Bereitstellung einer redundanten Datenschnittstelle in Azure FTD Verwaltet von CD-FMC

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration einer von cdFMC verwalteten virtuellen FTD zur Verwendung der redundanten Manager-Zugriffsdaten-Schnittstellenfunktion beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Secure Firewall Management Center
- Cisco Defense Orchestrator

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Firewall Management Center in der Cloud
- Virtual Secure Firewall Threat Defense Version 7.3.1, gehostet in Azure Cloud.

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.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- Jede physische Appliance, auf der Firepower Threat Defense Version 7.3.0 oder höher ausgeführt werden kann.

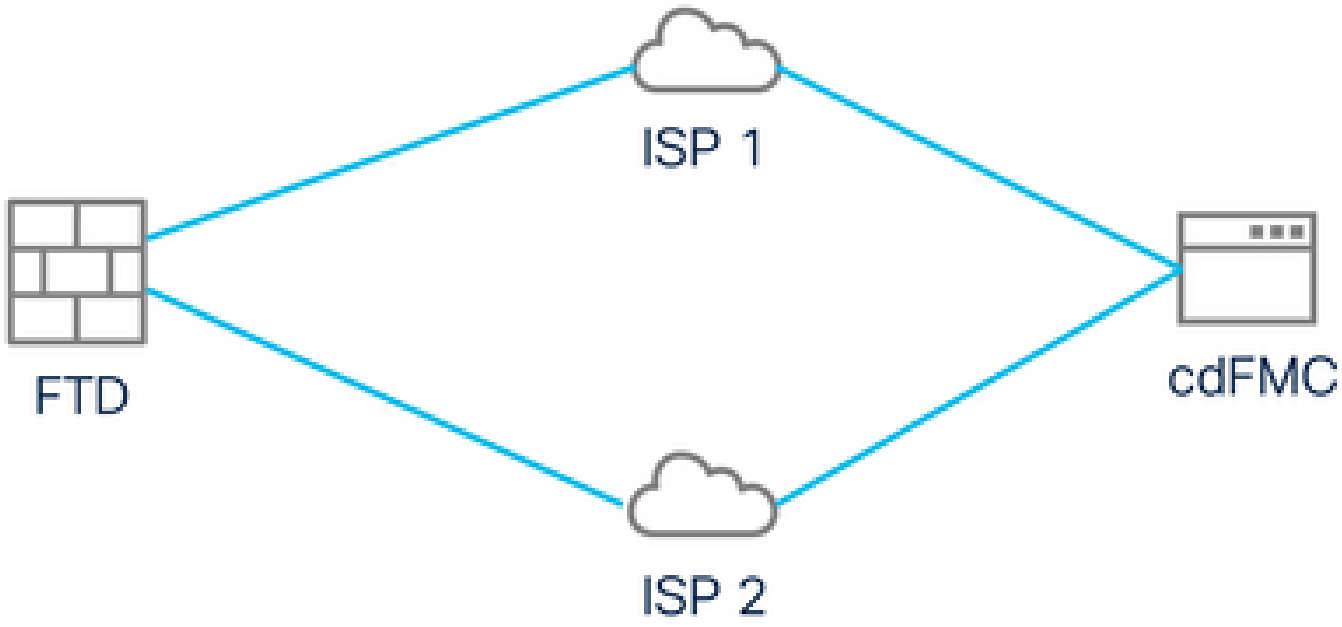
Hintergrundinformationen

In diesem Dokument werden die Schritte zur Konfiguration und Verifizierung eines von cdFMC verwalteten vFTD zur Verwendung von zwei Datenschnittstellen für Verwaltungszwecke beschrieben. Diese Funktion ist häufig nützlich, wenn Kunden eine zweite Datenschnittstelle benötigen, um ihre FTD über das Internet mit einem zweiten ISP zu verwalten. Standardmäßig führt der FTD einen Round-Robin-Lastenausgleich für den Managementverkehr zwischen beiden Schnittstellen durch. Dieser Vorgang kann wie in diesem Dokument beschrieben zu einer Active/Backup-Bereitstellung geändert werden.

Eine redundante Datenschnittstelle für die Verwaltungsfunktion wurde in Secure Firewall Threat Defense Version 7.3.0 eingeführt. Es wird davon ausgegangen, dass vFTD auf einen Namensserver zugreifen kann, der URLs für den CDO-Zugriff auflösen kann.

Konfiguration

Netzwerkdiagramm



Netzwerkdiagramm

Konfigurieren einer Datenschnittstelle für den Verwaltungszugriff

Melden Sie sich über die Konsole beim Gerät an, und konfigurieren Sie eine der Datenschnittstellen für den Verwaltungszugriff mit dem Befehl configure network management-data-interface:

<#root>

>

configure network management-data-interface

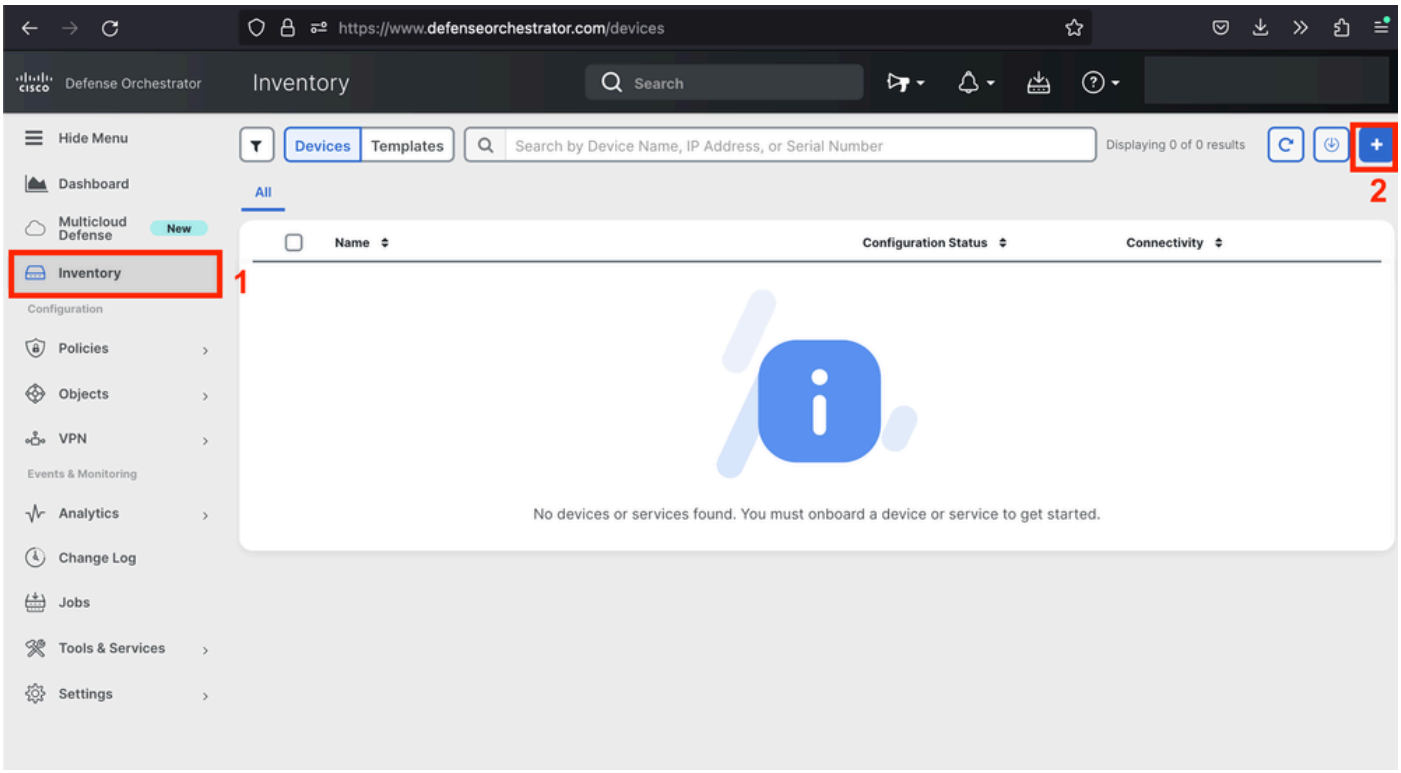
```
Note: The Management default route will be changed to route through the data interfaces. If you are conn
interface with SSH, your connection may drop. You must reconnect using the console port.

Data interface to use for management:

GigabitEthernet0/0


Specify a name for the interface [outside]:

outside-1


IP address (manual / dhcp) [dhcp]:

manual


IPv4/IPv6 address:

10.6.2.4


Netmask/IPv6 Prefix:

 255.255.255.0


Default Gateway:

10.6.2.1
```

Beachten Sie, dass die ursprüngliche Management-Schnittstelle nicht für die Verwendung von DHCP konfiguriert werden kann. Dies können Sie mit dem Befehl show network überprüfen.

FTD mit CDO integriert

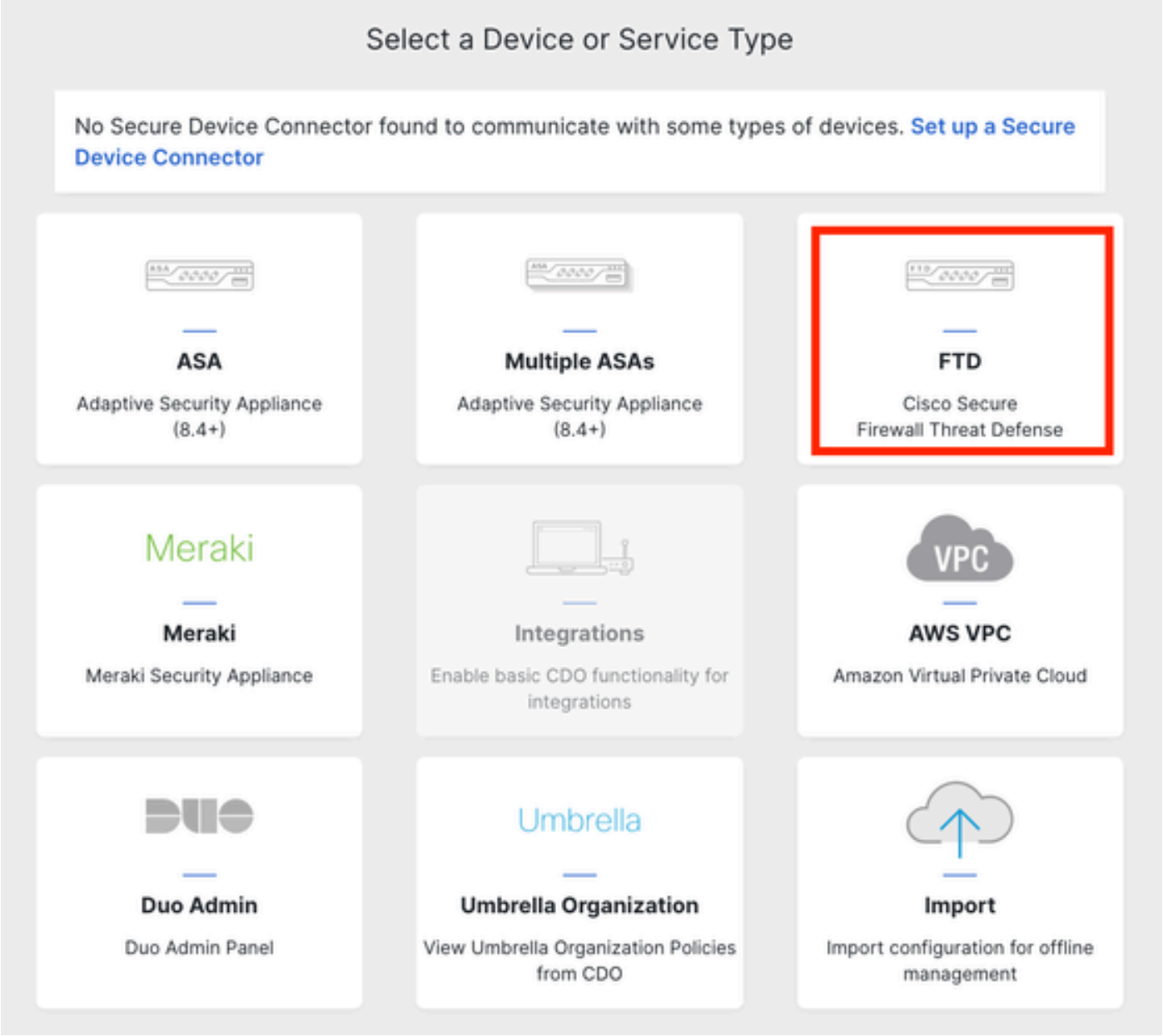
Dieser Prozess integriert Azure FTD mit CDO, sodass es von einem Cloud-basierten FMC verwaltet werden kann. Der Prozess verwendet einen CLI-Registrierungsschlüssel. Dies ist von Vorteil, wenn Ihrem Gerät eine IP-Adresse über DHCP zugewiesen wurde. Andere Onboarding-Methoden wie die Log-Touch-Bereitstellung und die Seriennummer werden nur auf Firepower 1000-, Firepower 2100- oder Secure Firewall 3100-Plattformen unterstützt.

