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

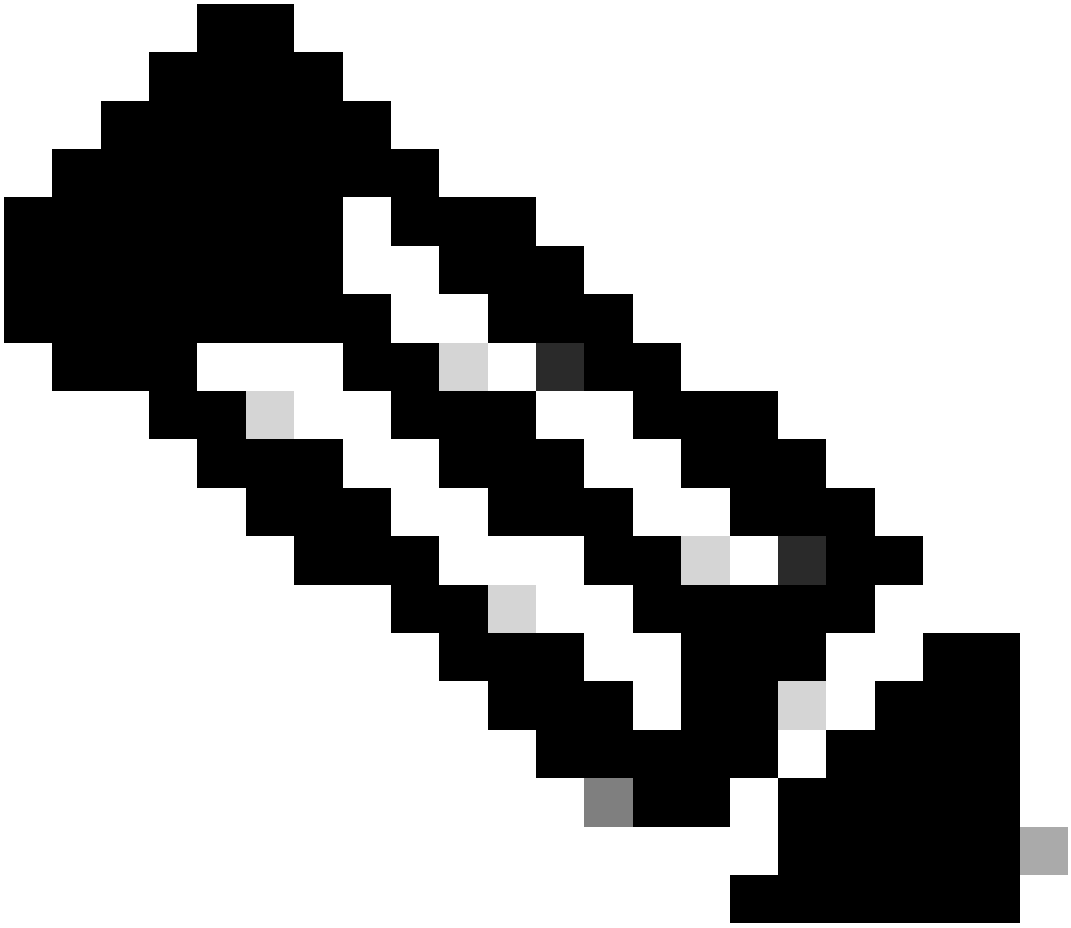
每个设备都包括一个专用管理接口，用于与FMC通信。您可以选择将设备配置为使用数据接口而不是专用管理接口进行管理。如果您想要从外部接口远程管理Firepower威胁防御，或者没有单独的管理网络，数据接口上的FMC访问非常有用。此更改必须在FMC管理的FTD Firepower管理中心上执行。

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调制解调器之间放置一台支持PPPoE的路由器。
- 不能使用单独的管理接口和仅事件接口。

