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

Inhalt

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:

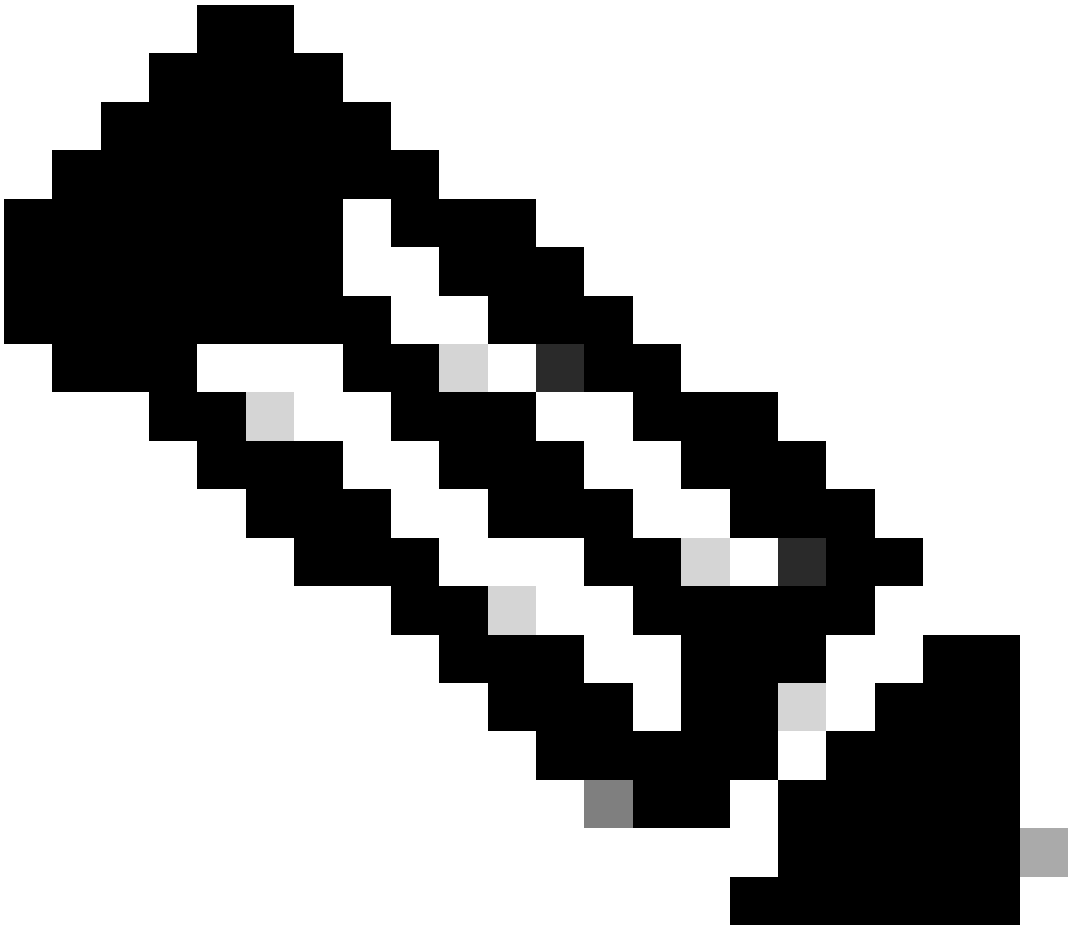
- Cisco Firepower Threat Defense (FTD) Version 7.0, verwaltet durch Firepower Device Manager (FDM).

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.

