Konfigurieren von sicherem Zugriff mit sicherem FTD und ASA für privaten Zugriff mit NAT

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
  - Netzwerkdiagramm
- Konfigurieren
  - Sicherer Zugriff und sicherer Firewall-Thread-Schutz - Dynamisches, routenbasiertes (BGP) VPN mit PBR
  - FTD-richtlinienbasiertes Routing
  - Konfigurieren von BGP auf FTD
  - Tunnel-Status überprüfen
  - Konfigurieren eines statischen, routenbasierten IPsec-VPNs auf der Adaptive Security Appliance (ASA) mit PBR
  - VPN-Konfiguration für sicheren Zugriff
  - VPN-Konfiguration auf ASA
  - Richtlinienbasiertes Routing
- Überprüfung

Einleitung

In diesem Dokument wird die Konfiguration der Secure Access Network Tunnel Group mit Network Address Translation beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Firewall Management Center
- Cisco Secure Firewall - Schutz vor Bedrohungen
- Sicherer Zugriff von Cisco

- Cisco Adaptive Security Appliance
- Network Address Translation
- Richtlinienbasiertes Routing
- Paketerfassung auf Firewall

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defense 7.10
- Sicherer Zugriff von Cisco
- Cisco Adaptive Security Appliance 9.22
- Cisco Router

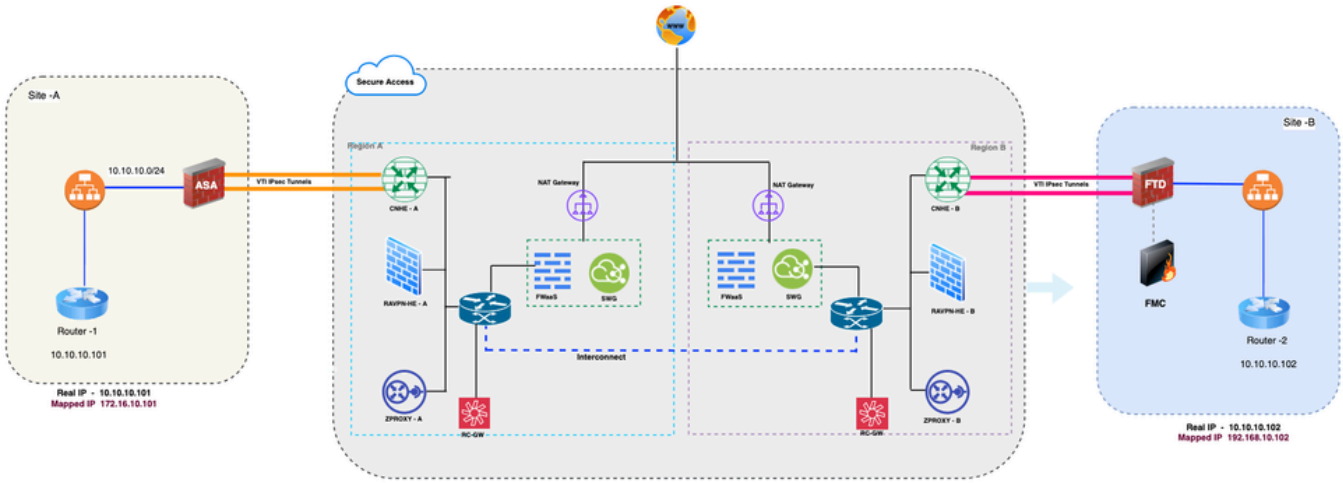
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

Cisco Secure Access bietet Cloud-native Secure Service Edge-Funktionen wie Secure Internet Access (SIA) und Secure Private Access (SPA). Für Unternehmen, die den Zugriff auf private Anwendungen für Remote-Benutzer erweitern, ohne den gesamten Datenverkehr über ein Rechenzentrum zu sichern, verwendet Secure Access IPsec Network Tunnel Groups (NTGs) zur Erstellung verschlüsselter Tunnel zwischen lokalen Netzwerkgeräten wie Cisco Firewall Threat Defense (FTD), Adaptive Security Appliance (ASA) und Cisco Secure Access Cloud Points-of-Presence (PoPs).

In diesem Dokument wird die Einrichtung eines routenbasierten IPsec-Tunnels mithilfe von IKEv2 zwischen Cisco FTD , ASA und Cisco Secure Access erläutert. Dadurch wird Network Address Translation (NAT) bei sicherem Zugriff und Policy-Based Routing (PBR) bei FTD und ASA aktiviert, sodass nur Datenverkehr mit privatem Zugriff in den Tunnel geleitet wird.

Netzwerkdiagramm



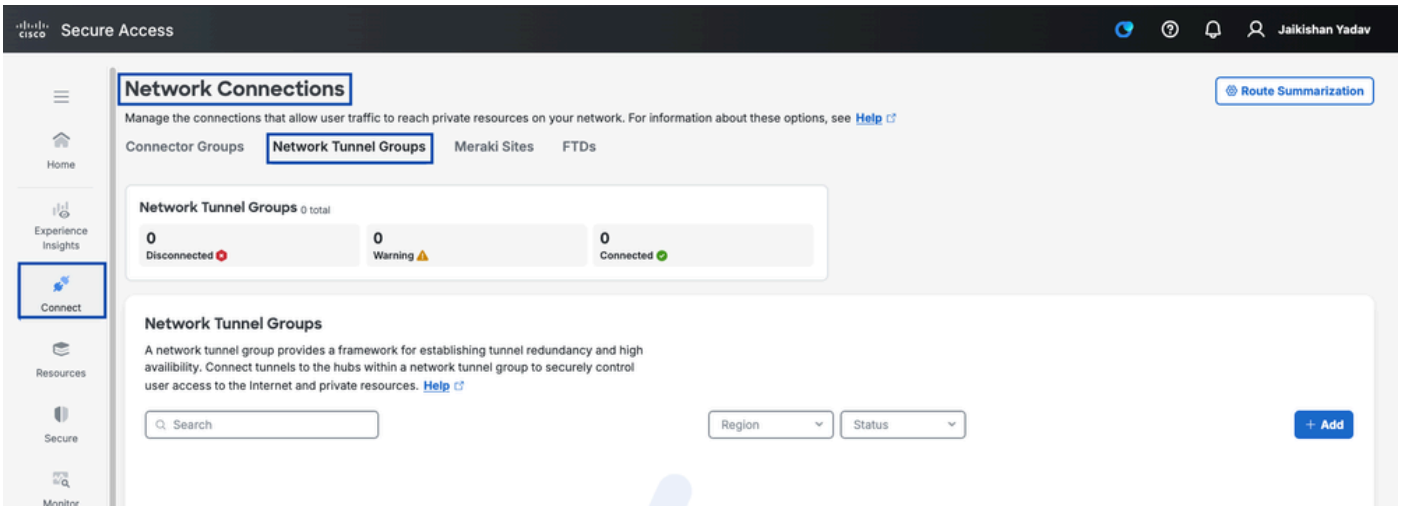
Netzwerktopologie

Konfigurieren

Sicherer Zugriff und sicherer Firewall-Thread-Schutz - Dynamisches, routenbasiertes (BGP) VPN mit PBR

Konfigurieren der Netzwerk-Tunnelgruppe für sicheren Zugriff

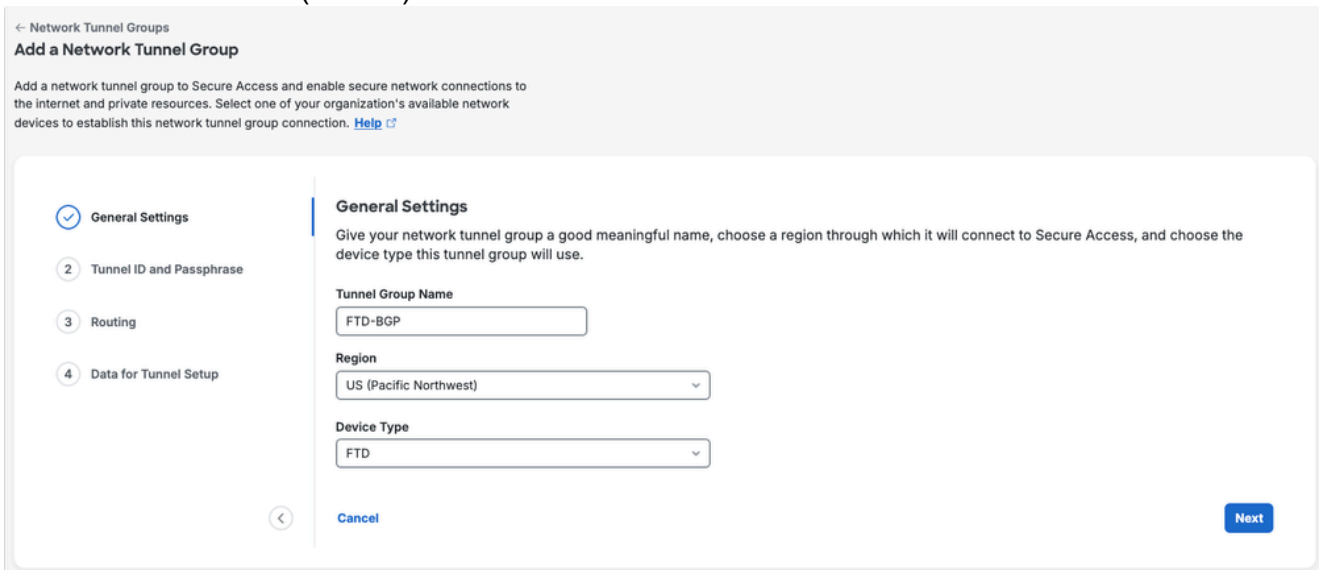
1. Anmeldung beim Dashboard für sicheren Zugriff Sicherer Zugriff
2. Navigieren Sie zu Verbinden > Netzwerkverbindungen > Netzwerk-Tunnelgruppen, und klicken Sie auf +Hinzufügen, um die Netzwerk-Tunnelgruppe zu konfigurieren.



Sicherer Zugriff - Netzwerk-Tunnelgruppen

3. Konfigurieren der Netzwerk-Tunnelgruppe - Allgemeine Einstellungen

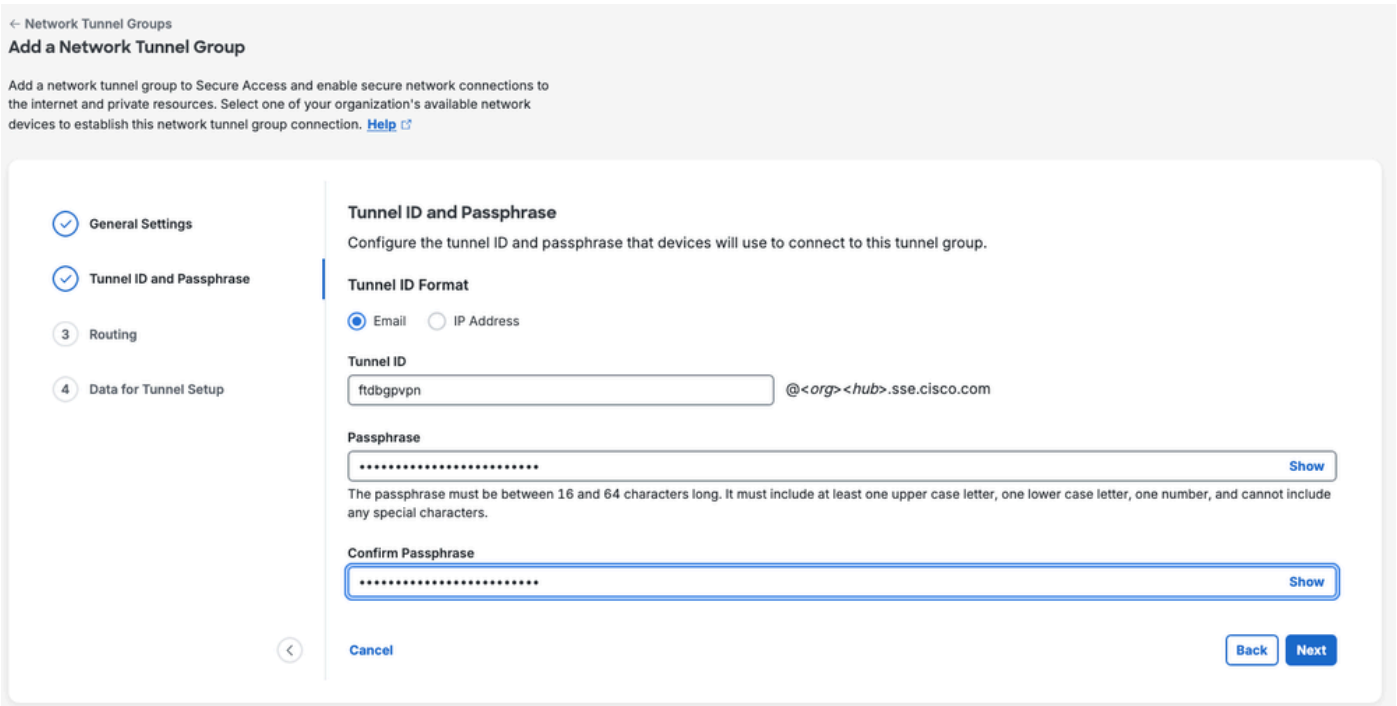
- Konfigurieren von Tunnelgruppenname, Region und Gerätetyp
- Klicken Sie auf Next (Weiter).



Sicherer Zugriff - Allgemeine Einstellungen für Netzwerk-Tunnelgruppen

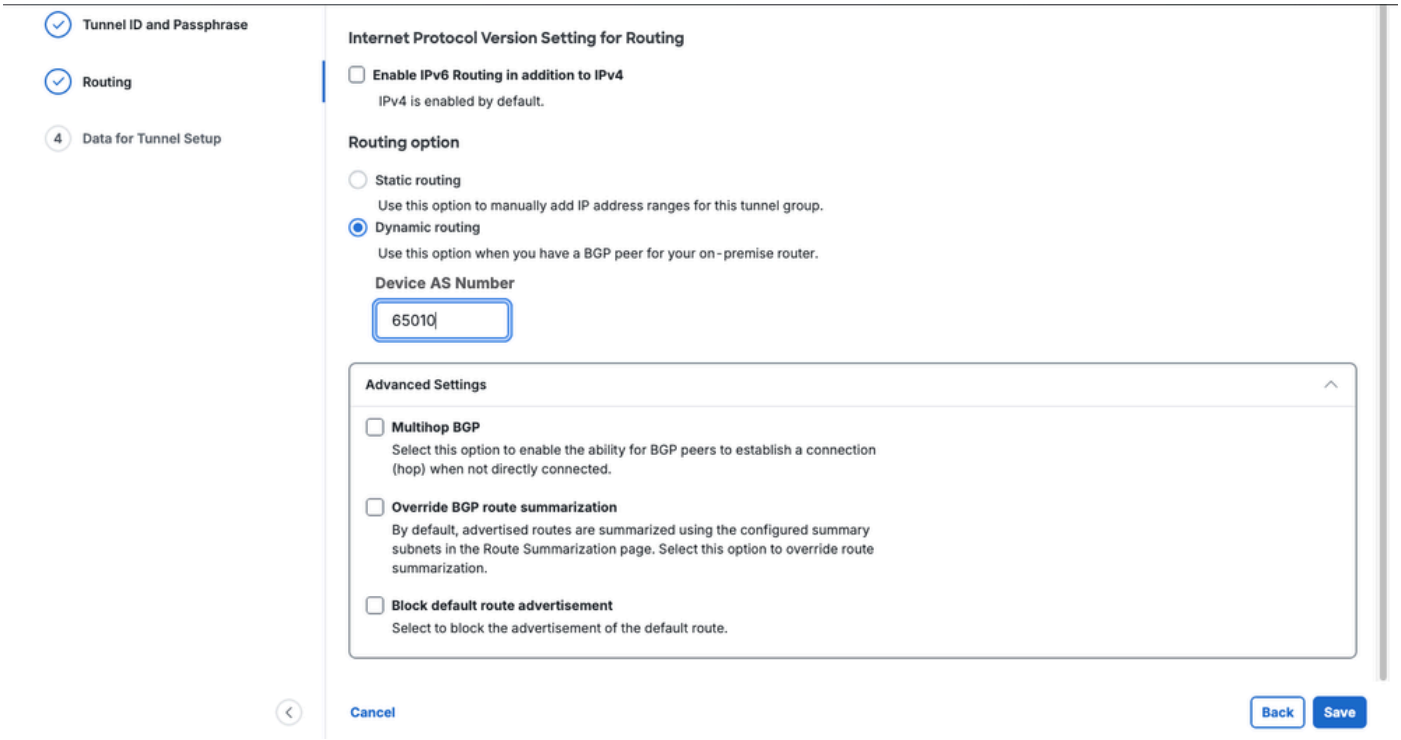
4. Konfigurieren Sie die Tunnel-ID und die Passphrase.