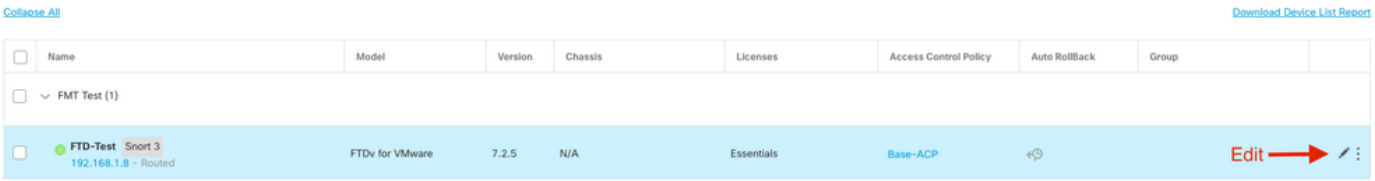
配置

继续接口迁移



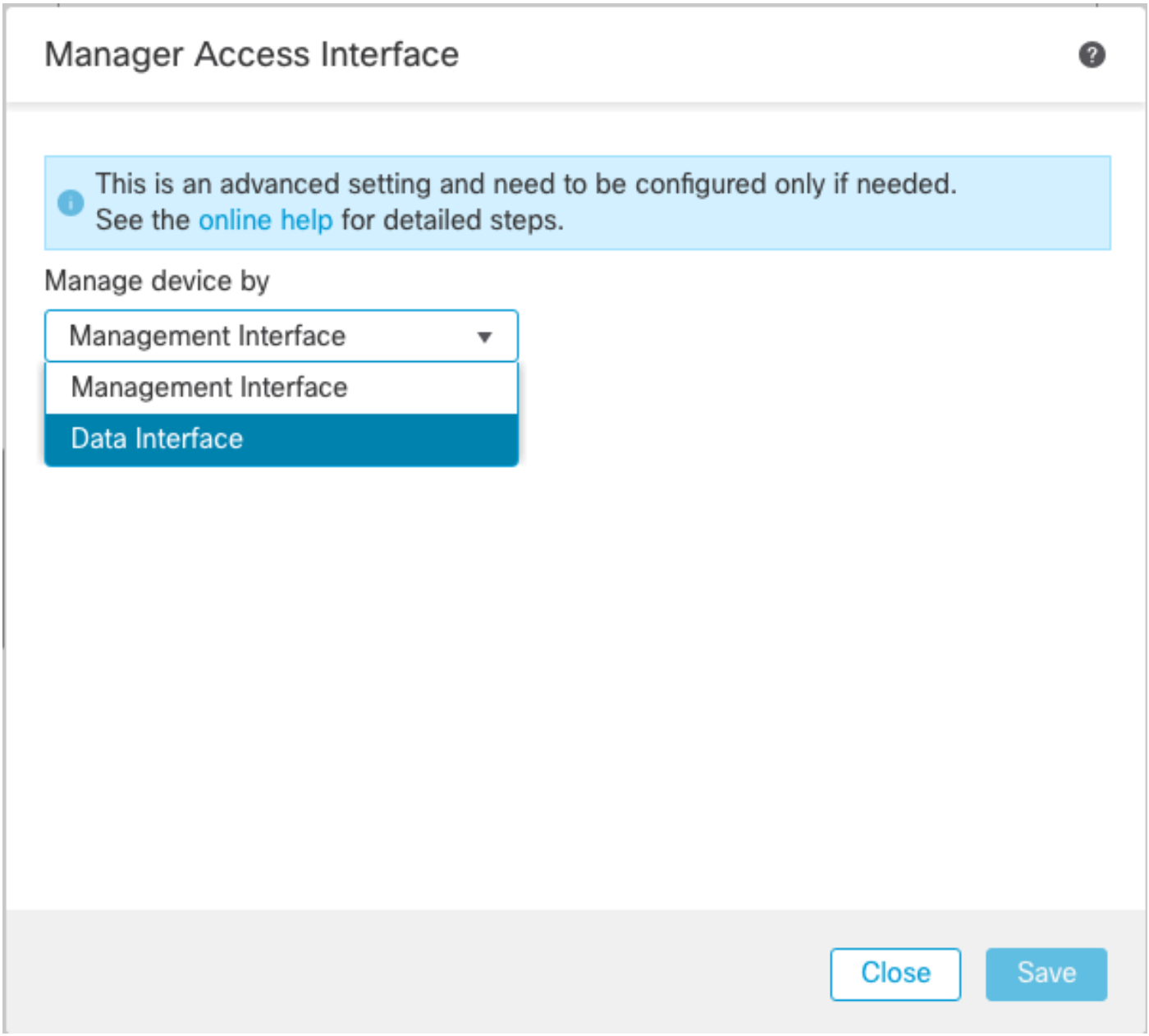
注意：强烈建议先对FTD和FMC进行最新备份，然后再继续进行更改。

1. 导航到设备>设备管理页，针对您正在更改的设备点击编辑。

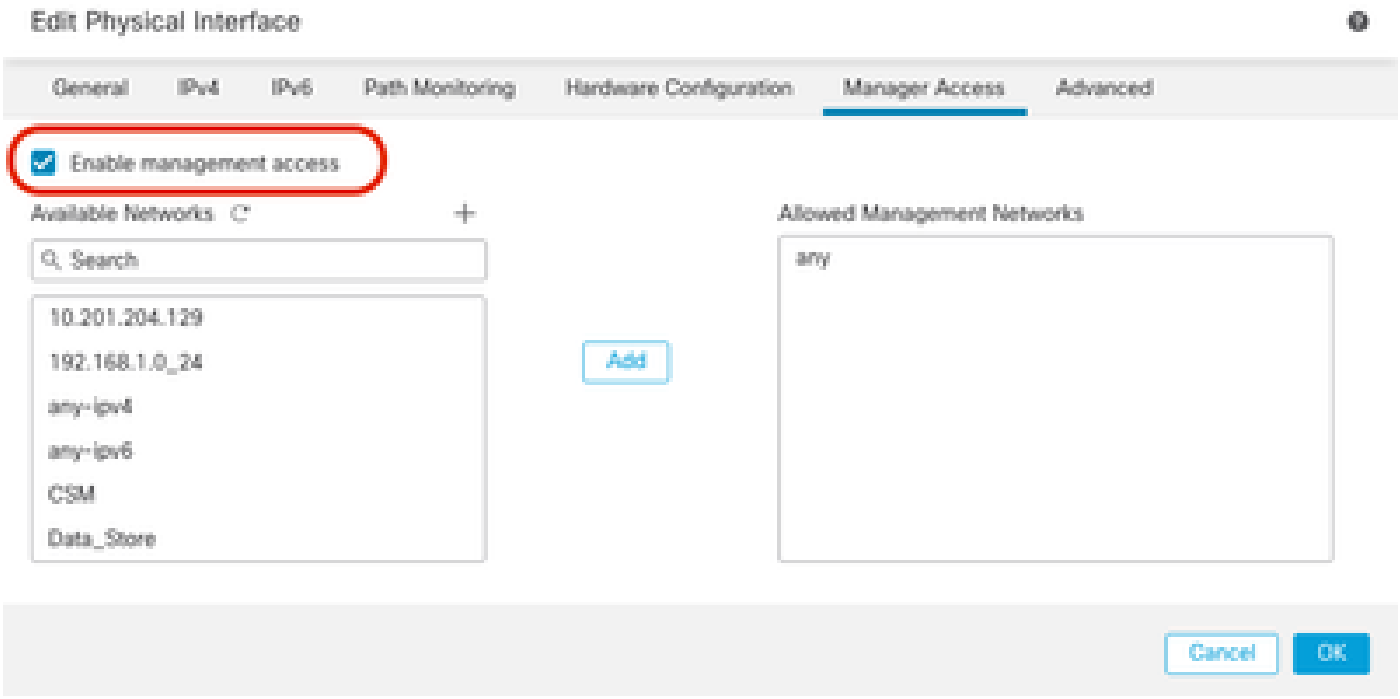


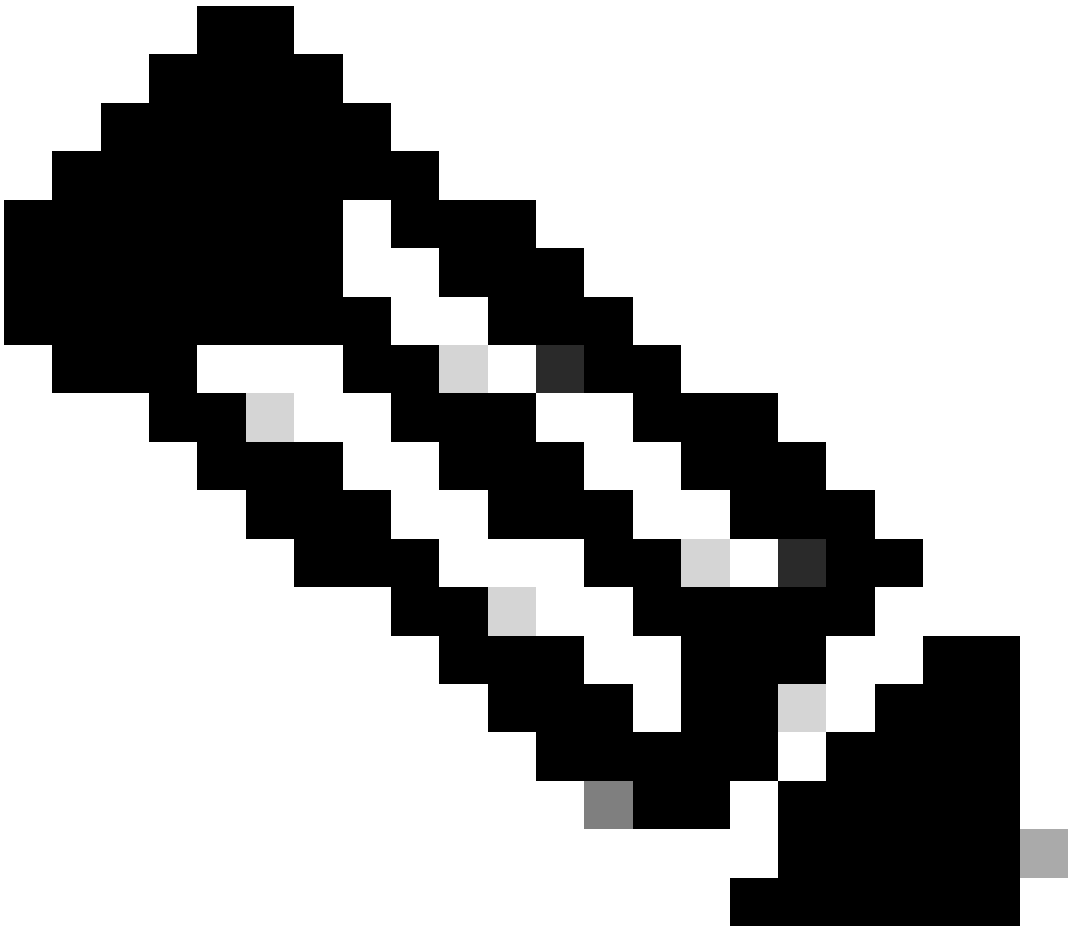
2.转到Device > Management部分，然后单击Manager Access Interface的链接。

Manager Access Interface字段显示现有管理接口。单击link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”>“设备管理”>“接口”>“编辑物理接口”>“编辑物理接口”>“管理器访问”。


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：（可选）如果使用辅助接口实现冗余，请在用于冗余的接口上启用管理访问。

（可选）如果使用DHCP作为接口，请在Devices > Device Management > DHCP > DDNS对话框中启用Web类型DDNS方法。

（可选）在Platform Settings策略中配置DNS，并将其应用到Devices > Platform Settings > DNS处的此设备。

4.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。

1. 根据要添加的静态路由的类型，单击IPv4或IPv6。
2. 选择此静态路由应用的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。

