

# Konfigurieren eines routenbasierten VPNs mit einer statischen Route auf einem von FDM verwalteten FTD

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurationsschritte bei FDM](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

---

## Einleitung

Dieses Dokument beschreibt die Konfiguration eines statischen, routenbasierten Site-to-Site-VPN-Tunnels auf einem durch FDM verwalteten FTD.

## Voraussetzungen

### Anforderungen

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

- Grundlegendes Verständnis der Funktionsweise eines VPN-Tunnels
- Vorkenntnisse der Navigation durch den FirePOWER Device Manager (FDM)

### Verwendete Komponenten

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

- Cisco Firepower Threat Defense (FTD) Version 7.0, verwaltet durch Firepower Device Manager (FDM).

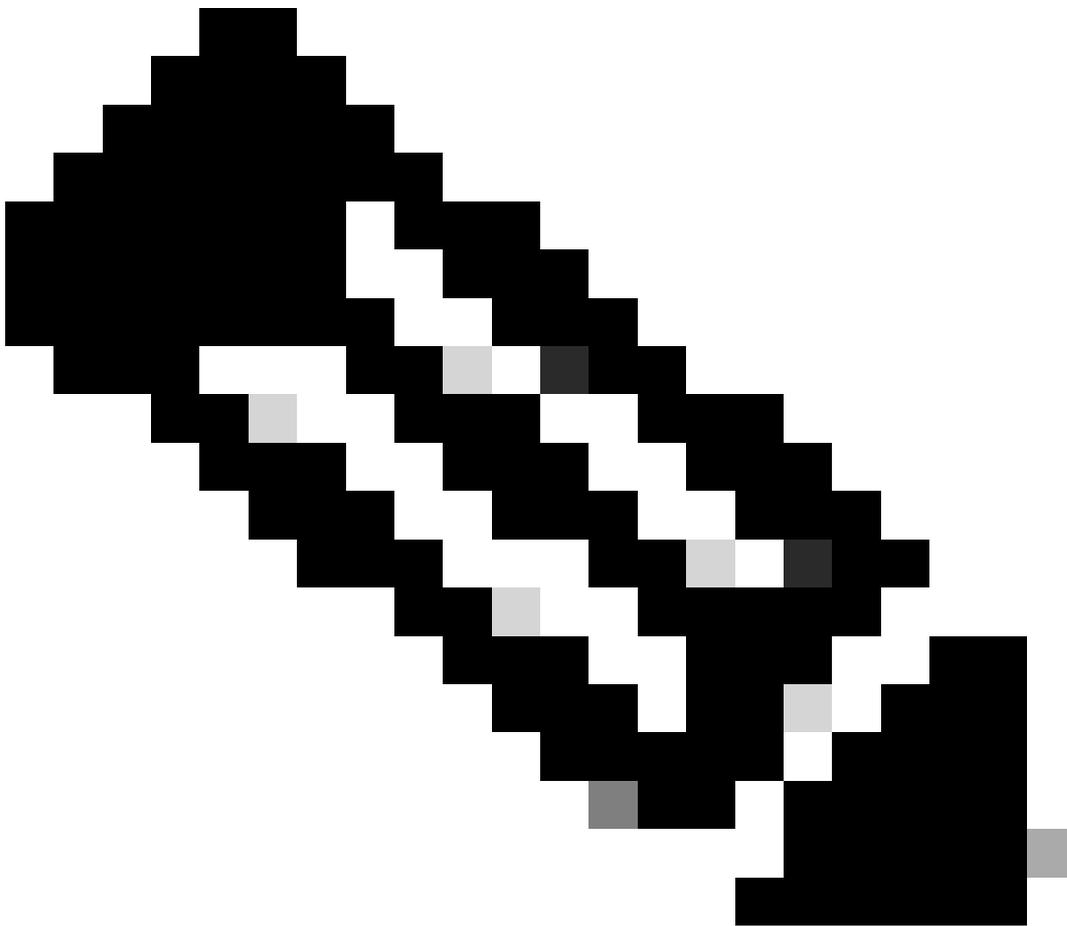
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

## Hintergrundinformationen

Routenbasiertes VPN ermöglicht die Bestimmung des interessanten Datenverkehrs, 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 konfiguriert, 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.

Das vorliegende Dokument behandelt die SVTI-Konfiguration (Static Virtual Tunnel Interface).

