网络连接
  - Ping管理中心
  - 检查接口状态、统计信息和数据包计数
  - 验证FTD上的路由以到达FMC
  - 检查Sftunnel和连接统计信息

相关信息

简介

本文档介绍在Firepower威胁防御(FTD)上将管理器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 Threat Defense (FTD)
- Firepower Management Center (FMC)

使用的组件

- Firepower威胁防御虚拟7.2.5
- Firepower管理中心虚拟7.4.1

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

每个设备都包括一个专用管理接口，用于与FMC通信。或者，您可以配置设备使用数据接口进行管理，而不是专用管理接口。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，数据接口上的FMC访问非常有用。此更改必须在FMC管理的FTD Firepower管理中心上执行。

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WAN调制解调器之间加入支持PPPoE的路由器。
- 不能使用单独的管理接口和仅事件接口。

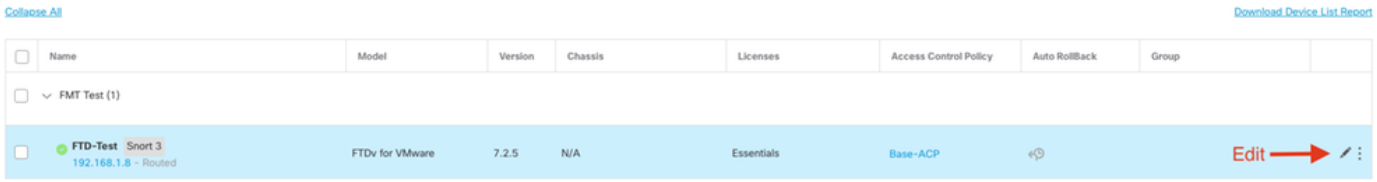
配置

继续接口迁移



注意：强烈建议先对FTD和FMC进行最新备份，然后再继续进行更改。

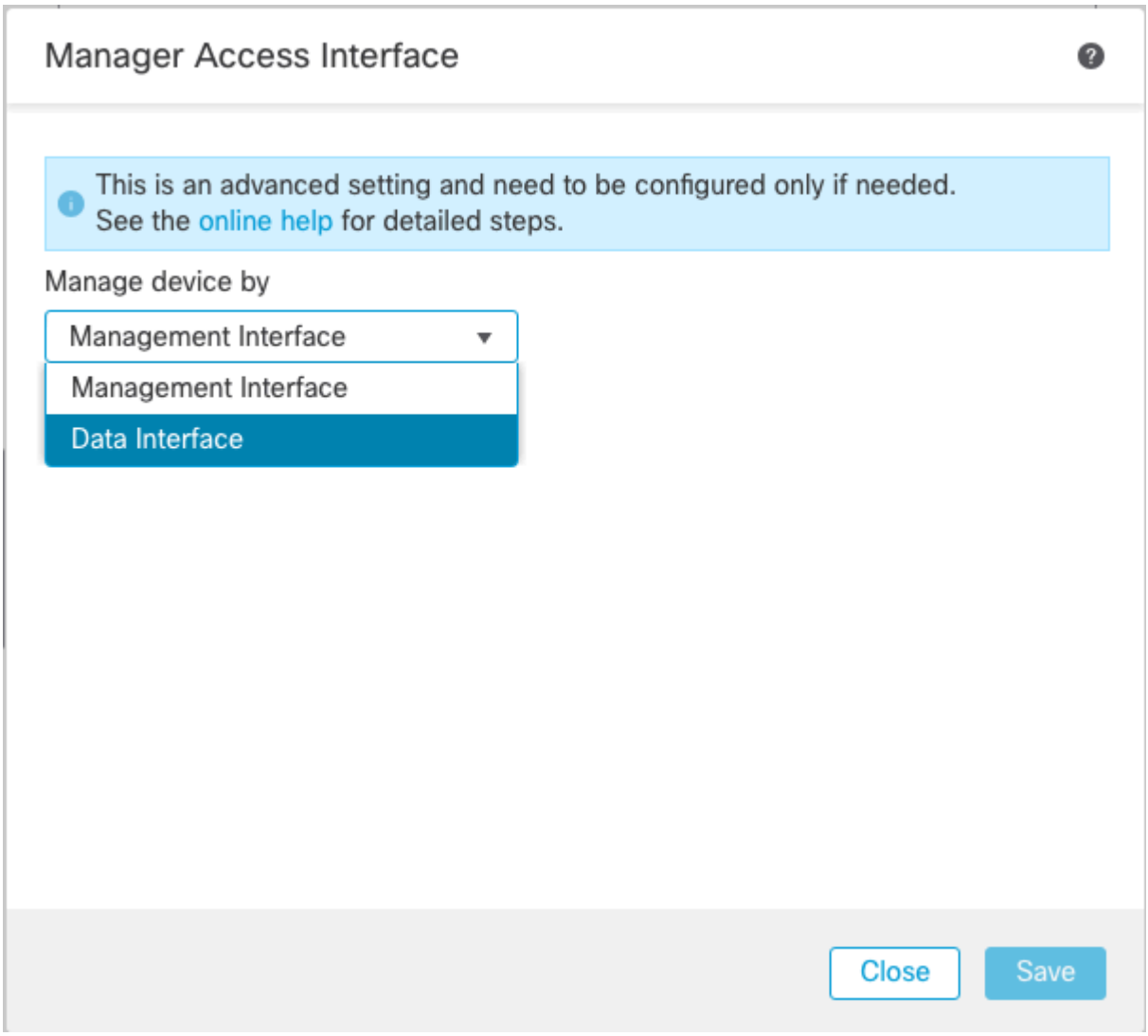
1.导航到设备>设备管理页，对于正在更改的设备，单击编辑。



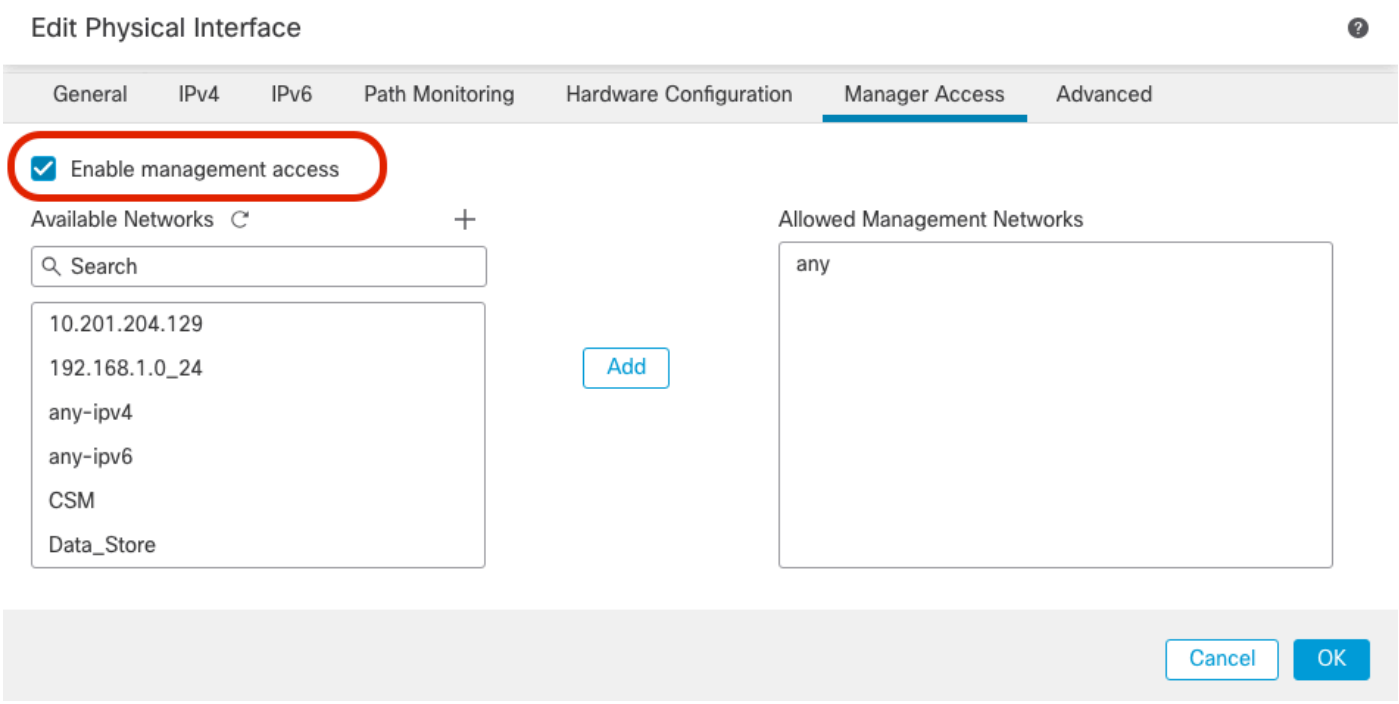
2.转到Device > Management部分，然后单击Manager Access Interface的链接。



