Konfigurieren des Manager-Zugriffs auf FTD von der Management- zur Datenschnittstelle

Inhalt

Einleitung

In diesem Dokument wird der Prozess zum Ändern des Manager-Zugriffs auf die Firepower Threat Defense (FTD) von einer Management- zu einer Datenschnittstelle beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Threat Defence
- FirePOWER Management Center

Verwendete Komponenten

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

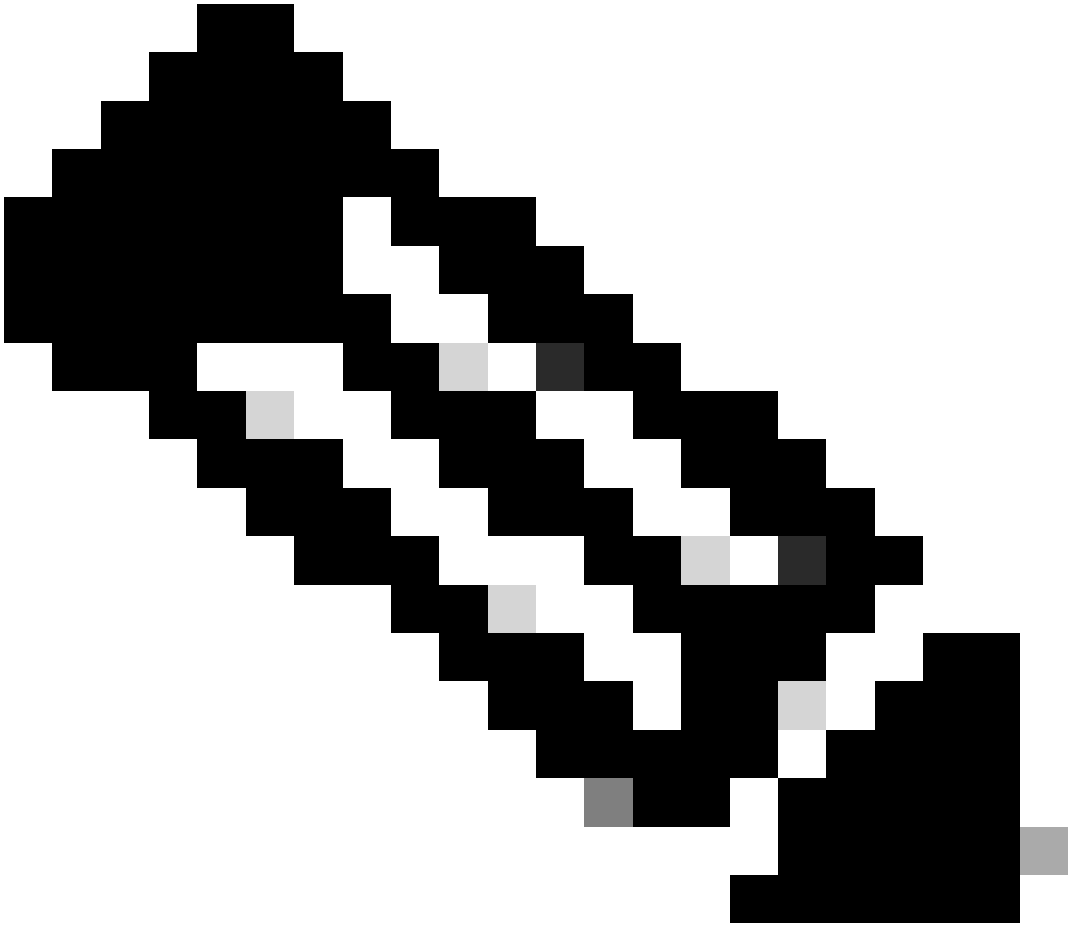
Jedes Gerät verfügt über eine dedizierte Management-Schnittstelle für die Kommunikation mit dem FMC. Sie können das Gerät optional so konfigurieren, dass es eine Datenschnittstelle für die Verwaltung anstelle der dedizierten Verwaltungsschnittstelle verwendet. Der FMC-Zugriff auf eine Datenschnittstelle ist nützlich, wenn Sie die FirePOWER-Bedrohungsabwehr von der externen Schnittstelle aus verwalten möchten oder wenn Sie kein separates Verwaltungsnetzwerk haben. Diese Änderung muss im FirePOWER Management Center (FMC) für vom FMC verwaltete FTD vorgenommen werden.

Der FMC-Zugriff über eine Datenschnittstelle hat einige Einschränkungen:

- Sie können den Manager-Zugriff nur über eine physische Datenschnittstelle aktivieren. Sie können keine Subschnittstelle oder keinen EtherChannel verwenden.
- Nur gerouteter Firewall-Modus mit gerouteter Schnittstelle.
- PPPoE wird nicht unterstützt. Wenn Ihr ISP PPPoE benötigt, müssen Sie zwischen der FirePOWER Threat Defense und dem WAN-Modem einen Router mit PPPoE-Unterstützung anordnen.
- Sie können keine separaten Schnittstellen für Management und Event Only verwenden.