Schritt 1: Navigieren Sie im CDO-Portal zu Inventory (Bestand), und klicken Sie dann auf Onboard (Integrierte Option):



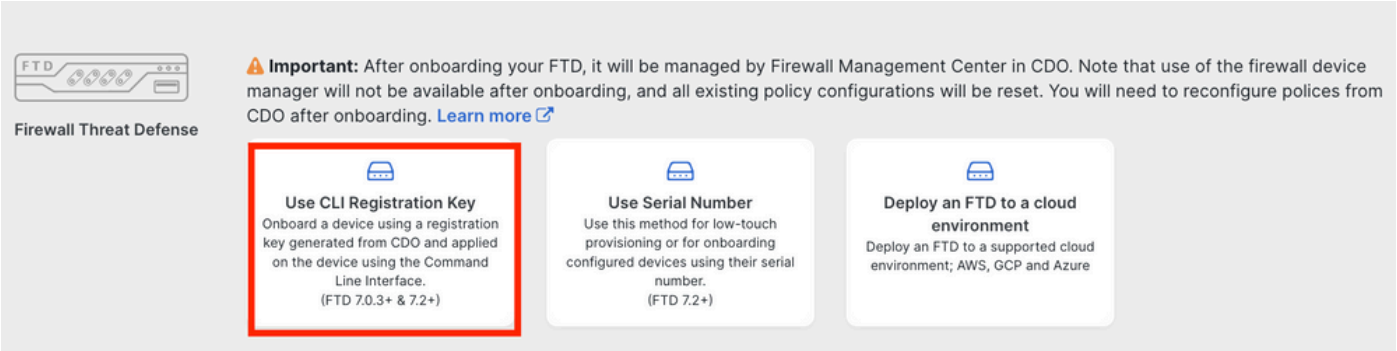
Inventar-Seite

Schritt 2. Klicken Sie in die FTD-Kachel:



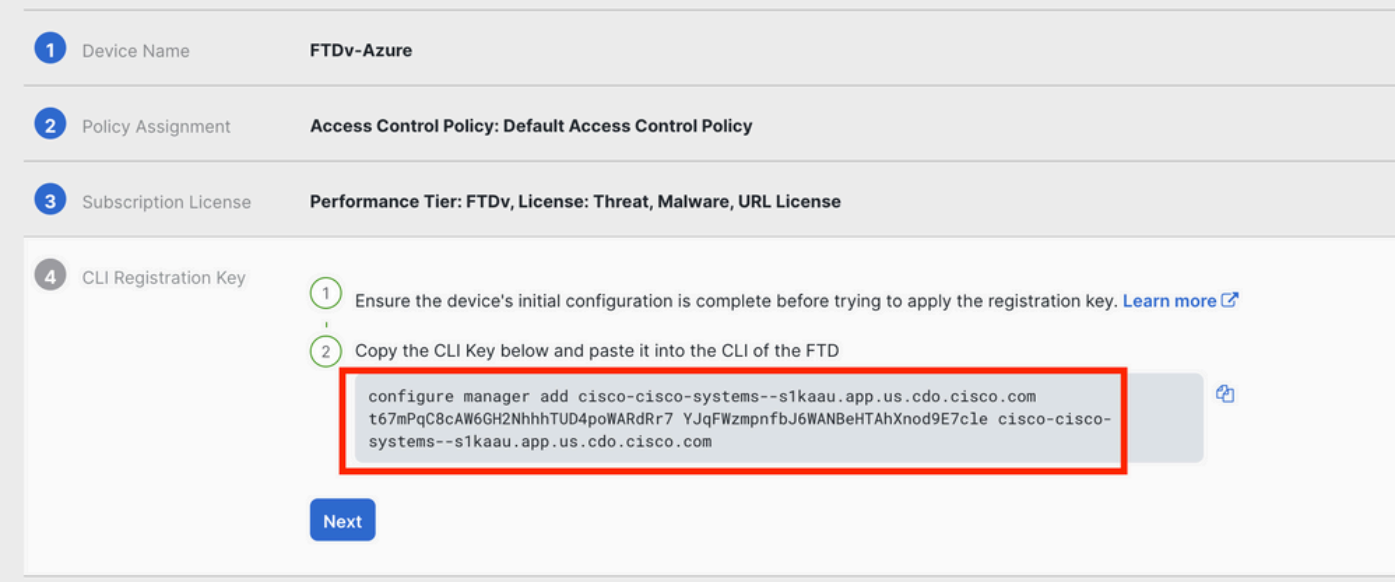
Integration der FTD

Schritt 3. Wählen Sie die Option CLI-Registrierungsschlüssel verwenden:

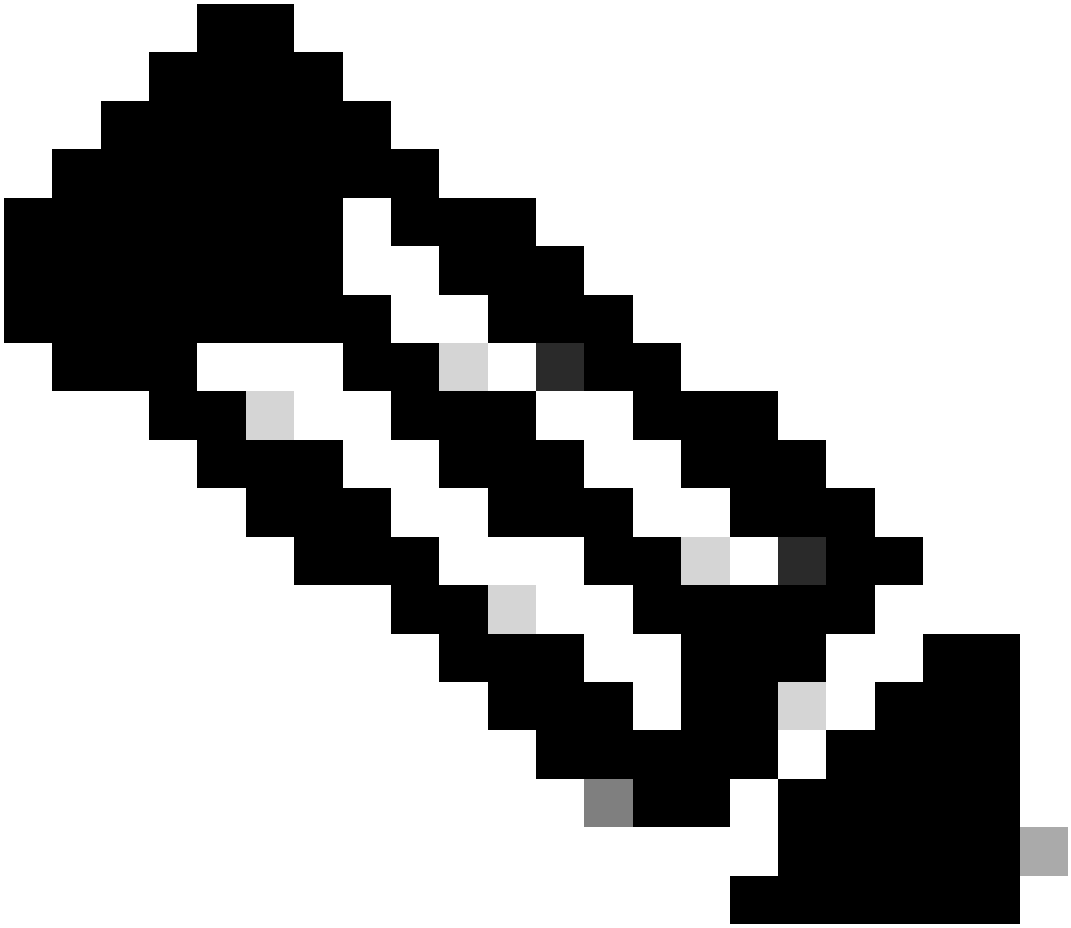


CLI-Registrierungsschlüssel verwenden

Schritt 4: Kopieren Sie den CLI-Schlüssel, beginnend mit dem Befehl configure manager:



Befehl "Configure Manager kopieren"



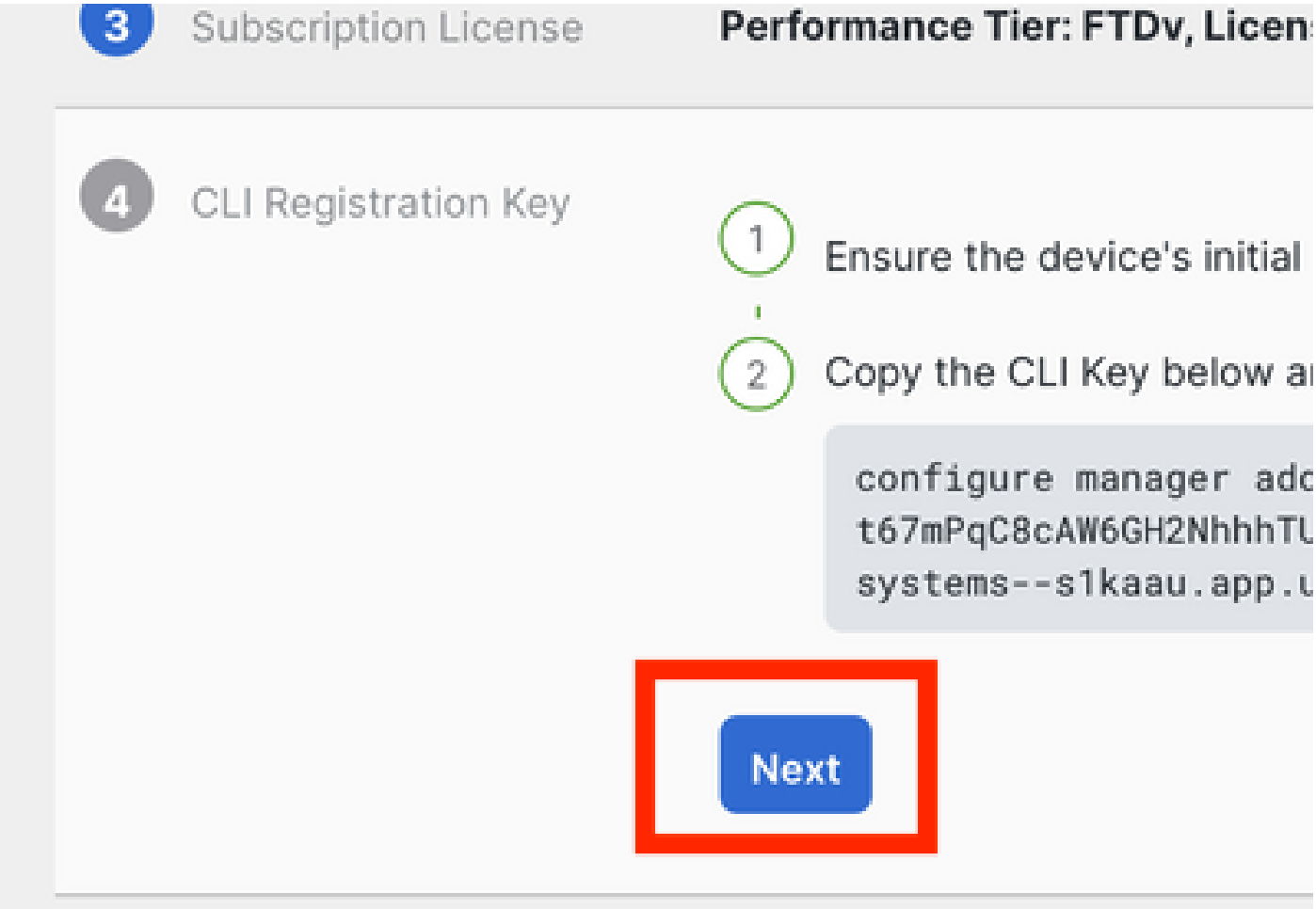
Hinweis: Der CLI-Schlüssel entspricht dem Format, das bei der Registrierung von FTDs