3. “管理员访问接口”字段显示现有的管理接口。单击link以选择新的接口类型，该类型是Manage device by下拉列表中的Data Interface选项，然后单击Save。



4.现在，您必须继续在数据接口上启用管理访问，导航到“设备”>“设备管理”>“接口”>“编辑物理接口”>>“管理器访问”。



可选：如果使用辅助接口实现冗余，请确保在用于冗余的接口上启用管理访问。如果使用DHCP作为接口，请在设备>设备管理> DHCP > DDNS对话框上启用Web类型DDNS方法。您可以在Platform Settings策略中配置DNS，并在Devices > Platform Settings > DNS下将其应用于此设备。

5.确保威胁防御能够通过数据接口路由到管理中心；如有必要，请在Devices > Device Management > Routing > Static Route中添加静态路由。

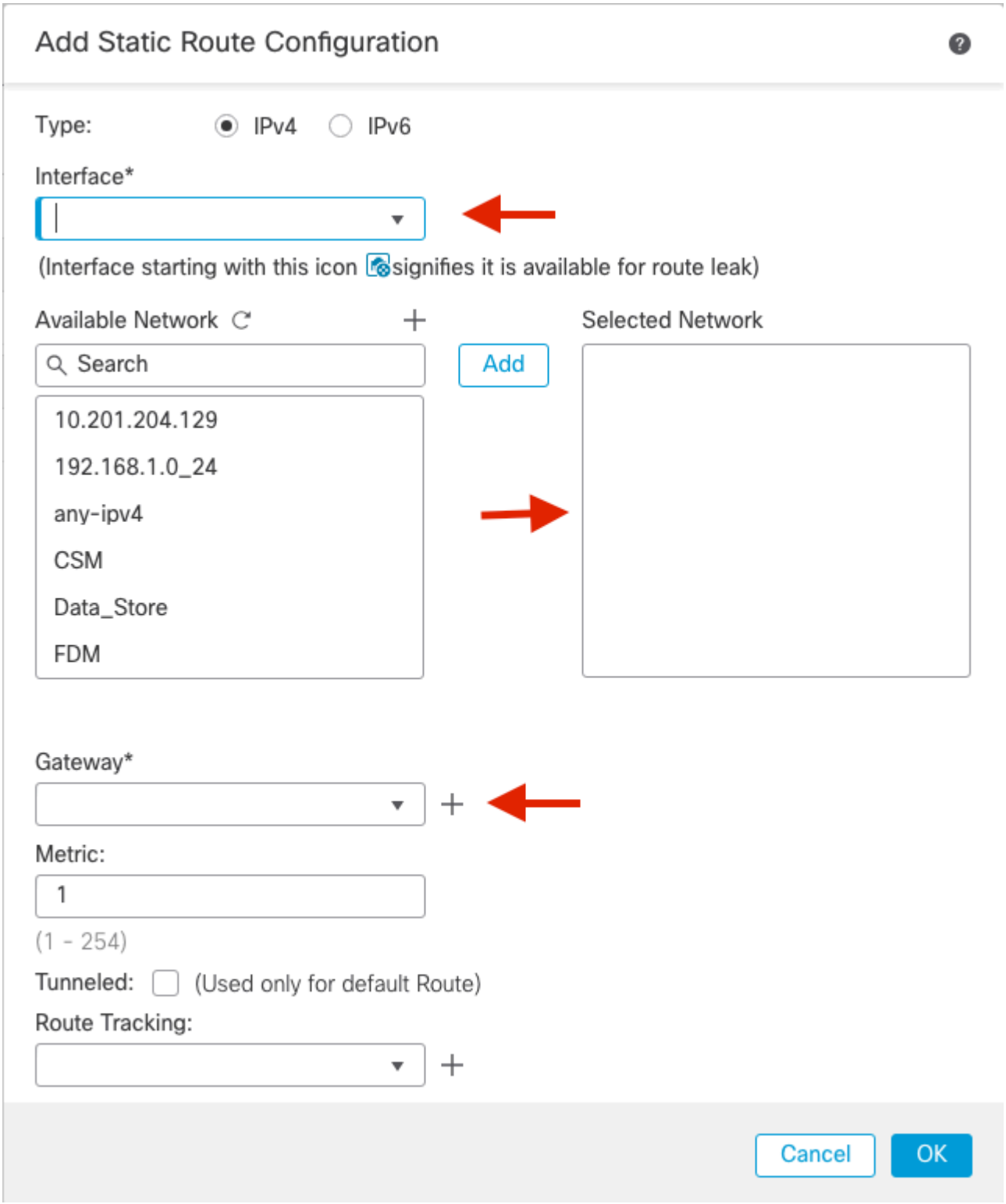
a.根据要添加的静态路由的类型，单击IPv4或IPv6。

b.选择应用此静态路由的Interface。

c.在Available Network列表中，选择目标网络。

d.在Gateway或IPv6 Gateway字段中，输入或选择网关路由器，该路由器是此路由的下一跳。

可选：要监控路由可用性，请在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。



6.部署配置更改，因为这些更新现在通过当前管理界面部署。

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

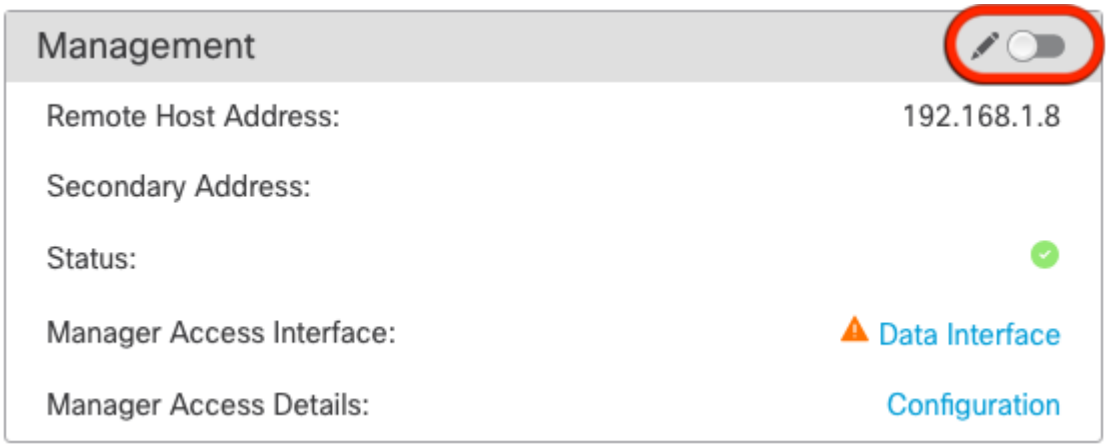
a.配置网络{ipv4 | ipv6} manual ip_address netmask data-interfaces