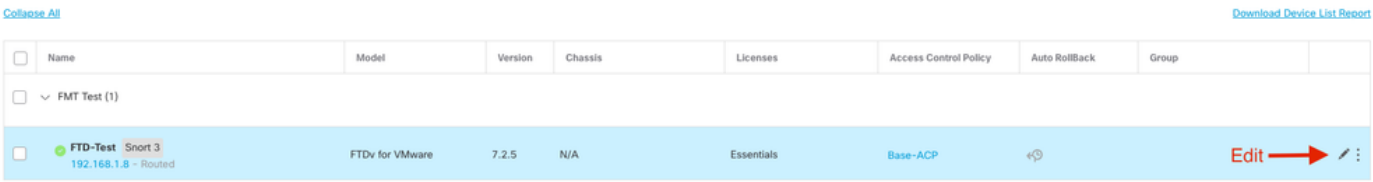
Konfigurieren

Schnittstellenmigration fortsetzen



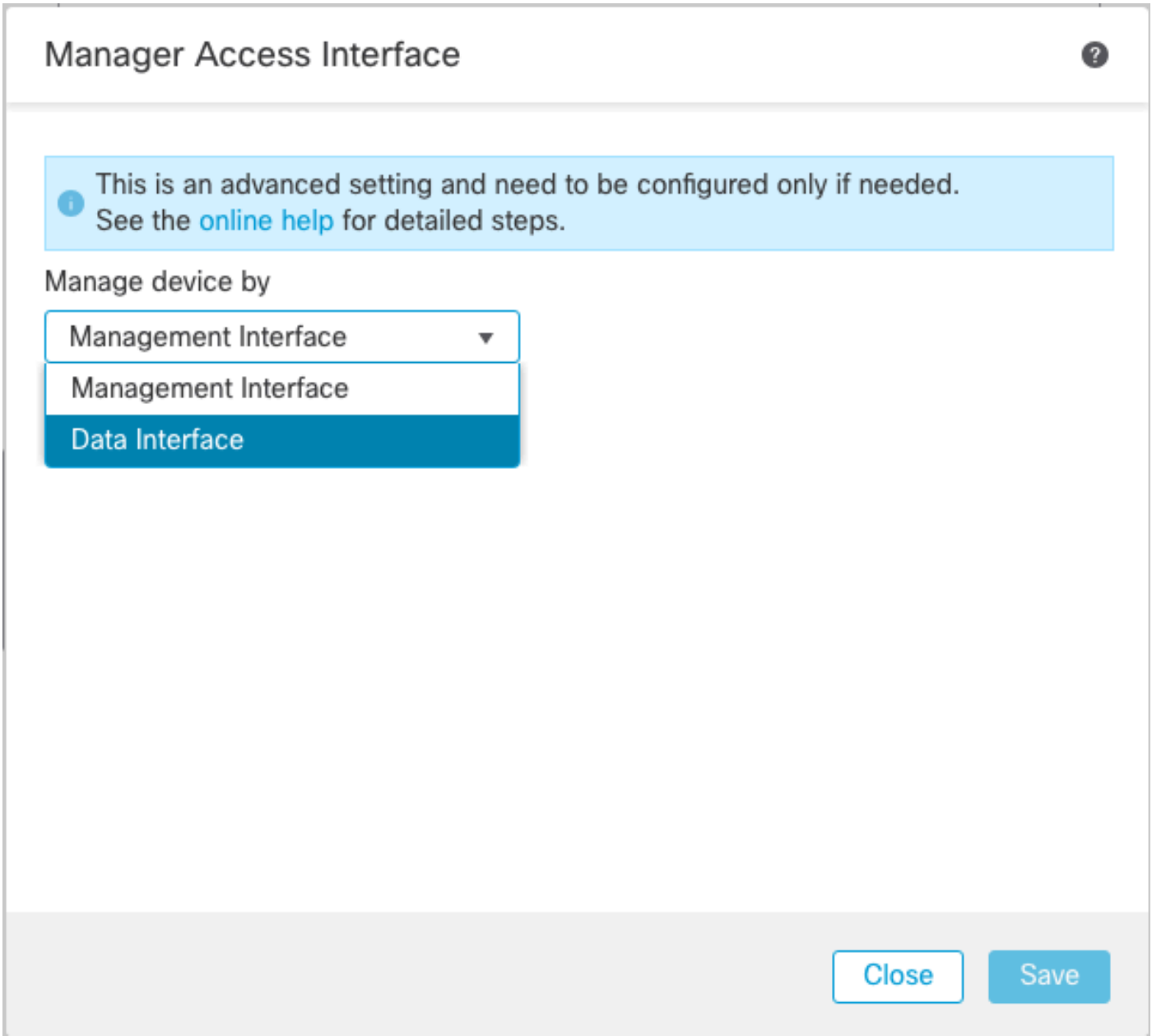
Hinweis: Es wird dringend empfohlen, über die neueste Sicherung von FTD und FMC zu verfügen, bevor Sie mit den Änderungen fortfahren.

1. Navigieren Sie zu Geräte > Geräteverwaltung, und klicken Sie für das Gerät, das Sie ändern, auf Bearbeiten.



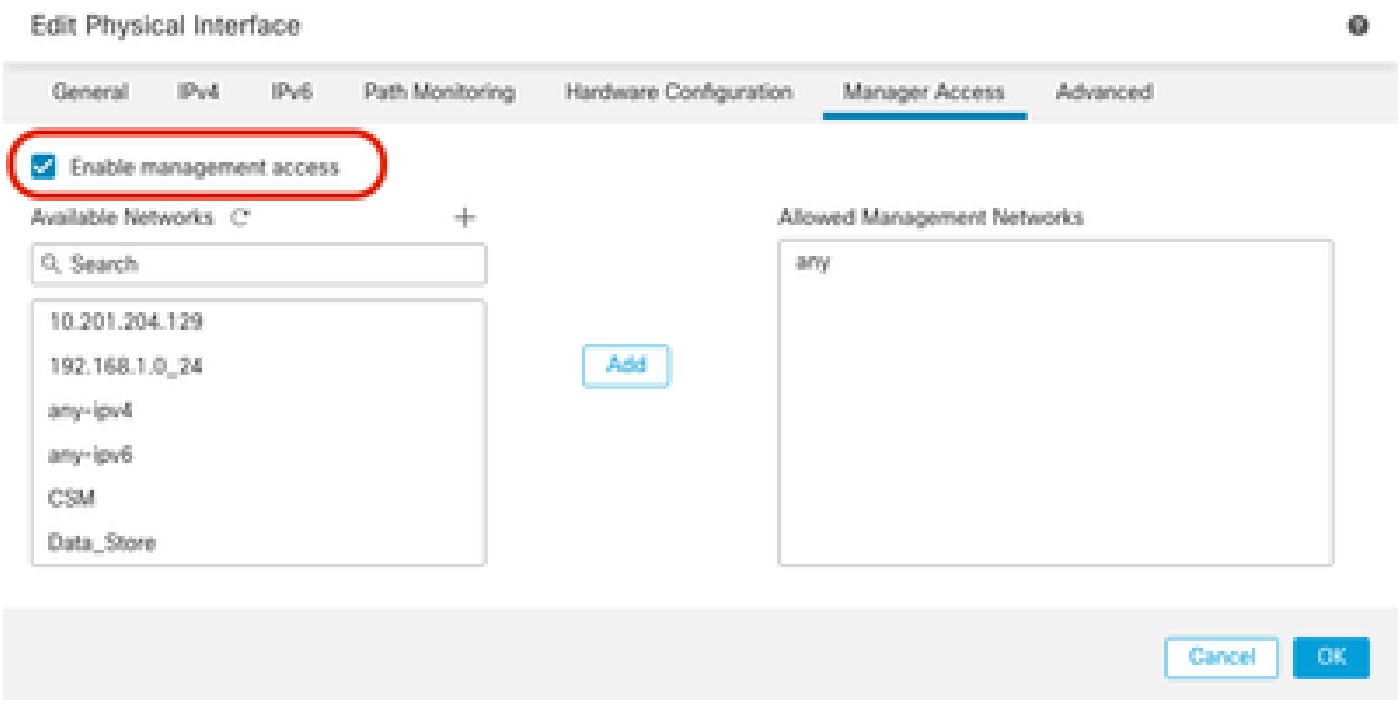
2. Gehen Sie zum Abschnitt Gerät > Verwaltung, und klicken Sie auf den Link für Manager Access Interface.