mit lokalen FMCs verwendet wird. Hier können Sie eine NAT-ID konfigurieren, um die Registrierung zu ermöglichen, wenn sich Ihr verwaltetes Gerät hinter einem NAT-Gerät befindet: configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>

Schritt 5: Fügen Sie den Befehl in die FTD-CLI ein. Sie müssen diese Nachricht erhalten, wenn die Kommunikation erfolgreich war:

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

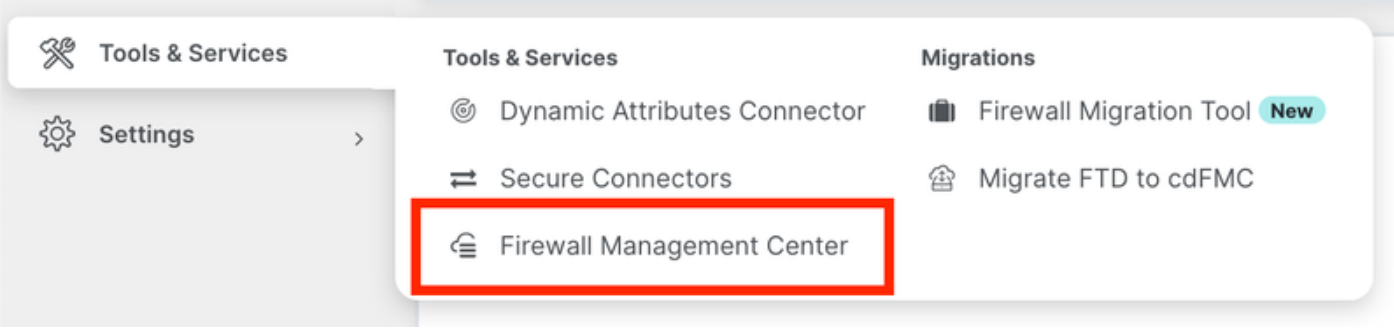
Schritt 6: Kehren Sie zum CDO zurück, und klicken Sie auf Weiter:



Klicken Sie auf Next (Weiter).

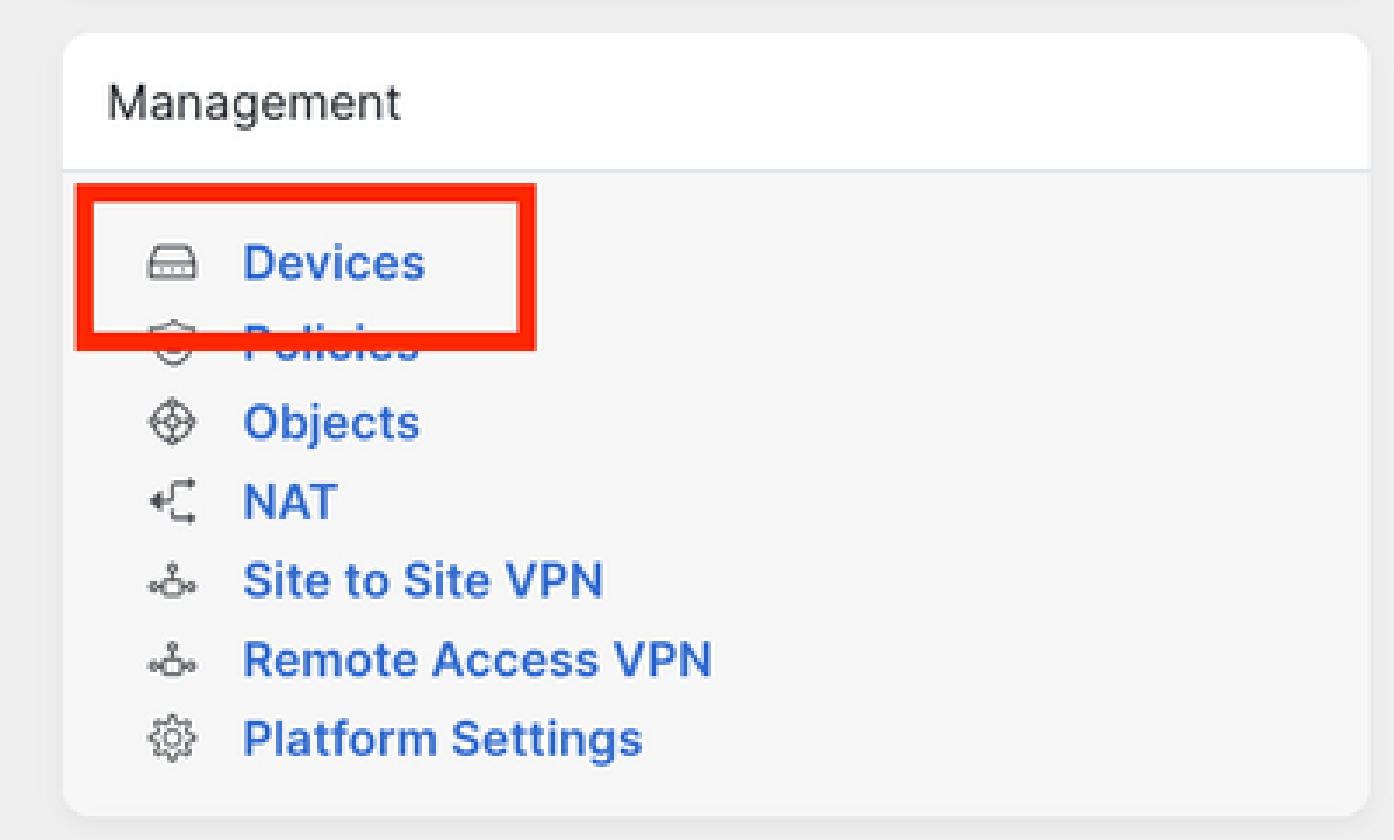
CDO setzt den Anmeldeprozess fort, und es wird eine Meldung angezeigt, die darauf hinweist, dass der Vorgang sehr lange dauern wird. Sie können den Status des Registrierungsprozesses überprüfen, indem Sie auf der Seite "Services" auf den Link Geräte klicken.

Schritt 7. Zugriff auf Ihr FMC über die Seite Tools & Services.



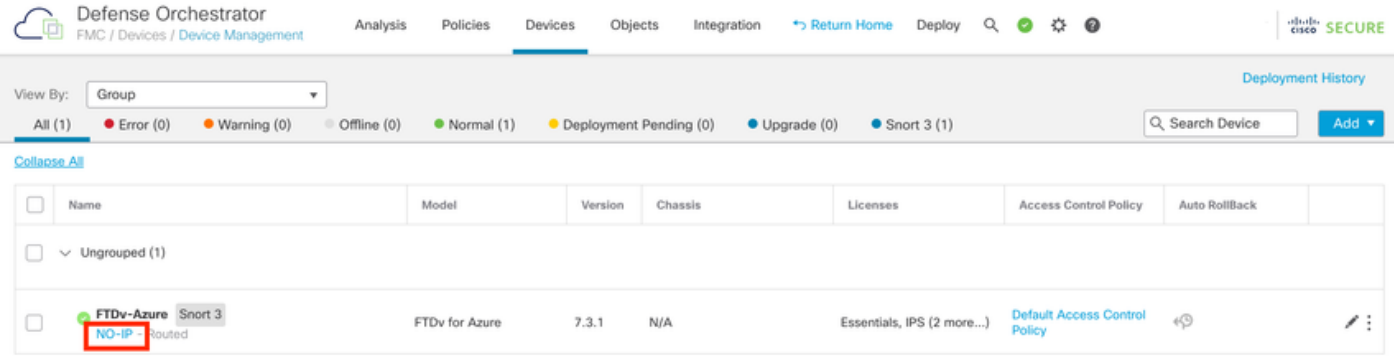
Zugriff auf das cdFMC

Klicken Sie auf den Link Geräte.



Geräte anklicken

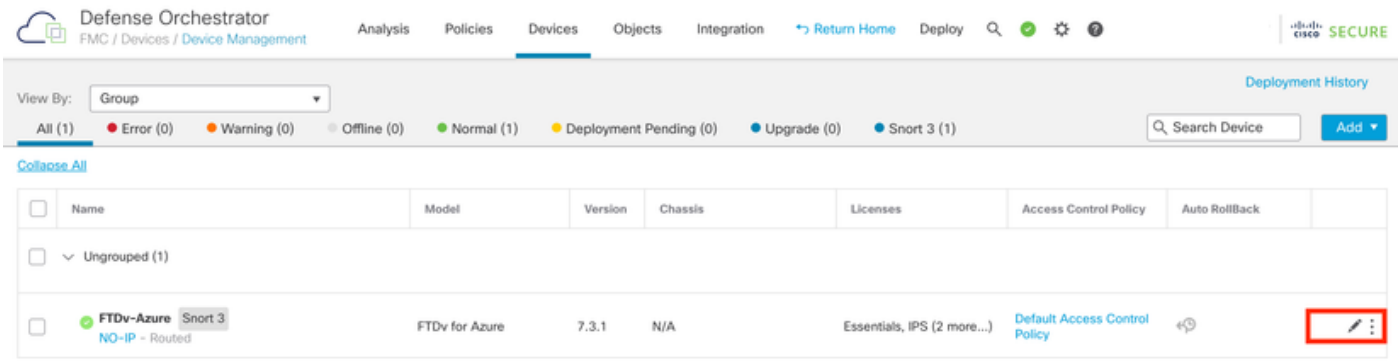
Ihr FTD ist nun in CDO integriert und kann vom Cloud-basierten FMC verwaltet werden. Beachten Sie im nächsten Bild, dass unter dem Gerätenamen eine NO-IP aufgeführt ist. Dies wird bei einem Onboarding-Prozess mit einem CLI-Registrierungsschlüssel erwartet.