---

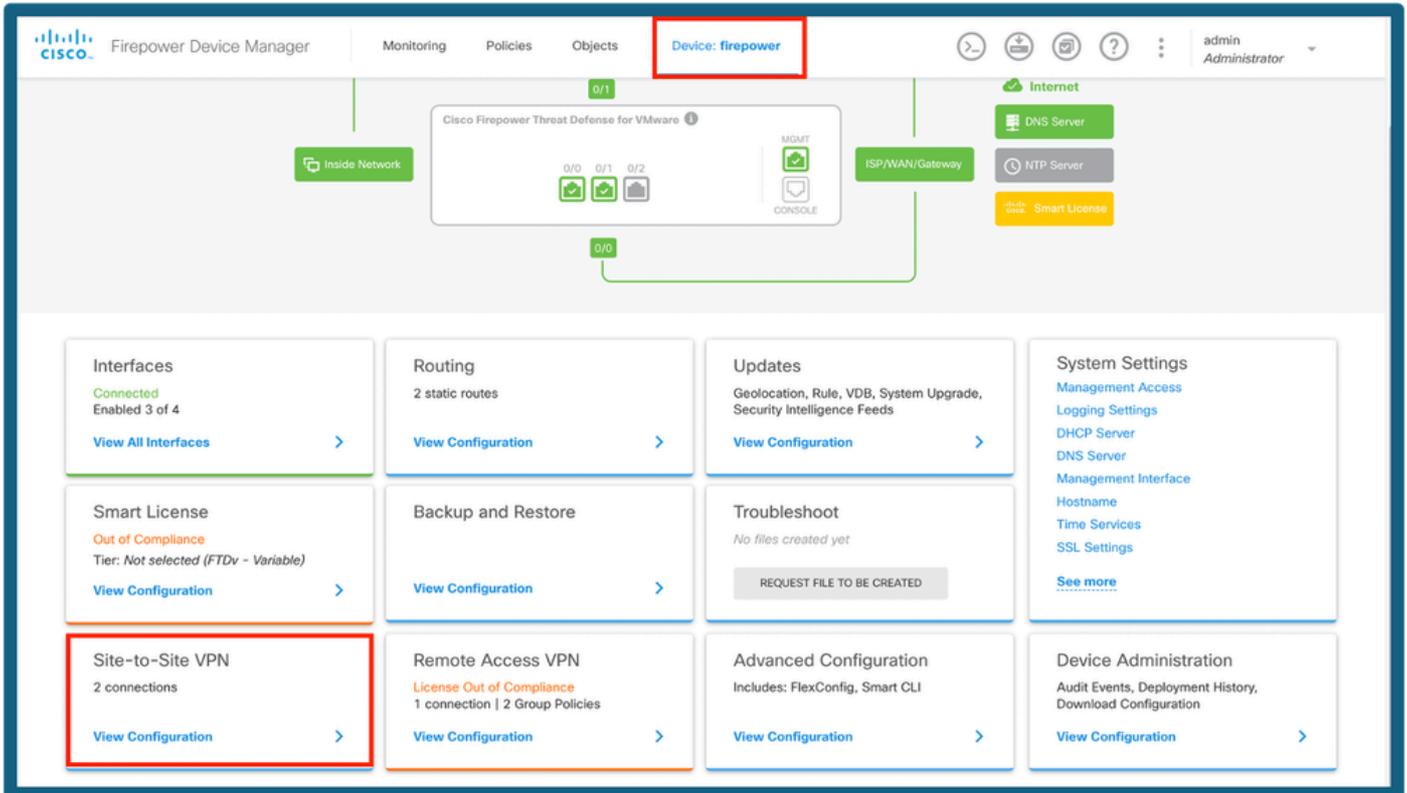


Anmerkung: Es ist keine zusätzliche Lizenzierung erforderlich. Routen-basiertes VPN kann sowohl im Lizenzmodus als auch im Evaluierungsmodus konfiguriert werden. Ohne Verschlüsselungskompatibilität (Export Controlled Features Enabled) kann nur DES als Verschlüsselungsalgorithmus verwendet werden.

---

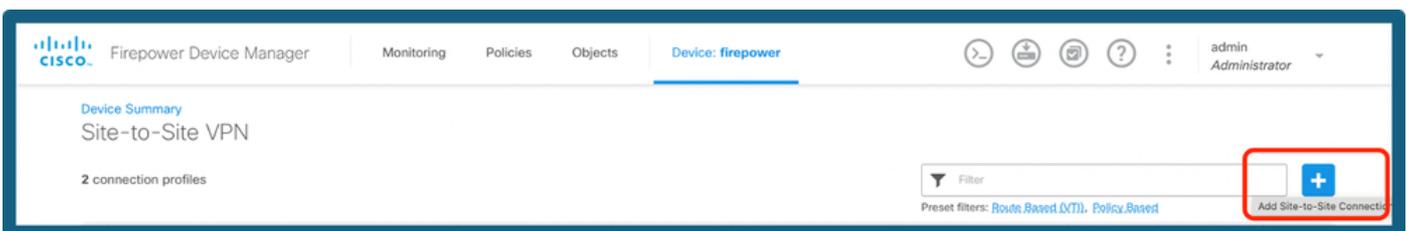
# Konfigurationsschritte bei FDM

Schritt 1: Navigieren Sie zu Gerät > Site-to-Site.



FDM-Dashboard

Schritt 2: Klicken Sie auf das +-Symbol, um eine neue Site zur Site-Verbindung hinzuzufügen.



S2S-Verbindung hinzufügen

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

Klicken Sie auf Local VPN Access Interface (Lokale VPN-Zugriffsschnittstelle), und klicken Sie dann auf Create new Virtual Tunnel Interface (Neue virtuelle Tunnelschnittstelle erstellen), oder wählen Sie eine vorhandene Schnittstelle in der Liste aus.

Firepower Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator

Local Network | FIREPOWER | VPN TUNNEL | INTERNET | PEER ENDPOINT | OUTSIDE INTERFACE | Remote Network

### Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name:  Type:  Route Based (VTI)  Policy Based

Sites Configuration

LOCAL SITE: Local VPN Access Interface:

REMOTE SITE: Remote IP Address:

[Create new Virtual Tunnel Interface](#)

Tunnelschnittstelle hinzufügen

Schritt 4: Definieren der Parameter der neuen virtuellen Tunnelschnittstelle Klicken Sie auf OK.

### Create Virtual Tunnel Interface

Name:  Status:

*Most features work with named interfaces only, although some require unnamed interfaces.*

Description:

Tunnel ID:  Tunnel Source:

*0 - 10413*

IP Address and Subnet Mask:  /

*e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0*

VTI-Konfiguration

Schritt 5: Wählen Sie den neu erstellten VTI oder einen VTI, der unter "Virtual Tunnel Interface" vorhanden ist. Geben Sie die Remote-IP-Adresse an.

New Site-to-site VPN

1 Endpoints      2 Configuration      3 Summary

### Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name:

Type:  Route Based (VTI)     Policy Based

Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface: <input type="text" value="tunnel10 (Tunnel10)"/>	Remote IP Address: <input type="text" value="10.106.63.23"/>

Peer-IP hinzufügen

Schritt 6: Wählen Sie die IKE-Version und wählen Sie die Schaltfläche Bearbeiten, um die IKE- und IPsec-Parameter wie im Bild dargestellt festzulegen.