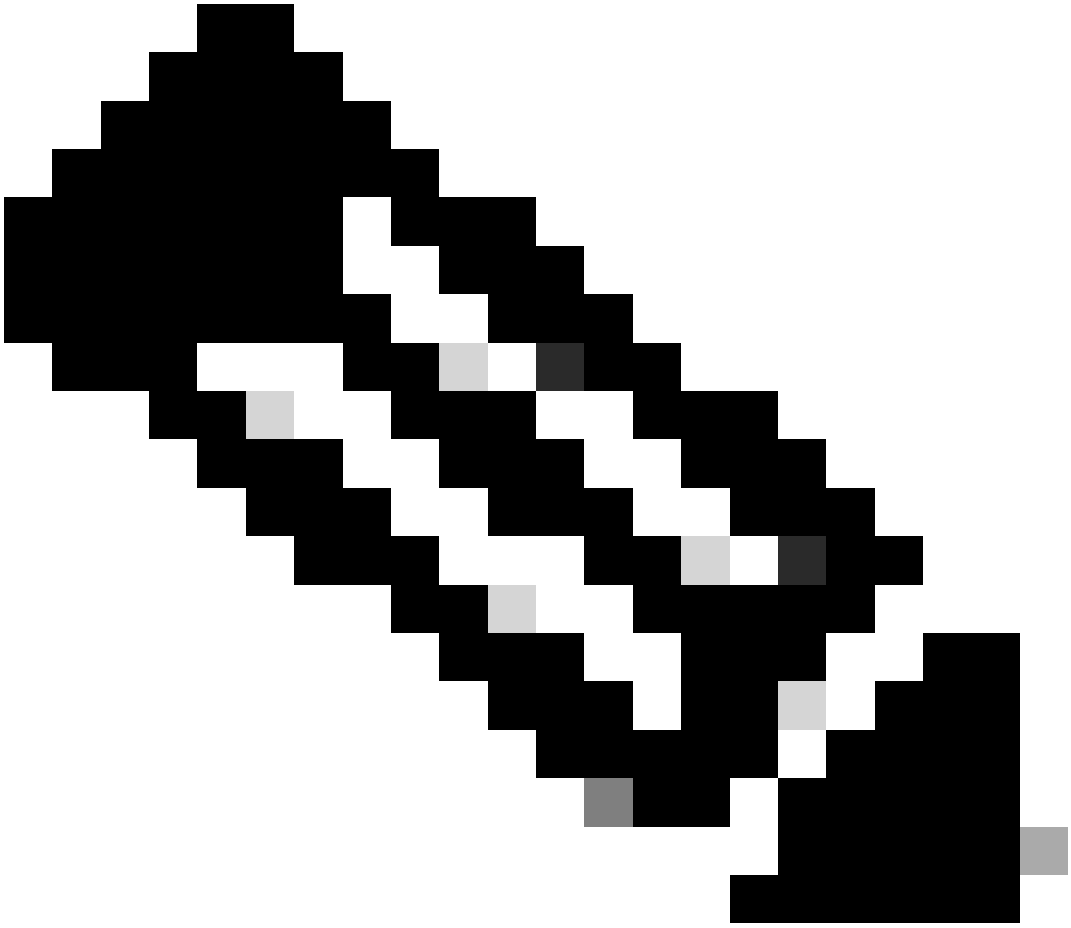
Im Feld "Manager Access Interface" (Verwaltungsschnittstelle) wird die vorhandene Verwaltungsschnittstelle angezeigt. Klicken Sie auf den Link, um den neuen Schnittstellentyp auszuwählen, d. h. die Option Datenschnittstelle in der Dropdown-Liste Gerät verwalten nach, und klicken Sie auf Speichern.



3. Sie müssen nun mit Enable management access on a data interface (Verwaltungszugriff auf einer Datenschnittstelle aktivieren) fortfahren und zu Devices (Geräte) > Device Management (Geräteverwaltung) > Interfaces (Schnittstellen) > Edit Physical Interface (Physische Schnittstelle

bearbeiten) > Manager Access (Verwaltungszugriff) navigieren.





Hinweis: (Optional) Wenn Sie eine sekundäre Schnittstelle für Redundanz verwenden, aktivieren Sie den Verwaltungszugriff für die Schnittstelle, die für Redundanzzwecke verwendet wird.

(Optional) Wenn Sie DHCP für die Schnittstelle verwenden, aktivieren Sie im Dialogfeld Devices (Geräte) > Device Management (Geräteverwaltung) > DHCP > DDNS (DHCP > DDNS) den Webtyp DDNS-Methode.

(Optional) Konfigurieren Sie DNS in einer Richtlinie für Plattformeinstellungen, und wenden Sie es auf dieses Gerät an unter Geräte > Plattformeinstellungen > DNS.