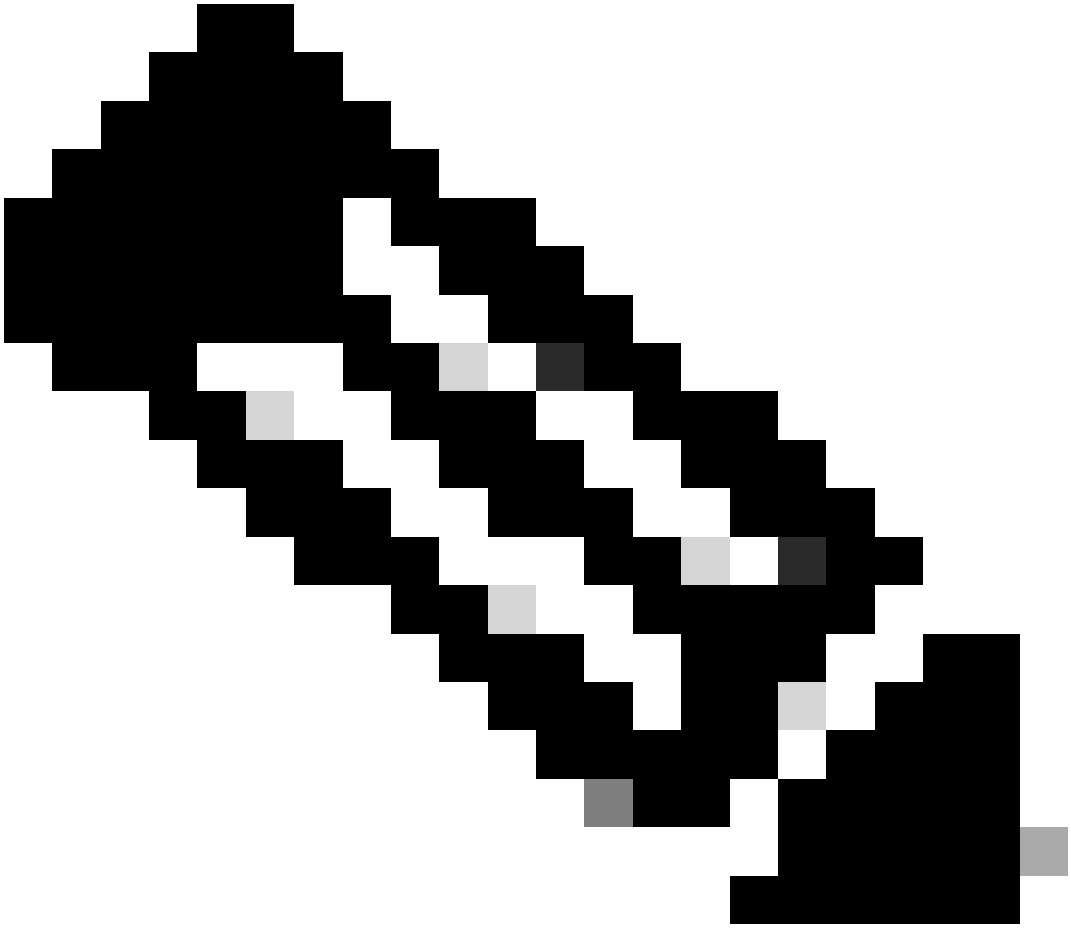
（可选）要监控路由可用性，请在Route Tracking字段中输入或选择定义监控策略的服务级别协议(Service Level Agreement， SLA)Monitor对象的名称。