Konfigurieren einer redundanten Datenschnittstelle für den Manager-Zugriff

Bei diesem Prozess wird eine zweite Datenschnittstelle für den Managementzugriff zugewiesen.

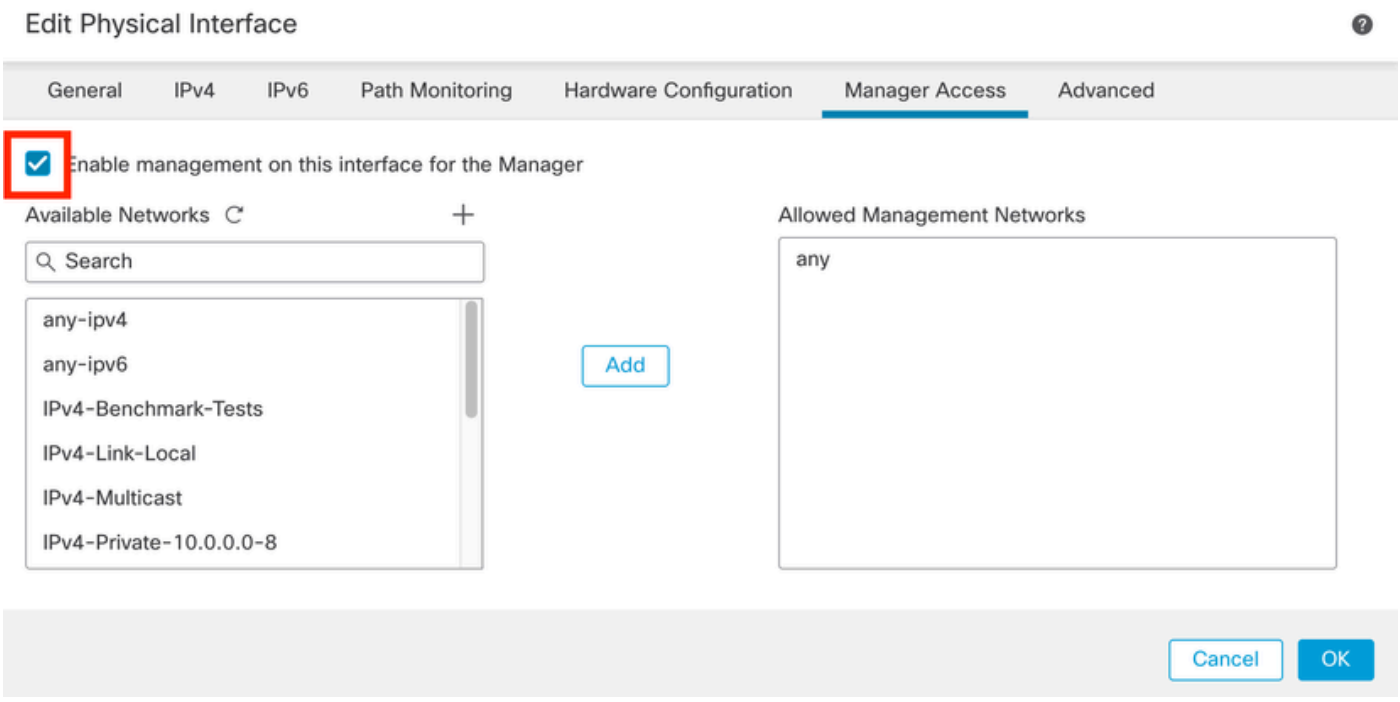
Schritt 1: Klicken Sie auf der Registerkarte Geräte auf das Bleistiftsymbol, um den FTD-Bearbeitungsmodus aufzurufen:



FTD bearbeiten

Schritt 2: Bearbeiten Sie auf der Registerkarte Interface (Schnittstelle) die Schnittstelle, die als redundante Management-Schnittstelle zugewiesen wird. Falls dies zuvor nicht der Fall war, konfigurieren Sie einen Schnittstellennamen und eine IP-Adresse.

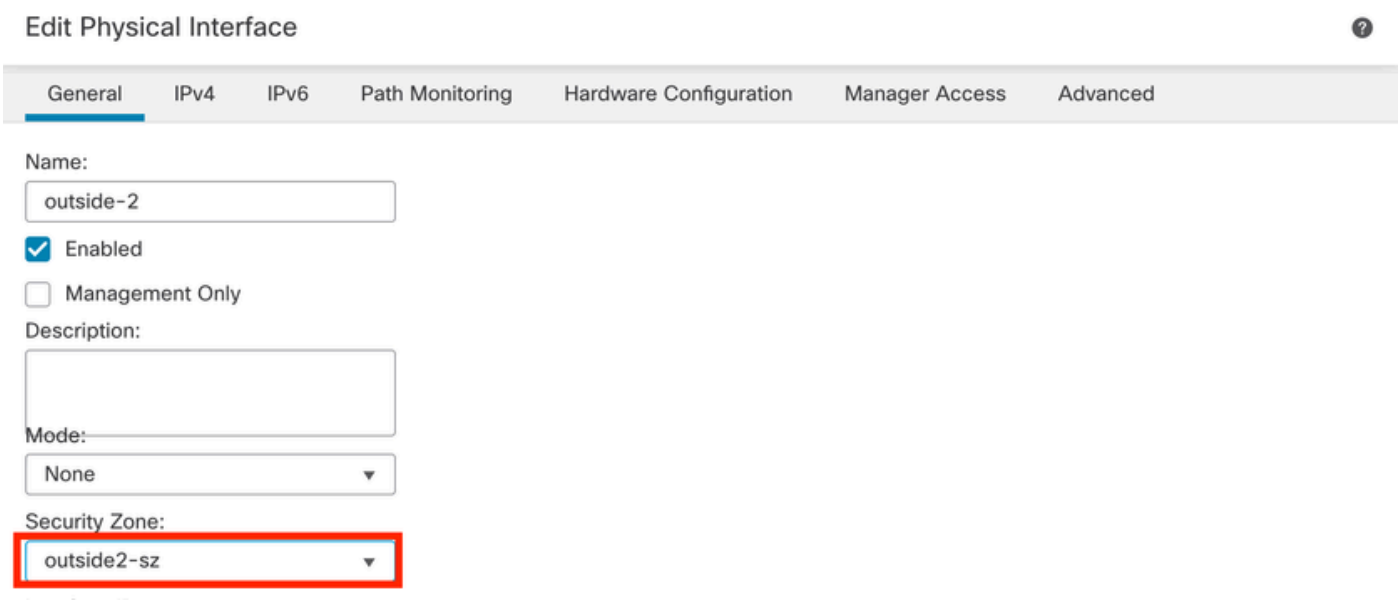
Schritt 3: Aktivieren Sie auf der Registerkarte Manager Access (Manager-Zugriff) das Kontrollkästchen Enable management on this interface for the manager (Verwaltung auf dieser Schnittstelle für den Manager aktivieren):



Aktivieren von Manager Access

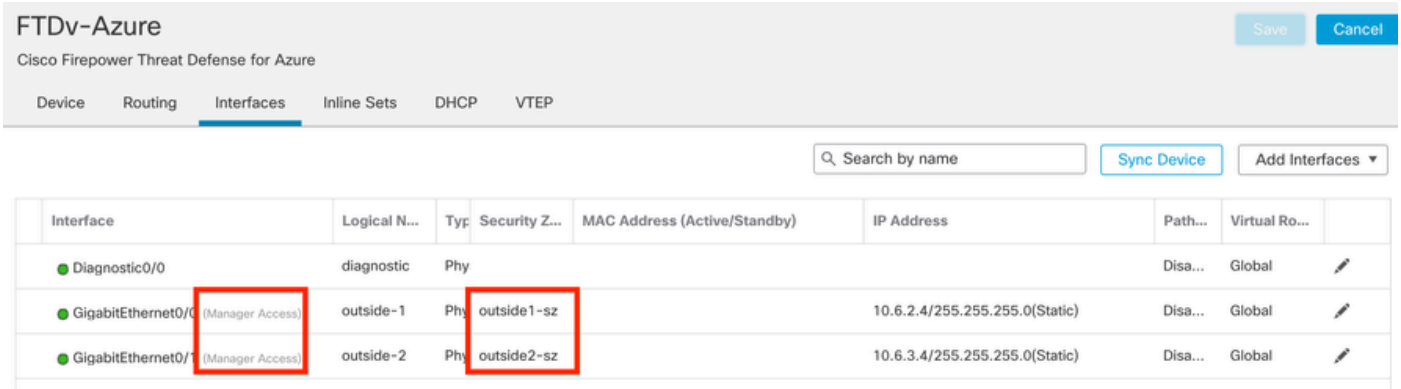
Schritt 4: Stellen Sie auf der Registerkarte Allgemein sicher, dass die Schnittstelle einer

Sicherheitszone zugewiesen ist, und klicken Sie auf OK:



Sicherheitszone für redundante Datenschnittstellen

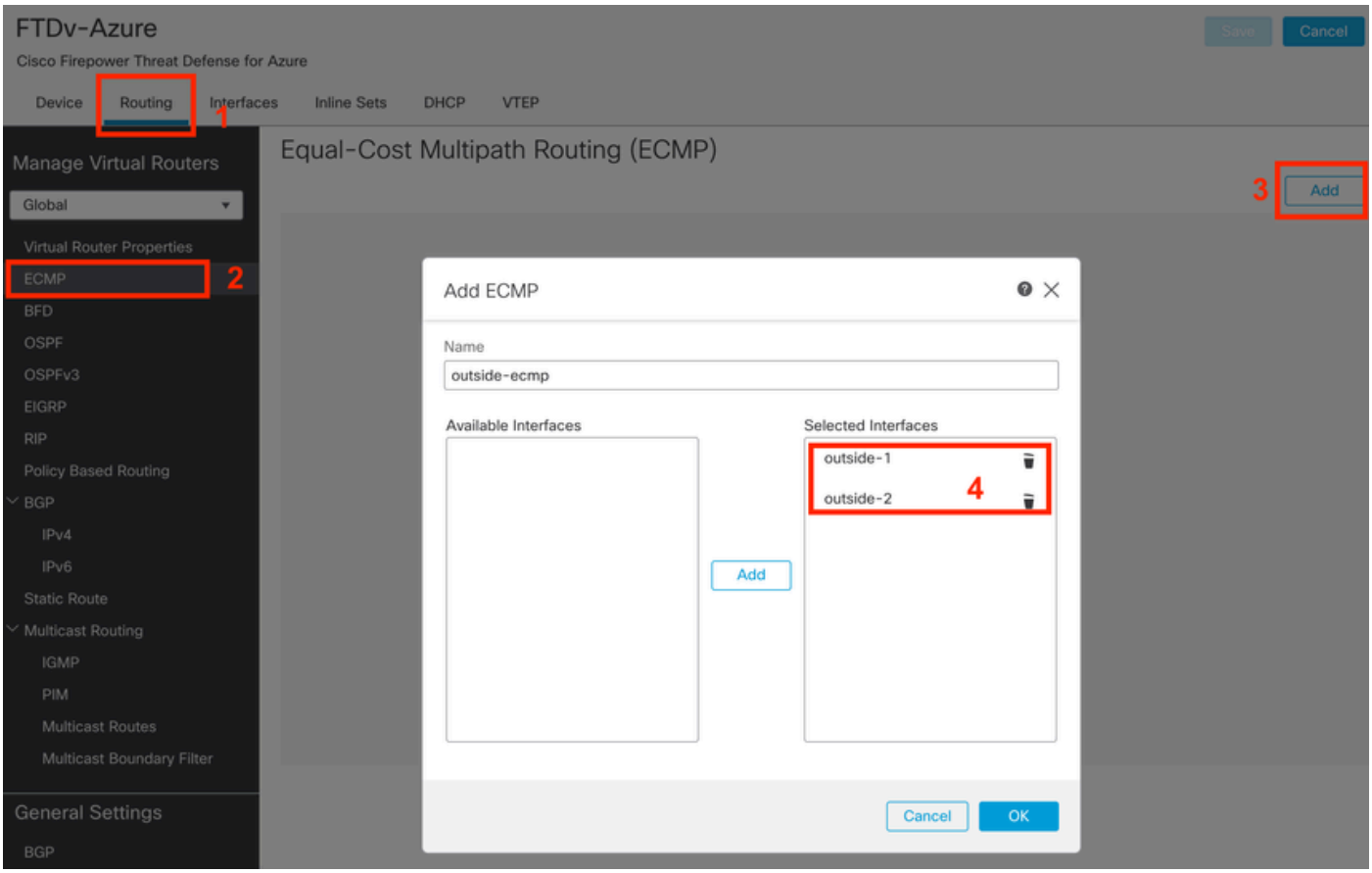
Schritt 5: Beachten Sie, dass nun beide Schnittstellen das Manager Access-Tag haben. Stellen Sie außerdem sicher, dass die primäre Datenschnittstelle einer anderen Sicherheitszone zugewiesen wurde:



Überprüfung der Schnittstellenkonfiguration

Im nächsten Abschnitt sollen in den Schritten 6 bis 10 zwei Standardrouten gleicher Kosten konfiguriert werden, um das CDO zu erreichen, die jeweils durch einen unabhängigen SLA-Tracking-Prozess überwacht werden. Die SLA-Nachverfolgung stellt sicher, dass über die überwachte Schnittstelle ein funktionaler Pfad für die Kommunikation mit dem cdFMC vorhanden ist.

Schritt 6: Navigieren Sie zur Registerkarte Routing, und erstellen Sie im ECMP-Menü eine neue ECMP-Zone mit beiden Schnittstellen:

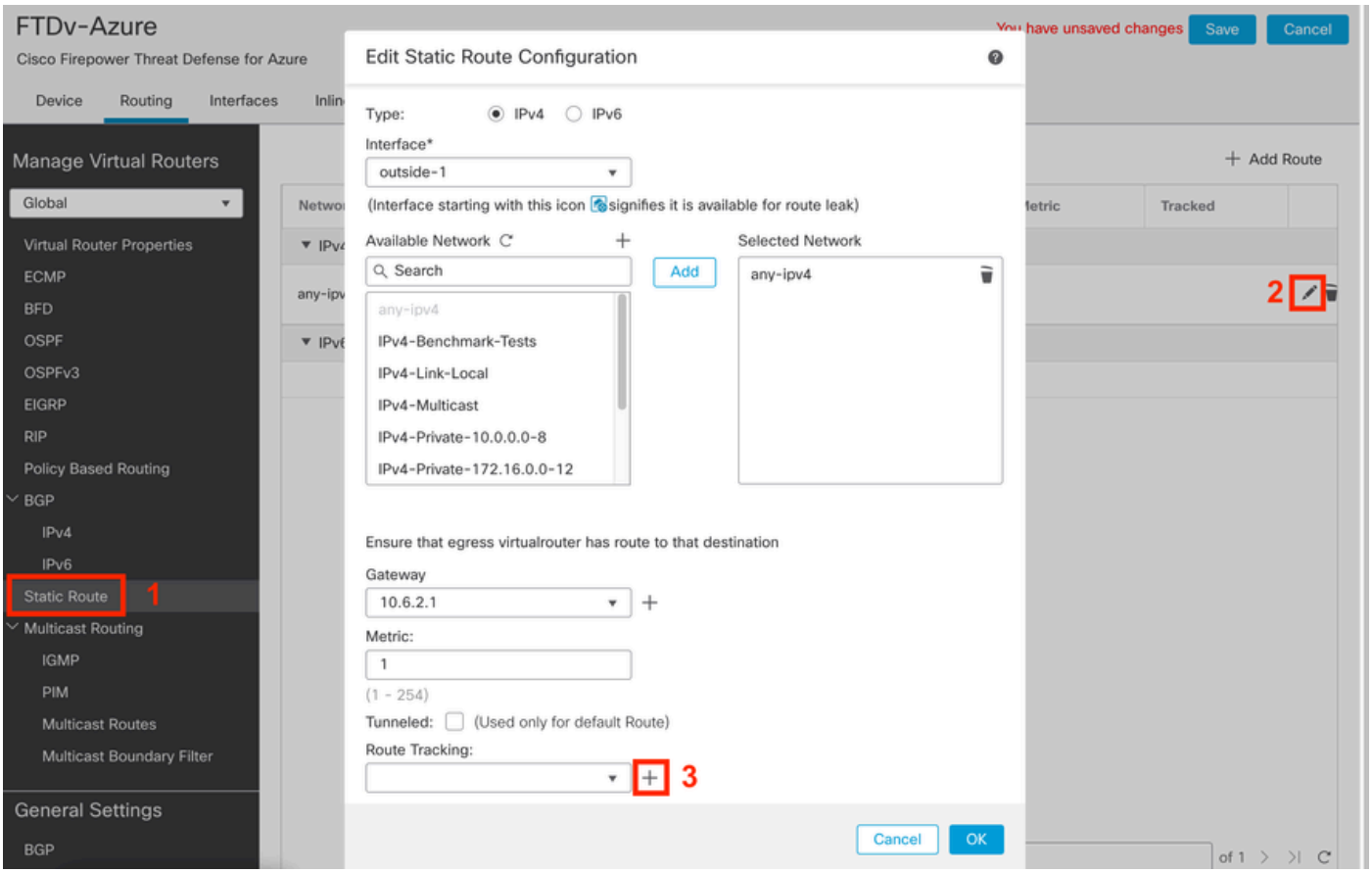


Konfigurieren eines ECMP-Bereichs

Klicken Sie auf OK und Speichern.

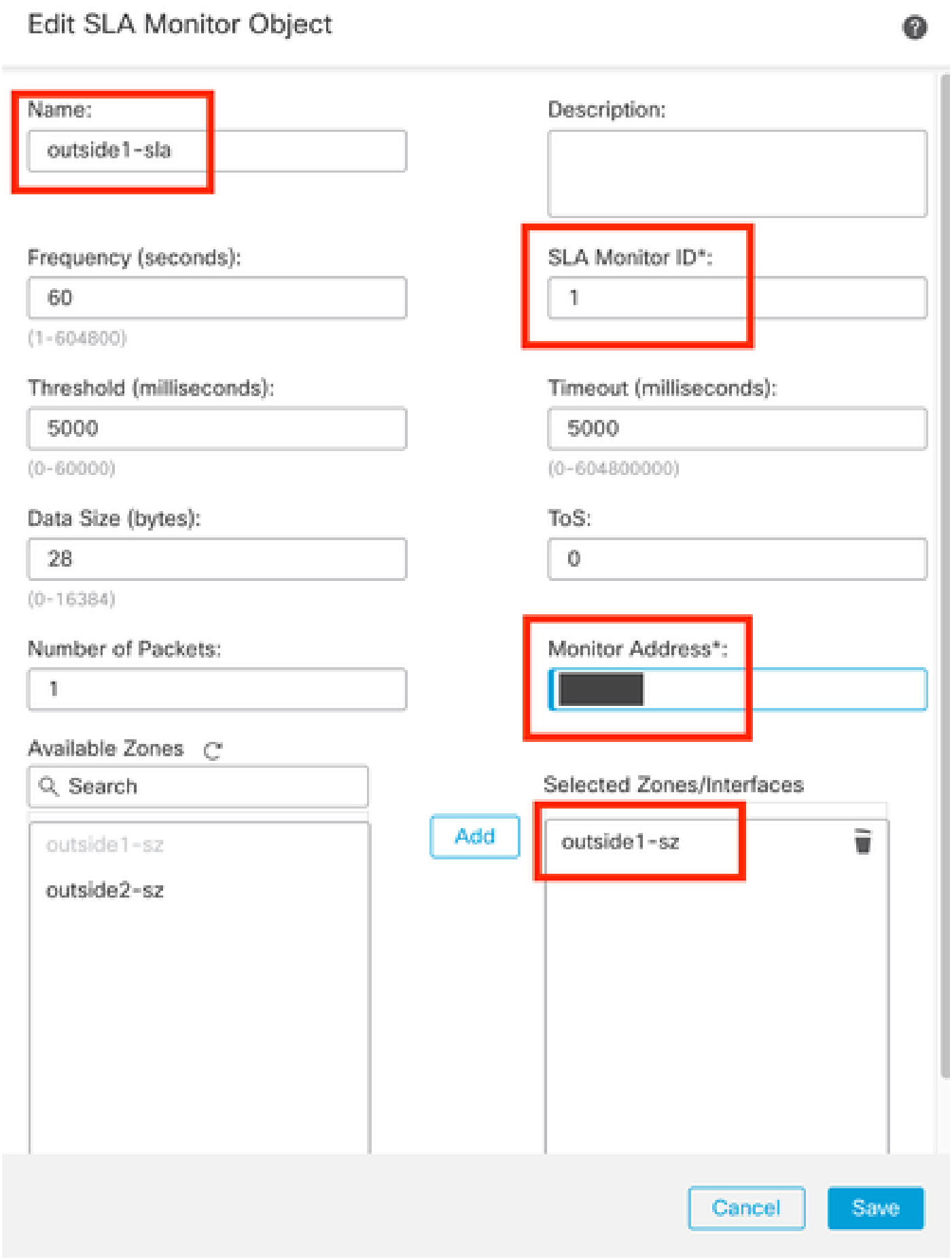
Schritt 7. Navigieren Sie auf der Registerkarte Routing zu Static Routes (Statische Routen).