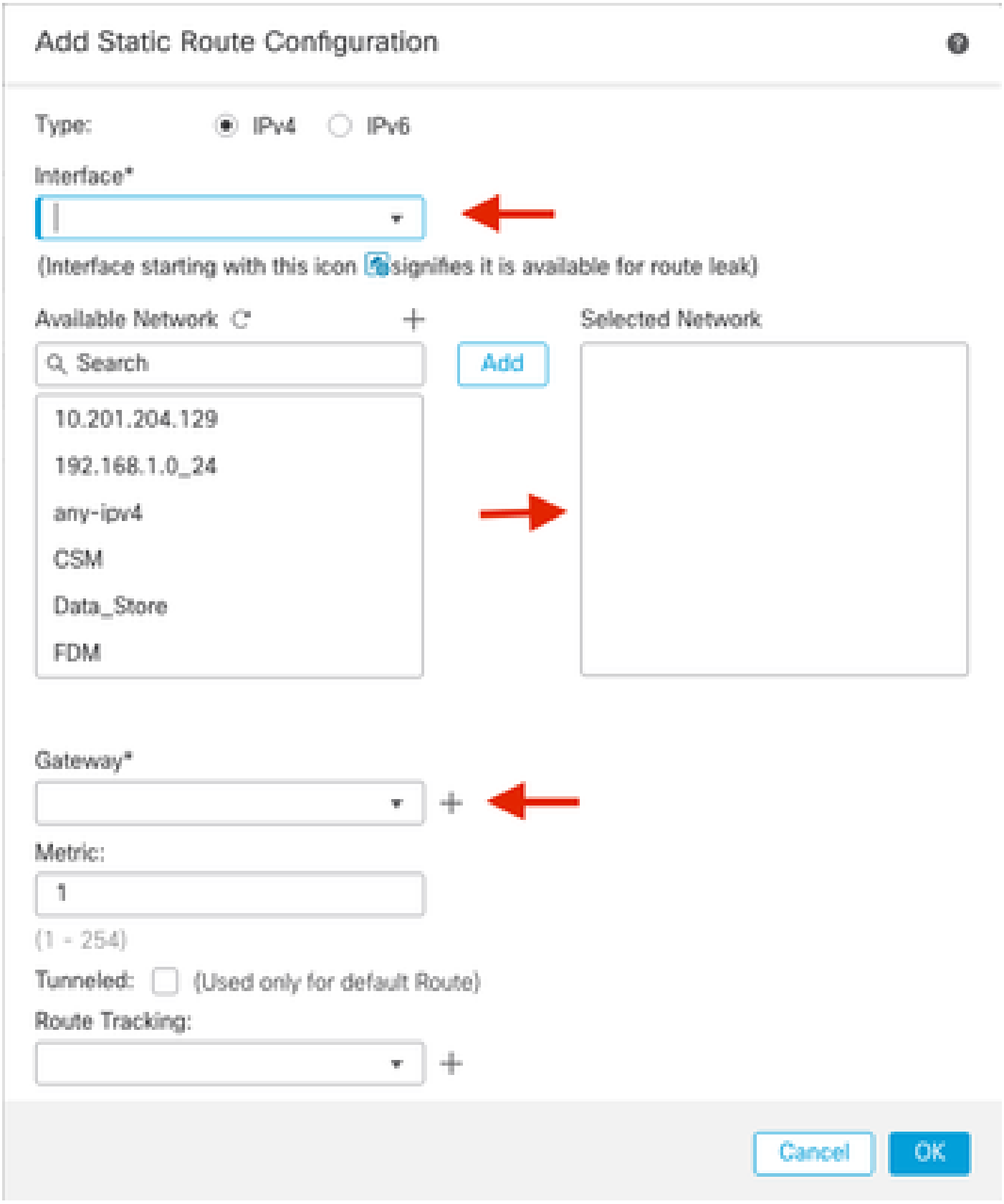
---

4. Stellen Sie sicher, dass der Bedrohungsschutz zum Verwaltungszentrum über die Datenschnittstelle weitergeleitet werden kann. Fügen Sie ggf. eine statische Route hinzu unter Devices (Geräte) > Device Management (Gerätemanagement) > Routing (Routing) > Static Route (Statische Route).

1. Klicken Sie abhängig vom hinzugefügten Typ der statischen Route auf IPv4oder IPv6.

2. Wählen Sie die Schnittstelle aus, auf die diese statische Route angewendet werden soll.
3. Wählen Sie in der Liste Available Network (Verfügbares Netzwerk) das Zielnetzwerk aus.
4. Geben Sie im Feld Gateway or IPv6 Gateway (Gateway oder IPv6-Gateway) den Gateway-Router ein, der den nächsten Hop für diese Route darstellt, oder wählen Sie ihn aus.

(Optional) Um die Verfügbarkeit der Route zu überwachen, geben Sie den Namen eines SLA-Überwachungsobjekts (Service Level Agreement), das die Überwachungsrichtlinie definiert, in das Feld Route Tracking (Routenverfolgung) ein, oder wählen Sie diesen aus.

