

# Konfigurieren eines routenbasierten Site-to-Site-VPN-Tunnels auf dem vom FMC verwalteten FTD

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Einschränkungen und Einschränkungen](#)

[Konfigurationsschritte auf FMC](#)

[Überprüfung](#)

[Von der FMC-GUI](#)

[Von FTD CLI](#)

## Einleitung

In diesem Dokument wird die Konfiguration eines routenbasierten Site-to-Site-VPN-Tunnels auf einem von einem FirePOWER Management Center (FMC) verwalteten FirePOWER Threat Defense (FTD) beschrieben.

## Voraussetzungen

### Anforderungen

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

- Grundlegendes Verständnis der Funktionsweise eines VPN-Tunnels
- Sie wissen, wie Sie durch das FMC navigieren.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco FirePOWER Management Center (FMC) Version 6.7.0
- Cisco Firepower Threat Defense (FTD) Version 6.7.0

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 verstehen.

# Hintergrundinformationen

Routenbasiertes VPN ermöglicht die Bestimmung von interessantem Datenverkehr, der verschlüsselt oder über einen VPN-Tunnel gesendet werden soll, und die Verwendung von Traffic Routing anstelle von Richtlinien/Zugriffslisten, wie in richtlinienbasiertem oder Crypto-Map-basiertem VPN. Die Verschlüsselungsdomäne ist so festgelegt, dass jeder Datenverkehr, der in den IPsec-Tunnel eintritt, zugelassen wird. Die Auswahl für lokalen und Remote-IPsec-Datenverkehr ist auf 0.0.0.0/0.0.0.0 festgelegt. Dies bedeutet, dass jeder Datenverkehr, der in den IPsec-Tunnel geleitet wird, unabhängig vom Quell-/Ziel-Subnetz verschlüsselt wird.

## Einschränkungen und Einschränkungen

Dies sind bekannte Einschränkungen und Einschränkungen für routenbasierte Tunnel auf FTD:

- Unterstützt nur IPsec. GRE wird nicht unterstützt.
- Dynamisches VTI wird nicht unterstützt.
- Unterstützt nur IPv4-Schnittstellen sowie IPv4, geschützte Netzwerke oder VPN-Nutzlasten (keine Unterstützung für IPv6).
- Für VTI-Schnittstellen, die den VPN-Datenverkehr klassifizieren, wird statisches Routing und nur das dynamische BGP-Routing-Protokoll unterstützt (keine Unterstützung für andere Protokolle wie OSPF, RIP usw.).
- Pro Schnittstelle werden nur 100 VTIs unterstützt.
- VTI wird auf einem FTD-Cluster nicht unterstützt.
- VTI wird in diesen Richtlinien nicht unterstützt:
  - QoS
  - NAT
  - Plattformeinstellungen

Diese Algorithmen werden auf FMC/FTD Version 6.7.0 für neue VPN-Tunnel nicht mehr unterstützt (FMC unterstützt alle entfernten Chiffren zur Verwaltung von FTD < 6.7):

- 3DES-, DES- und NULL-Verschlüsselung werden von der IKE-Richtlinie nicht unterstützt.
- Die DH-Gruppen 1, 2 und 24 werden von der IKE-Richtlinie und dem IPsec-Vorschlag nicht unterstützt.
- Die MD5-Integrität wird in der IKE-Richtlinie nicht unterstützt.
- PRF MD5 wird in der IKE-Richtlinie nicht unterstützt.

- Die Verschlüsselungsalgorithmen DES, 3DES, AES-GMAC, AES-GMAC-192 und AES-GMAC-256 werden von IPsec Proposal nicht unterstützt.

**Hinweis:** Dies gilt sowohl für standortübergreifende als auch für richtlinienbasierte VPN-Tunnel. Um eine ältere FTD von FMC auf 6.7 zu aktualisieren, löst sie eine Überprüfung vor der Validierung aus, die den Benutzer vor Änderungen warnt, die sich auf die entfernten Chiffren beziehen, die die Aktualisierung blockieren.

### FTD 6.7 verwaltet über FMC 6.7

### Verfügbare Konfiguration

### Site-to-Site-VPN-Tunnel

Neuinstallation

Es sind schwache Chiffren verfügbar, die jedoch nicht für die Konfiguration des FTD 6.7 verwendet werden können.

Es sind schwache Chiffren verfügbar, die jedoch nicht für die Konfiguration des FTD 6.7 verwendet werden können.

Upgrade: FTD nur mit schwachen Chiffren konfiguriert

Upgrade von der FMC 6.7-Benutzeroberfläche. Eine Überprüfung vor der Validierung zeigt einen Fehler an. Das Upgrade wird bis zur Neukonfiguration blockiert.

Nach dem FTD-Upgrade und der Annahme, dass der Peer seine Einstellungen nicht geändert hat, wird der Tunnel beendet.

Upgrade: FTD wurde nur mit einigen schwachen und einigen starken Chiffren konfiguriert.

Upgrade von der FMC 6.7-Benutzeroberfläche. Eine Überprüfung vor der Validierung zeigt einen Fehler an. Das Upgrade wird bis zur Neukonfiguration blockiert.

Nach dem FTD-Upgrade und der Annahme, dass der Peer seine Chiffren hat, wird der Tunnel wiederhergestellt.

Upgrade: Land der Klasse C (keine starke Crypto-Lizenz)

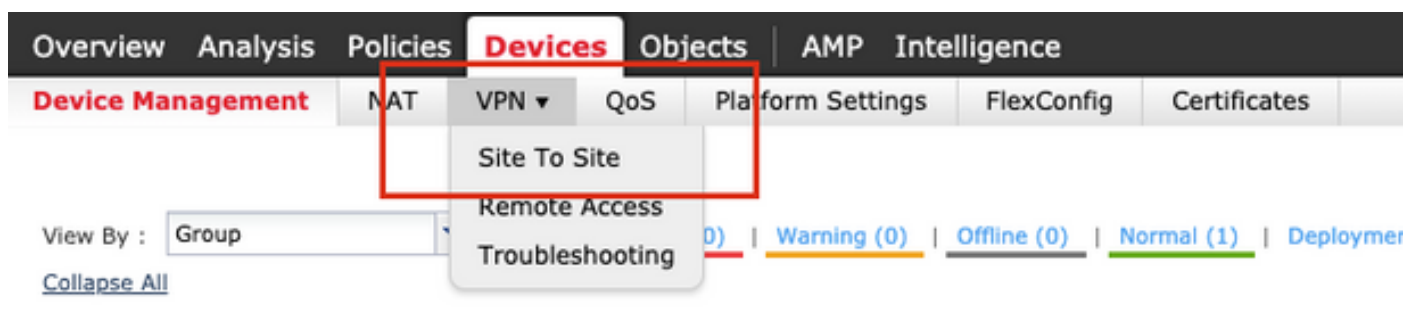
DES zulassen ist zulässig

DES zulassen ist zulässig

**Hinweis:** Es sind keine zusätzlichen Lizenzen erforderlich. Routen-basiertes VPN kann sowohl im Lizenzierungs- als auch im Evaluierungsmodus konfiguriert werden. Ohne Verschlüsselungskompatibilität (Export Controlled Features Enabled) kann nur DES als Verschlüsselungsalgorithmus verwendet werden.