### IKE Policy

**i** IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

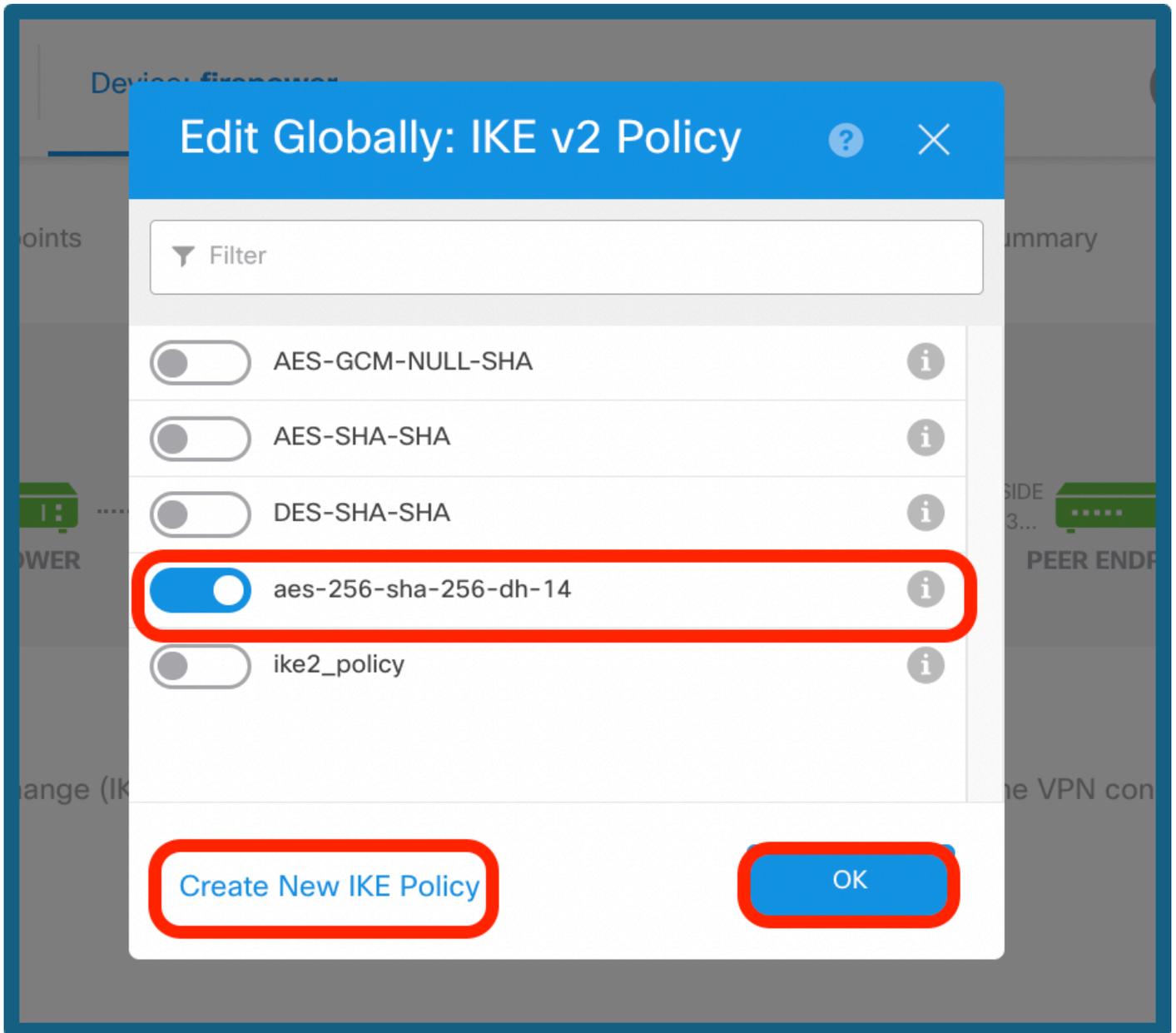
**IKE VERSION 2**       **IKE VERSION 1**