- Konfigurieren Sie die Tunnel-ID und die Passphrase.
- Klicken Sie auf Weiter



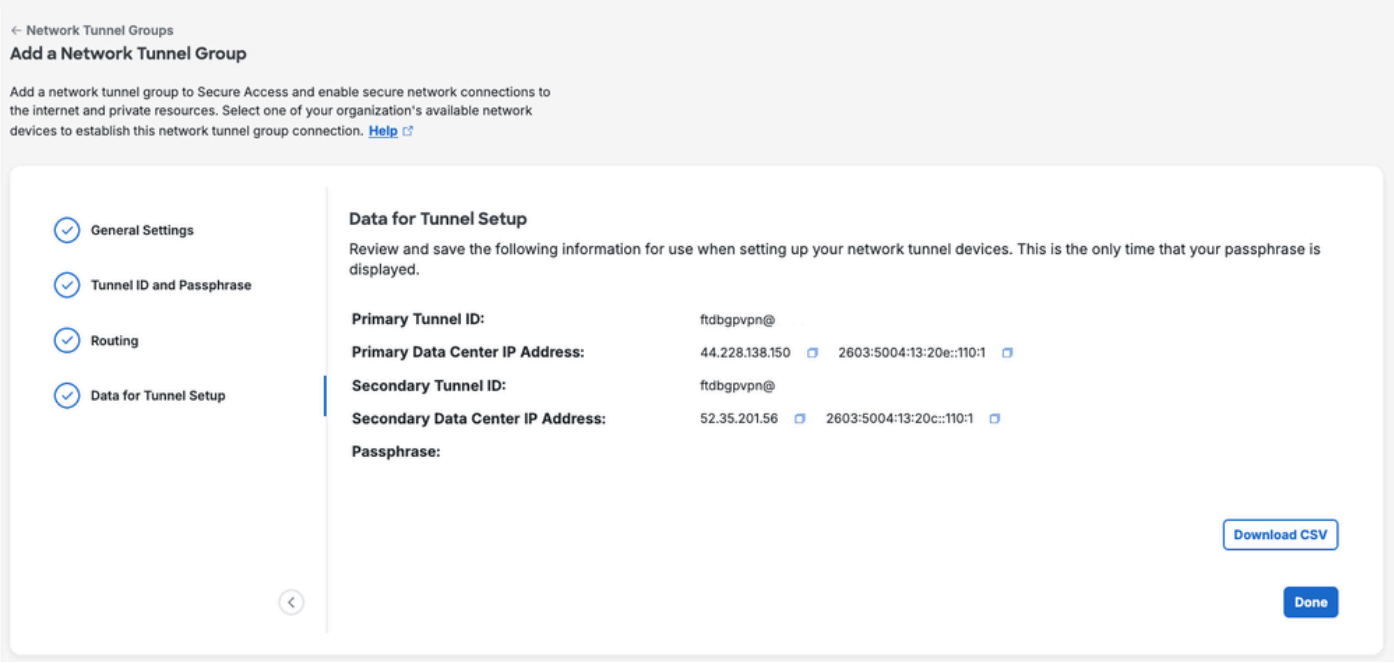
5. Konfigurieren von Routing

- AS-Nummer für Gerät konfigurieren
- Klicken Sie auf Save (Speichern).



Sicherer Zugriff - Netzwerk-Tunnelgruppen-Routing

6. Netzwerktunnelgruppenkonfiguration speichern



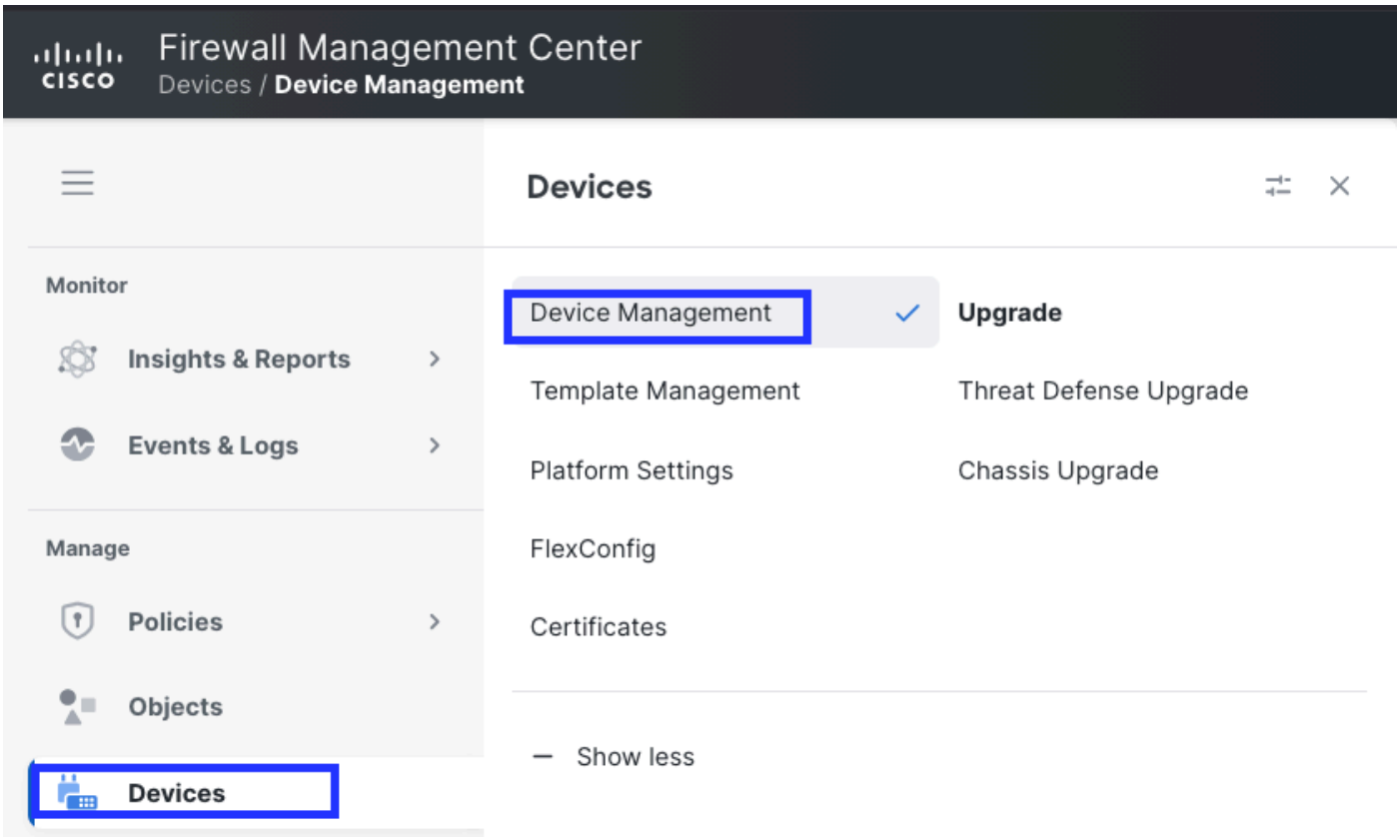
Sicherer Zugriff - Netzwerk-Tunnelgruppen

Konfigurieren eines dynamischen, routenbasierten IPsec-VPN auf Secure Firewall Threat Defense (FTD) mit PBR

1. Anmeldung beim Firewall Management Center (FMC)

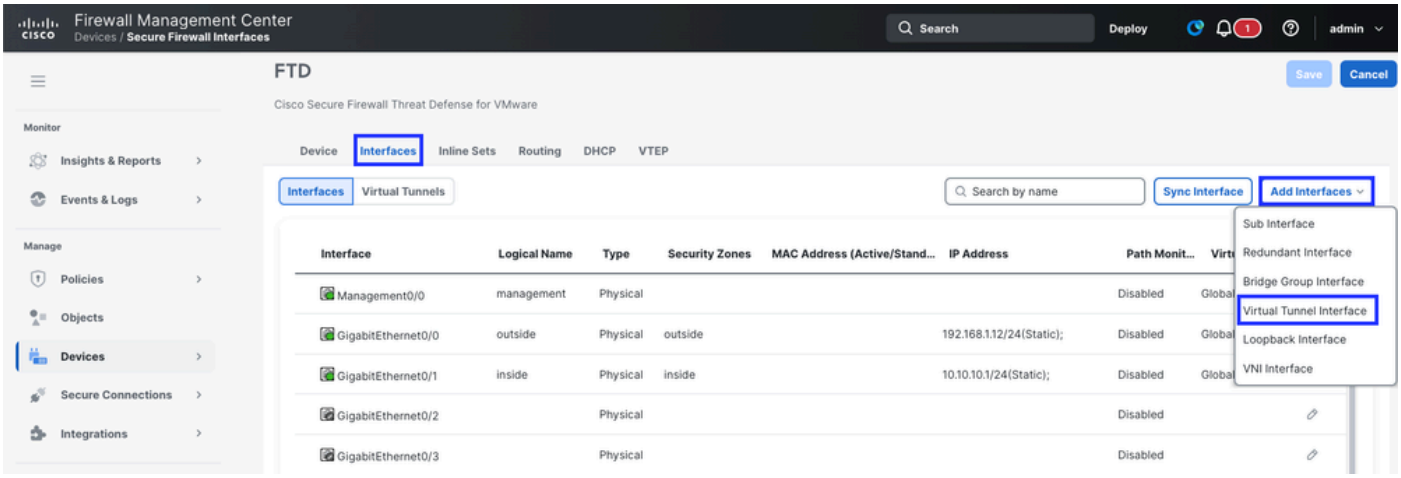
2. Virtual Tunnel Interface VTI konfigurieren

- Navigieren Sie zu Geräte > Geräteverwaltung.



Sichere Firewall-Verwaltung - Dashboard

- Klicken Sie auf das Bleistiftsymbol neben dem Gerät, und navigieren Sie zum Schnittstellenabschnitt.
- Klicken Sie auf Schnittstellen hinzufügen, und wählen Sie Virtuelle Tunnelschnittstelle aus.



Sichere Firewall-Verwaltung - FTD VTI-Konfiguration

- Konfigurieren von VTI

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

VTI-1

[x] Enabled

Description:

Virtual Tunnel interface for Primary VTI VPN

Security Zone:

vti

Priority:

0 *(0 - 65535)*

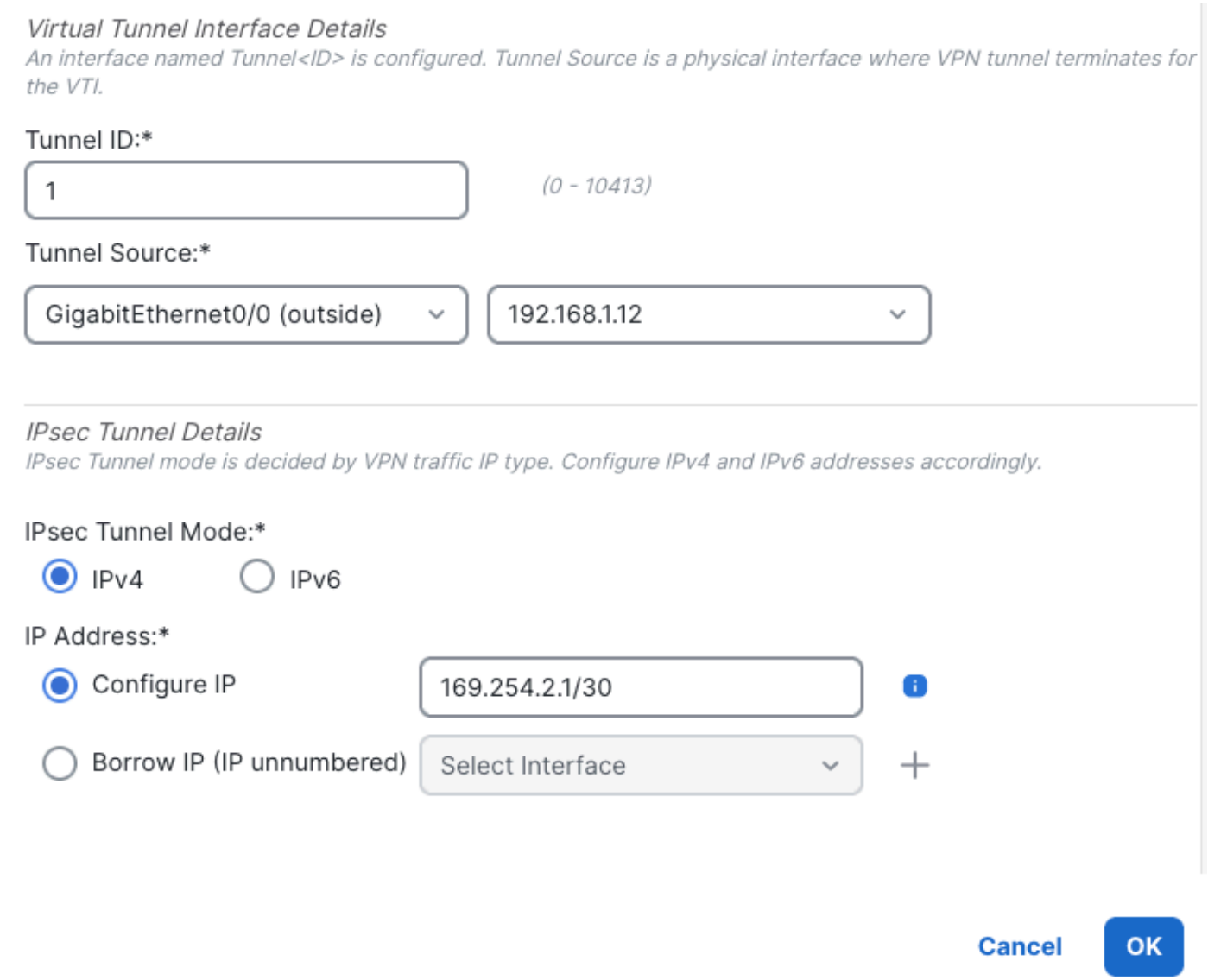
Propagate Security Group Tag: [x]