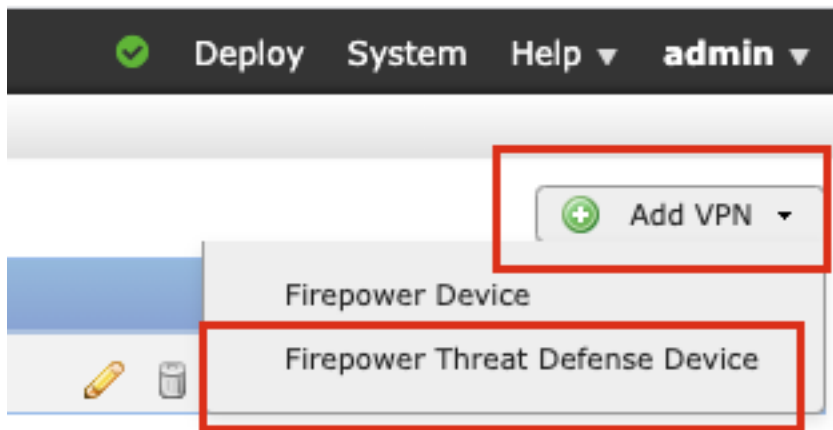
## Konfigurationsschritte auf FMC

Schritt 1: Navigieren Sie zu **Geräte > VPN > Site-to-Site**.



Schritt 2. Klicken Sie auf **VPN hinzufügen** und wählen Sie **Firepower Threat Defense Device**, wie

im Bild dargestellt.

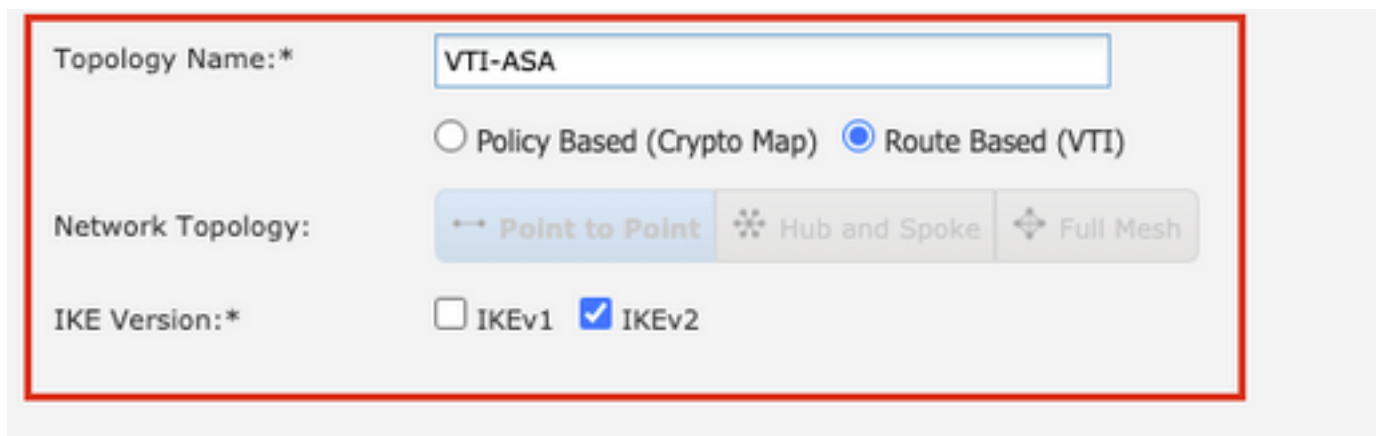


Schritt 3: Geben Sie einen **Topologienamen** an, und wählen Sie den VPN-Typ als **routenbasiert (VTI)**. Wählen Sie die **IKE-Version** aus.

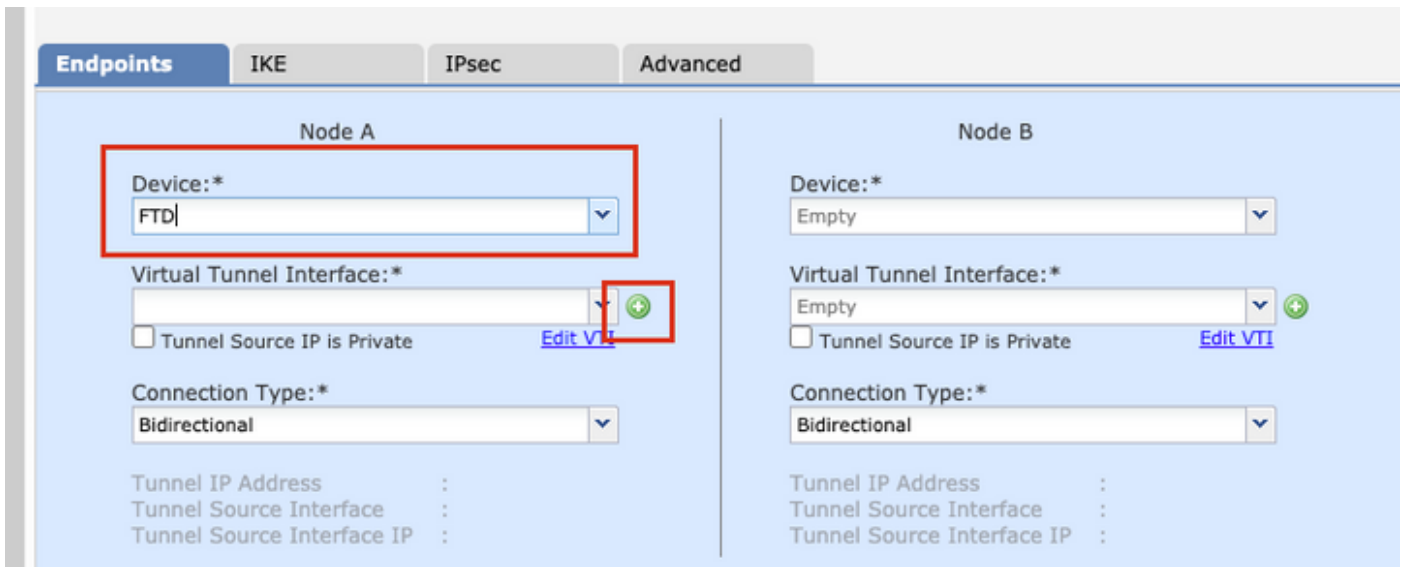
Für diese Demonstration gilt Folgendes:

**Topologiename:** VTI-ASA

**IKE-Version:** IKEv2



Schritt 4. Wählen Sie das **Gerät**, auf dem der Tunnel konfiguriert werden muss. Sie können eine neue **virtuelle Vorlagenschnittstelle** hinzufügen (klicken Sie auf das **+**-Symbol) oder eine vorhandene Schnittstelle aus der Liste auswählen.



Schritt 5: Definieren Sie die Parameter der **neuen virtuellen Tunnelschnittstelle**. Klicken Sie auf OK.