IKE Policy: **Globally applied**

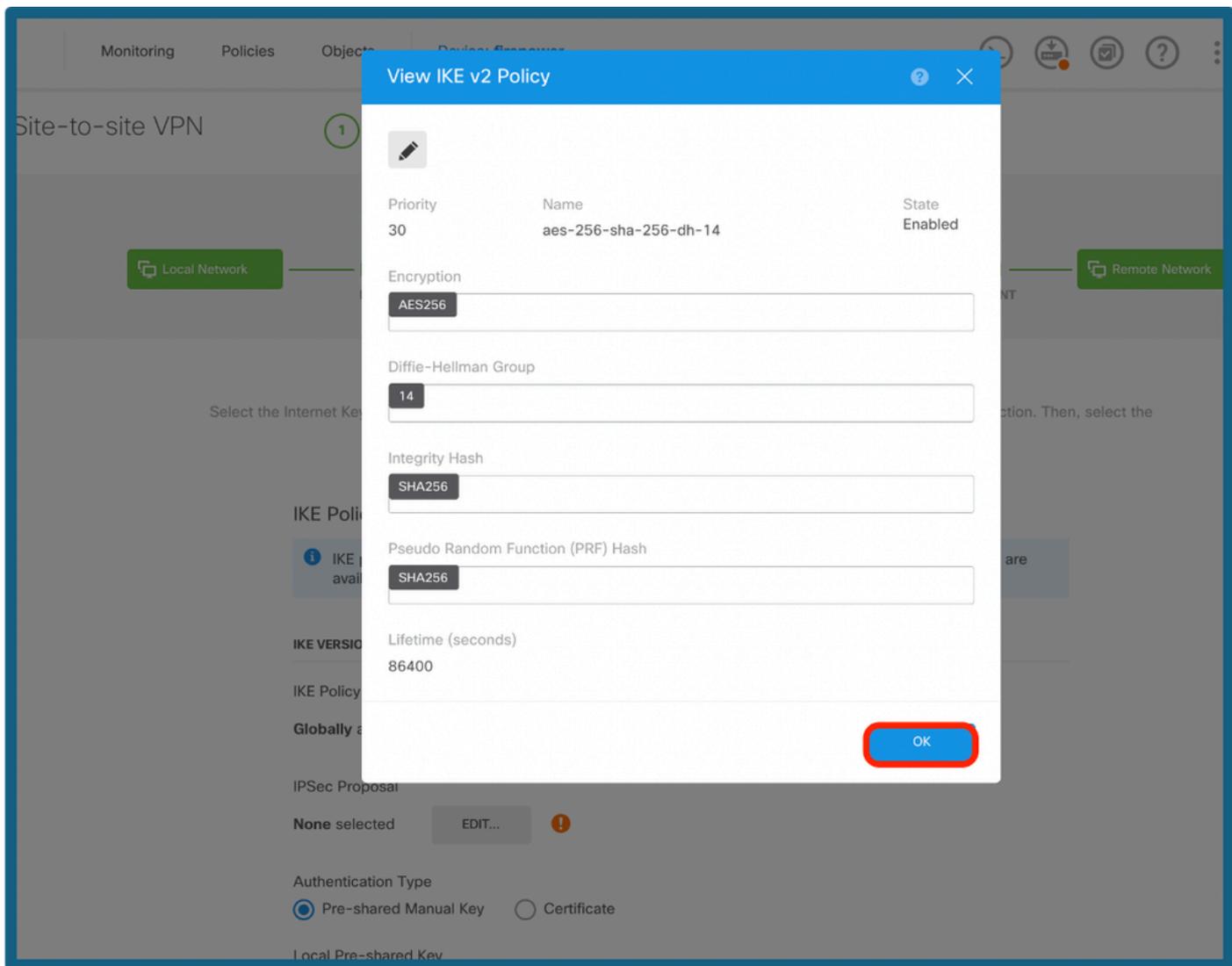
IPSec Proposal: **Custom set selected**

IKE-Version konfigurieren

Schritt 7a: Wählen Sie die Schaltfläche IKE Policy (IKE-Richtlinie) wie im Bild dargestellt, und klicken Sie auf die Schaltfläche ok oder auf Create New IKE Policy (Neue IKE-Richtlinie erstellen), wenn Sie eine neue Richtlinie erstellen möchten.

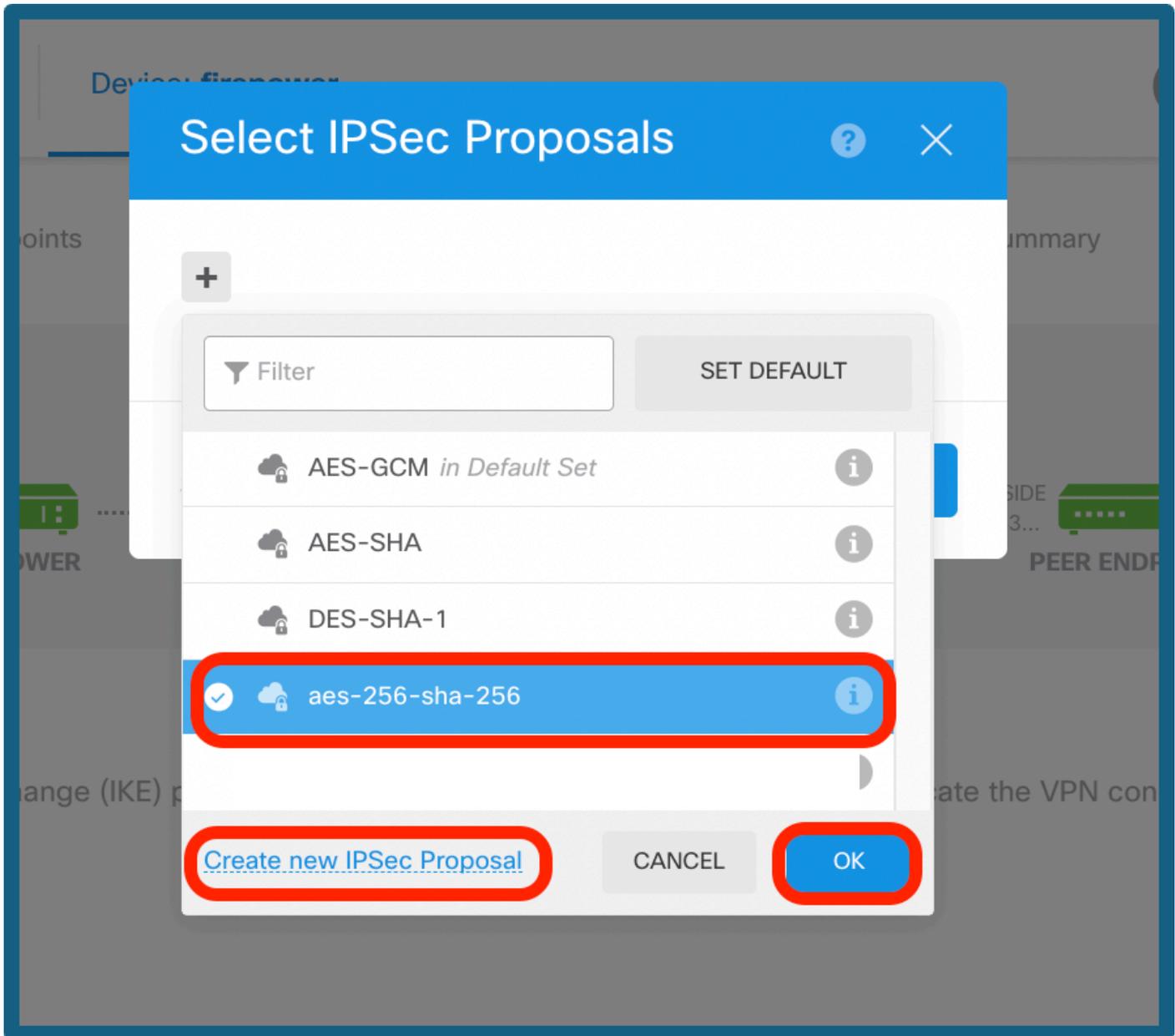


IKE-Richtlinie auswählen



Konfiguration der IKE-Richtlinie

Schritt 7b: Wählen Sie die Schaltfläche IPsec Policy (IPsec-Richtlinie) aus, wie im Bild dargestellt, und klicken Sie auf die Schaltfläche ok oder Create New IPsec Proposal (Neues IPsec-Angebot erstellen), wenn Sie ein neues Angebot erstellen möchten.