Klicken Sie auf das Bleistiftsymbol, um Ihre primäre Route zu bearbeiten. Klicken Sie dann auf das Pluszeichen, um ein neues SLA-Verfolgungsobjekt hinzuzufügen:



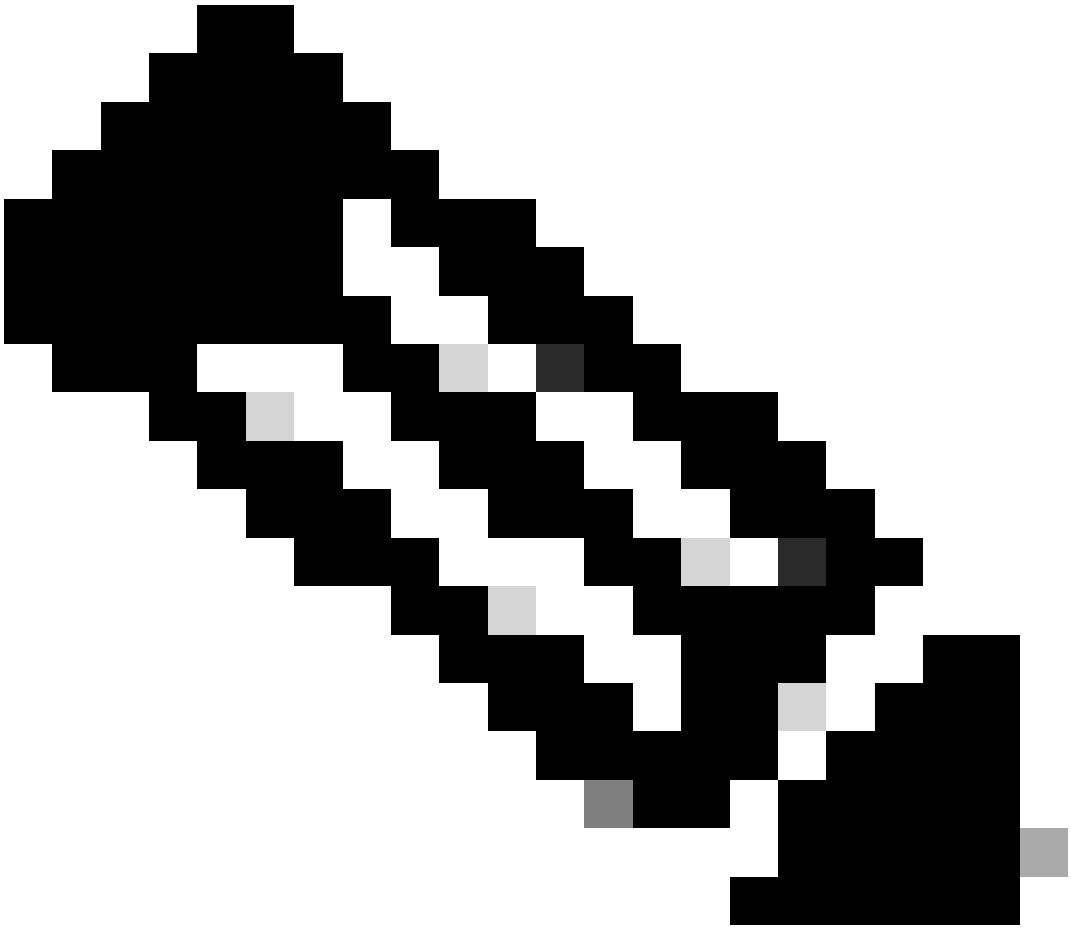
Bearbeiten der primären Route zum Hinzufügen der SLA-Nachverfolgung

Schritt 8: Erforderliche Parameter für eine funktionale SLA-Nachverfolgung sind im nächsten Bild hervorgehoben. Optional können Sie auch andere Einstellungen wie Anzahl der Pakete, Zeitüberschreitung und Frequenz anpassen.



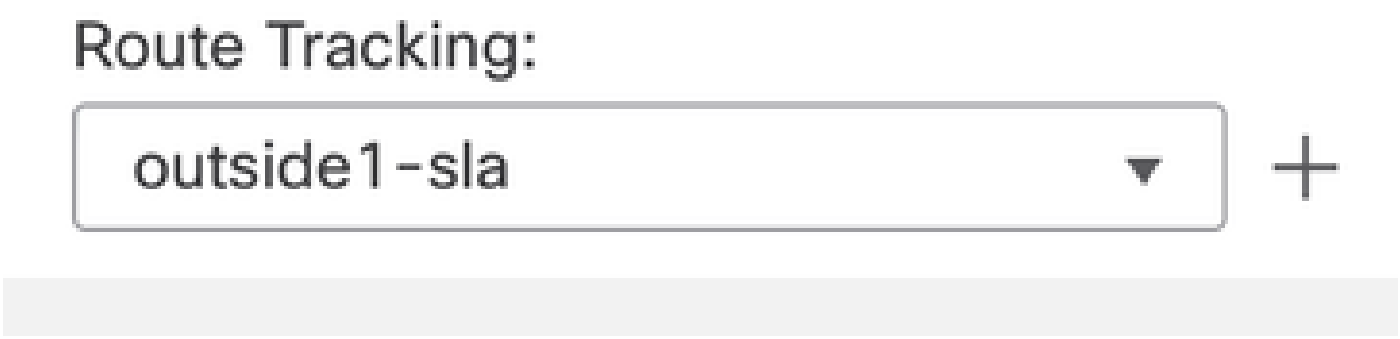
Konfigurieren der SLA-Verfolgung für ISP 1

In diesem Beispiel wurde Google DNS IP verwendet, um FTD-Funktionen zu überwachen, um über die Schnittstelle outside1 auf das Internet (und CDO) zuzugreifen. Klicken Sie anschließend auf OK.



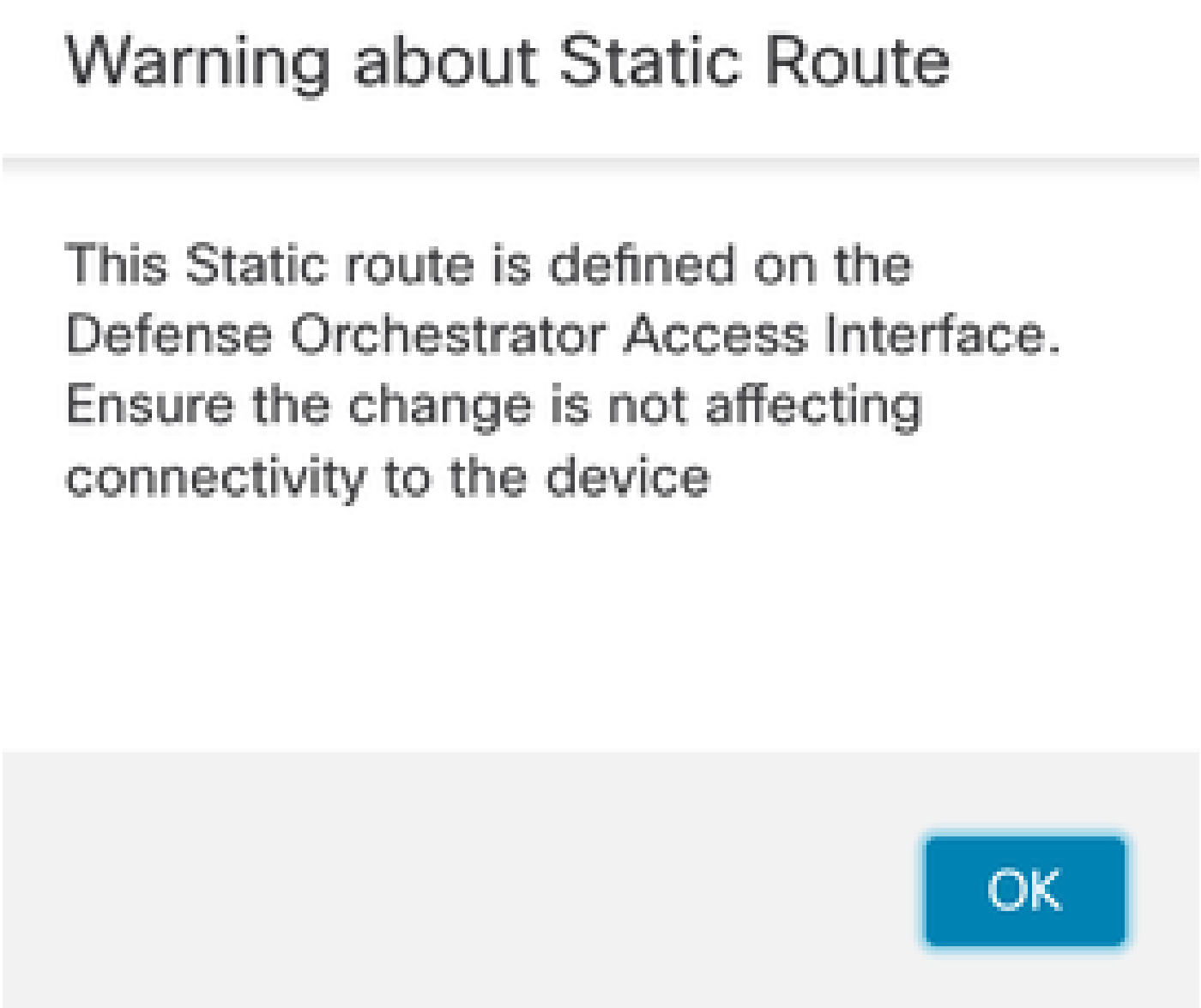
> Hinweis: Achten Sie darauf, dass Sie eine IP-Adresse verfolgen, deren Erreichbarkeit über Ihre externe FTD-Schnittstelle bereits verifiziert wurde. Wenn Sie eine Spur mit einer nicht erreichbaren IP konfigurieren, kann die Standardroute in dieser FTD reduziert werden, und dann wird verhindert, dass diese mit CDO kommunizieren kann.

Schritt 9. Klicken Sie auf Save (Speichern), und stellen Sie sicher, dass die neue SLA-Nachverfolgung der Route zugewiesen ist, die auf die primäre Schnittstelle verweist:



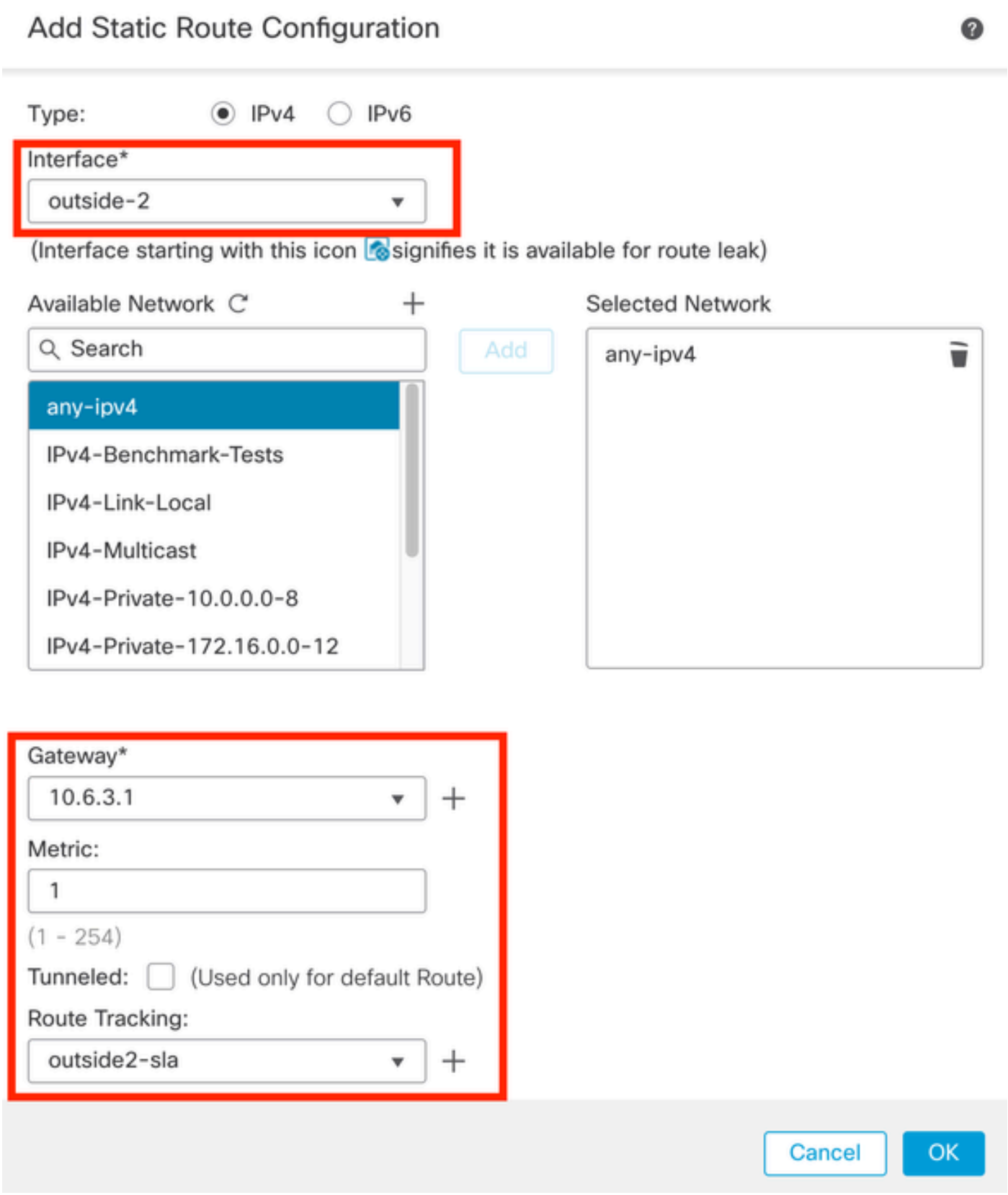
Außerhalb 1 SLA-Nachverfolgung

Wenn Sie auf OK klicken, wird ein Popup-Fenster mit der nächsten WARNUNG angezeigt:

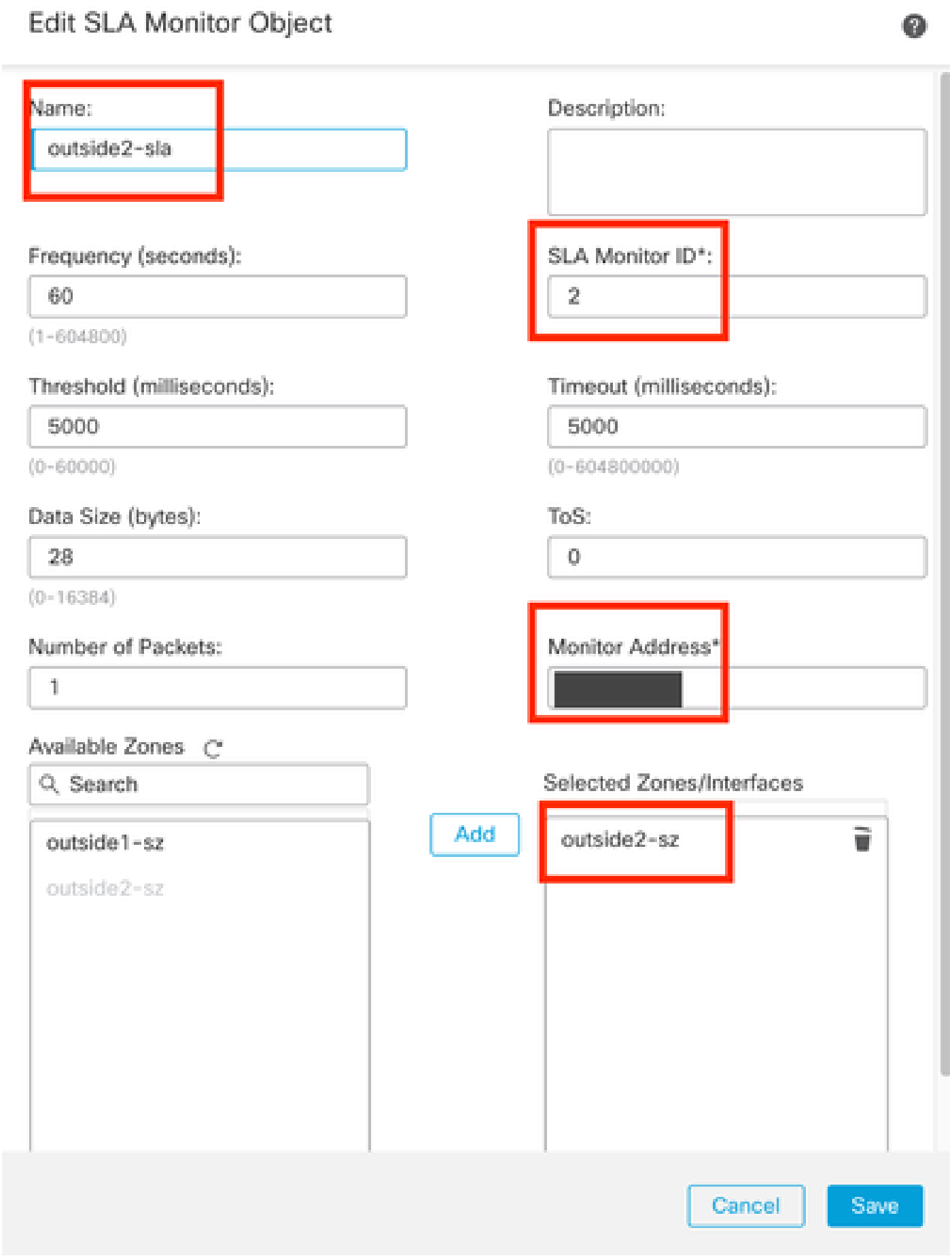


Konfiguration

Schritt 10. Klicken Sie auf die Option Add Route (Route hinzufügen), um eine neue Route für die redundante Datenschnittstelle hinzuzufügen. Beachten Sie im nächsten Bild, dass der metrische Wert für die Route identisch ist. Außerdem hat die SLA-Verfolgung eine andere ID:



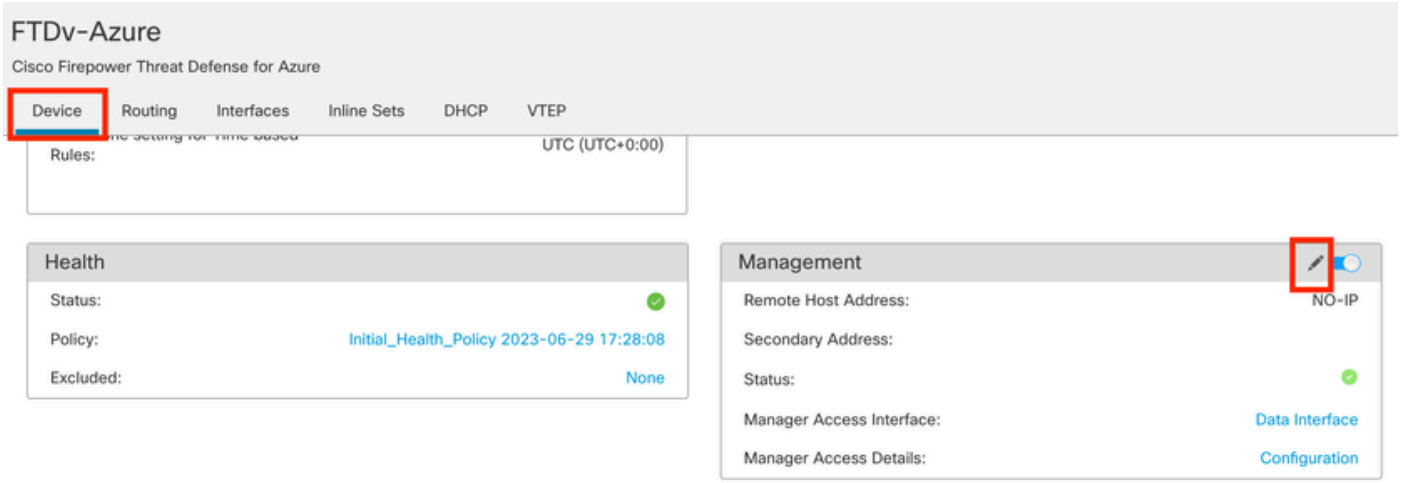
Redundante statische Route konfigurieren



Nachverfolgung für redundante Datenschnittstelle konfigurieren

Klicken Sie auf Speichern.

Schritt 11. Optional können Sie die sekundäre Datenschnittstellen-IP unter Gerät > Management angeben. Dies ist jedoch nicht erforderlich, da bei der aktuellen Integrationsmethode der CLI-Registrierungsschlüssel verwendet wurde:



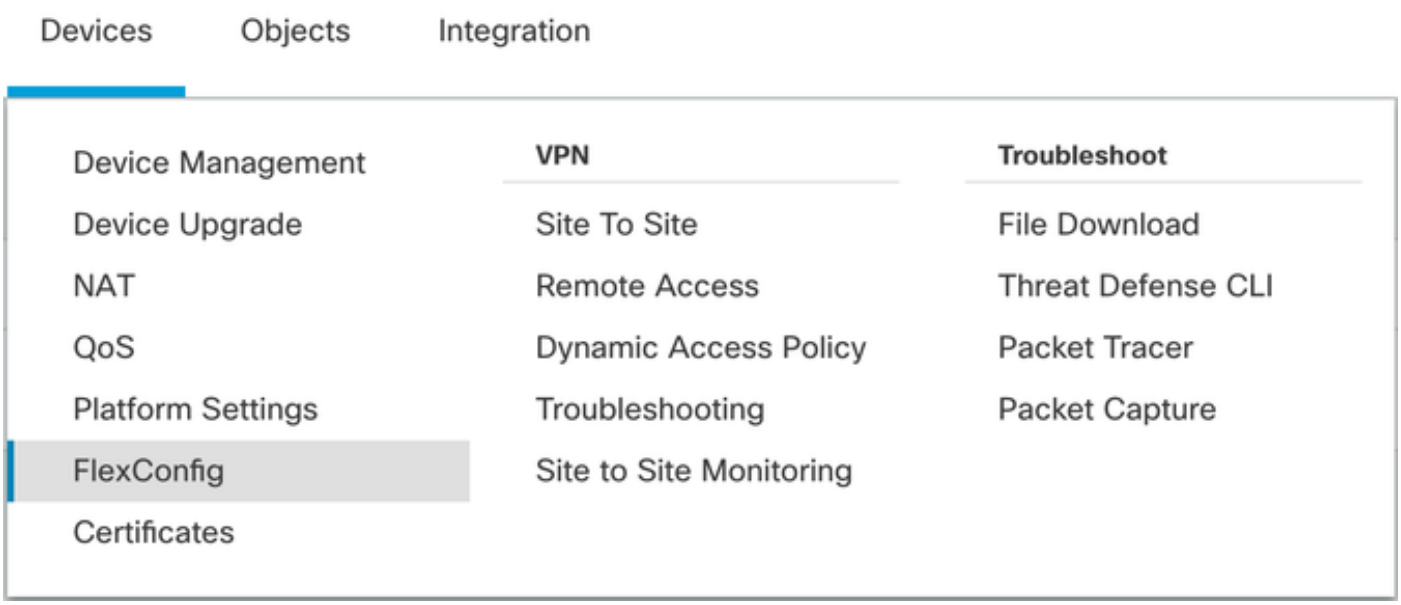
(Optional) Geben Sie im Feld "Management" eine IP für die redundante Datenschnittstelle an.