Für diese Demonstration gilt Folgendes:

**Name:** VTI-ASA

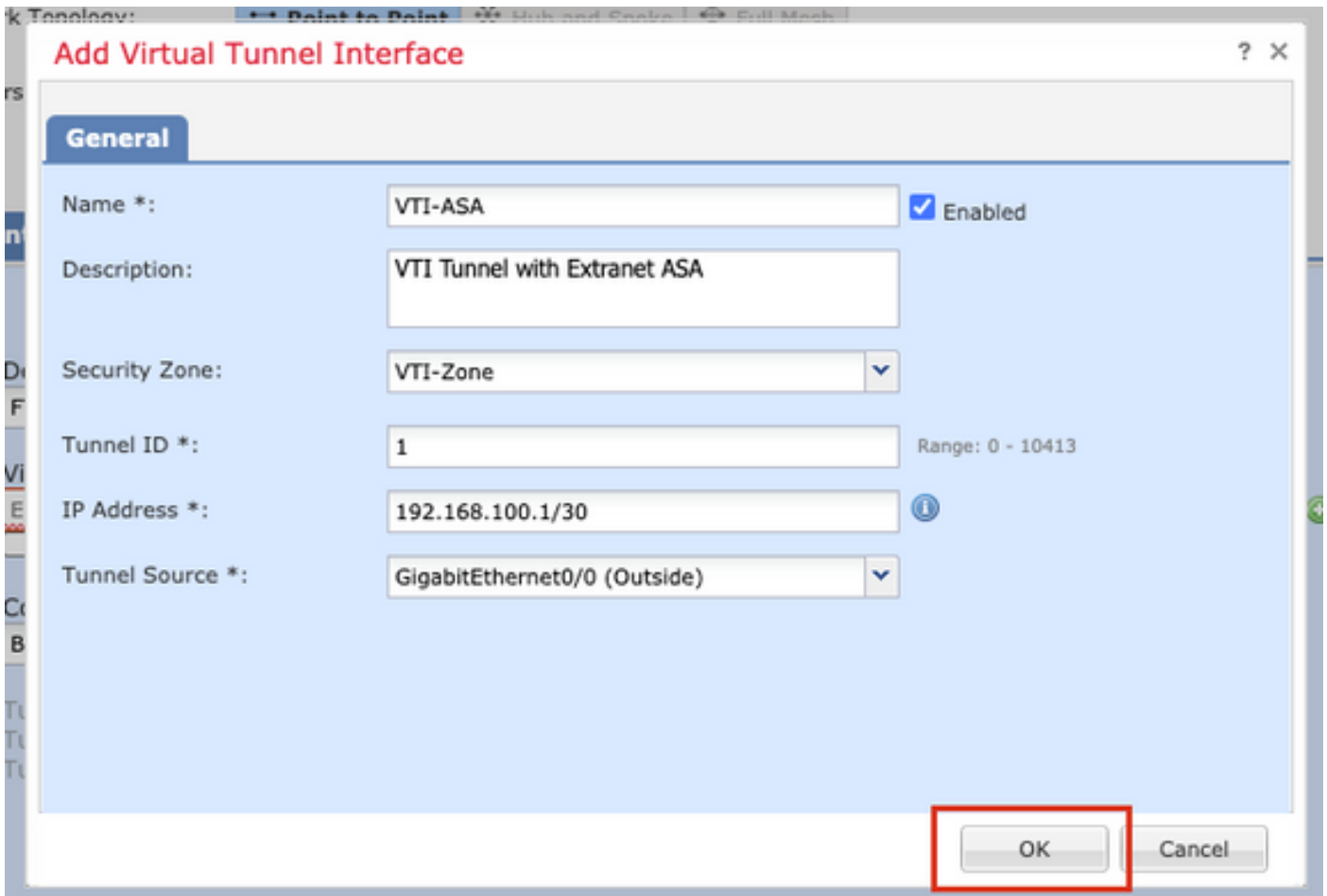
**Beschreibung (optional):** VTI-Tunnel mit Extranet-ASA

**Sicherheitszone:** VTI-Zone

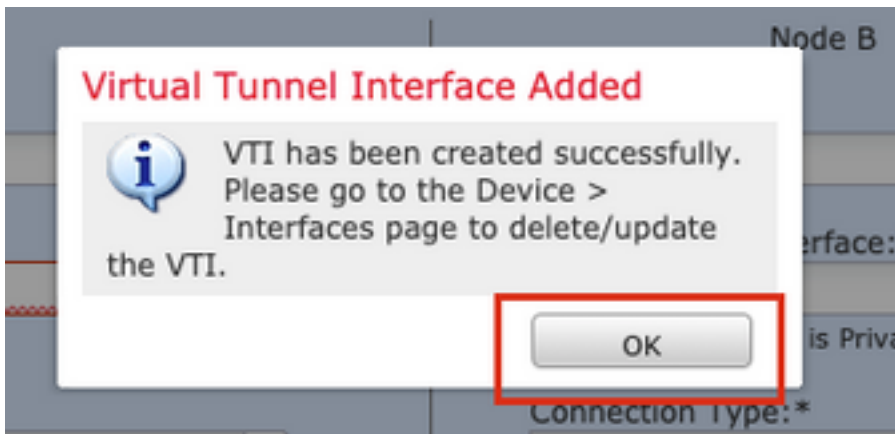
**Tunnel-ID:** 1

**IP-Adresse:** 192.168.100.1/30

**Tunnelquelle:** GigabitEthernet0/0 (Außenbereiche)



Schritt 6: Klicken Sie im Popup-Fenster auf **OK**, um anzugeben, dass der neue VTI erstellt wurde.



Schritt 7: Wählen Sie den neu erstellten VTI oder einen VTI, der unter "**Virtual Tunnel Interface**" vorhanden ist. Geben Sie die Informationen für **Knoten B** (das Peer-Gerät) an.

Für diese Demonstration gilt Folgendes:

"Slot0": Extranet

Gerätename: ASA-Peer

Endpunkt-IP-Adresse: 10.106.67.252

**Create New VPN Topology**

Topology Name: \*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version: \*  IKEv1  IKEv2

**Endpoints** IKE IPsec Advanced

**Node A**

Device: \*

**Virtual Tunnel Interface: \***  +

Tunnel Source IP is Private [Edit VTI](#)

Connection Type: \*

Tunnel IP Address : 192.168.100.1  
 Tunnel Source Interface : Outside  
 Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ  
 Route traffic to the VTI : [Routing Policy](#)  
 Permit VPN traffic : [AC Policy](#)

**Node B**

Device: \*

Device Name: \*

Endpoint IP Address: \*

Schritt 8: Navigieren Sie zur Registerkarte **IKE**. Sie können eine vordefinierte **Richtlinie** verwenden oder auf die Schaltfläche **+** neben der Registerkarte **Richtlinie** klicken und eine neue erstellen.

**IKEv2 Settings**

Policy: \*  +

Authentication Type:

Pre-shared Key Length: \*  Characters (Range 1-127)

Schritt 9: (Optional, wenn Sie eine neue IKEv2-Richtlinie erstellen) Geben Sie einen **Namen** für die Richtlinie ein, und wählen Sie die in der Richtlinie zu verwendenden **Algorithmen** aus. Klicken Sie auf **Speichern**.