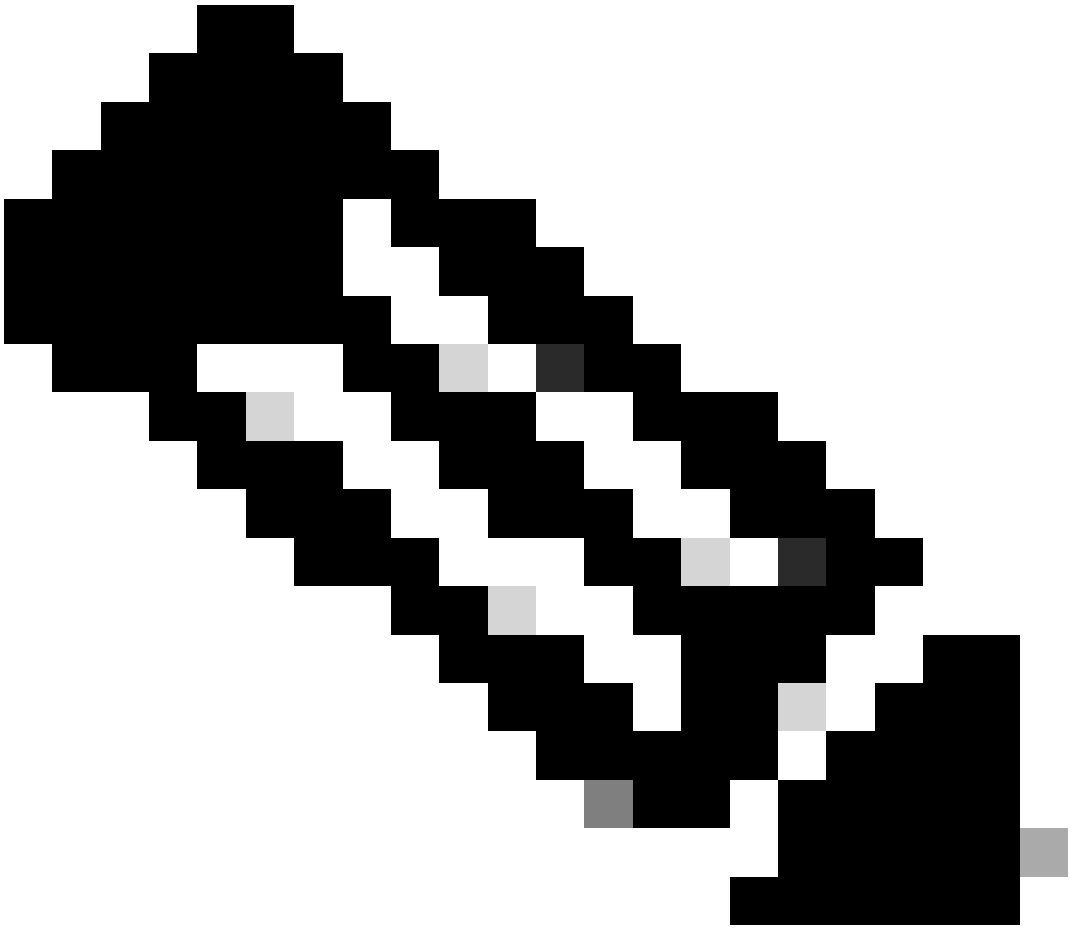


5. Stellen Sie Konfigurationsänderungen bereit. Die Konfigurationsänderungen werden jetzt über die aktuelle Management-Schnittstelle bereitgestellt.

6. Legen Sie in der FTD-CLI die Management-Schnittstelle auf eine statische IP-Adresse und das Gateway auf Datenschnittstellen fest.