IPsec-Angebot auswählen

IKE v2 IPsec Proposal

Name  
aes-256-sha-256

Encryption  
AES256

Integrity Hash  
SHA256

OK

Konfiguration des IPsec-Angebots

Schritt 8a: Wählen Sie den Authentifizierungstyp aus. Wenn ein vorinstallierter manueller Schlüssel verwendet wird, geben Sie den vorinstallierten lokalen und Remote-Schlüssel an.

Schritt 8b: (Optional) Wählen Sie die Einstellungen Perfect Forward Secrecy (Perfektes Weiterleitungsgeheimnis) aus. Konfigurieren Sie die IPsec-Lebenszeitdauer und -Größe, und klicken Sie dann auf Weiter.

IKE VERSION 2  IKE VERSION 1

IKE Policy  
Globally applied

IPSec Proposal  
Custom set selected

Authentication Type  
 Pre-shared Manual Key  Certificate

Local Pre-shared Key  
.....

Remote Peer Pre-shared Key  
.....

IPSEC SETTINGS

Lifetime Duration  seconds  
120 - 2147483647; (Default: 28800)

Lifetime Size  kilobytes  
10 - 2147483647; (Default: 4608000).  
Leave empty for Unlimited.

Additional Options  
Diffie-Hellman Group for Perfect Forward Secrecy  
 ⓘ

PSK- und Lebenszeitkonfiguration

Schritt 9: Überprüfen Sie die Konfiguration, und klicken Sie auf Fertig stellen.

## Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

### Vti-Ipsec Connection Profile

**i** Peer endpoint needs to be configured according to specified below configuration.

**VPN Access Interface IP**  tunnel10 (1.1.1.1)



**Peer IP Address** 10.106.63.23

#### IKE V2

**IKE Policy** aes-256-sha256-sha256-14

**IPSec Proposal** aes-256-sha-256

**Authentication Type** Pre-shared Manual Key

#### IKE V1: DISABLED

#### IPSEC SETTINGS

**Lifetime Duration** 28800 seconds

**Lifetime Size** 4608000 kilobytes

#### ADDITIONAL OPTIONS

**Diffie-Hellman Group** Null (not selected)

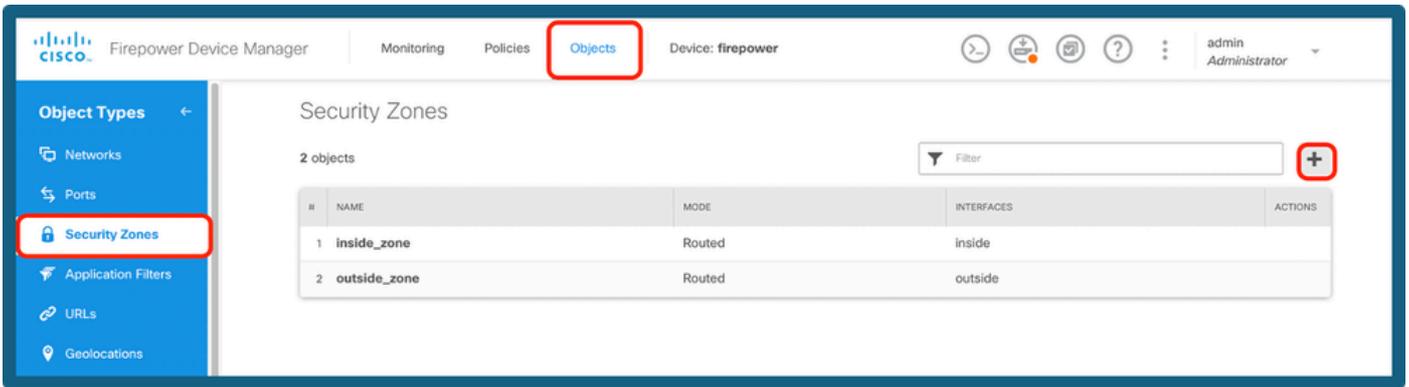
**i** Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