Schritt 12: Bereitstellen der Änderungen

(Optional) Legen Sie die Schnittstellenkosten für einen Aktiv/Backup-Schnittstellenmodus fest:

Standardmäßig wird bei der redundanten Verwaltung über die Datenschnittstelle Round-Robin verwendet, um den Managementverkehr zwischen beiden Schnittstellen zu verteilen. Wenn eine WAN-Verbindung eine höhere Bandbreite als die andere hat und Sie diese als primäre Management-Verbindung bevorzugen, während die andere als Backup verbleibt, können Sie der primären Verbindung den Wert 1 zuweisen und der Backup-Verbindung den Wert 2 zuweisen. Im nächsten Beispiel wird die Schnittstelle GigabitEthernet0/0 als primäre WAN-Verbindung beibehalten, während GigabiEthernet0/1 als Backup-Management-Verbindung dient:

1. Navigieren Sie zu Devices (Geräte) > FlexConfig (FlexConfig), und erstellen Sie eine flexConfig-Richtlinie. Falls bereits eine flexConfig-Richtlinie konfiguriert und Ihrem FTD zugewiesen wurde, bearbeiten Sie sie wie folgt:

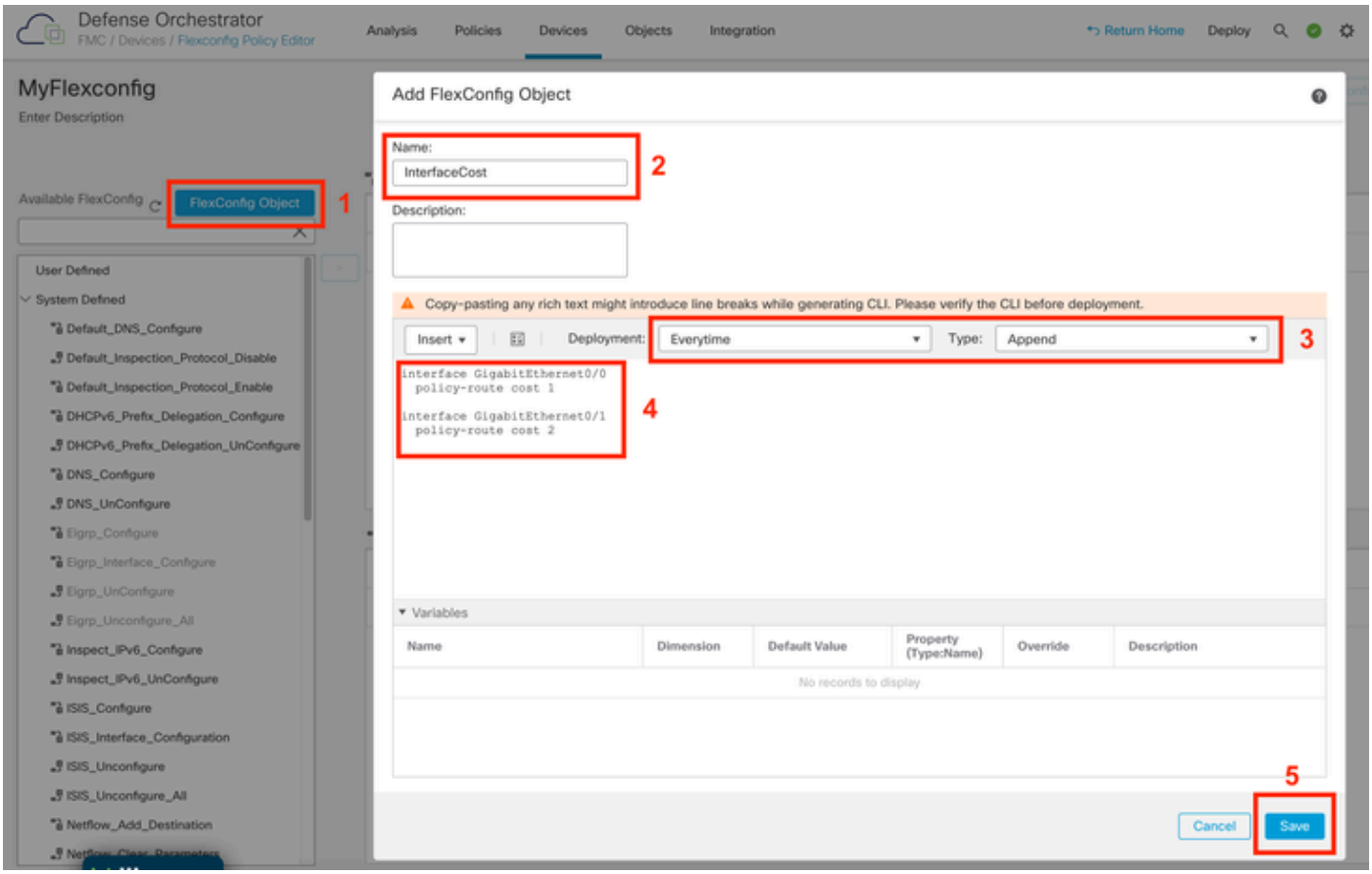


Zugriff auf das FlexConfig-Menü

2. Erstellen Sie ein neues FlexConfig-Objekt:

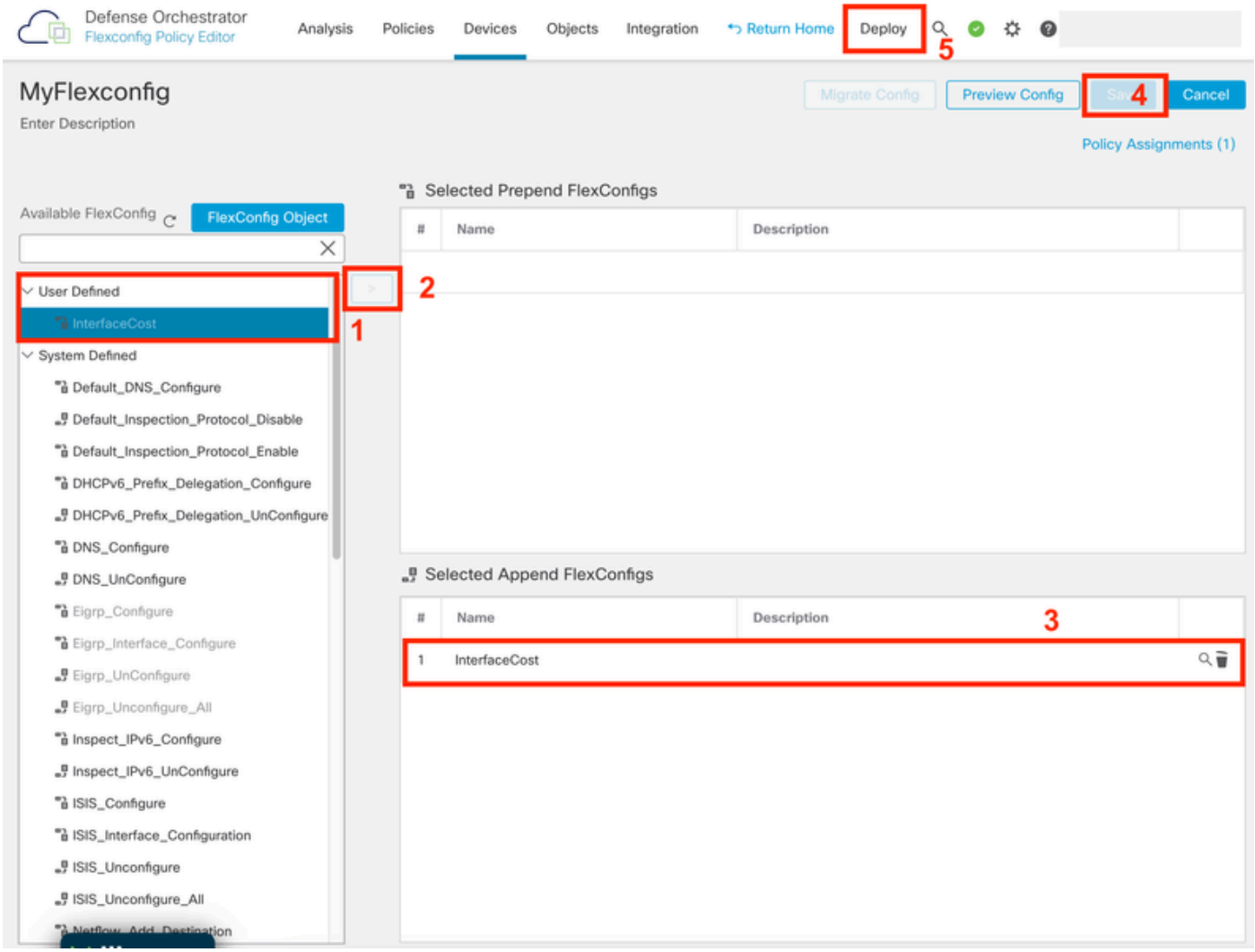
- Geben Sie dem FlexConfig-Objekt einen Namen.
- Wählen Sie in den Abschnitten Deployment (Bereitstellung) und Type (Typ) die Option Everytime (Jederzeit) und Append (Anfügen).
- Legen Sie die Kosten für die Schnittstellen mit den nächsten Befehlen fest, wie in Abbildung 22 dargestellt.
- Klicken Sie auf Speichern.

```
<#root>
interface GigabitEthernet0/0

  policy-route cost 1

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.
interface GigabitEthernet0/1

  policy-route cost 2

<=== Cost 2 sets this interface as a backup interface.
```



Hinzufügen eines Flexconfig-Objekts

3. Wählen Sie das zuletzt erstellte Objekt und fügen Sie es dem Abschnitt "Ausgewählte FlexConfigs anhängen" wie im Bild dargestellt hinzu. Speichern Sie die Änderungen, und stellen Sie Ihre Konfiguration bereit.



Zuweisen des Objekts zur Flexconfig-Richtlinie

4. Bereitstellen der Änderungen

Überprüfung

1. Verwenden Sie zum Überprüfen den Befehl show network. Eine neue Instanz für die redundante Management-Schnittstelle wird gebildet:

```
> show network

<<---------- output omitted for brevity ---------->>

======================[ eth0 ]======================
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
---------------------[ IPv4 ]---------------------
Configuration : Manual
```

```
Address : 10.6.0.4
Netmask : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration : Disabled

================[ Proxy Information ]================
State : Disabled
Authentication : Disabled
. . .

===============[ GigabitEthernet0/0 ]===============
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled

===============[ GigabitEthernet0/1 ]===============
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
----------------------[ IPv4 ]----------------------
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
----------------------[ IPv6 ]----------------------
Configuration : Disabled
```

2. Die Schnittstelle ist nun Teil der sftunnel-Domäne. Sie können dies mit den Befehlen show sftunnel interface und show running-config sftunnel bestätigen:

```
<#root>

>

show sftunnel interfaces


Physical Interface Name of the Interface
GigabitEthernet0/0 outside-1
GigabitEthernet0/1 outside-2

>

show running-config sftunnel


sftunnel interface outside-2
sftunnel interface outside-1
```

```
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. Eine richtlinienbasierte Route wird automatisch buchstabiert. Wenn Sie keine Schnittstellenkosten angegeben haben, legt die Option "Adaptive Schnittstelle" die Round-Robin-Verarbeitung so fest, dass der Verwaltungsdatenverkehr zwischen beiden Schnittstellen auf einen Lastenausgleich angewendet wird:

```
<#root>

>

show running-config route-map


!
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2

>

show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392


access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. Verwenden Sie den Befehl show running-config interface <interface>, um die Schnittstelleneinstellungen zu überprüfen:

```
<#root>

>

 show running-config interface GigabitEthernet 0/0


!
interface GigabitEthernet0/0
nameif outside-1
security-level 0
zone-member outside-ecmp
ip address 10.6.2.4 255.255.255.0
policy-route cost 1

>

show running-config interface GigabitEthernet 0/1


!
interface GigabitEthernet0/1
nameif outside-2
security-level 0
```

```
zone-member outside-ecmp
ip address 10.6.3.4 255.255.255.0
policy-route cost 2
```

Einige zusätzliche Befehle können verwendet werden, um die Nachverfolgung der konfigurierten Routen zu überprüfen:

<#root>

>

show track

```
Track 1
Response Time Reporter 2 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interfa
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 10
Tracked by:
STATIC-IP-ROUTING 0
Track 2
Response Time Reporter 1 reachability
Reachability is Up                    <============== Ensure reachability is up for the monitored interfa
2 changes, last change 09:45:00
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
STATIC-IP-ROUTING 0
```

>

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 10.6.3.1 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
                   [1/0] via 10.6.2.1, outside-1
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Management des Firewall-Bedrohungsschutzes mit dem Cloud-basierten Firewall Management Center in Cisco Defense Orchestrator

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.