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

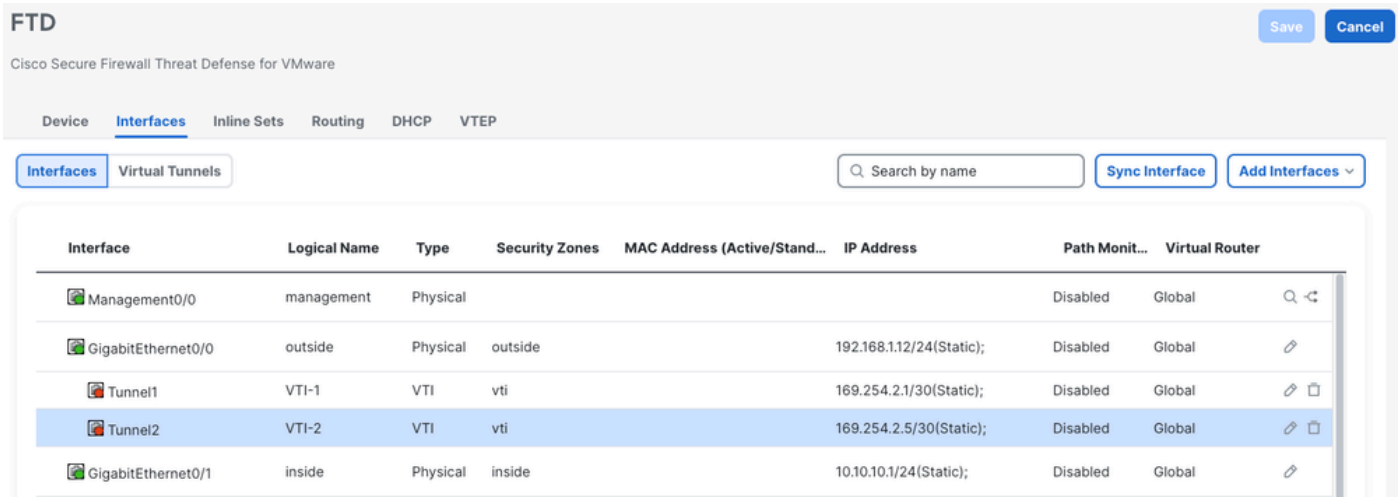
Tunnel ID:*

1 *(0 - 10413)*

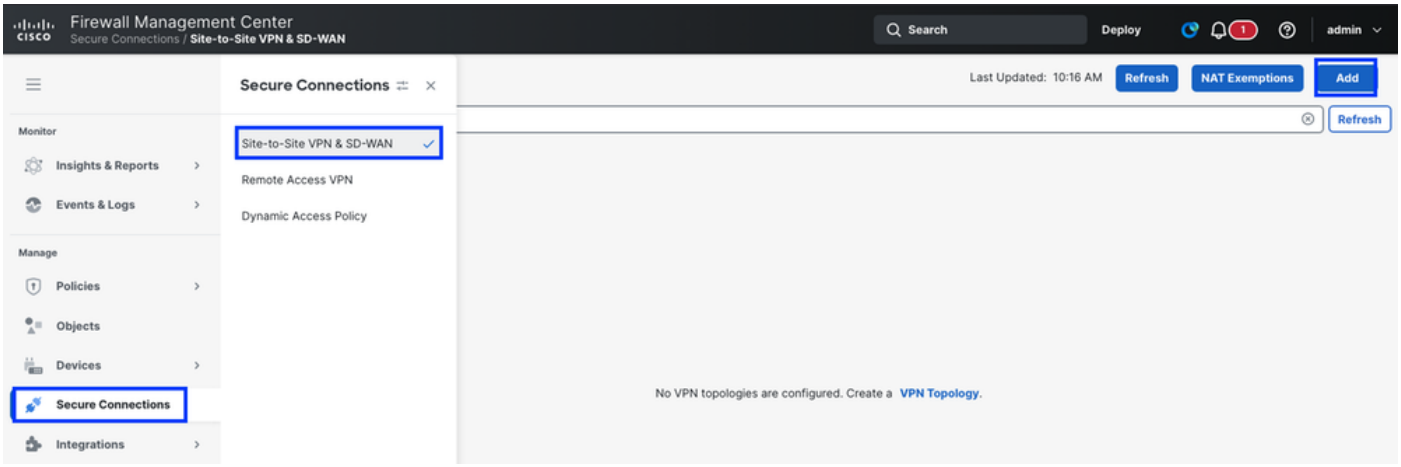


Sichere Firewall-Verwaltung - FTD VTI-Konfiguration

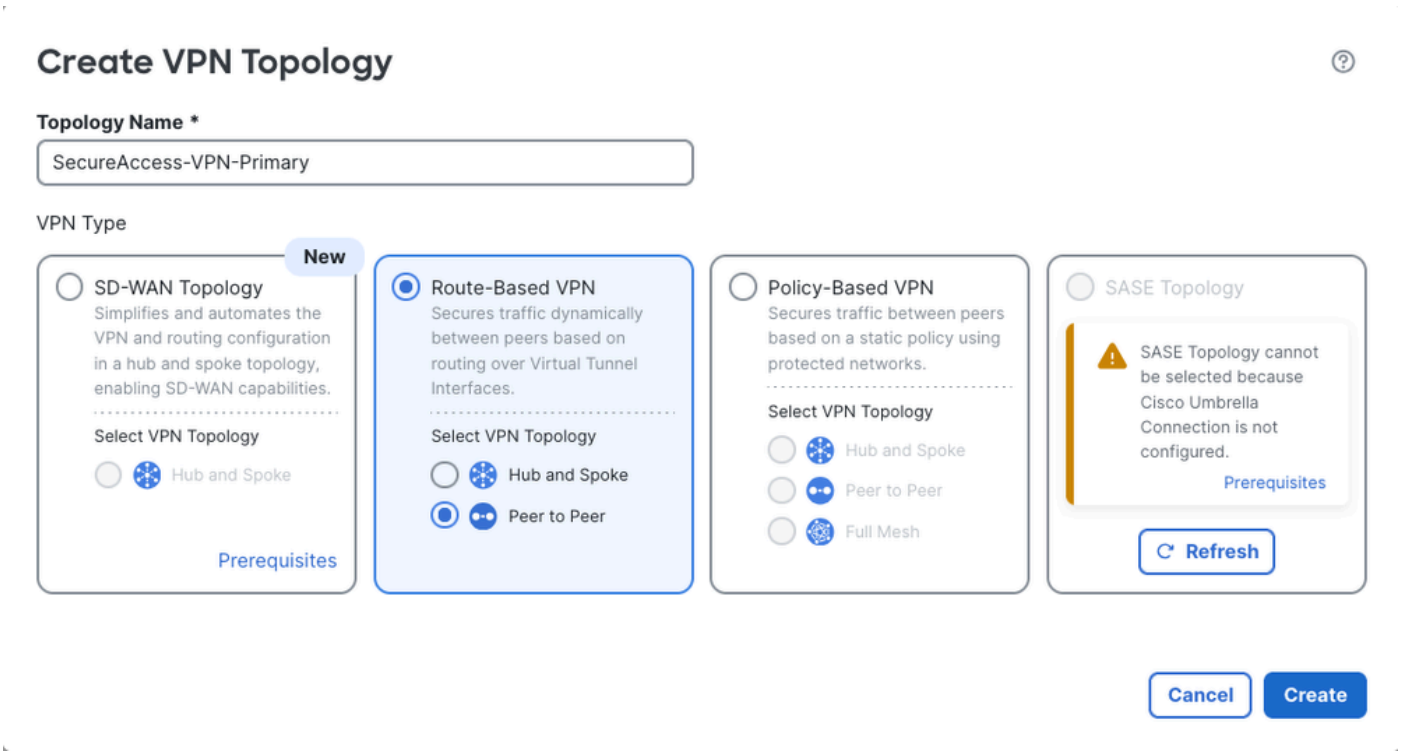
- Konfiguration von VTI-2 sowie für sekundäres IPsec-VPN mit sicherem Zugriff



3. Navigieren Sie zu Sichere Verbindungen > Site-to-Site VPN & SD-WAN, und klicken Sie auf Hinzufügen, um das VPN zu konfigurieren.



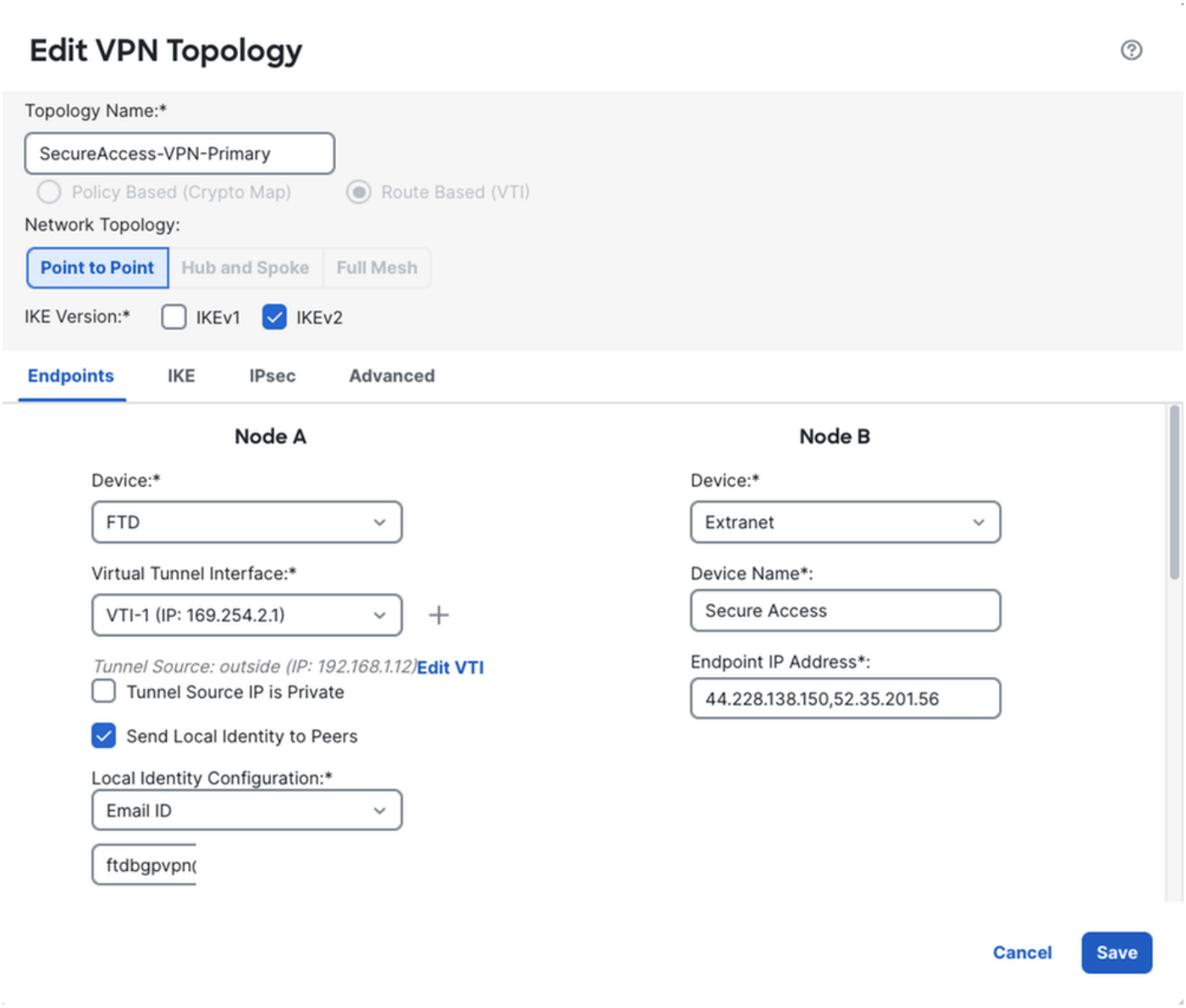
- VPN-Topologie erstellen



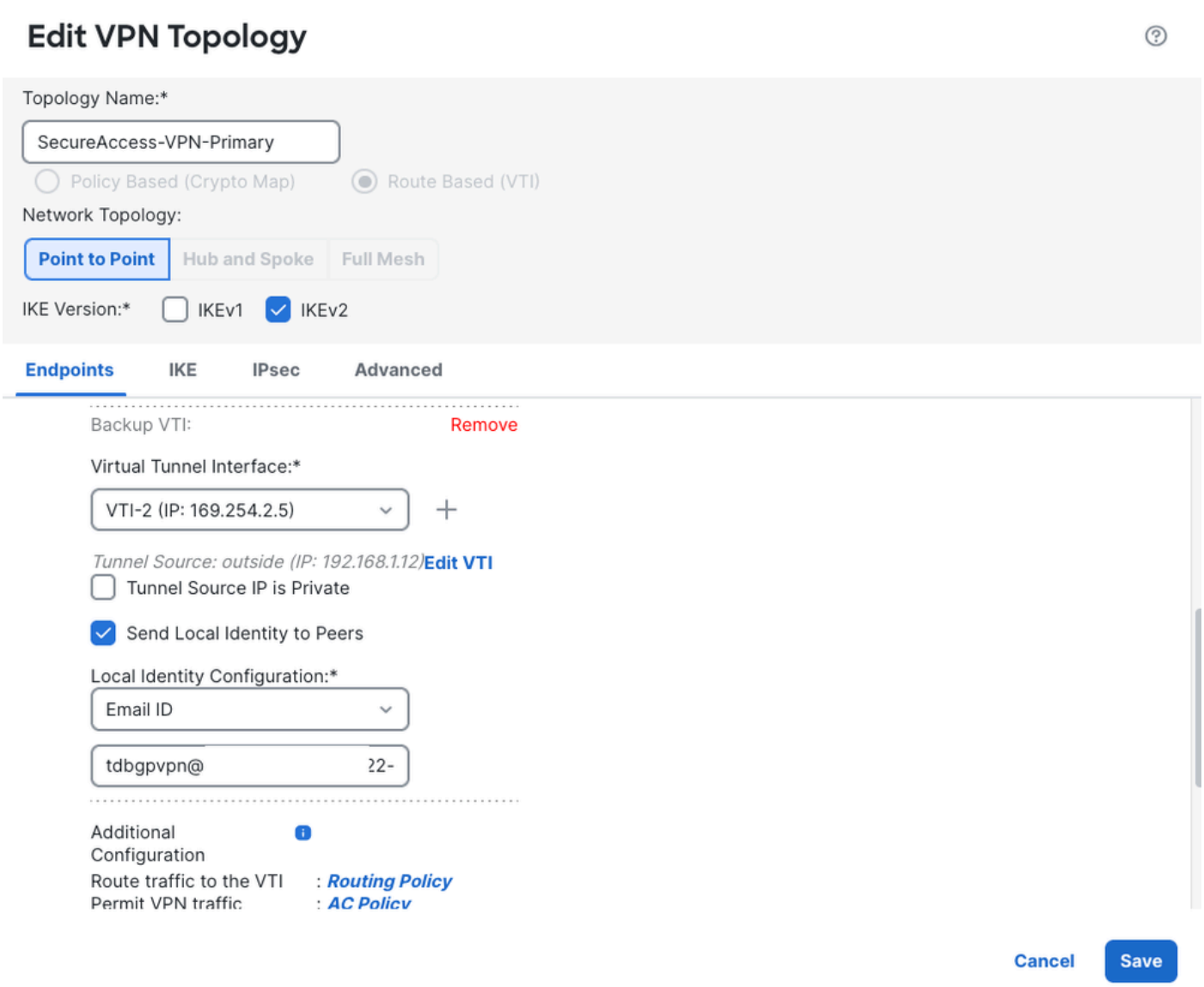
- Rufen Sie in Schritt 6 der Configure Network Tunnel Group on Secure Access die Tunnel-

IDs und IP-Adressen für das primäre und sekundäre Rechenzentrum ab.