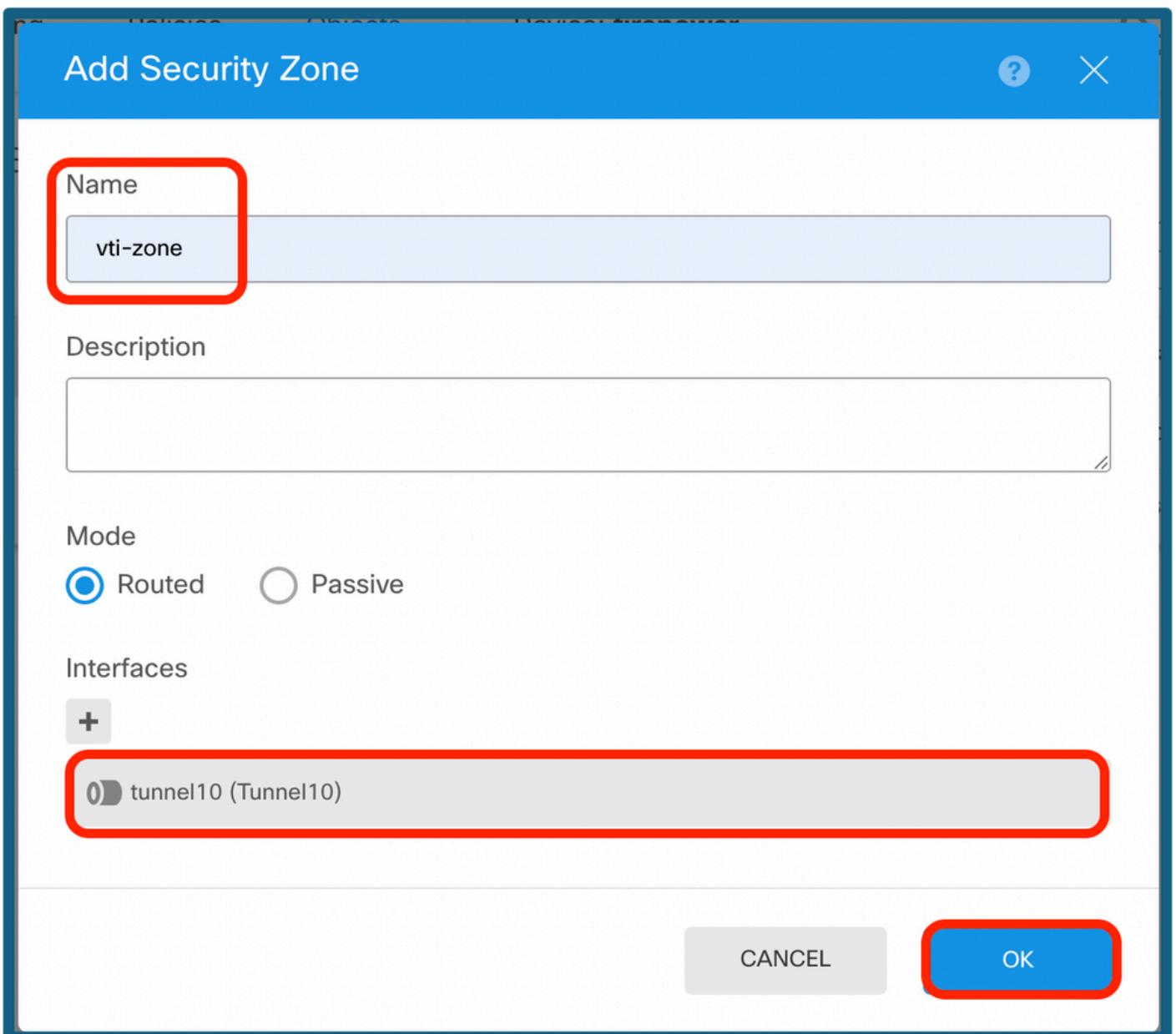
Konfigurationszusammenfassung

Schritt 10a: Navigieren Sie zu Objekte > Sicherheitszonen, und klicken Sie dann auf + Symbol.



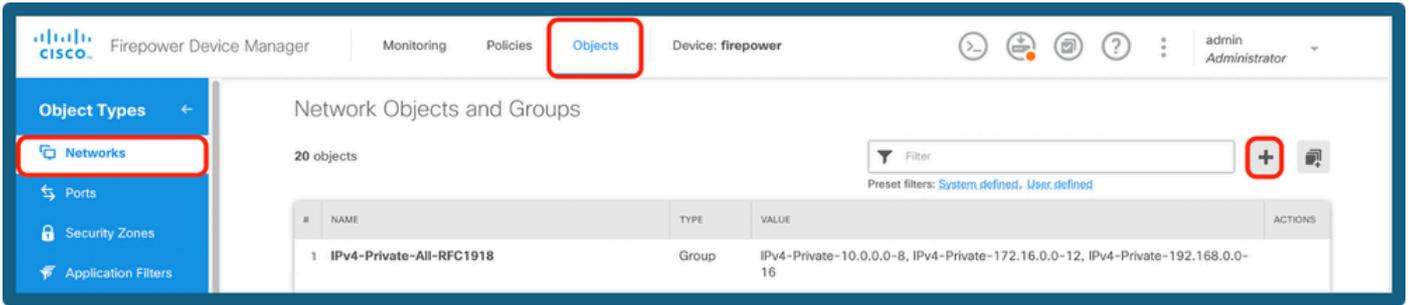
Hinzufügen einer Sicherheitszone

Schritt 10b: Erstellen Sie eine Zone, und wählen Sie die VTI-Schnittstelle wie unten gezeigt aus.