Für diese Demonstration gilt Folgendes:

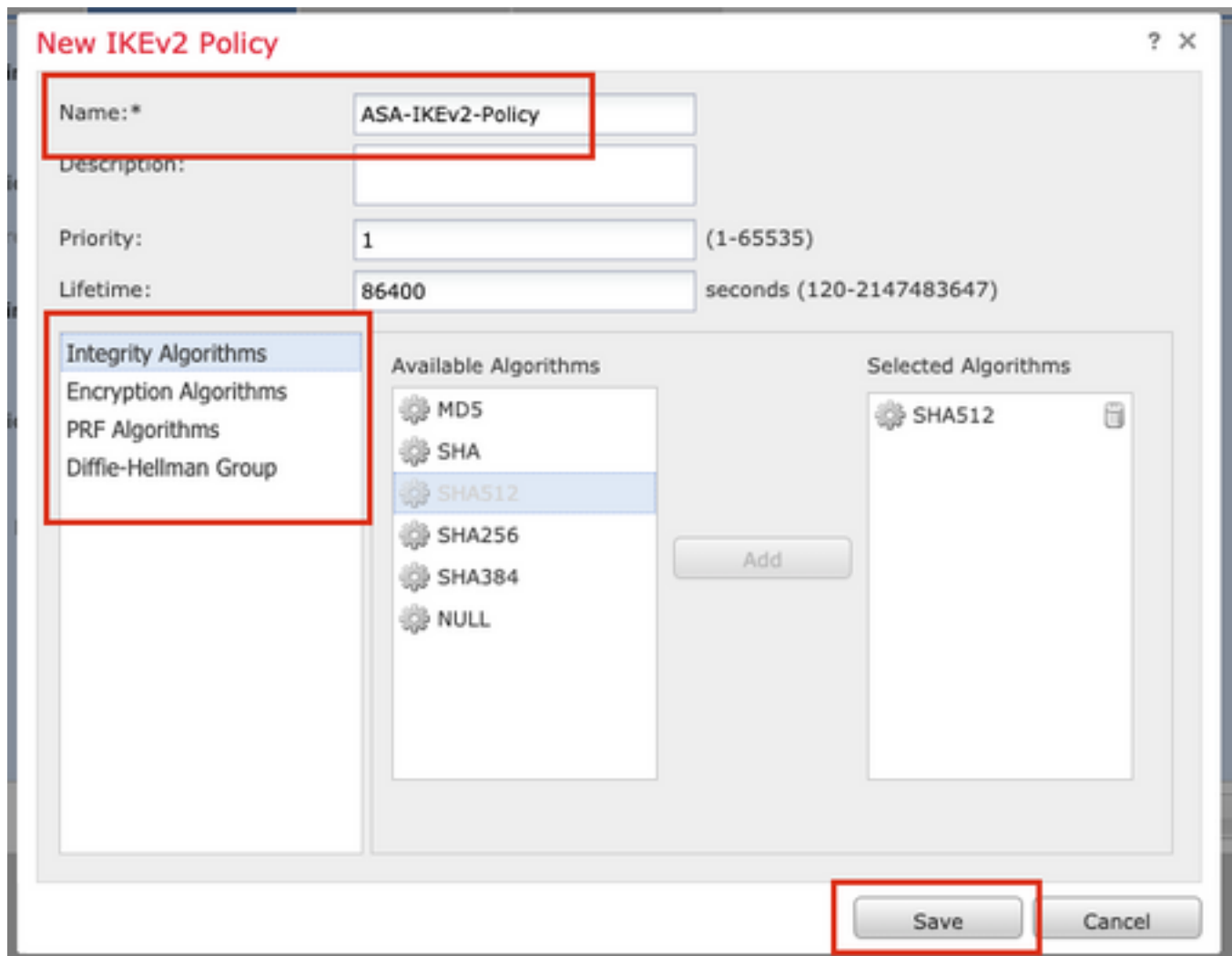
Name: ASA-IKEv2-Richtlinie

Integritätsalgorithmen: SHA-512

Verschlüsselungsalgorithmen: AES-256

PRF-Algorithmen: SHA-512

Diffie-Hellman-Gruppe: 21



Schritt 10: Wählen Sie die neu erstellte oder die vorhandene **Richtlinie**. Wählen Sie den **Authentifizierungstyp** aus. Wenn ein **vorinstallierter manueller Schlüssel** verwendet wird, geben Sie den Schlüssel in den Feldern **Schlüssel** und **Schlüssel bestätigen** ein.

Für diese Demonstration gilt Folgendes:

**Richtlinie:** ASA-IKEv2-Richtlinie

**Authentifizierungstyp:** Vorinstallierter manueller Schlüssel

**Wichtigste:** cisco123

**Schlüssel bestätigen:** cisco123



Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\* preshared\_sha\_aes256\_dh14\_3

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

**IKEv2 Settings**

Policy:\* ASA-IKEv2-Policy

Authentication Type: Pre-shared Manual Key

Key:\* .....

Confirm Key:\* .....

Enforce hex-based pre-shared key only

**Hinweis:** Wenn beide Endpunkte auf demselben FMC registriert sind, kann auch die Option "Pre-shared Automatic Key" verwendet werden.

Schritt 11. Navigieren Sie zur Registerkarte **IPsec**. Sie können einen vordefinierten **IKEv2-IPsec-Vorschlag** verwenden oder einen neuen erstellen. Klicken Sie auf die Schaltfläche Bearbeiten neben der Registerkarte **IKEv2 IPsec-Angebot**.

Crypto Map Type:  Static  Dynamic

IKEv2 Mode: Tunnel

Transform Sets:

IKEv1 IPsec Proposals

tunnel\_aes256\_sha

IKEv2 IPsec Proposals\*

AES-GCM

Enable Security Association (SA) Strength Enforcement

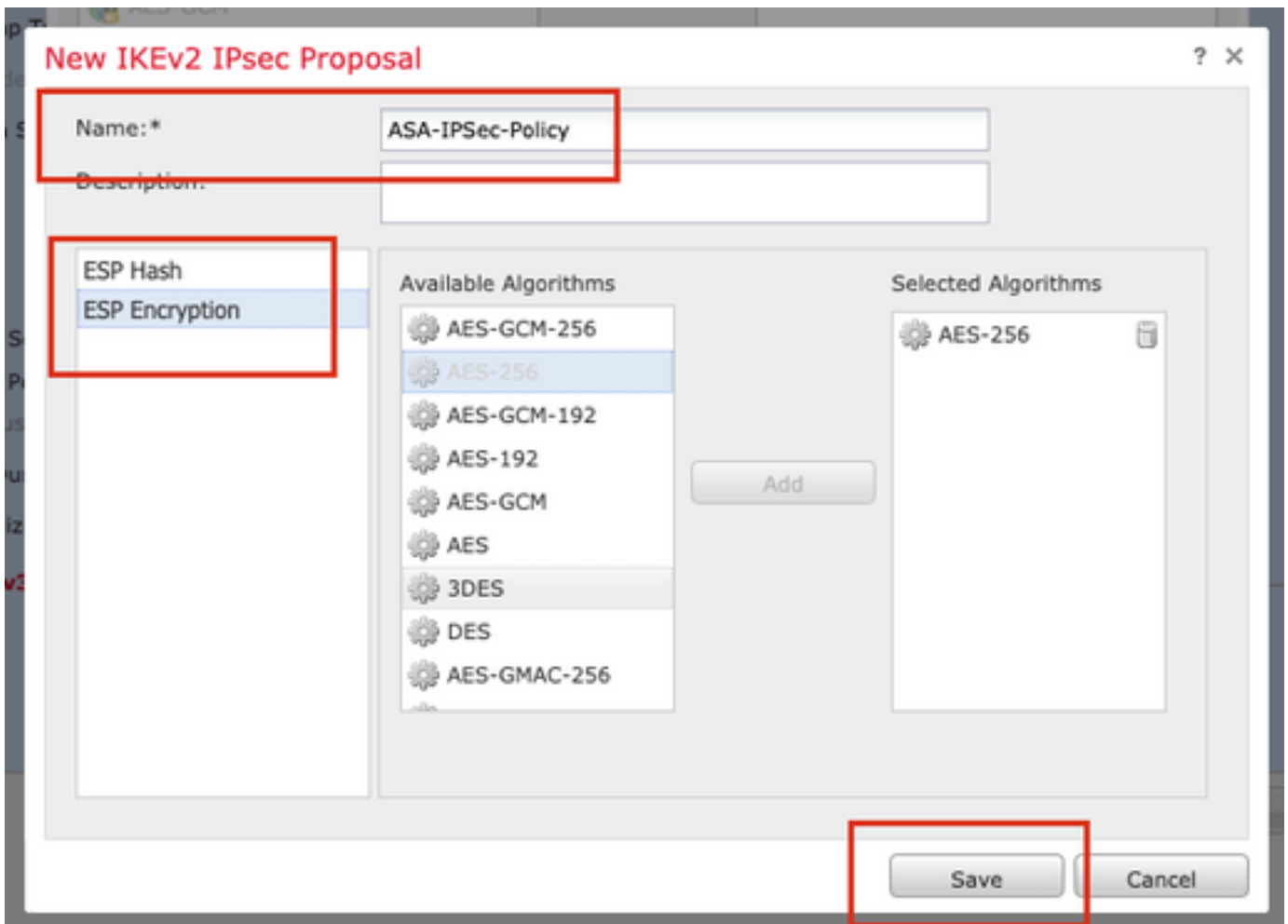
Schritt 12: (Optional, wenn Sie einen neuen IKEv2 IPsec-Vorschlag erstellen) Geben Sie einen **Namen** für den Vorschlag an, und wählen Sie die **Algorithmen** aus, die im Vorschlag verwendet werden sollen. Klicken Sie auf **Speichern**.

Für diese Demonstration gilt Folgendes:

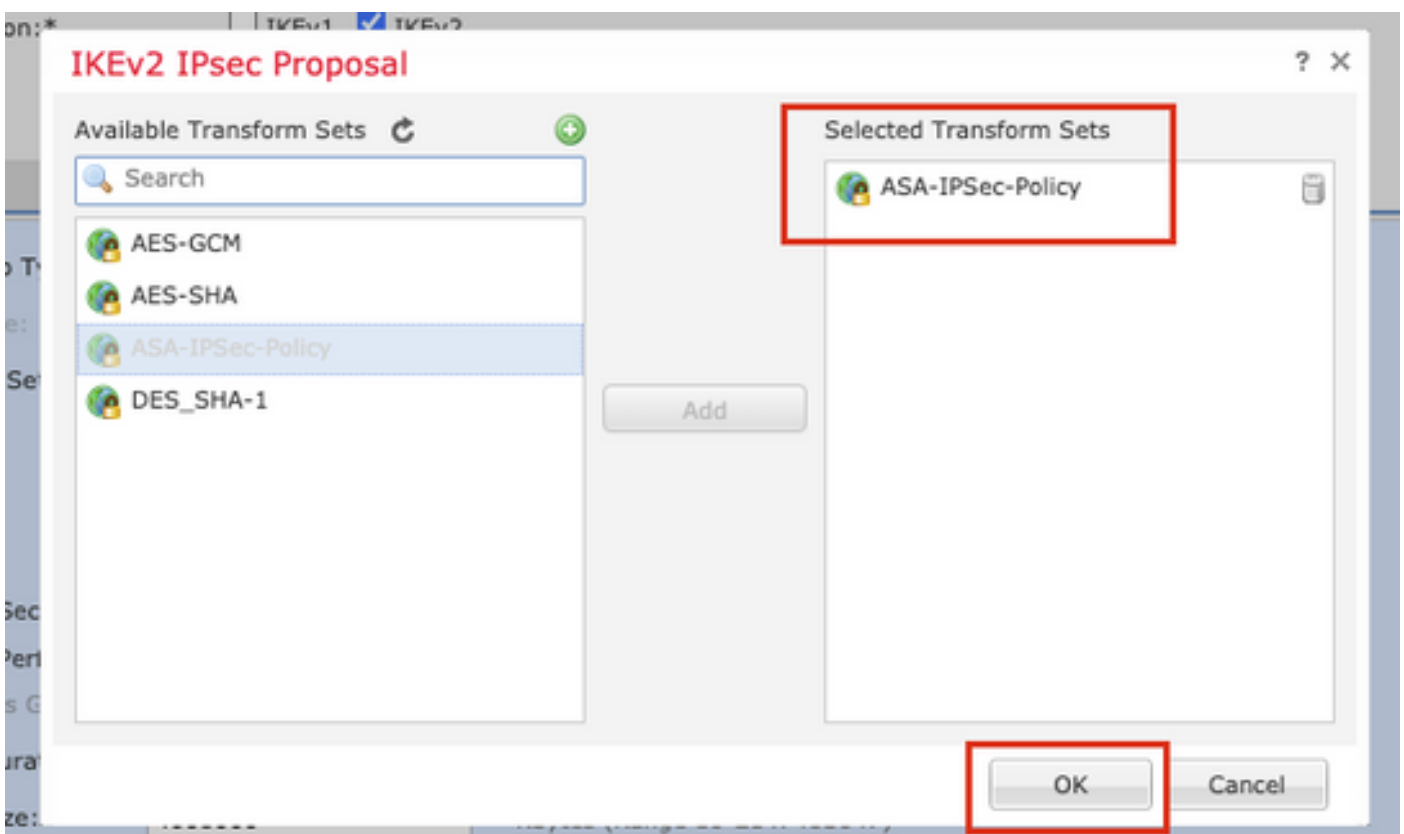
**Name:** ASA-IPSec-Richtlinie

**ESP-Hash:** SHA-512

## ESP-Verschlüsselung: AES-256



Schritt 13: Wählen Sie aus der Liste der verfügbaren Angebote den neu erstellten **Vorschlag** oder **Vorschlag** aus. Klicken Sie auf OK.