- Klicken Sie auf Endgeräte
- Klicken Sie unter Knoten A auf Gerät, und wählen Sie Ihr FTD-Gerät aus.
- Klicken Sie auf Virtual Tunnel Interface (Virtuelle Tunnelschnittstelle), und wählen Sie die erste im vorherigen Schritt erstellte VTI-Schnittstelle aus.
- Klicken Sie auf Send Local Identity to Peers (Lokale Identität an Peers senden), und wählen Sie E-Mail-ID, geben Sie die primäre Tunnel-ID ein (aus "Save Network Tunnel Group Configuration" (Netzwerk-Tunnelgruppenkonfiguration speichern) unter Configure Network Tunnel Group on Secure Access (Netzwerktunnelgruppe für sicheren Zugriff konfigurieren)).
- Klicken Sie unter Knoten B auf Gerät, und wählen Sie Extranet aus.
- Klicken Sie auf den Gerätenamen, und geben Sie ihm einen Namen.
- Klicken Sie auf Endpunkt-IP-Adressen, und geben Sie die primäre und sekundäre IP-Adresse für sicheren Zugriff durch Kommas getrennt ein (aus "Save Network Tunnel Group Configuration" unter "Configure Network Tunnel Group on Secure Access").
- Klicken Sie auf Add Backup VTI.
- Klicken Sie auf Virtual Tunnel Interface, und wählen Sie die zweite VTI-Schnittstelle aus, die im vorherigen Schritt erstellt wurde.
- Klicken Sie auf Send Local Identity to Peers (Lokale Identität an Peers senden), und wählen Sie E-Mail-ID, geben Sie die sekundäre Tunnel-ID ein (aus "Save Network Tunnel Group Configuration" (Netzwerk-Tunnelgruppenkonfiguration speichern) unter Configure Network Tunnel Group on Secure Access (Netzwerktunnelgruppe für sicheren Zugriff konfigurieren)).
- Klicken Sie auf Speichern

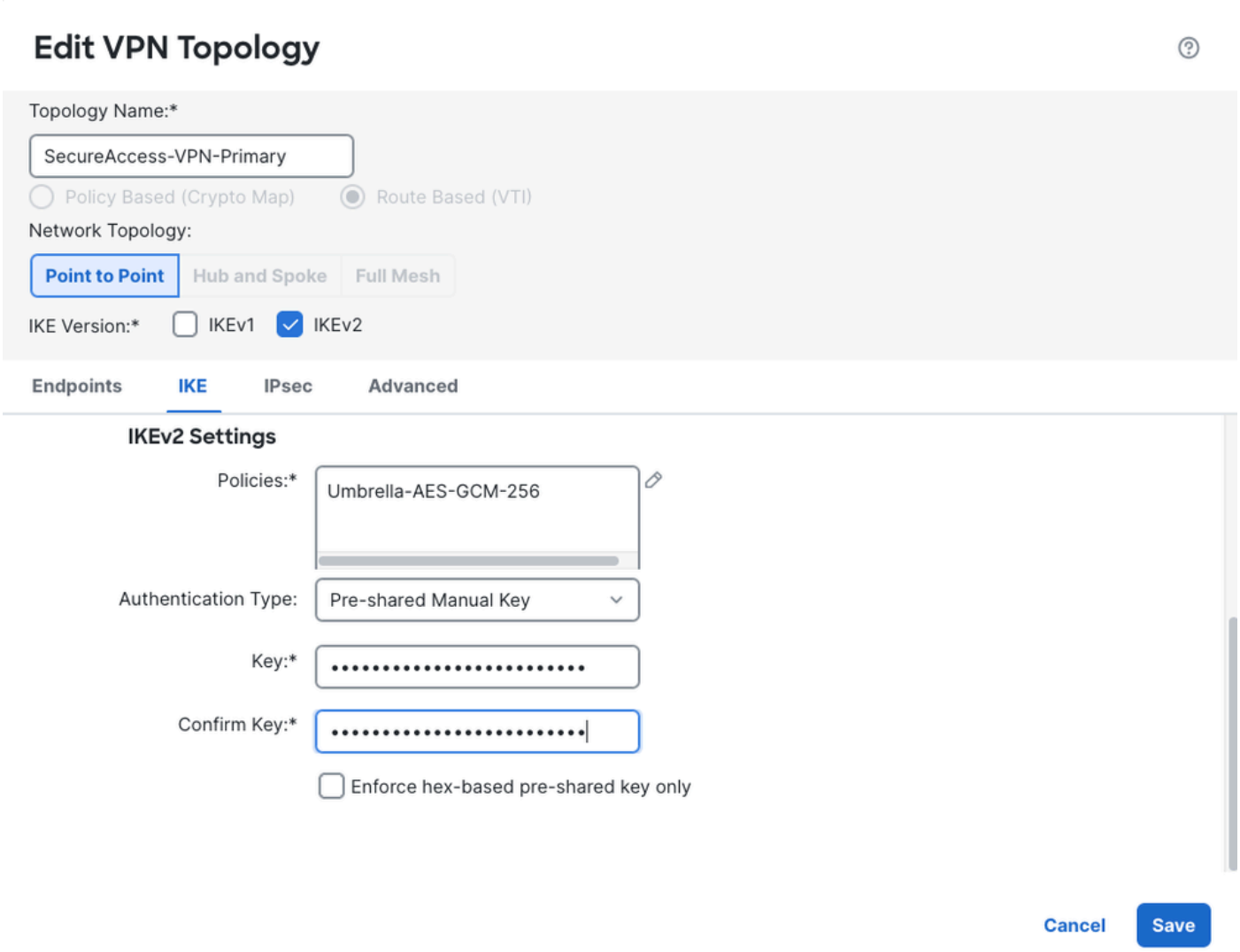


Secure FTD - VPN-Endpunktkonfiguration



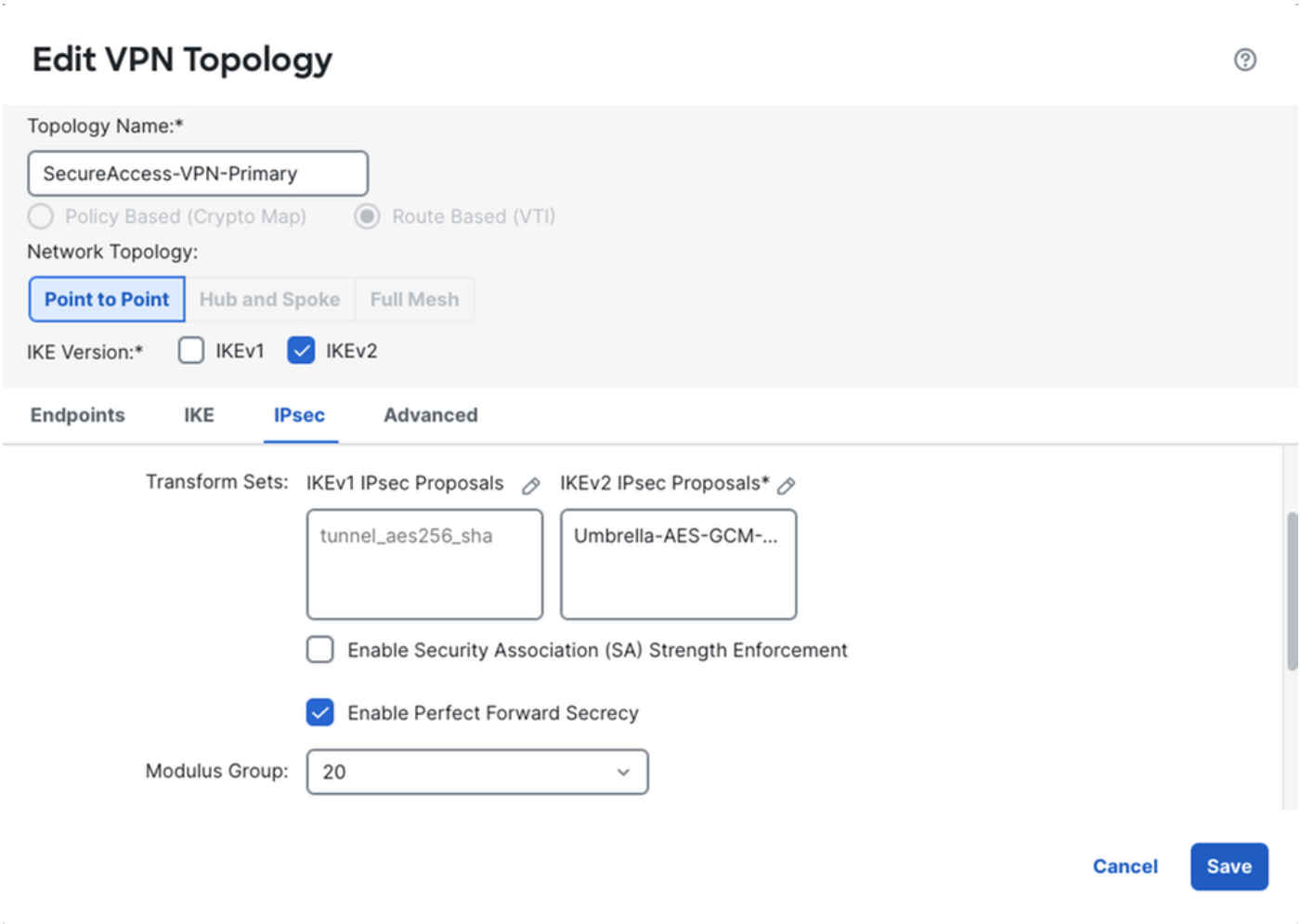
Secure FTD - VPN-Endpunktkonfiguration

- Konfigurieren der IKEv2-Einstellungen gemäß den unterstützten IPsec-Parametern
  - Wählen Sie Richtlinien als Umbrella-AES-GCM-256 aus
  - Authentifizierungstyp als vorinstallierten manuellen Schlüssel auswählen



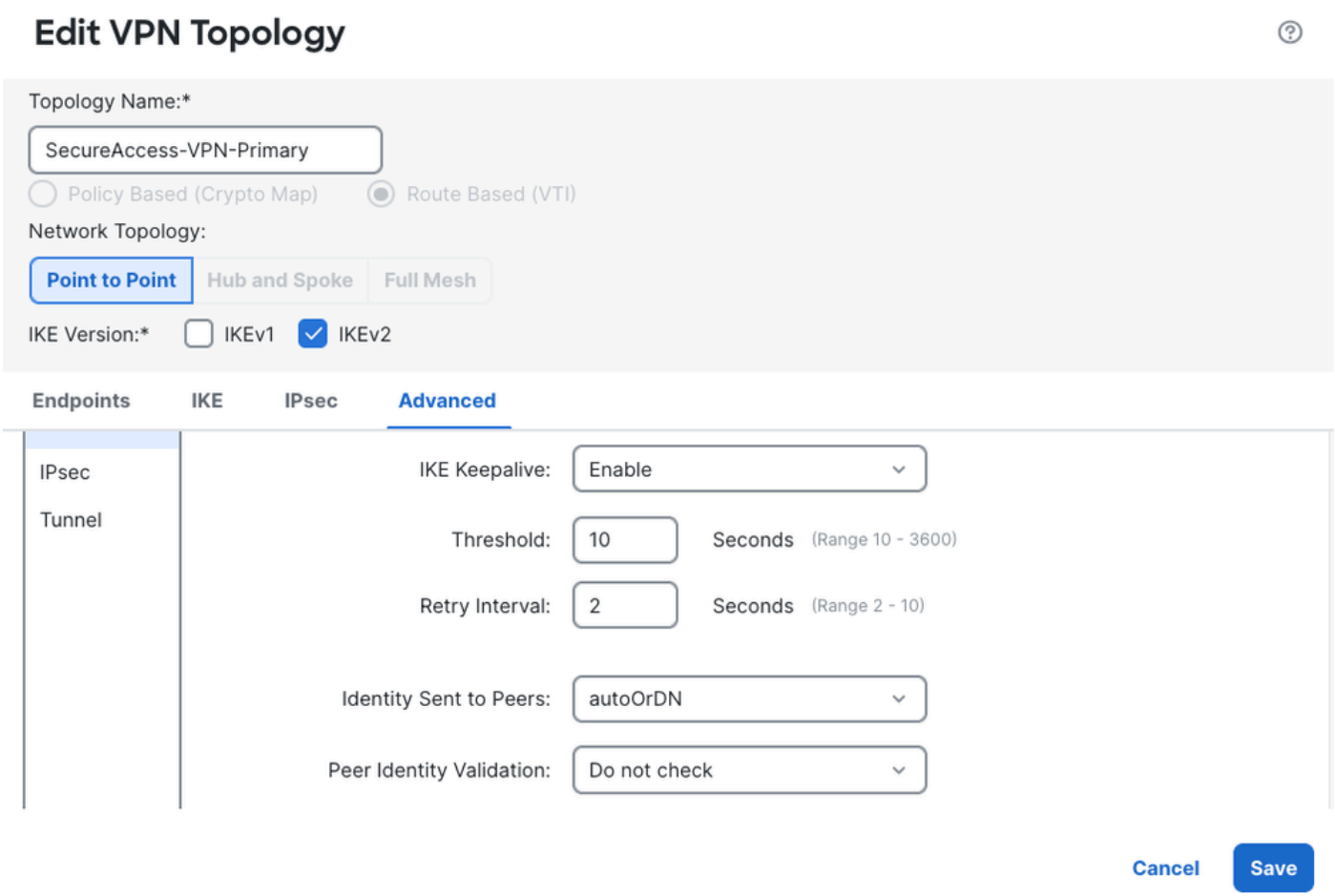
Secure FTD - VPN IKE-Einstellungen

- Konfigurieren von IPsec-Einstellungen
  - Wählen Sie IKEv2 IPsec-Angebote als Umbrella-AES-GCM-256 aus.
  - PFS als ausgewählte Modulgruppe als 20 aktivieren



Sichere FTD - VPN IPsec-Einstellungen

- Erweiterte Einstellungen
- Klicken Sie auf Save (Speichern).



Secure FTD - Erweiterte VPN-Einstellungen

FTD-richtlinienbasiertes Routing

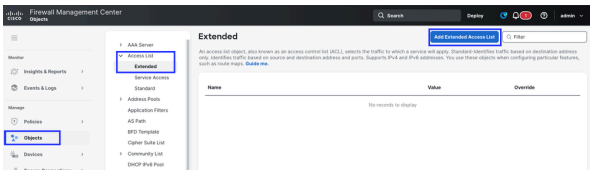
Beim herkömmlichen Routing werden Pakete basierend auf der Ziel-IP-Adresse geroutet. Es ist schwierig, die Weiterleitung eines bestimmten Verkehrs in einem zielbasierten Weiterleitungssystem zu ändern. Policy Based Routing (PBR) erweitert und ergänzt die von Routing-Protokollen bereitgestellten Mechanismen und bietet Ihnen so mehr Kontrolle über das Routing.

Mit PBR können Sie die IP-Rangfolge festlegen. Außerdem können Sie einen Pfad für bestimmten Datenverkehr festlegen, z. B. für Prioritätsdatenverkehr über eine teure Verbindung. Mit PBR können Sie Routing definieren, das auf anderen Kriterien als dem Zielnetzwerk basiert, z. B. Quellport, Zieladresse, Zielport, Protokoll, Anwendungen oder einer Kombination dieser Objekte. Weitere Informationen finden Sie unter Richtlinienbasiertes Routing.