---

```
>
>                                    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：虽然不打算使用管理接口，但必须设置静态IP地址。例如，私有地址，这样您就可以将网关设置为数据接口。此管理用于使用tap_nlp接口将管理流量转发到数据接口。

8.在管理中心中禁用管理。单击“设备”>“设备管理”>“设备”>“管理”部分中的编辑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。



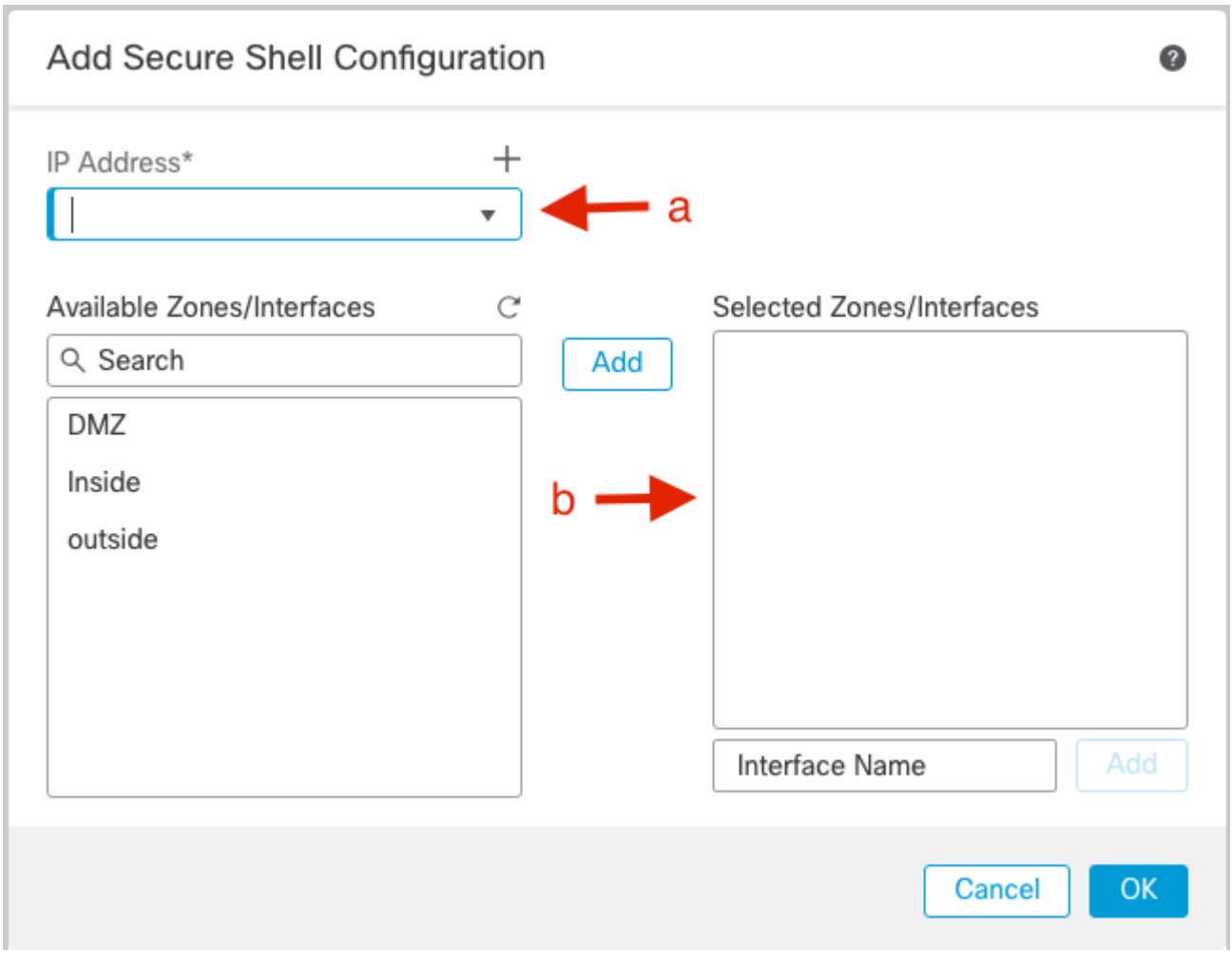
在平台设置上启用SSH

1.在Platform Settings Policy中启用数据接口的SSH，并将其应用于Devices > Platform Settings > SSH Access处的设备。

2.单击Add。

3.允许进行SSH连接的主机或网络。添加包含接口的区域，以允许SSH连接。对于不在区域中的接口，可以在Selected Zones/Interfaces字段中键入接口名称，然后单击Add。

4.单击确定。部署更改。



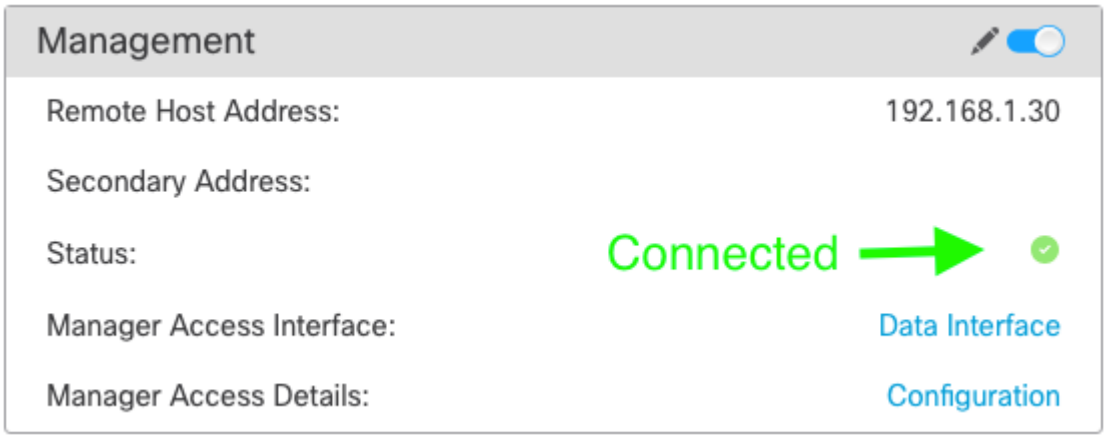
注意：默认情况下，数据接口上未启用SSH，因此，如果您希望使用SSH管理威胁防御，需要明确允许它。

验证

确保通过数据接口建立管理连接。

从FMC图形用户界面(GUI)进行验证

在管理中心中，检查管理连接状态（位于Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status页）。



从FTD命令行界面(CLI)进行验证

在威胁防御CLI中，运行sftunnel-status-brief命令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

在管理中心中，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，运行sftunnel-status-brief命令以查看管理连接状态。您还可以运行sftunnel-status以查看更完整的信息。

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
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.168.1.30
Netmask                   : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

验证管理器状态

在威胁防御CLI上，验证管理中心注册已完成。

```
> 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
```



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threat defense CLI上，运行命令以从数据接口ping管理中心：

```
> 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threat defense CLI上，运行命令以从管理接口（通过背板路由到数据接口）ping管理中心:

```
> 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 defense CLI中，查看内部背板接口nlp_int_tap上的信息：

```
> 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 defense CLI中，检查默认路由(S*)是否已添加且存在管理接口(nlp_int_tap)的内部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：在更改管理器访问权限的过程中，不要删除FTD上的管理器或取消注册/强制从FMC中删除FTD。

相关信息

- 配置基于平台的DNS设置

- 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）。