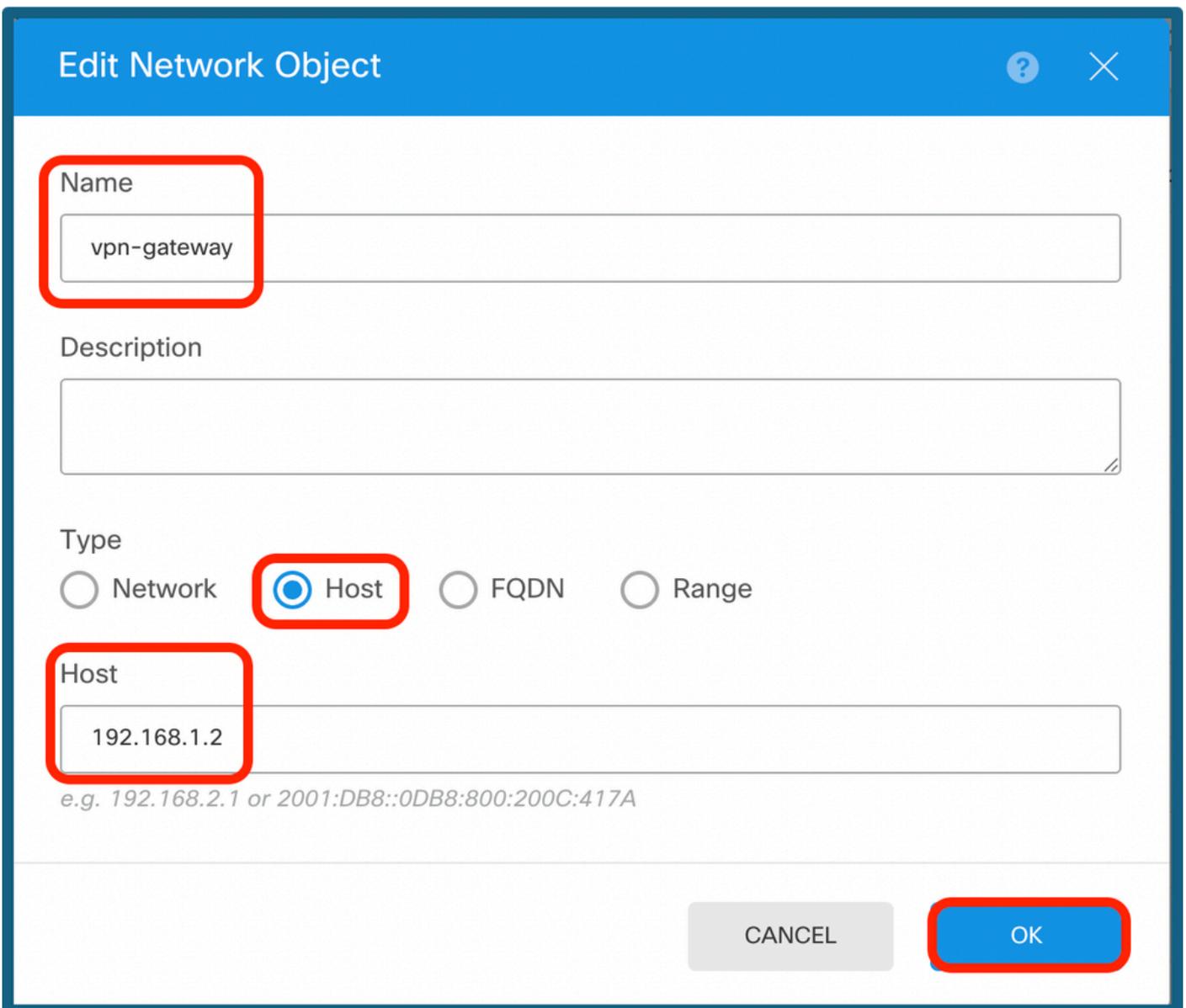
Konfiguration der Sicherheitszone

Schritt 11a: Navigieren Sie zu Objekte > Netzwerke, und klicken Sie auf + Symbol.



Netzwerkobjekte hinzufügen

Schritt 11b: Fügen Sie ein Host-Objekt hinzu, und erstellen Sie ein Gateway mit Tunnel-IP des Peer-End.



VPN-Gateway konfigurieren

Schritt 11c: Fügen Sie das Remote- und das lokale Subnetz hinzu.

### Edit Network Object

Name  
remote-vpn-network

Description

Type  
 Network  Host  FQDN  Range

Network  
172.16.10.0/24  
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL OK

Remote-IP-Konfiguration

### Edit Network Object

Name  
inside-network

Description

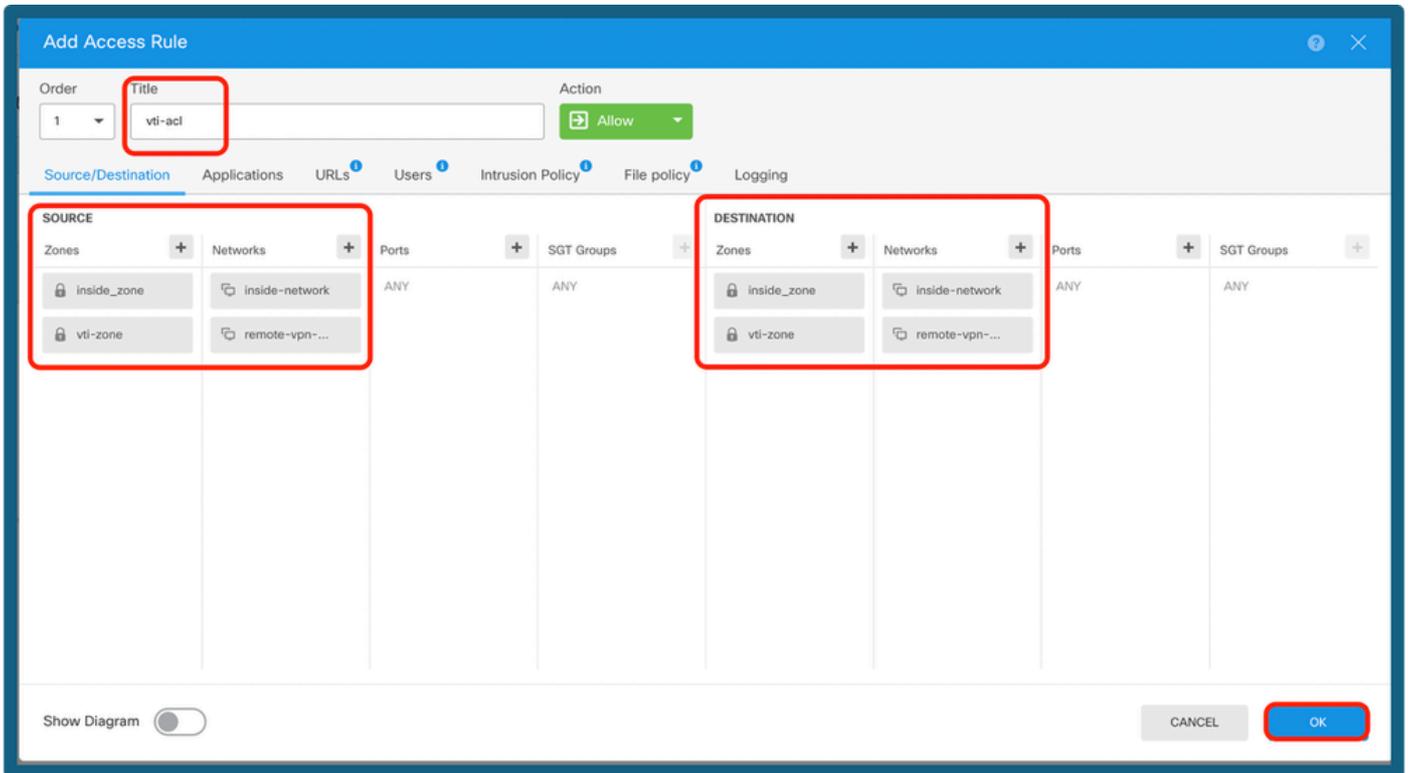
Type  
 Network  Host  FQDN  Range

Network  
10.10.10.0/24  
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL OK