1. Konfigurieren der Zugriffsliste

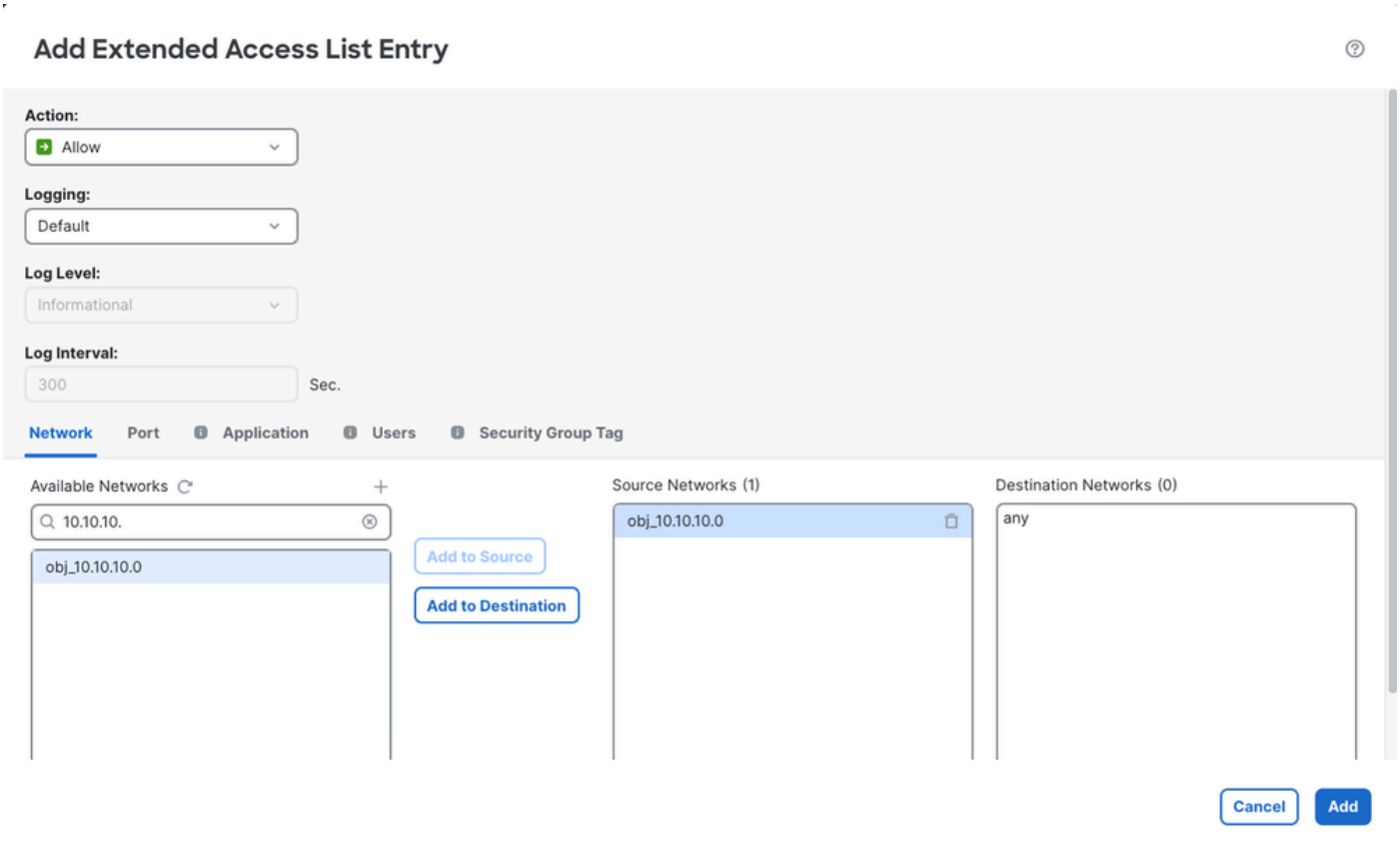
- Navigieren Sie zu Objekte > Zugriffsliste > Erweitert

- Klicken Sie auf Erweiterte Zugriffsliste hinzufügen.

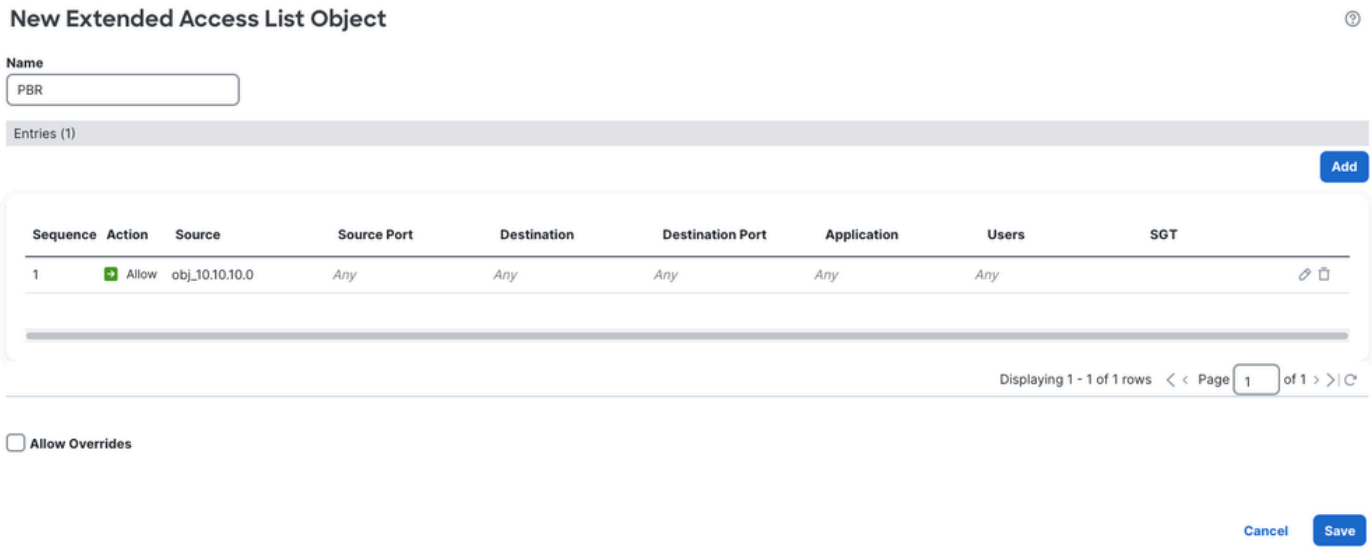


Secure FTD - erweiterte Zugriffsliste

- Geben Sie den Namen der Zugriffsliste an
- Aktion definieren
  - Zulassen. - Definierter Datenverkehr wird an IPsec-Tunnel gesendet
  - Blockieren - Datenverkehr wird vom IPsec-Tunnel umgangen
  - Die Regel wird basierend auf der Sequenznummer zugeordnet (von niedriger zu höher).
  - Klicken Sie auf Hinzufügen
  - Klicken Sie auf Save (Speichern).



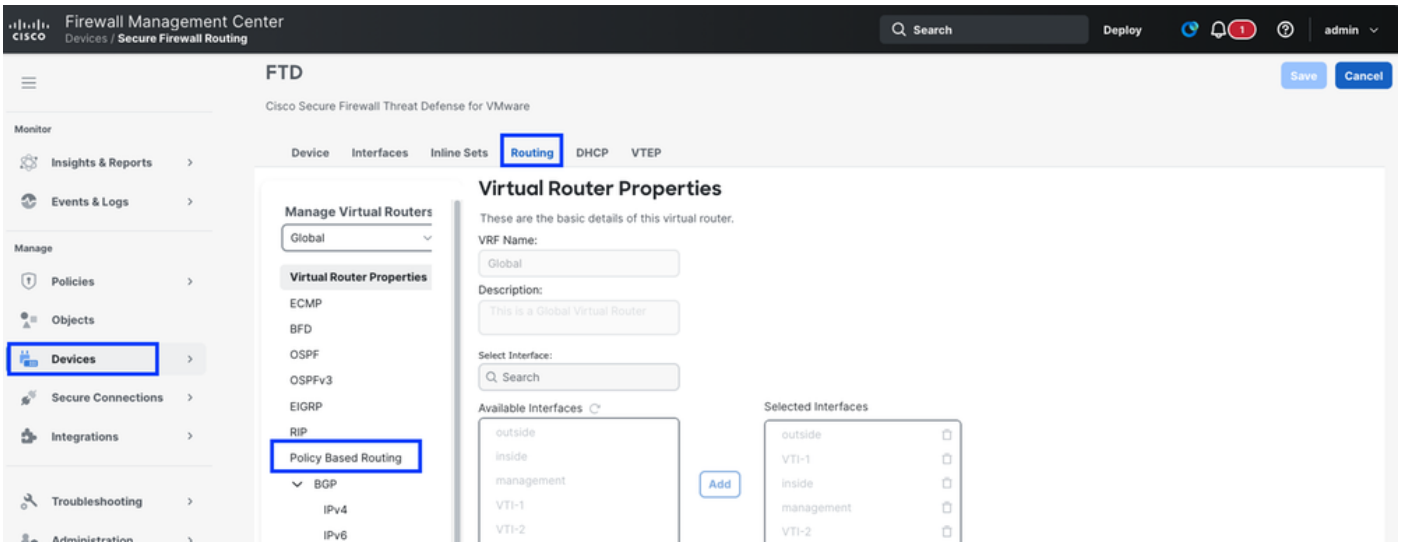
Secure FTD - erweiterte Zugriffsliste



Secure FTD - erweiterte Zugriffsliste

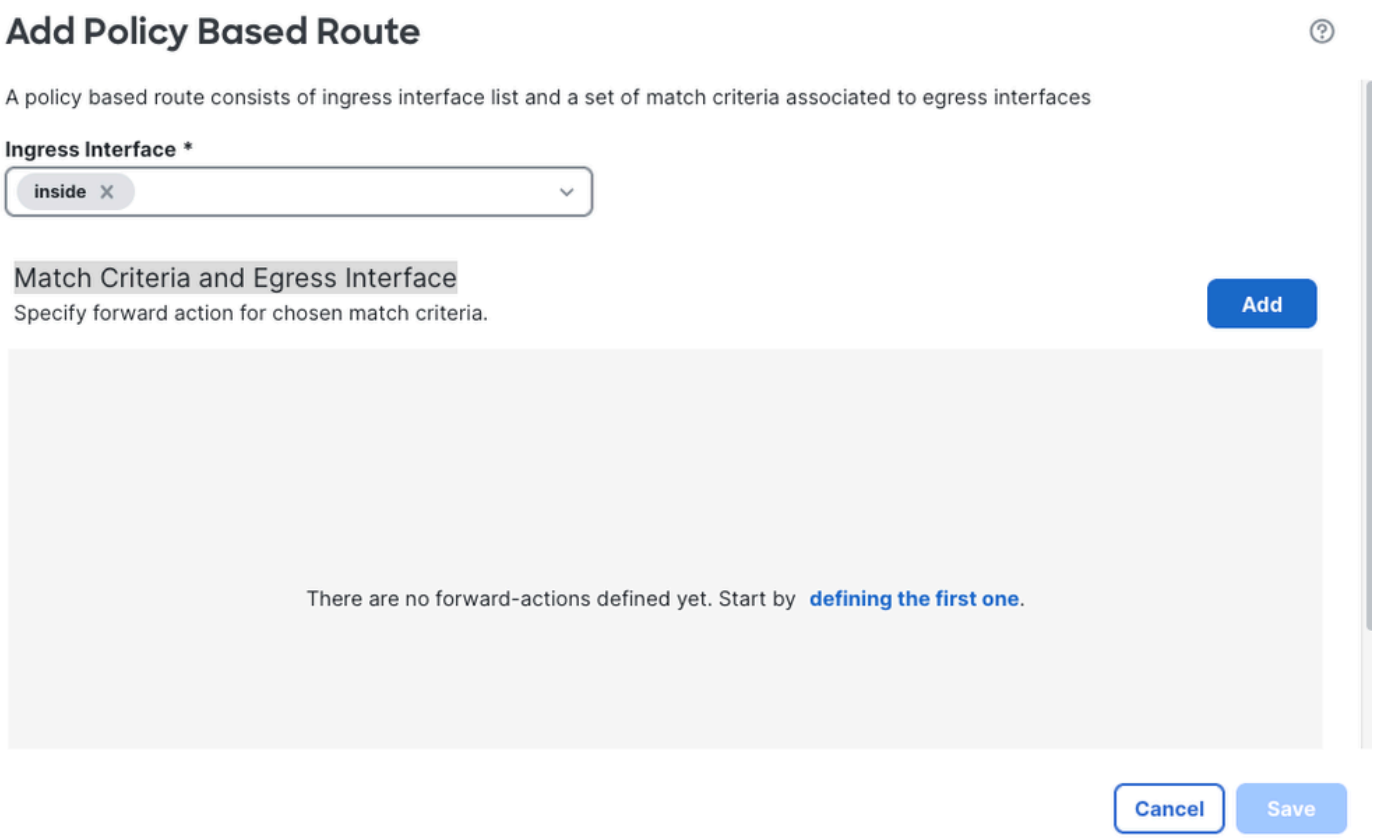
2. Richtlinienbasiertes Routing konfigurieren

- Navigieren Sie zu Geräte > Geräteverwaltung > FTD > Routing.



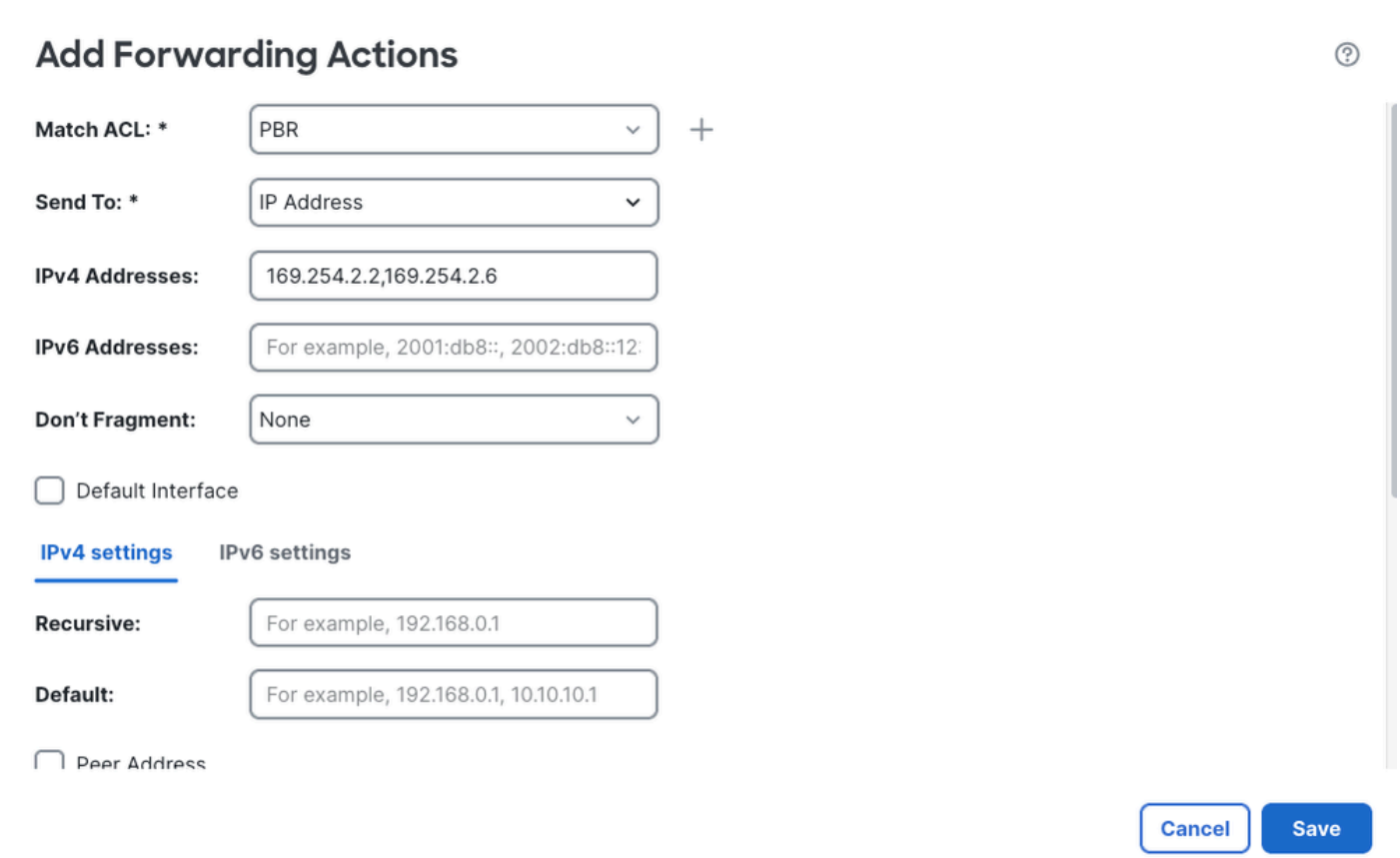
Secure FTD = Policy Based Routing (richtlinienbasiertes Routing)

- Klicken Sie auf Hinzufügen
- Wählen Sie Ingress Interface (Eingangsschnittstelle) - Eingangsschnittstelle für das in der Zugriffsliste definierte Subnetz aus.