5.部署配置更改。配置更改现在通过当前管理界面进行部署。

6.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。

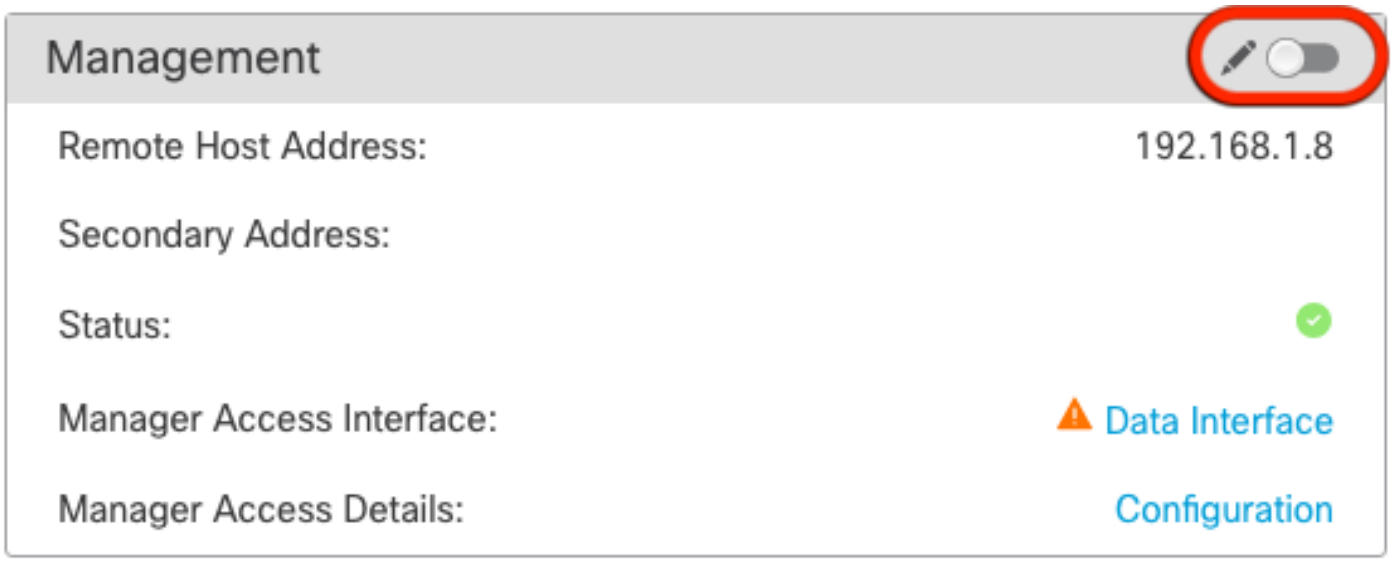
- configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

```
>
>                                    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：虽然不打算使用管理接口，但必须设置静态IP地址。例如，私有地址，以便您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。

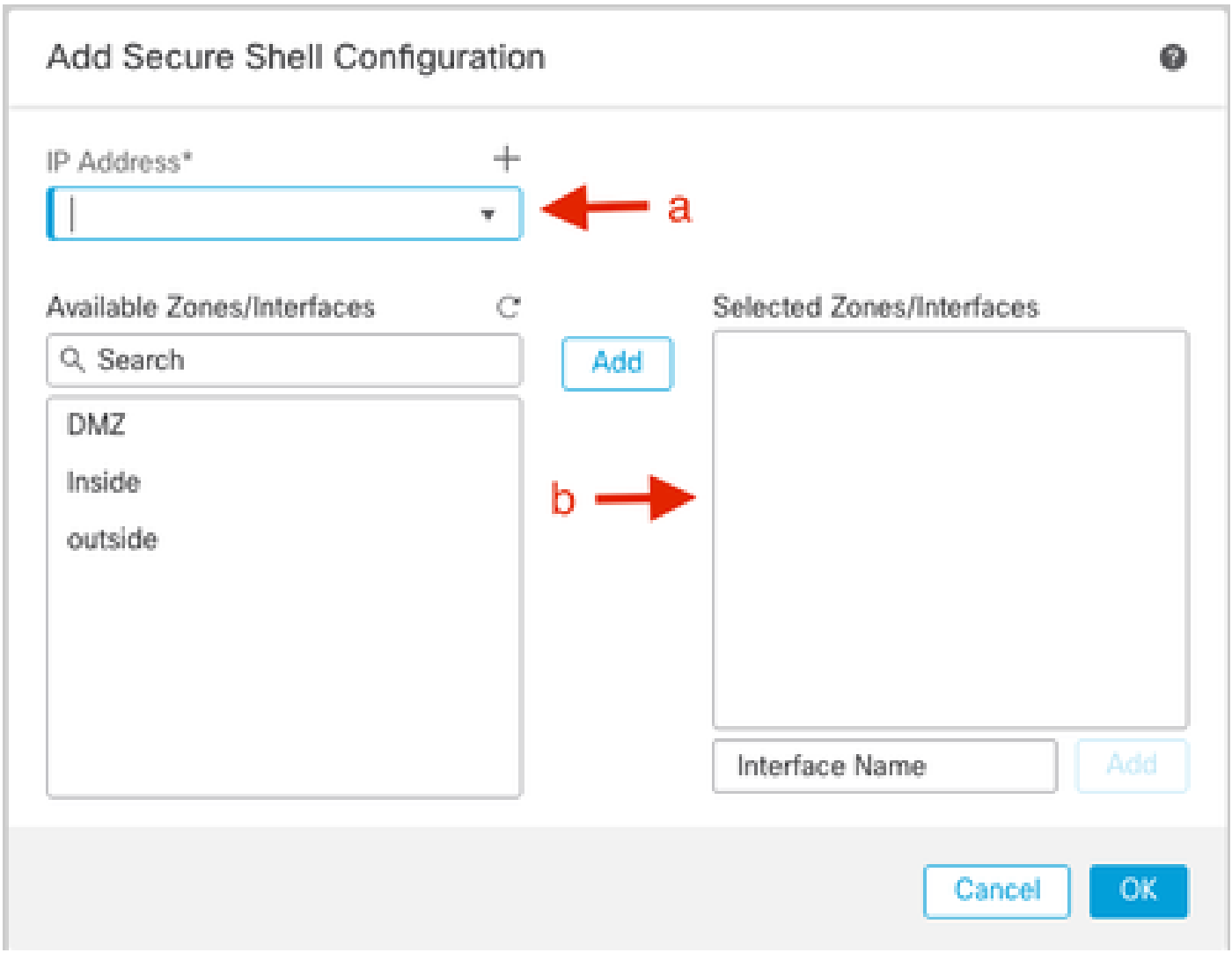
7.禁用管理中心中的管理。单击Devices > Device Management > Device > Management部分中的Edit and update the Remote