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

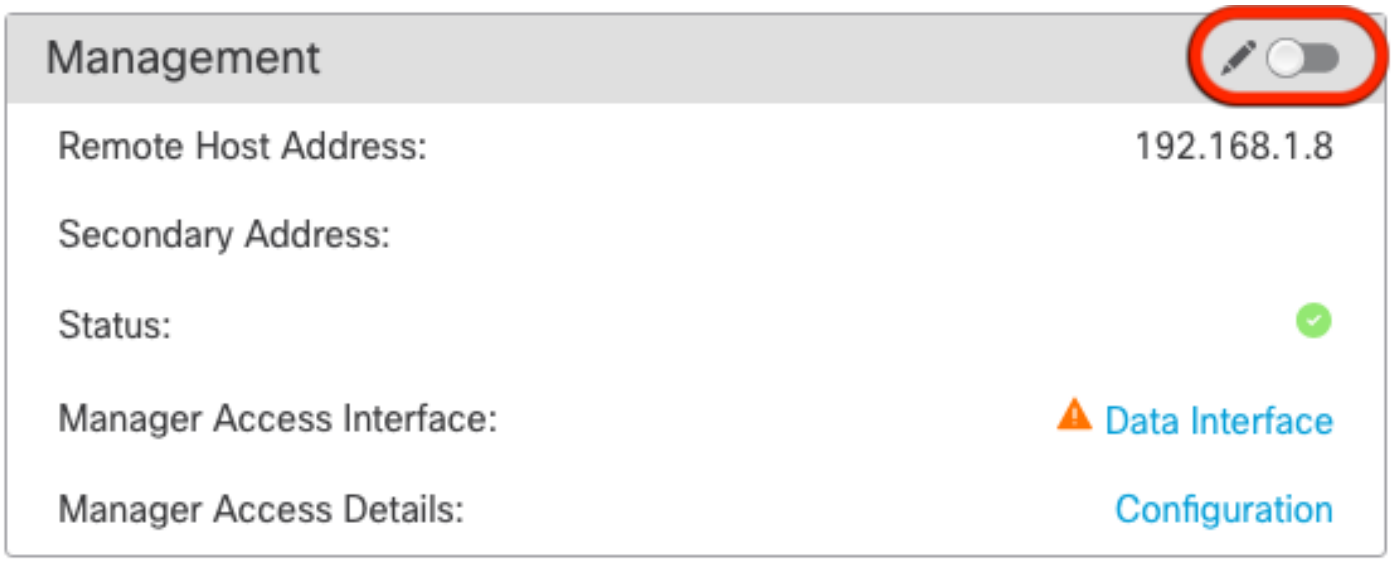
```
>
>                                  IP_ADDRESS      NETMASK         GATEWAY
> configure network ipv4 manual 192.168.1.8 255.255.255.0 data-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```



Hinweis: Sie planen zwar nicht, die Management-Schnittstelle zu verwenden, müssen aber eine statische IP-Adresse festlegen. Beispielsweise eine private Adresse, damit Sie das Gateway auf **Datenschnittstellen** setzen können. Dieses Management wird verwendet, um den Management-Datenverkehr über die Schnittstelle tap_nlp an die Datenschnittstelle weiterzuleiten.

---

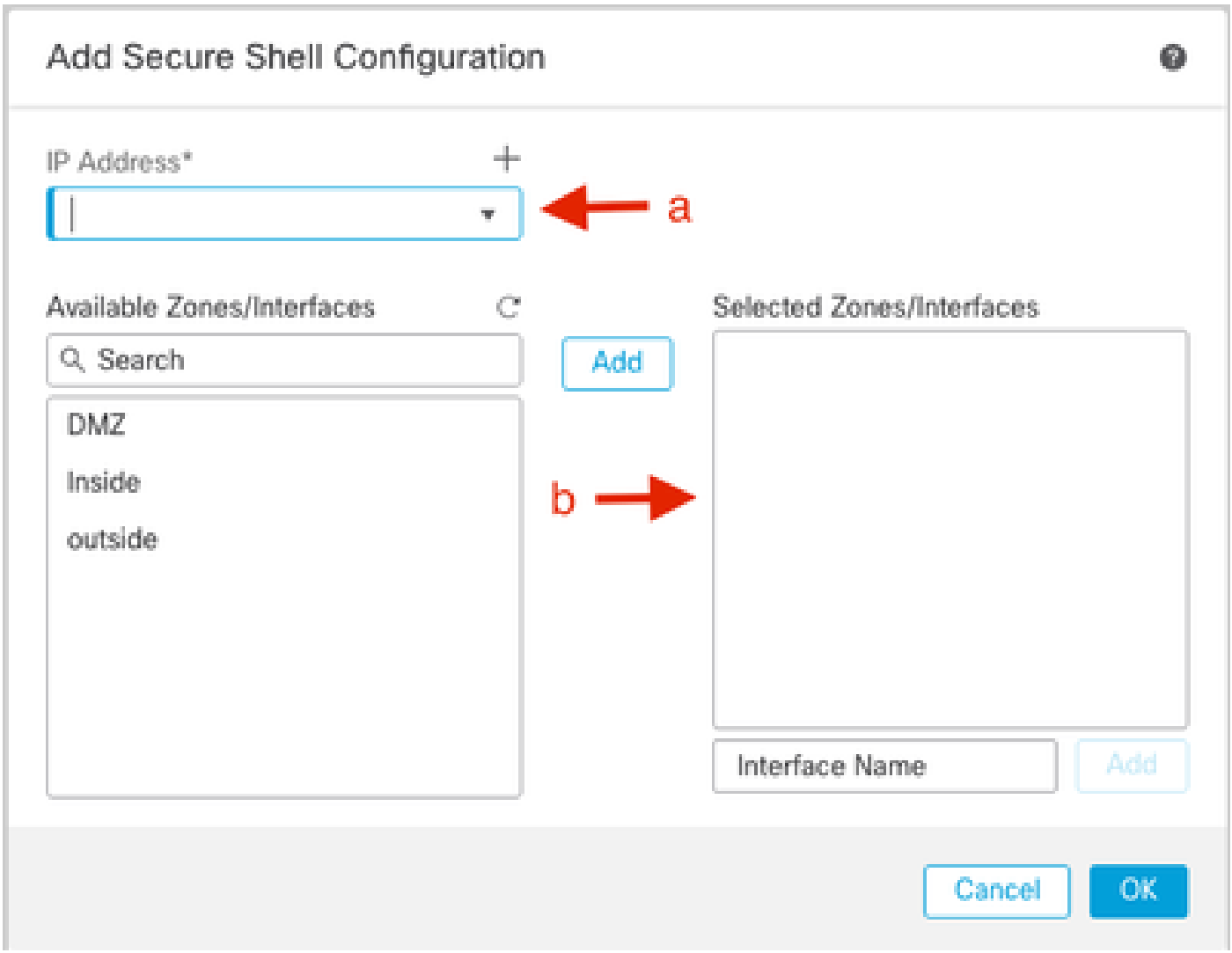
7. Deaktivieren Sie die Verwaltung im Management Center, klicken Sie auf Bearbeiten, und aktualisieren Sie die **IP-Adresse** des Remotehosts sowie die (**optionale)sekundäre Adresse** für den Schutz vor Bedrohungen in den **Abschnitten** Geräte **> Geräteverwaltung > Gerät und Verwaltung, und aktivieren Sie die Verbindung.**

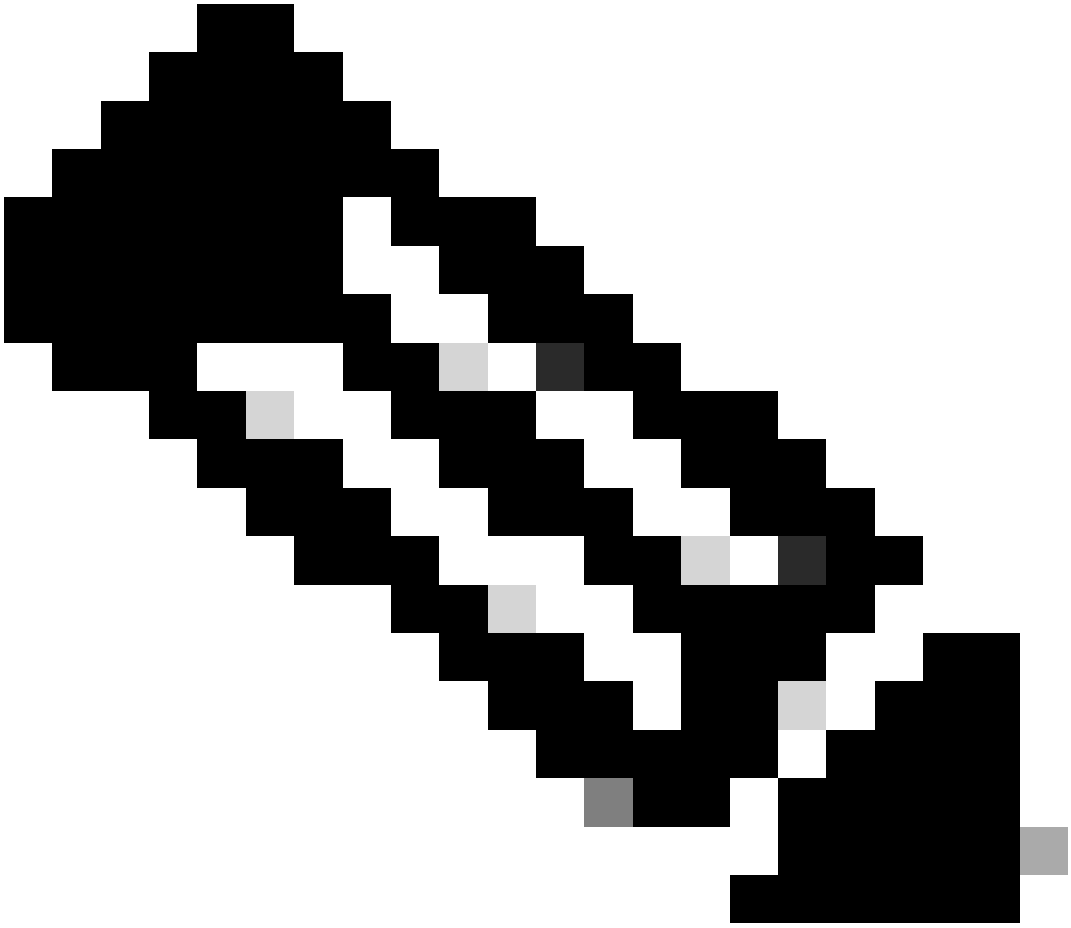


SSH auf Plattformeinstellungen aktivieren

Aktivieren Sie SSH für die Datenschnittstelle in der Richtlinie für die Plattformeinstellungen, und wenden Sie es auf dieses Gerät an unter Geräte **> Plattformeinstellungen > SSH-Zugriff.**Klicken Sie auf Hinzufügen .