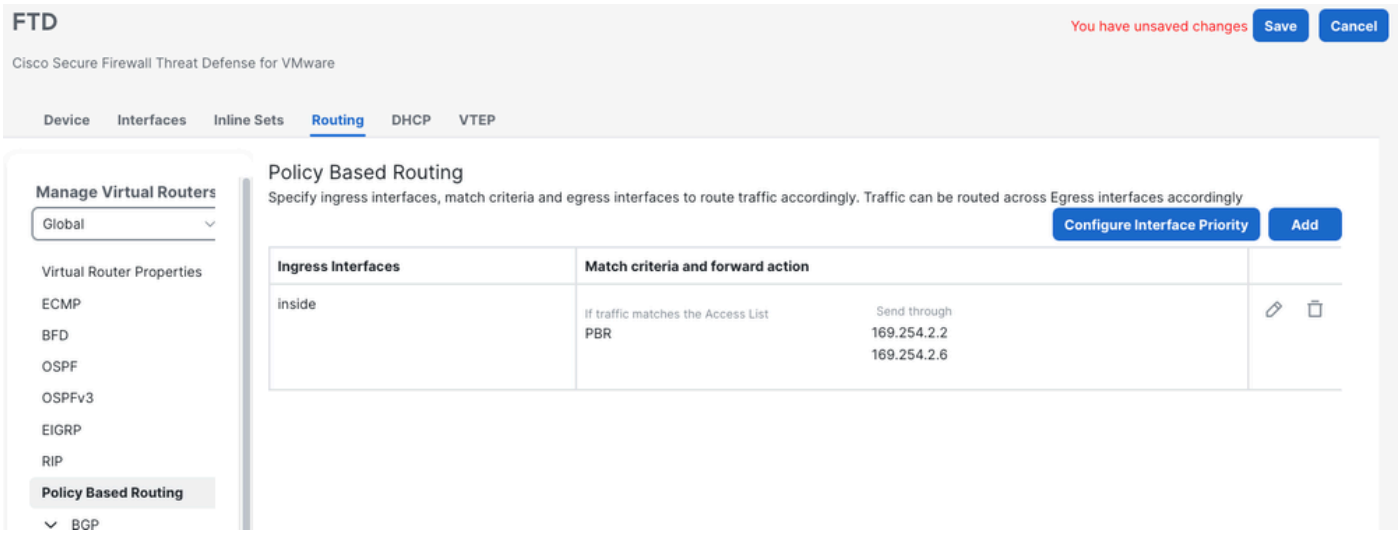


Secure FTD = Policy Based Routing (richtlinienbasiertes Routing)

- Zuordnungskriterien und Ausgangsschnittstelle definieren
  - Klicken Sie auf Hinzufügen
  - Wählen Sie die zutreffende ACL aus.
  - Wählen Sie Senden an als IP-Adresse aus.
  - Fügen Sie die IP-Adresse für den nächsten Hop hinzu. - IP-Adressen der VTIs-Schnittstelle sind. 169.254.2.130 und 169.254.2.5/30. Die nächsten Hop-IP-Adressen für VTI -1 und VTI-2 sind also 169.254.2.2 und. 169.254.2.6
  - Klicken Sie auf Speichern



Secure FTD = Policy Based Routing (richtlinienbasiertes Routing)

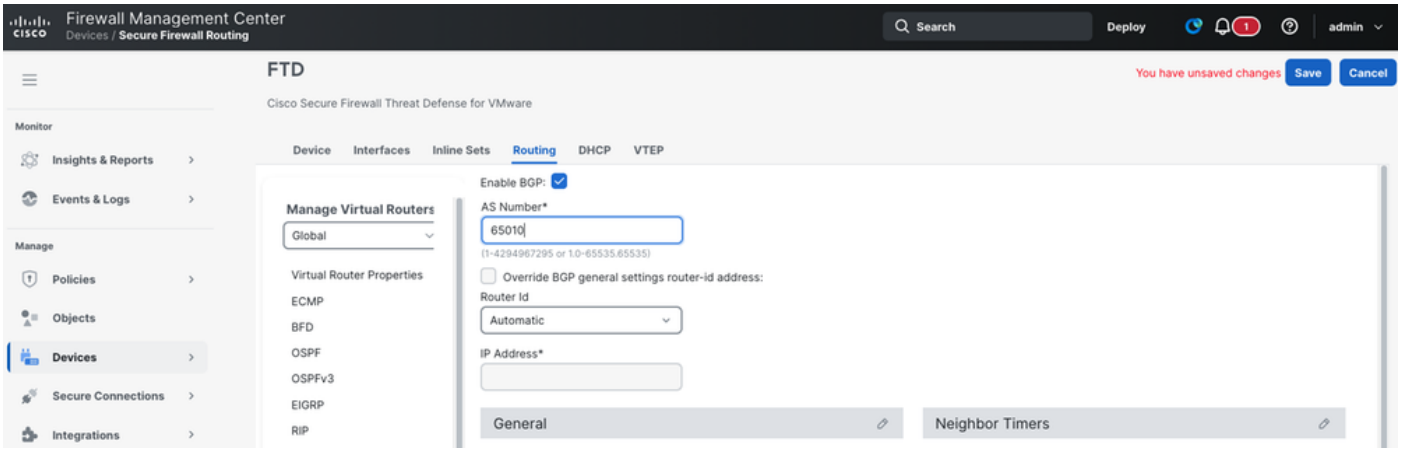


Secure FTD = Policy Based Routing (richtlinienbasiertes Routing)

Konfigurieren von BGP auf FTD

1. BGP aktivieren

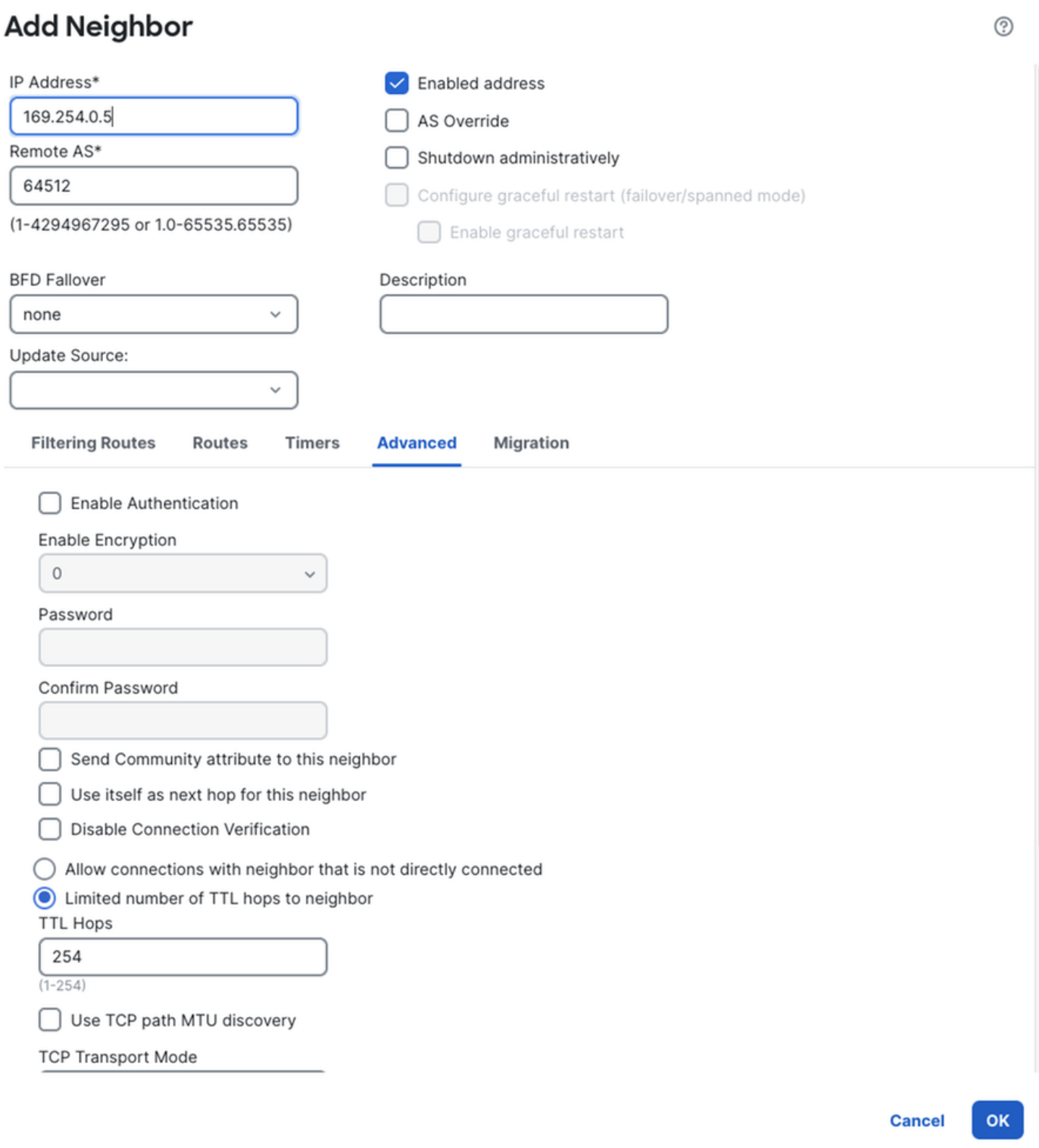
- Navigieren Sie zu Geräte > Geräteverwaltung > FTD > Routing > Allgemeine Einstellungen > BGP
- Aktivieren Sie BGP, und fügen Sie die AS-Nummer hinzu (FTD, lokale AS-Nummer).
- Klicken Sie auf Save (Speichern).

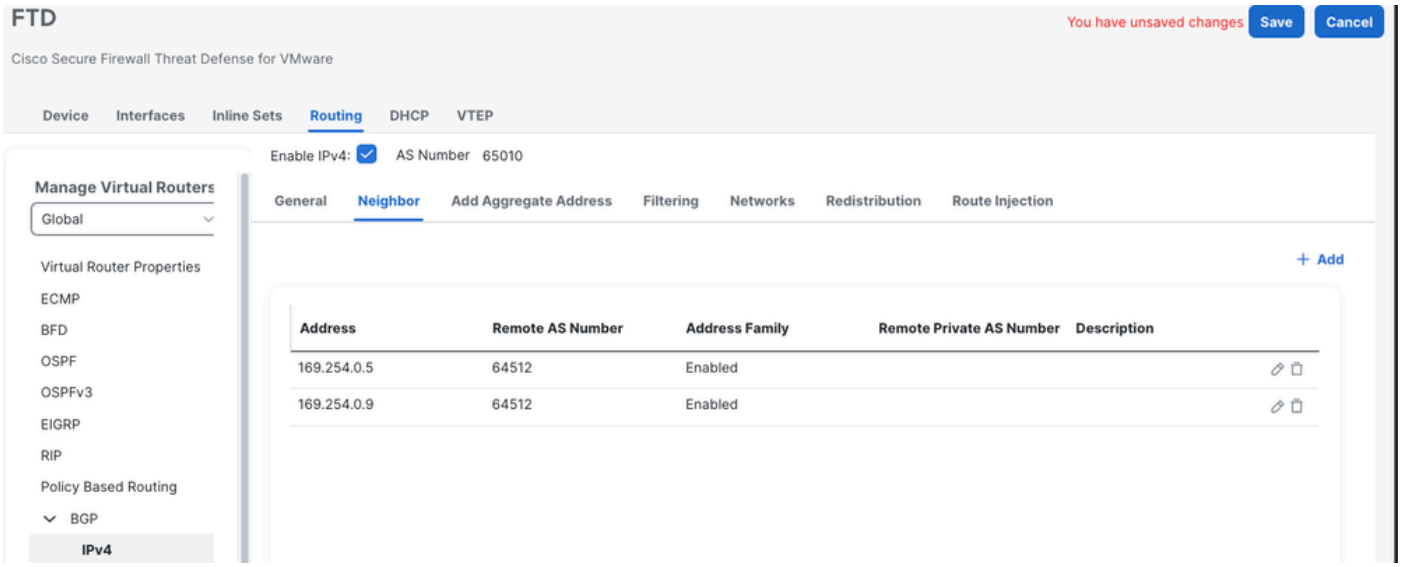


Secure FTD - BGP-Routing

- Navigieren Sie zu BGP > IPv4.

2. BGP-Nachbarn hinzufügen - BGP-Peers für sicheren Zugriff sind 169.254.0.5 und. 169.254.0.9

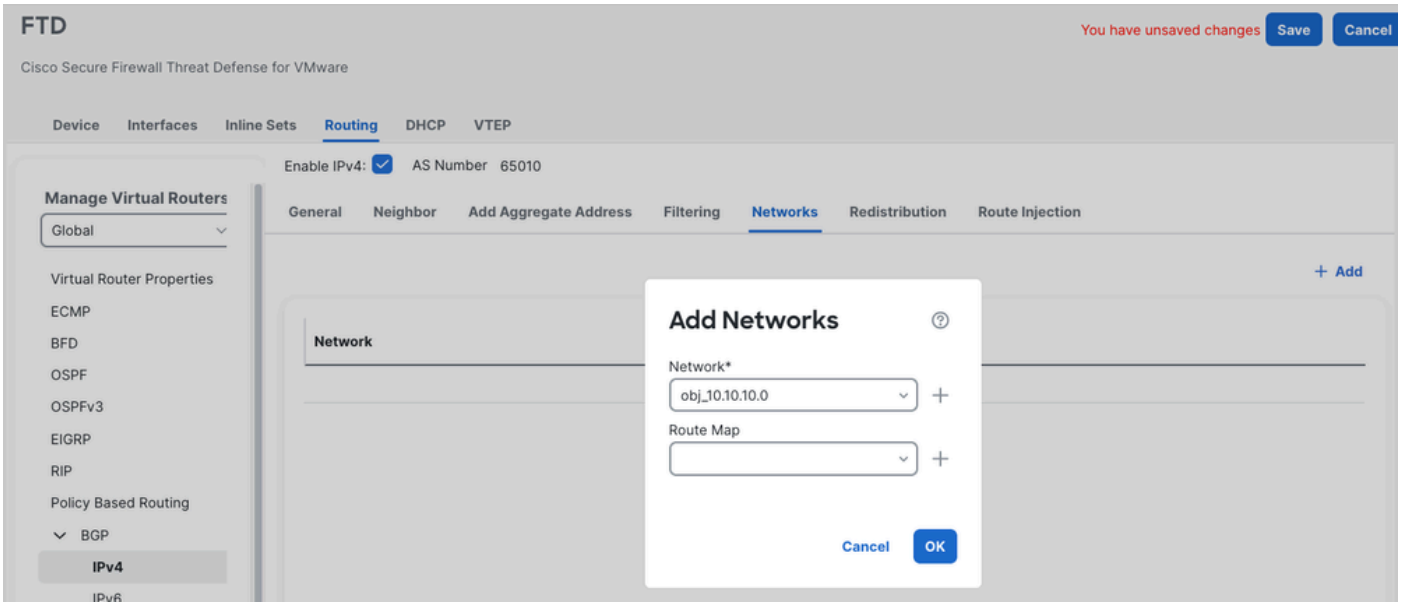

Add Neighbor
IP Address*
169.254.0.5
Remote AS*
64512
(1-4294967295 or 1.0-65535.65535)
Enabled address
AS Override
Shutdown administratively
Configure graceful restart (failover/spanned mode)
Enable graceful restart
BFD Fallover
none
Description
Update Source:
Filtering Routes
Routes
Timers
Advanced
Migration
Enable Authentication
Enable Encryption
0
Password
Confirm Password
Send Community attribute to this neighbor
Use itself as next hop for this neighbor
Disable Connection Verification
Allow connections with neighbor that is not directly connected
Limited number of TTL hops to neighbor
TTL Hops
254
(1-254)
Use TCP path MTU discovery
TCP Transport Mode
Cancel
OK



Secure FTD - BGP-Routing

3. Fügen Sie die Netzwerke hinzu - Netzwerke, die für den sicheren Zugriff angekündigt werden müssen.

- Klicken Sie auf OK.