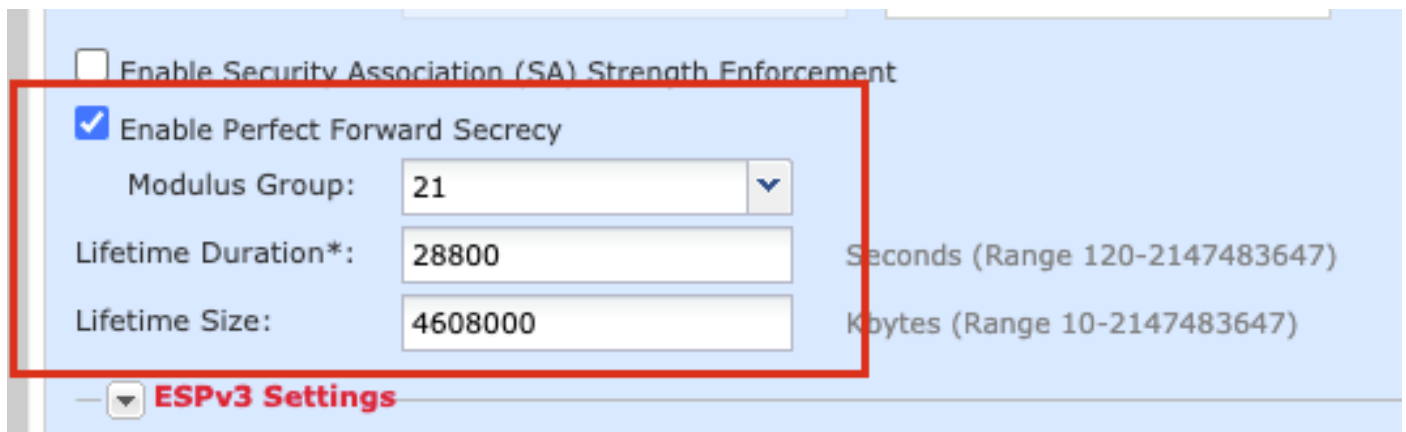
Schritt 14. (Optional) Wählen Sie die Einstellungen **Perfect Forward Secrecy (Perfektes Weiterleitungsgeheimnis) aus**. Konfigurieren der IPsec-Lebenszeitdauer und -Größe.

Für diese Demonstration gilt Folgendes:

**Perfect Forward Secrecy:** Modulgruppe 21

**Lebensdauer:** 28800 (Standard)

**Lebenszeitgröße:** 4608000 (Standard)



The image shows a configuration window titled "ESPv3 Settings" with a red border. It contains the following settings:

- Enable Security Association (SA) Strength Enforcement
- Enable Perfect Forward Secrecy
  - Modulus Group: 21 (dropdown menu)
  - Lifetime Duration\*: 28800 (text input) Seconds (Range 120-2147483647)
  - Lifetime Size: 4608000 (text input) Kbytes (Range 10-2147483647)

Schritt 15: Überprüfen Sie die konfigurierten Einstellungen. Klicken Sie auf **Speichern**, wie in diesem Bild dargestellt.

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode:

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals\*

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration\*:  Seconds (Range 120-2147483647)

Lifetime Size:  Kbytes (Range 10-2147483647)

—  ESPv3 Settings

Schritt 16: Konfigurieren Sie optional die **NAT-Richtlinie**. Navigieren Sie zu **Geräte > NAT**. Wählen Sie die diesem FTD zugewiesene NAT-Richtlinie aus.

Geben Sie auf der Registerkarte **Interface Objects (Schnittstellenobjekte)** die **Quellschnittstellenobjekte** und die **Zielschnittstellenobjekte** an.

Geben Sie die Originalquelle, das **ursprüngliche Ziel**, die **übersetzte Quelle** und das **übersetzte Ziel** auf der Registerkarte "**Übersetzung**" ein. Klicken Sie auf OK.

Für diese Demonstration gilt Folgendes:

**Quellschnittstellenobjekte:** In-Zone

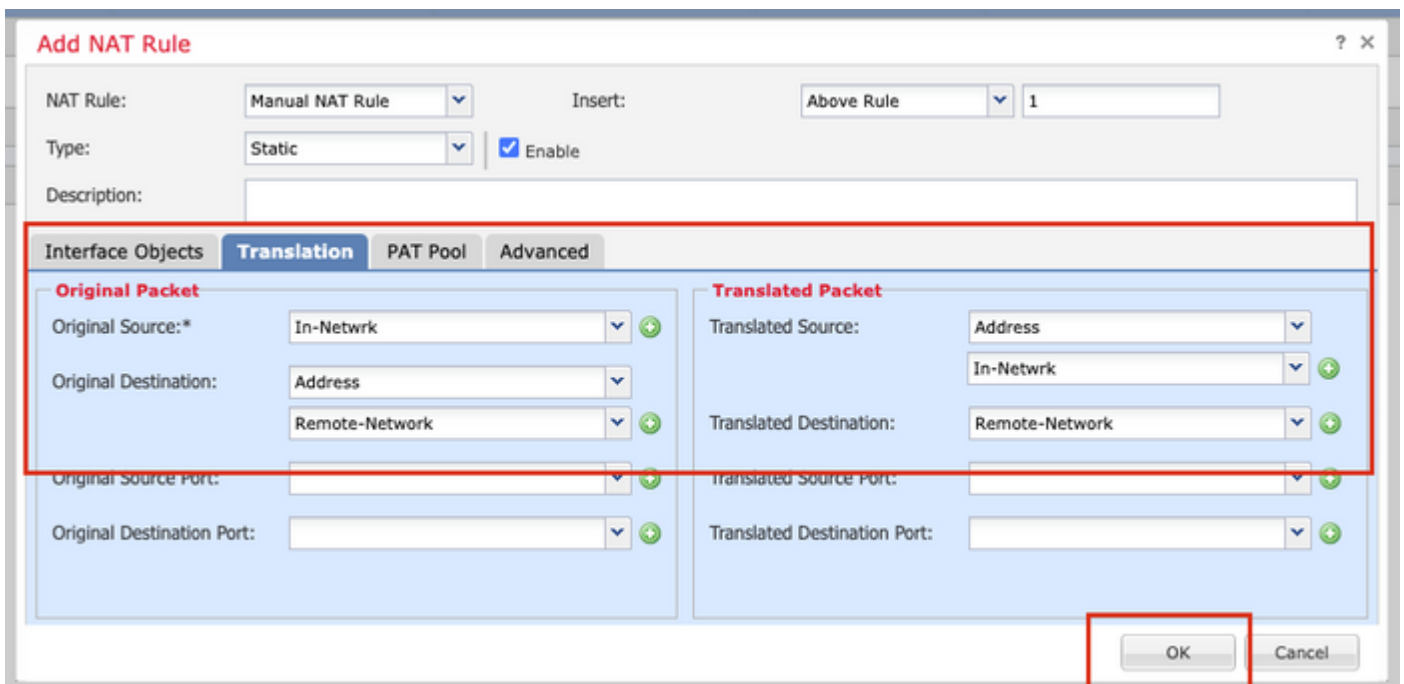
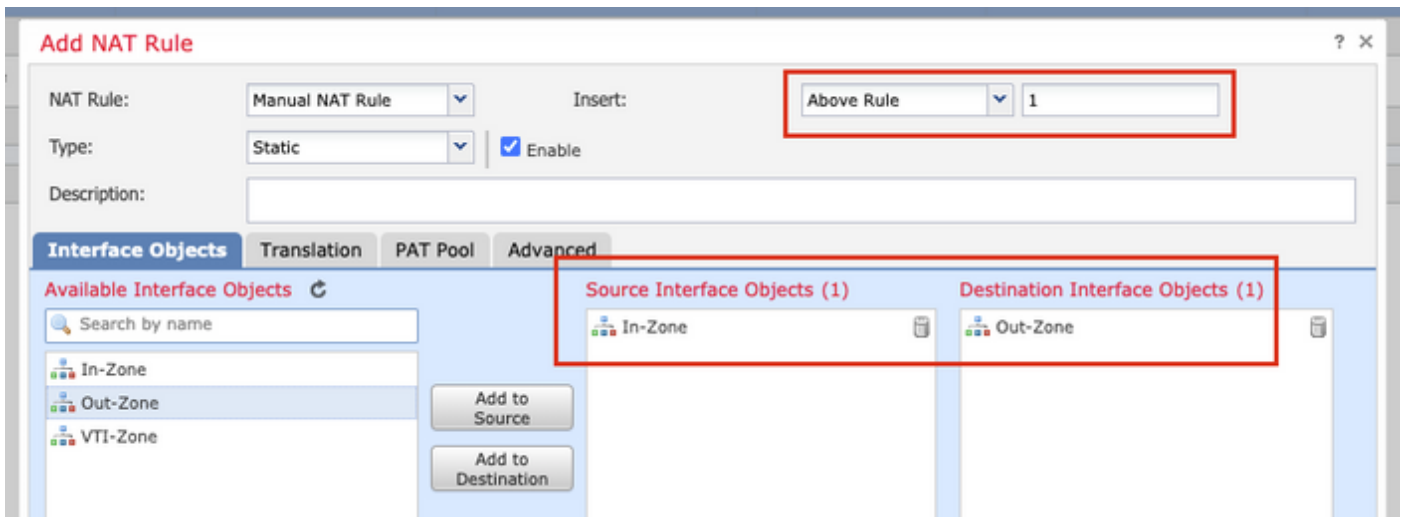
**Zielschnittstellenobjekte:** Out-Zone