- Die Hosts oder Netzwerke, die SSH-Verbindungen herstellen dürfen.
- Fügen Sie die Zonen hinzu, die die Schnittstellen enthalten, zu denen SSH-Verbindungen zugelassen werden sollen. Bei Schnittstellen, die sich nicht in einer Zone befinden, können Sie den **Schnittstellennamen** in das Feld **Ausgewählte Zonen/Schnittstellen** eingeben und auf **Hinzufügen** klicken.
- Klicken Sie auf **OK**. **Bereitstellen** der Änderungen


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



Hinweis: SSH ist auf den Datenschnittstellen nicht standardmäßig aktiviert. Wenn Sie die Bedrohungsabwehr mit SSH verwalten möchten, müssen Sie dies explizit zulassen.

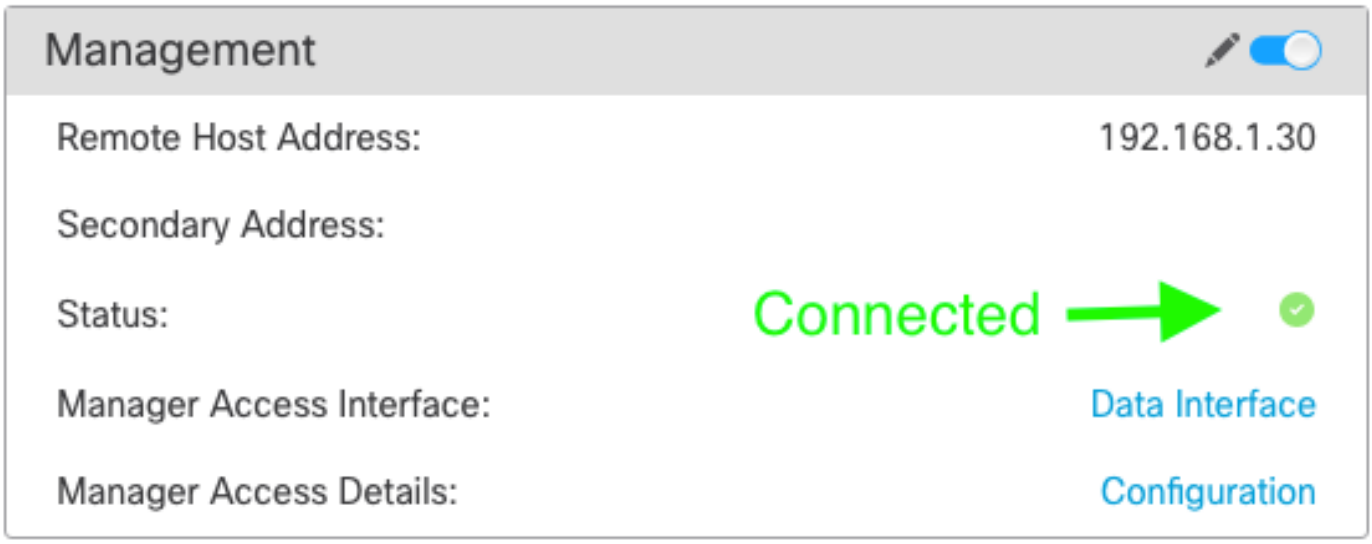
Überprüfung

Stellen Sie sicher, dass die Managementverbindung über die Datenschnittstelle hergestellt wird.

Von der grafischen Benutzeroberfläche (GUI) des FMC überprüfen

Überprüfen Sie im Management Center den Status der Management-Verbindung auf der **Seite** Devices (Geräte) **> Device Management (Geräteverwaltung) > Device (Gerät) > Management (Verwaltung) > Manager Access (Manager-Zugriff) - Configuration Details**

(Konfigurationsdetails) > Connection Status (Verbindungsstatus).



Überprüfen von der FTD-Befehlszeilenschnittstelle (CLI)

Geben Sie in der Threat DefenseCLI den Befehl **ftunnel-status-**brief ein, um den Management-Verbindungsstatus anzuzeigen.