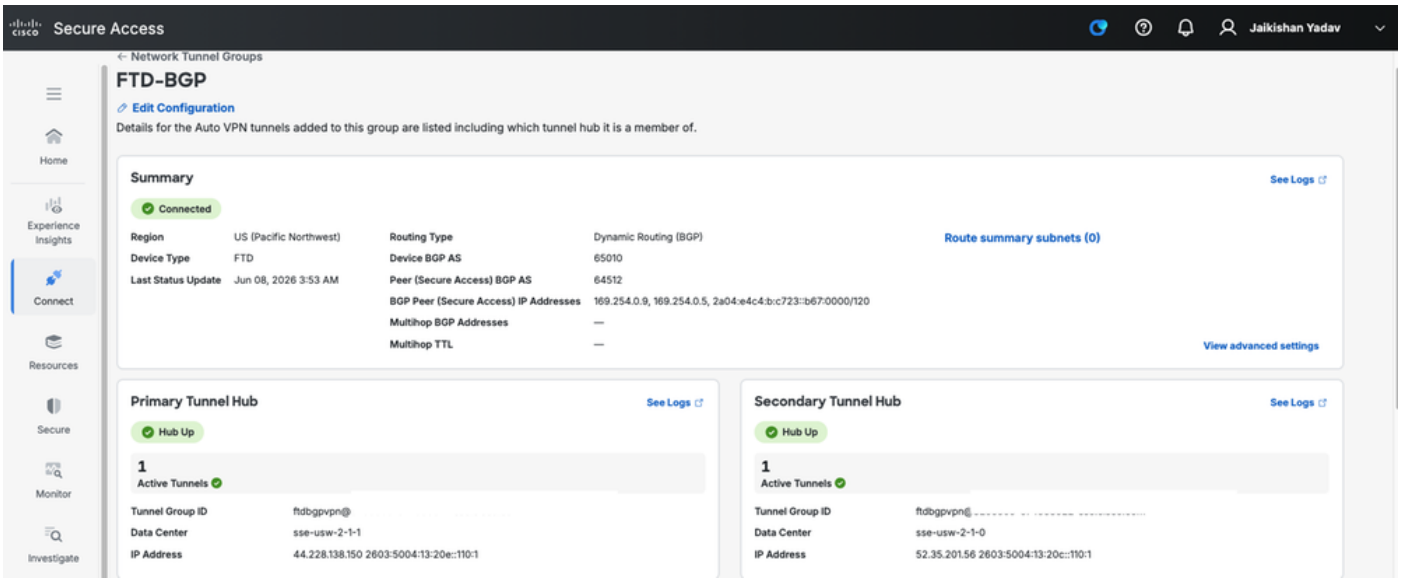


Secure FTD - BGP-Routing

- Speichern und Bereitstellen der Änderungen

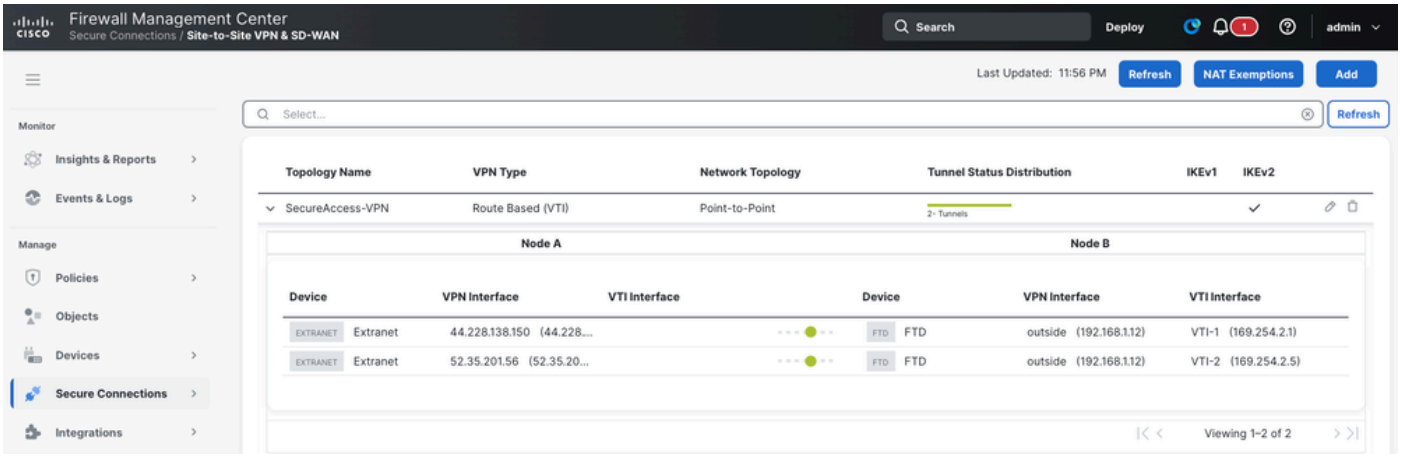
Tunnel-Status überprüfen

Sicherer Zugriff



Sichere FTD - IPsec-Tunnelstatus

Auf FMC



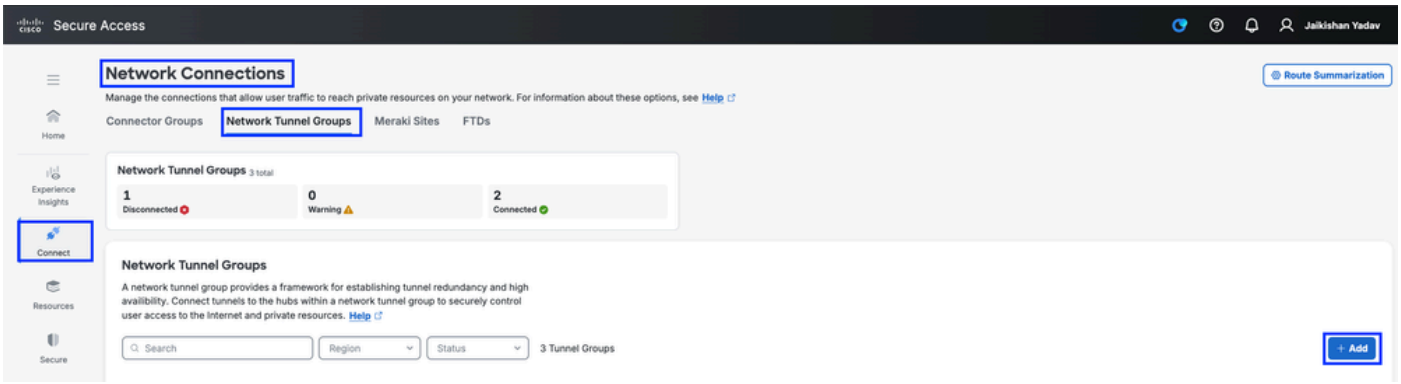
Sicheres FMC - IPsec-Tunnelstatus

Konfigurieren eines statischen, routenbasierten IPsec-VPNs auf der Adaptive Security Appliance (ASA) mit PBR

VPN-Konfiguration für sicheren Zugriff

1. Anmeldung beim Dashboard für sicheren Zugriff Sicherer Zugriff
2. Navigieren Sie zu Verbinden > Netzwerkverbindungen > Netzwerk-Tunnelgruppen, und klicken

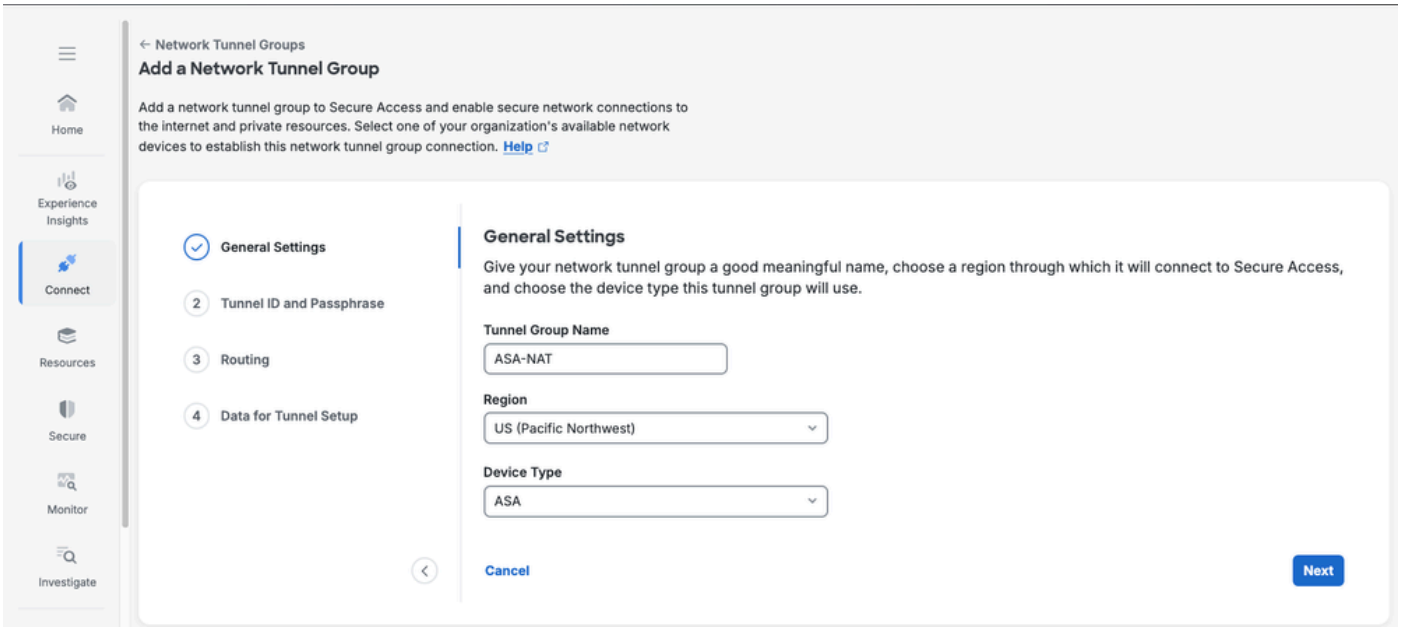
Sie auf +Hinzufügen, um die Netzwerk-Tunnelgruppe zu konfigurieren.



Sicherer Zugriff - Netzwerk-Tunnelgruppen

3. Konfigurieren der Netzwerk-Tunnelgruppe - Allgemeine Einstellungen

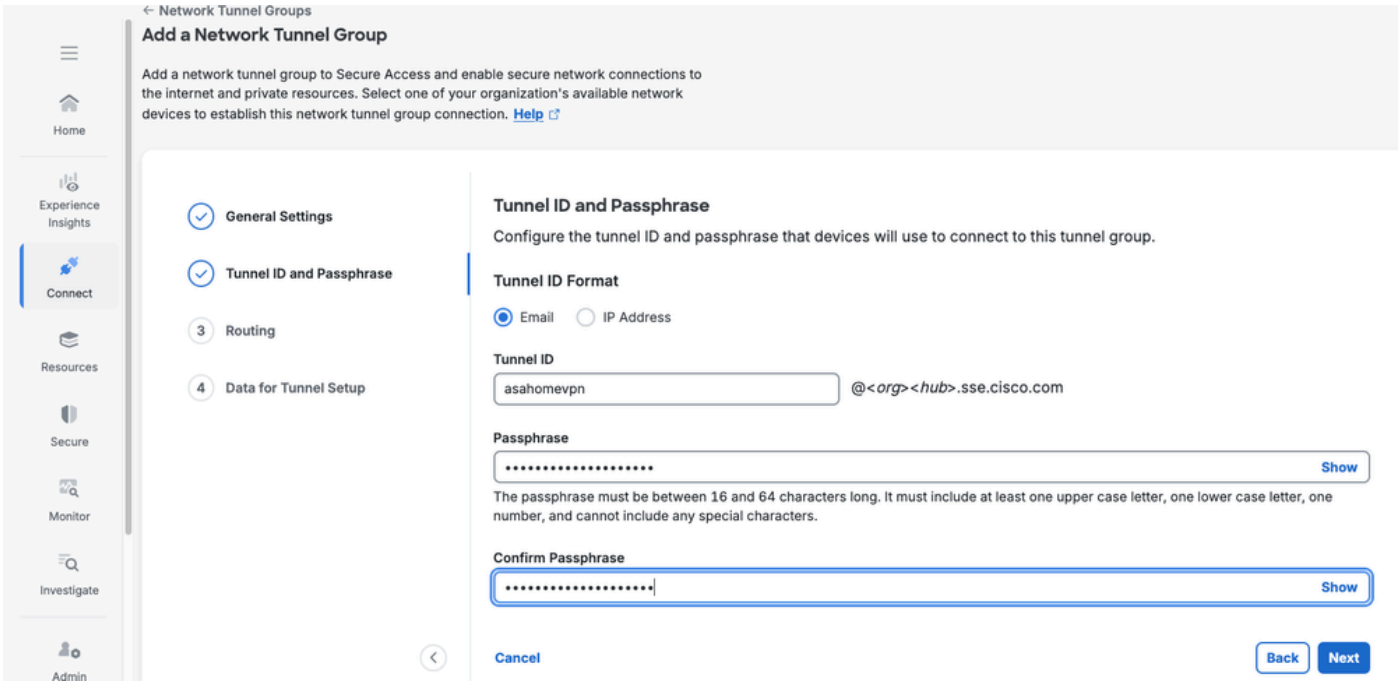
- Konfigurieren von Tunnelgruppenname, Region und Gerätetyp
- Klicken Sie auf Next (Weiter).



Sicherer Zugriff - Allgemeine Einstellungen für Netzwerk-Tunnelgruppen

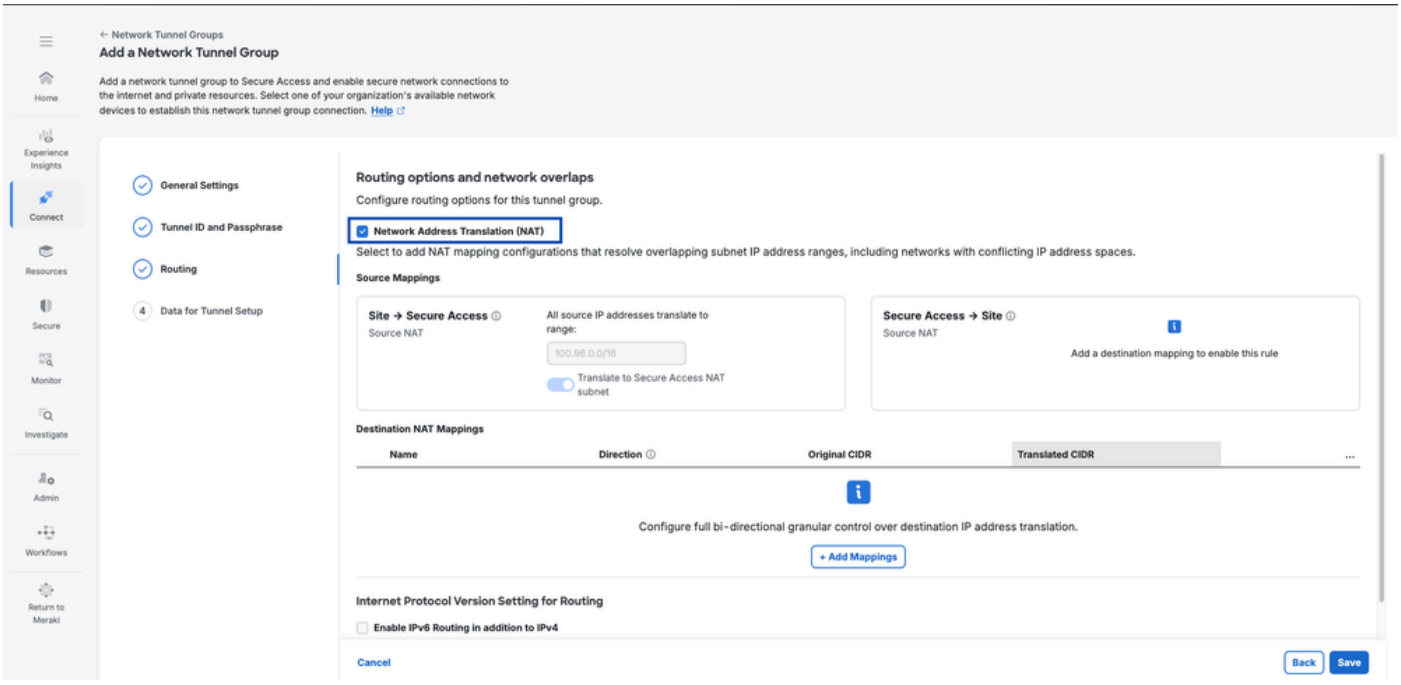
4. Konfigurieren Sie die Tunnel-ID und die Passphrase.