Host Address IP address and(Optional)Secondary Address for threat defense，然后启用连接。

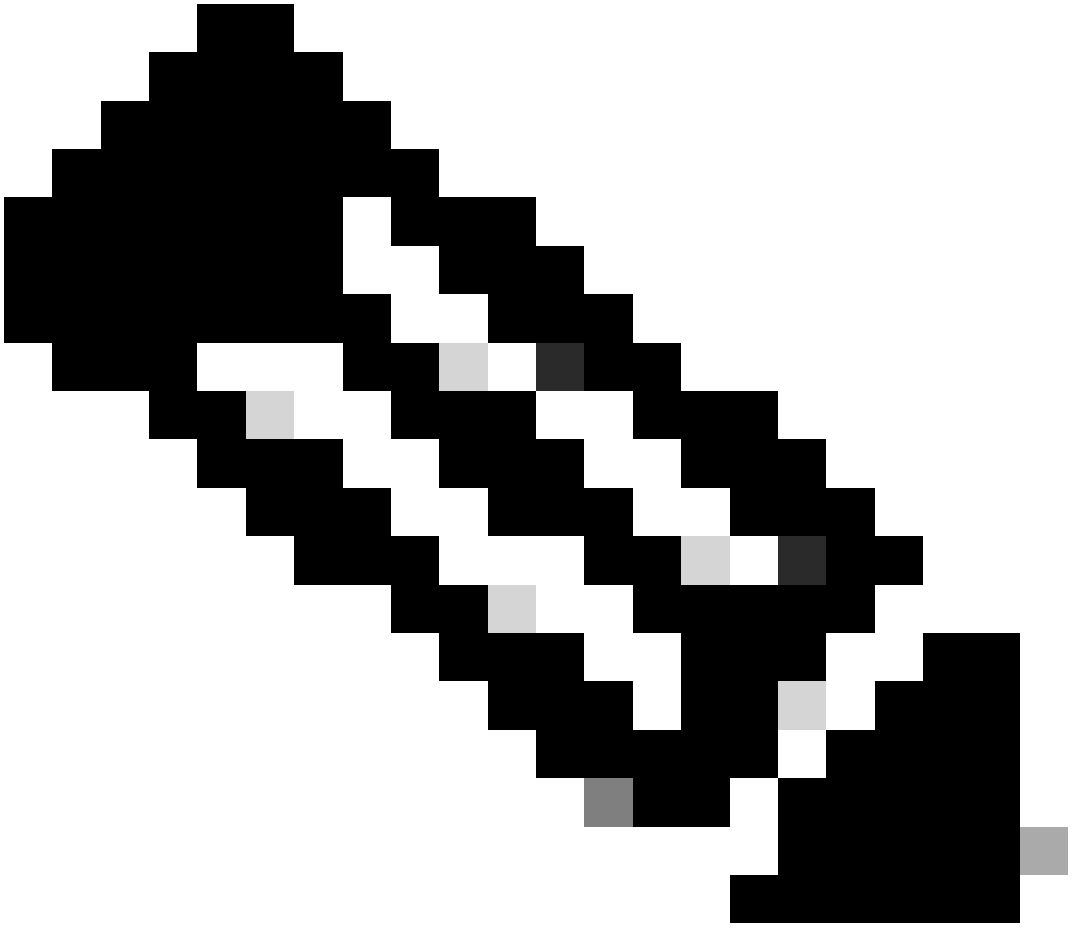


在平台设置上启用SSH

在Platform Settings(平台设置)策略中启用数据接口的SSH，并在Devices（设备）> Platform Settings（平台设置）> SSH Access(SSH访问)下将其应用到此设备。单击Add（添加）。

1. 允许进行SSH连接的主机或网络。
2. 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。
3. 单击确定。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



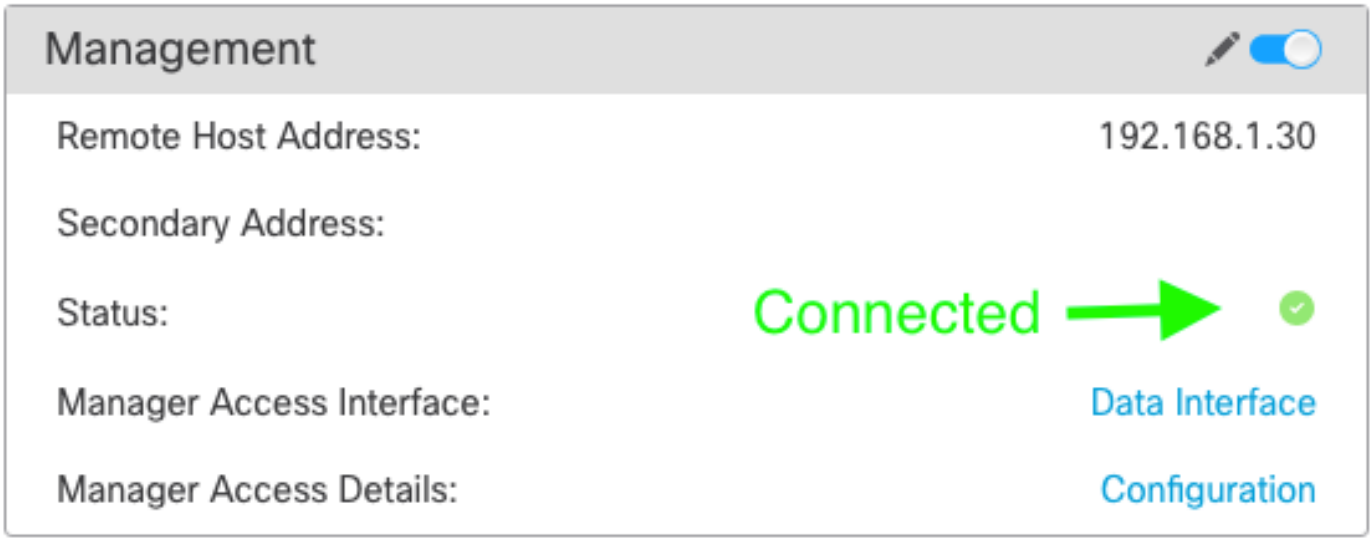
注意：默认情况下，数据接口上未启用SSH，因此，如果您希望使用SSH管理威胁防御，需要明确允许它。

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，在Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status页上检查管理连接状态。



从FTD命令行界面(CLI)进行验证

在threat defenseCLI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

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

在threat defenseCLI中，输入thesftunnel-status-briefcommand以查看管理连接状态。您还可以使用ftunnel-statuss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threat defenseCLI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
```

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）。