**Ursprüngliche Quelle:** Im Netzwerk

**Ursprüngliches Ziel:** Remote-Netzwerk

**Übersetzte Quelle:** Im Netzwerk

**Übersetztes Ziel:** Remote-Netzwerk



**Hinweis:** Stellen Sie sicher, dass die Freistellung für statische NAT für den standortübergreifenden Tunnel zusätzlich zu den dynamischen NAT/PAT-Regeln hinzugefügt wird.

Schritt 17: Konfigurieren der **Zugriffskontrollrichtlinie**. Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle**. Bearbeiten Sie die auf das FTD angewendete Richtlinie.

**Hinweis:** `sysopt connection permit-vpn` funktioniert nicht mit Routen-basierten VPN-Tunneln. Die Zugriffskontrollregeln müssen sowohl für IN-> OUT-Zonen als auch für OUT-> IN-Zonen konfiguriert werden.

Geben Sie die **Quellzonen** und die **Zielzonen** auf der Registerkarte **Zonen** an.

Geben Sie auf der Registerkarte **"Netzwerke"** die **Namen Quellnetzwerke** und **Zielnetzwerke** ein. Klicken Sie auf Hinzufügen.

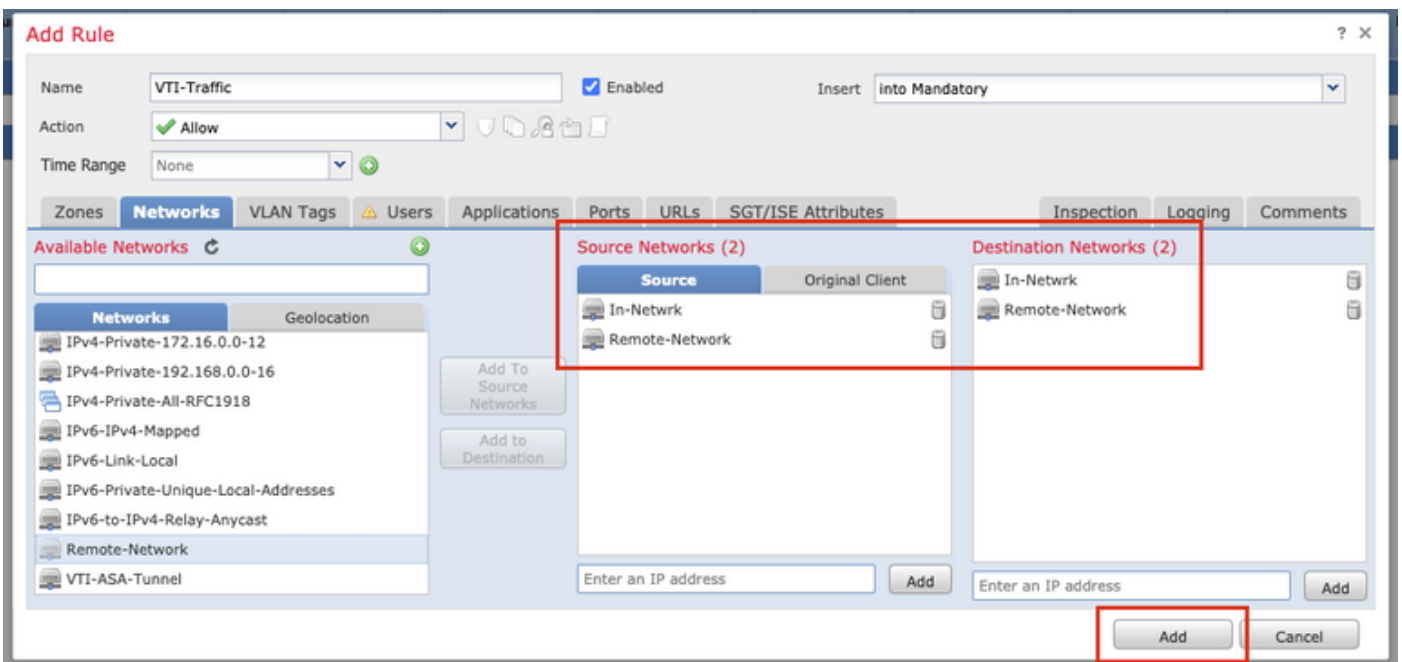
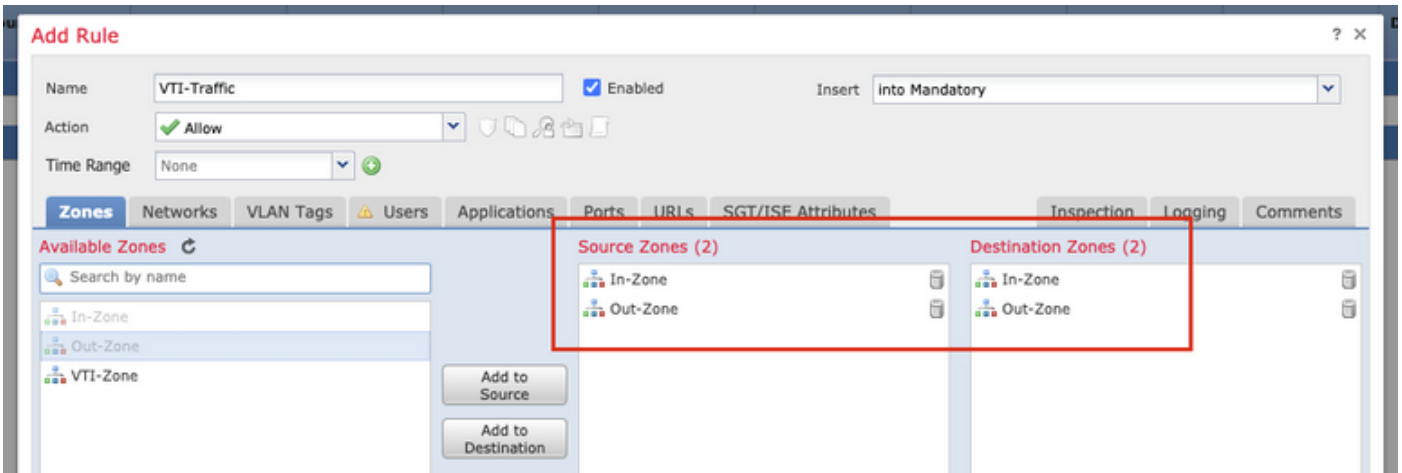
Für diese Demonstration gilt Folgendes:

Quellzonen: In- und Out-Zone

Zielzonen: Out-Zone und In-Zone

Quellnetzwerke: In- und Remote-Netzwerk

Zielnetzwerke: Remote-Netzwerk und In-Network



Schritt 18: Fügen Sie das Routing über den VTI-Tunnel hinzu. Navigieren Sie zu **Geräte > Geräteverwaltung**. Bearbeiten Sie das Gerät, auf dem der VTI-Tunnel konfiguriert ist.

Navigieren Sie auf der Registerkarte **Routing** zu **Static Route**. Klicken Sie auf **Route hinzufügen**.

Stellen Sie die **Schnittstelle bereit**, wählen Sie das **Netzwerk**, und stellen Sie das **Gateway bereit**. Klicken Sie auf OK.

Für diese Demonstration gilt Folgendes:

**Schnittstelle:** VTI-ASA

**Netzwerk:** Remote-Netzwerk

## Gateway: VTI-ASA-Tunnel

Type:  IPv4  IPv6

Interface\* VTI-ASA  
(Interface starting with this icon signifies it is available for route leak)

Available Network

- any-ipv4
- In-Network
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-1
- IPv4-Private-All-RFC1918

Selected Network

- Remote-Network

Add

Gateway\* VTI-ASA-Tunnel

Metric: 1 (1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

OK Cancel

Schritt 19: Navigieren Sie zu **Bereitstellen > Bereitstellung**. Wählen Sie den FTD aus, für den die Konfiguration bereitgestellt werden soll, und klicken Sie auf **Deploy (Bereitstellen)**.

Konfiguration wird nach erfolgreicher Bereitstellung auf die FTD-CLI übertragen:

```
crypto ikev2 policy 1
encryption aes-256
integrity sha512
group 21
prf sha512
lifetime seconds 86400
crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1
protocol esp encryption aes-256
protocol esp integrity sha-512
crypto ipsec profile FMC_IPSEC_PROFILE_1
set ikev2 ipsec-proposal CSM_IP_1
set pfs group21
```

```
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev1 ikev2

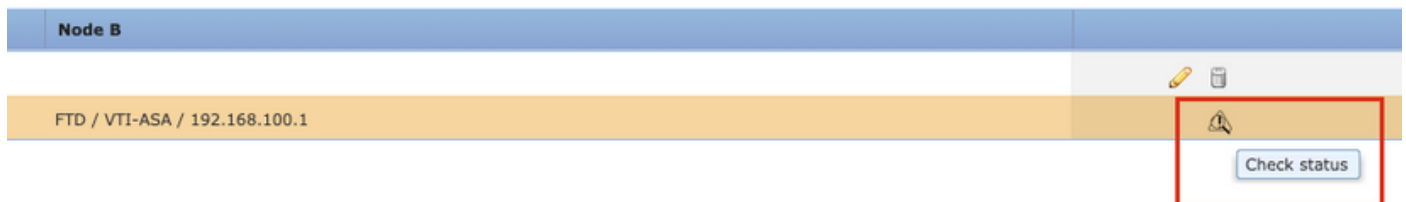
tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

```
interface Tunnel1
description VTI Tunnel with Extranet ASA
nameif VTI-ASA
ip address 192.168.100.1 255.255.255.252
tunnel source interface Outside
tunnel destination 10.106.67.252
tunnel mode ipsec ipv4
tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

## Überprüfung

### Von der FMC-GUI

Klicken Sie auf die Option **Check Status (Status prüfen)**, um den Live-Status des VPN-Tunnels über die Benutzeroberfläche selbst zu überwachen.



Dazu gehören die folgenden Befehle aus der FTD-CLI:

- **show crypto ipsec sa peer <Peer-IP-Adresse>**
- **show vpn-sessiondb detail l2l filter ipaddress <Peer-IP-Adresse>**



**Tunnel Status**

**extranet : ASA-Peer**

```
> show crypto ipsec sa peer
Not applicable for extranet peer
```

```
> show vpn-sessiondb detail l2l filter ipaddress
Not applicable for extranet peer
```

**FTD/VTI-ASA**

```
> show crypto ipsec sa peer 10.106.67.252
peer address: 10.106.67.252
Crypto map tag: __vti-crypto-map-4-0-1, seq num: 65280, local addr:
10.197.224.90

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.106.67.252

#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 100, #pkts comp failed: 0, #pkts decomp
failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.197.224.90/500, remote crypto endpt.:
10.106.67.252/500
```

```
> show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252
Session Type: LAN-to-LAN Detailed
Connection : 10.106.67.252
Index : 44 IP Addr : 10.106.67.252
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA512 IPsec: (1)SHA512
Bytes Tx : 10000 Bytes Rx : 10000
Login Time : 03:54:57 UTC Thu Nov 12 2020
Duration : 0h:02m:12s
Tunnel Zone : 0

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID : 44.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA512
Rekey Int (T): 86400 Seconds Rekey Left(T): 86268 Seconds
PRF : SHA512 D/H Group : 21
```

Refresh Close

## Von FTD CLI

Diese Befehle können über die FTD-CLI verwendet werden, um die Konfiguration und den Status der VPN-Tunnel anzuzeigen.

```
show running-config crypto
show running-config nat
show running-config route
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail l2l
```

## 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.