- Konfigurieren Sie die Tunnel-ID und die Passphrase.
- Klicken Sie auf Weiter



Sicherer Zugriff - Netzwerk-Tunnelgruppen

5. Network Address Translation (NAT) aktivieren

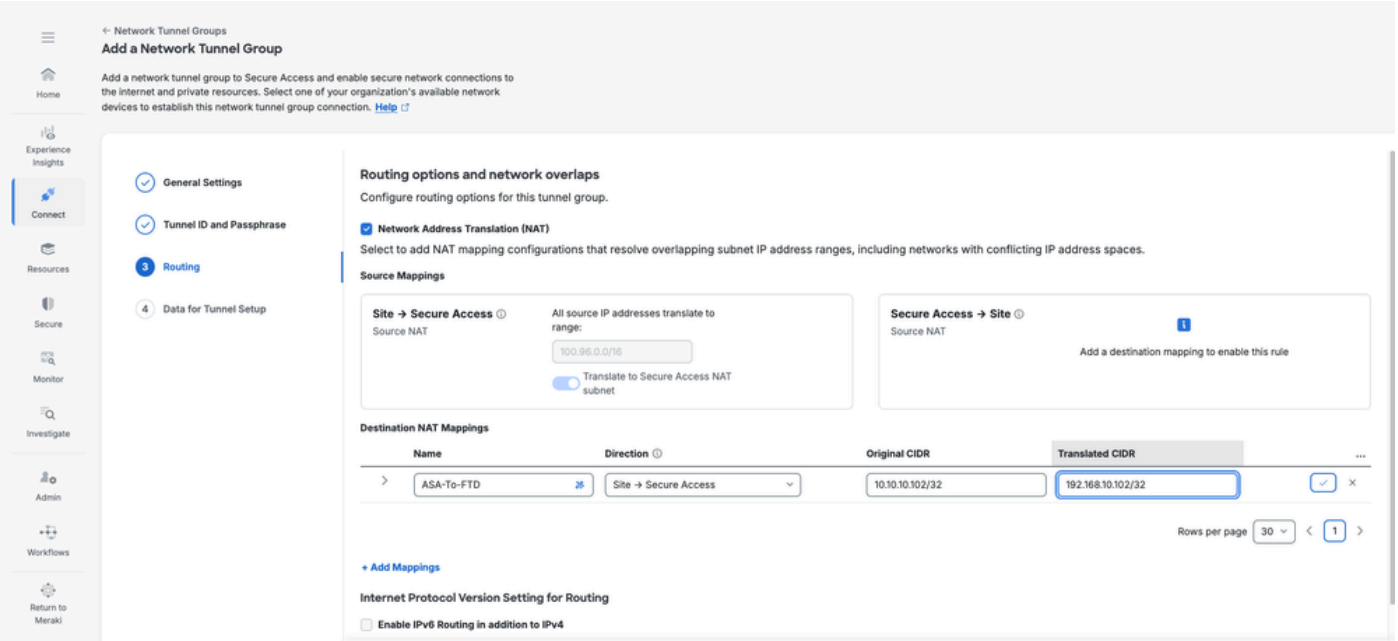


Sicherer Zugriff - Network Tunnel Groups NAT-Einstellungen

6. Ziel-NAT-Zuordnung hinzufügen

Fluss 1 - Router 1 zu Router 2 (Standort für sicheren Zugriff)

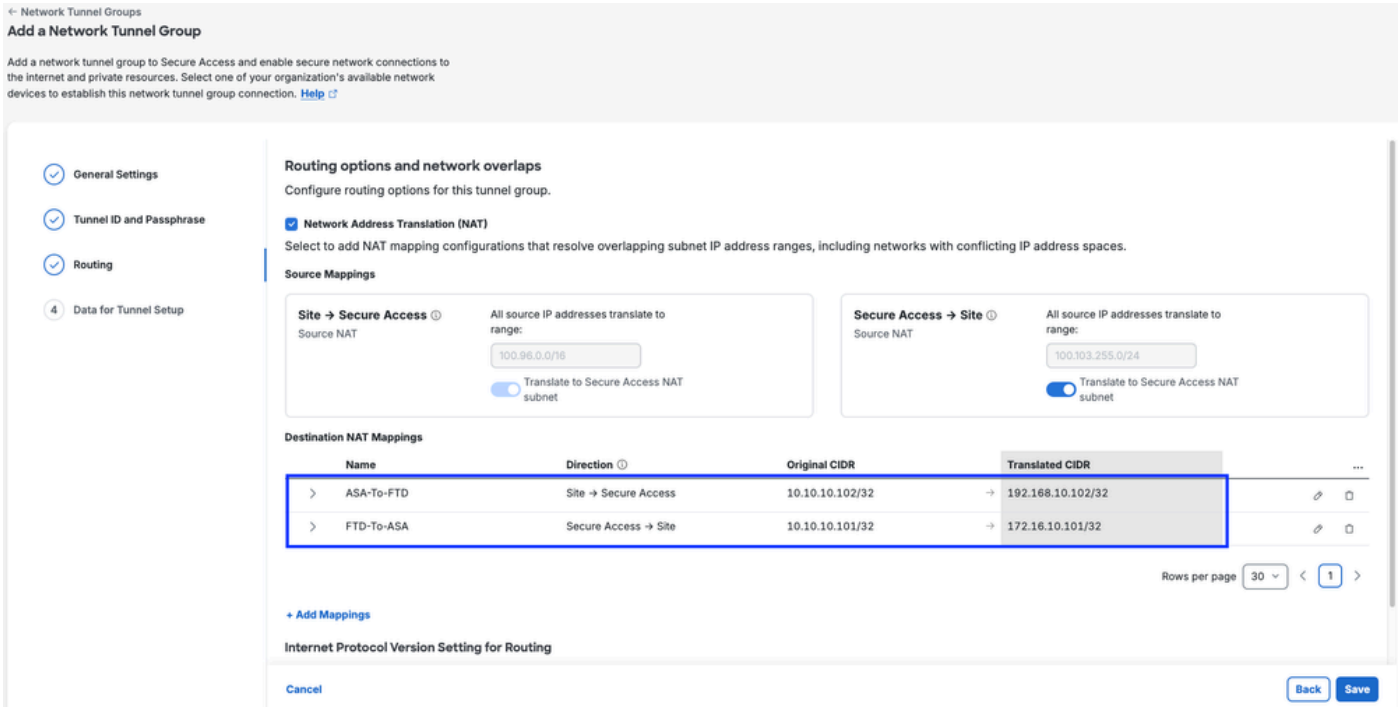
Fluss 2 - Router 2 zu Router 1 (sicherer Zugriff auf den Standort)



Sicherer Zugriff - Network Tunnel Groups NAT-Einstellungen

Vorsicht: Wenn NAT aktiviert ist, ist BGP nicht möglich. Konfigurieren Sie auch statisches VPN auf Customer Edge-Geräten.

Tipp: Denken Sie immer daran, einen Ping an eine übersetzte IP zu senden.
Translated IP goes in Translated CIDR und Real IP goes in Original CIDR.



Sicherer Zugriff - Network Tunnel Groups NAT-Einstellungen

Klicken Sie Speichern

Tipp: Für den Datenverkehr von "Standort A" zu "Standort B" lautet die CNHE-1-Richtung "Standort-> SecureAccess".
Für den Datenverkehr von "Standort B" zu "Standort A" lautet die CNHE-1-Richtung "SecureAccess -> Standort".

VPN-Konfiguration auf ASA

1. Melden Sie sich bei der ASA CLI an, wechseln Sie in den privilegierten Modus, und überprüfen Sie die grundlegende IP-Verbindung zum Internet.

ASA# sh ip
System-IP-Adressen:
Schnittstellenname IP-Adresse Subnetzmaske Methode
GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0 manual
GigabitEthernet0/1 inside 10.10.10.1 255.255.255.0 manual

Aktuelle IP-Adressen:
Schnittstellenname IP-Adresse Subnetzmaske Methode
GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0 manual

GigabitEthernet0/1 inside 10.10.10.1 255.255.255.0 manual

```
ASA# ping 8.8.8.8
Geben Sie Escape-Sequenz ein, um den Vorgang abzubrechen.
Senden von 5 100-Byte-ICMP-Echos an 8.8.8.8, Zeitüberschreitung beträgt 2 Sekunden:
!!!!!
Erfolgsrate: 100 Prozent (5/5), Round-Trip-Wert (Min./Durchschnitt/Max.) = 20/28/30 ms
ASA#
```

2. Konfigurieren Sie die IKEv2-Richtlinie, und aktivieren Sie IKEv2 auf der externen Schnittstelle.

```
crypto ikev2 policy 10
Verschlüsselung aes-gcm-256
Integrität Null
Gruppe 19
Lebensdauersekunden 86400
crypto ikev2 enable outside
```

3. IPSec-Angebot konfigurieren

```
crypto ipsec ikev2 ipsec-vorschlag ipsec-vorschlag primär
Protokoll-ESP-Verschlüsselung aes-gcm-256
```

4. Konfigurieren des IPsec-Profils

```
crypto ipsec-Profil csa-profile-primary
set ikev2 ipsec-Proposal Ipsec-Proposal-Primary
set ikev2 local-identity email-id <primäre Tunnel-ID>
```

5. Konfigurieren Sie die Gruppenrichtlinie, und aktivieren Sie das IKEv2-Protokoll unter dem Attribut.

```
Gruppenrichtlinie CSA-Richtlinie-primär intern
Gruppenrichtlinien-CSA-Richtlinie-primäre Attribute
vpn-tunnel-protocol ikev2
```

6. Konfigurieren der Tunnelgruppe

```
tunnel-group 44.228.138.150 Typ ipsec-l2l
tunnel-group 44.228.138.150 allgemeine Attribute
```

default-group-policy, csa-policy-primary
tunnel-group 44.228.138.150 ipsec-attribute
ikev2 Remote-Authentifizierung Pre-Shared-Key <Pre-Shared-Key>
ikev2 local-authentication pre-shared-key <pre-shared-key>

7. Konfigurieren der virtuellen Tunnelschnittstelle (VTI)

- Nameif kann sein, wenn Sie Ihre Wahl
- Die dem VTI zugewiesene IP-Adresse darf sich nicht mit anderen Schnittstellen auf der ASA überschneiden.
- TunnelquelleStellt die externe Schnittstelle der Firewall dar
- Tunnelziel muss die IP-Adresse des Rechenzentrums sein

interface Tunnel1
NameEIF VTI-1
ip address 169.254.2.1 255.255.255.252
Tunnelquellenschnittstelle außen
Tunnelziel 44.228.138.150
Tunnelmodus IPsec IPv4
tunnel protection ipsec profil csa-profile-primary

8. Konfigurieren Sie das Routing so, dass der Datenverkehr zur zugeordneten IP-Adresse oder zum Subnetz innerhalb der VTI-Schnittstelle geroutet wird. Next Hop muss nach IP innerhalb des VTI-Bereichs sortiert werden.

route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5. (für internetbasierten RAVPN-Pool- oder CGNAT-Verkehr)

Oder

Route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

Richtlinienbasiertes Routing

1. Zugriffsliste

access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any

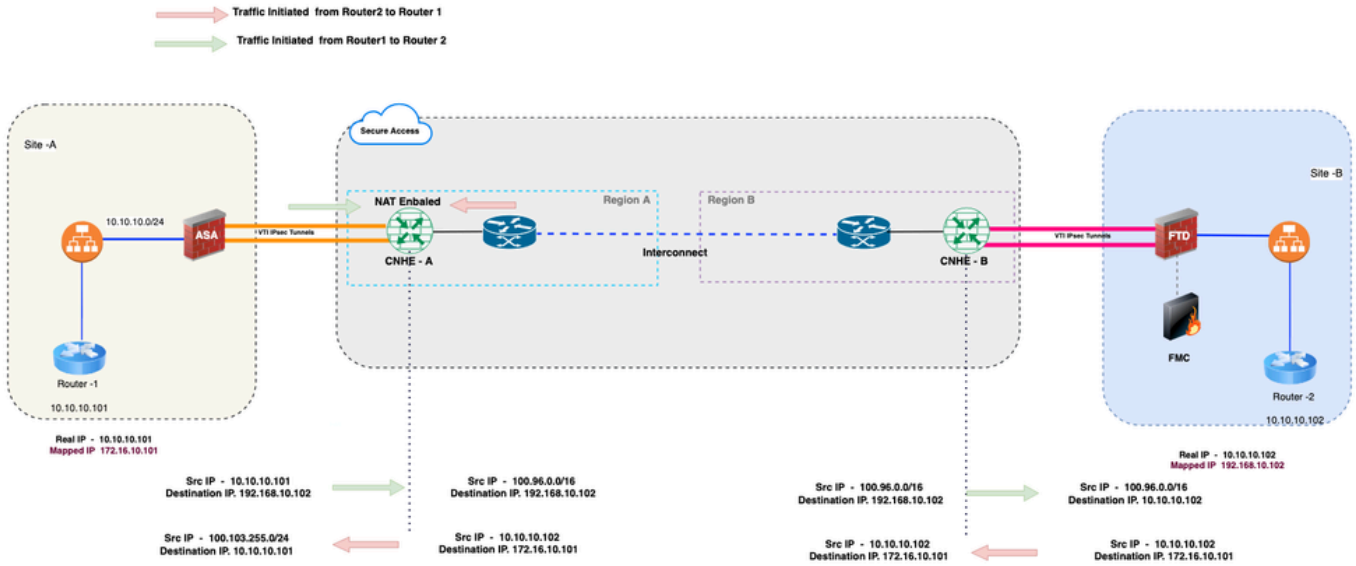
2. Routenkarte

route-map RM-CSA permit 10
Match-IP-Adresse PBR
set ip next-hop 169.254.2.2 169.254.2.6

3. Anwenden der Routenübersicht auf die Eingangsschnittstelle

interface GigabitEthernet0/1
nameif inside
Sicherheitsstufe 100
ip address 10.10.10.1 255.255.255.0
policy-route-route-map RM-CSA

Überprüfung



Router-Schnittstelle und GW-Erreichbarkeitsstatus

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.101   YES NVRAM  down                  down
GigabitEthernet2       10.10.10.101    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet9       unassigned      YES unset  administratively down down
Router1#ping  10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Test 1- Router2 —> Router1. - Ping-Test

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

Paketerfassung auf ASA (lokale Firewall)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

   1: 10:56:45.024244       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.231143       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232470       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441856       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443122       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652477       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653423       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875397       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876450       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082301       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 10:56:45.024458       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.230914       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232516       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441795       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443153       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652432       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653454       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875351       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876480       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082240       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

Paketerfassung auf FTD (Remote-FW)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

10 packets captured

   1: 16:06:41.122292       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124856       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.329557       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330442       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546327       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547106       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752036       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752814       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.967891       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968501       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:06:41.123299       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124825       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.330000       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330396       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546800       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547090       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752448       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752783       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.968242       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968486       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
```

Test 2: - Ping-Test für Router 2 —> Router 1

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.10.10.102    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

FTD-Paketerfassung (lokale FW)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

   1: 16:11:45.622450       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823825       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825762       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045667       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046857       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252321       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253572       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453803       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454764       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664119       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:11:45.622083       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823886       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825442       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045697       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046582       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252352       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253313       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453849       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454596       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664150       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
```

ASA-Paketerfassung (Remote FW)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

   1: 11:08:30.288391       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289123       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504566       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.504963       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710992       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711404       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917112       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917402       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128243       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128640       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 11:08:30.287964       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289322       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504505       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.505009       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710961       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711434       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917066       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917417       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128197       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128685       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```

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.