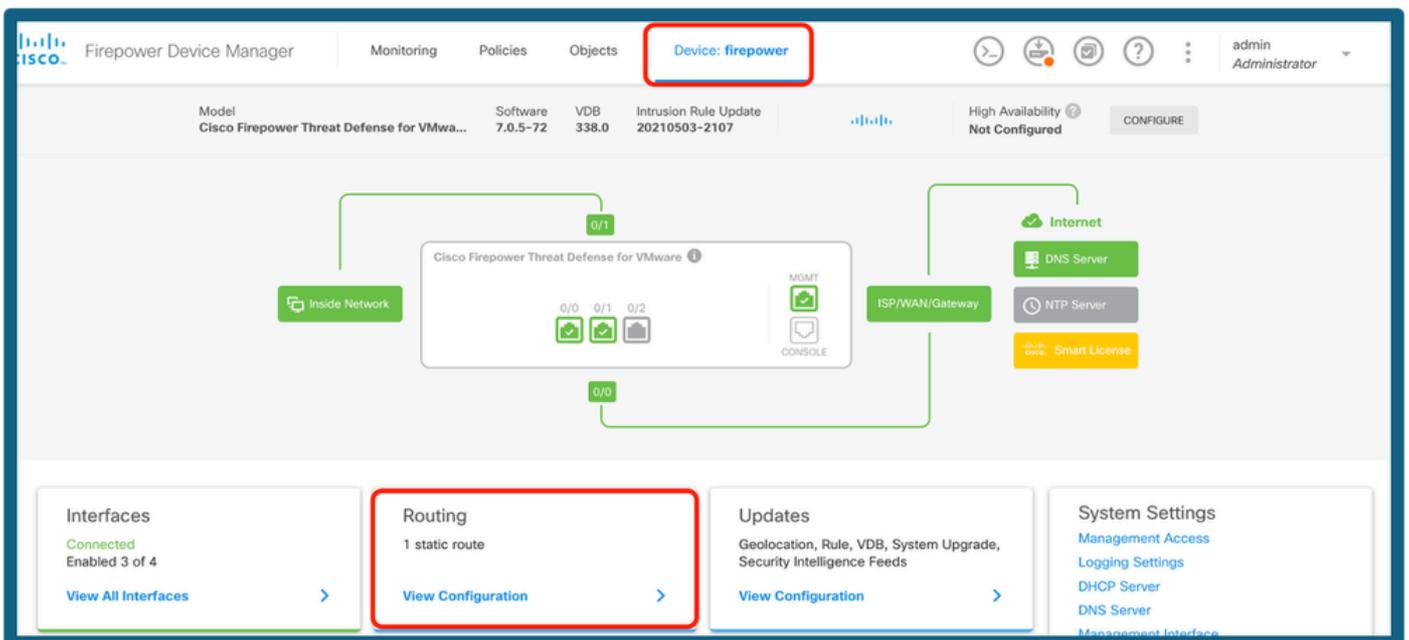
Lokale IP-Konfiguration

Schritt 12: Navigieren Sie zu Device > Policies (Gerät > Richtlinien), und konfigurieren Sie die Zugriffskontrollrichtlinie.



Zugriffskontrollrichtlinie hinzufügen

Schritt 13a: Fügen Sie das Routing über den VTI-Tunnel hinzu. Navigieren Sie zu Gerät > Routing.



Routing auswählen

Schritt 13b: Navigieren Sie auf der Registerkarte Routing zu Static Route. Klicken Sie auf + Symbol.

Device Summary  
Routing

Add Multiple Virtual Routers ▾ Commands ▾ BGP Global Settings

**Static Routing** | BGP | OSPF | EIGRP | ECMP Traffic Zones

1 route Filter +

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	default	outside	IPv4	0.0.0.0/0	10.106.52.1		1	

Route hinzufügen

Schritt 13c: Stellen Sie die Schnittstelle bereit, wählen Sie das Netzwerk, und stellen Sie das Gateway bereit. Klicken Sie auf OK.

## Add Static Route

Name  
vti-route

Description

Interface  
tunnel10 (Tunnel10)

Protocol  
 IPv4  IPv6

Networks  
+  
remote-vpn-network

Gateway  
vpn-gateway

Metric  
1

SLA Monitor Applicable only for IPv4 Protocol type  
Please select an SLA Monitor

CANCEL OK

Statische Route konfigurieren

Schritt 14: Navigieren Sie zu Bereitstellen. Überprüfen Sie die Änderungen, und klicken Sie dann

auf Jetzt bereitstellen.

**Pending Changes**

✓ **Last Deployment Completed Successfully**  
26 Jun 2025 05:27 PM. [See Deployment History](#)

Deployed Version (26 Jun 2025 05:27 PM)	Pending Version
<b>+ Static Route Added: vti-route</b>	
-	metricValue: 1
-	ipType: IPv4
-	name: vti-route
iface:	
-	tunnel10
gateway:	
-	vpn-gateway
networks:	
-	remote-vpn-network
<b>+ Access Rule Added: vti-acl</b>	
-	logFiles: false
-	eventLogAction: LOG_NONE
-	ruleId: 268435458
-	name: vti-acl
sourceZones:	
-	vti-zone
-	inside_zone
destinationZones:	
-	vti-zone
-	inside_zone
sourceNetworks:	
-	remote-vpn-network
-	inside-network
destinationNetworks:	

MORE ACTIONS ▾ CANCEL **DEPLOY NOW** ▾

Konfig. bereitstellen

## Überprüfung

Nach Abschluss der Bereitstellung können Sie den Tunnelstatus in der CLI mithilfe der folgenden Befehle überprüfen:

1. show crypto ikev2 sa
2. show crypto ipsec sa <Peer-IP>

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote Status Role
3294213359 10.106.52.222/500 10.106.63.23/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/141 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x26a14554/0xd5db88bc
```

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
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: 10.106.63.23
```

show-Befehle

## Zugehörige Informationen

Weitere Informationen zu Site-to-Site-VPNs auf dem von FDM verwalteten FTD finden Sie im vollständigen Konfigurationsleitfaden:

[FTD verwaltet durch FDM - Konfigurationsleitfaden](#)

## 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.