```
>
> 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
```

Der Status zeigt eine erfolgreiche Verbindung für eine Datenschnittstelle an und zeigt die interne Schnittstelle tap_nlp an.

Fehlerbehebung

Überprüfen Sie im Management Center den Status der Management-Verbindung auf der **Seite** Devices (Geräte) **> Device Management (Geräteverwaltung) > Device (Gerät) > Management (Verwaltung) > Manager Access (Manager-Zugriff) - Configuration Details (Konfigurationsdetails) > Connection Status (Verbindungsstatus).**

Geben Sie in der Threat DefenseCLI den Befehl **ftunnel-status-**brief ein, um den Management-Verbindungsstatus anzuzeigen. Sie können auch **ftunnel-**statustzur Anzeige vollständiger Informationen verwenden.

Management-Verbindungsstatus

Arbeitsszenario

```
> 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
```

Nicht-Arbeitsszenario

```
> 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
```

Überprüfen der Netzwerkinformationen

Zeigen Sie in der CLI zur Bedrohungsabwehr die Netzwerkeinstellungen der Management- und Manager-Zugriffsschnittstelle an:

> 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
```

Hinweis: Dieser Befehl zeigt nicht den aktuellen Status der Verwaltungsverbindung an.

Netzwerkverbindungen überprüfen

Pingen des Management Center

Verwenden Sie in der Threat DefenseCLI den Befehl, um das Management Center über die Datenschnittstellen zu pingen:

> 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
```

Verwenden Sie in der Threat DefenseCLI den Befehl, um das Management Center von der Management-Schnittstelle aus zu pingen, die über die Rückwandplatine zu den Datenschnittstellen routet:

> 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
```

Schnittstellenstatus, Statistiken und Paketanzahl überprüfen

Informationen zur internen Backplane-Schnittstelle nlp_int_tap finden Sie in der CLI Threat Defense:

> Schnittstellendetails anzeigen

```
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
```

Route auf FTD validieren, um FMC zu erreichen

Überprüfen Sie in der Threat DefenseCLI, ob die Standardroute (S*) hinzugefügt wurde und ob interne NAT-Regeln für die Management-Schnittstelle (nlp_int_tap) vorhanden sind.

> Route anzeigen

```
> 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
```

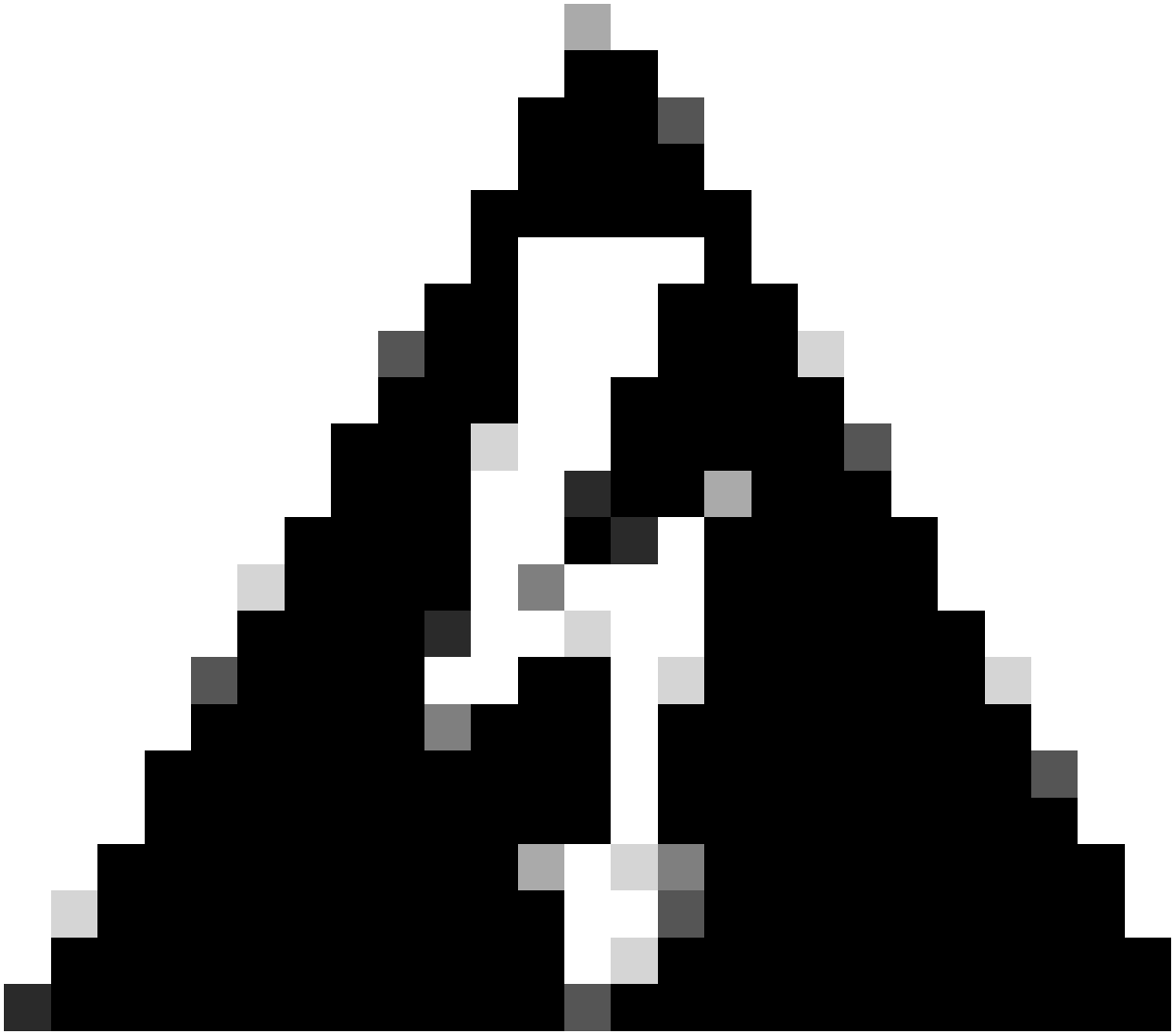
> nat anzeigen

```
> 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
```

Sftunnel- und Verbindungsstatistiken überprüfen

> show running-config sftunnel

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



Warnung: Unterlassen Sie während des gesamten Prozesses der Änderung des Managerzugriffs das Löschen des Managers auf der FTD oder das Aufheben der Registrierung/Erzwingen des Löschens der FTD vom FMC.

Zugehörige Informationen

- Konfiguration von DNS over Plattform-Einstellungen
- Konfigurieren des Managementzugriffs auf FTD (HTTPS und SSH) über FMC

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.