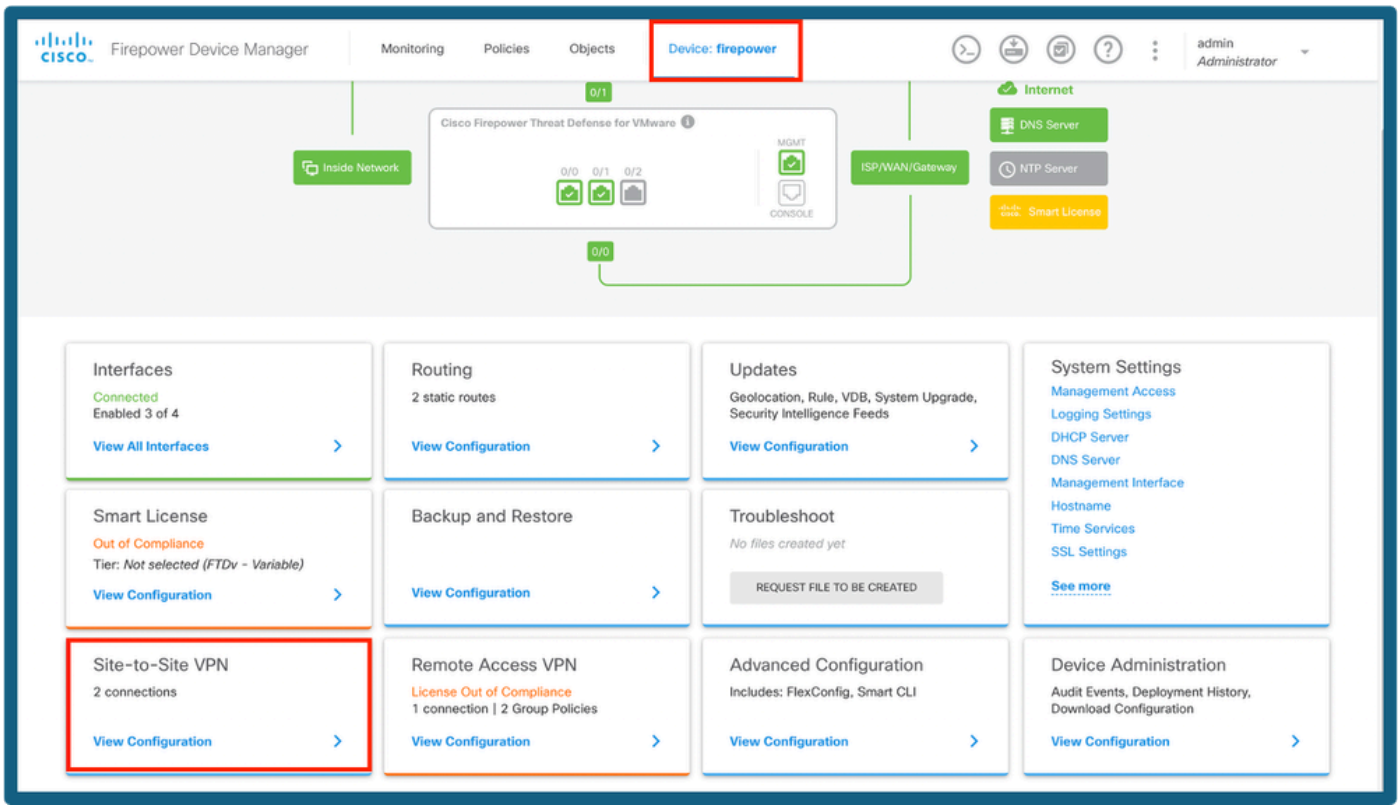
Das vorliegende Dokument behandelt die SVTI-Konfiguration (Static Virtual Tunnel Interface).



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.

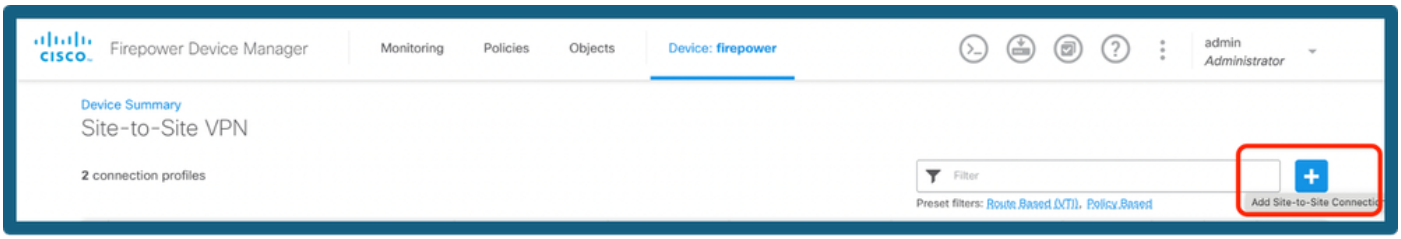
Konfigurationsschritte bei FDM

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



FDM-Dashboard

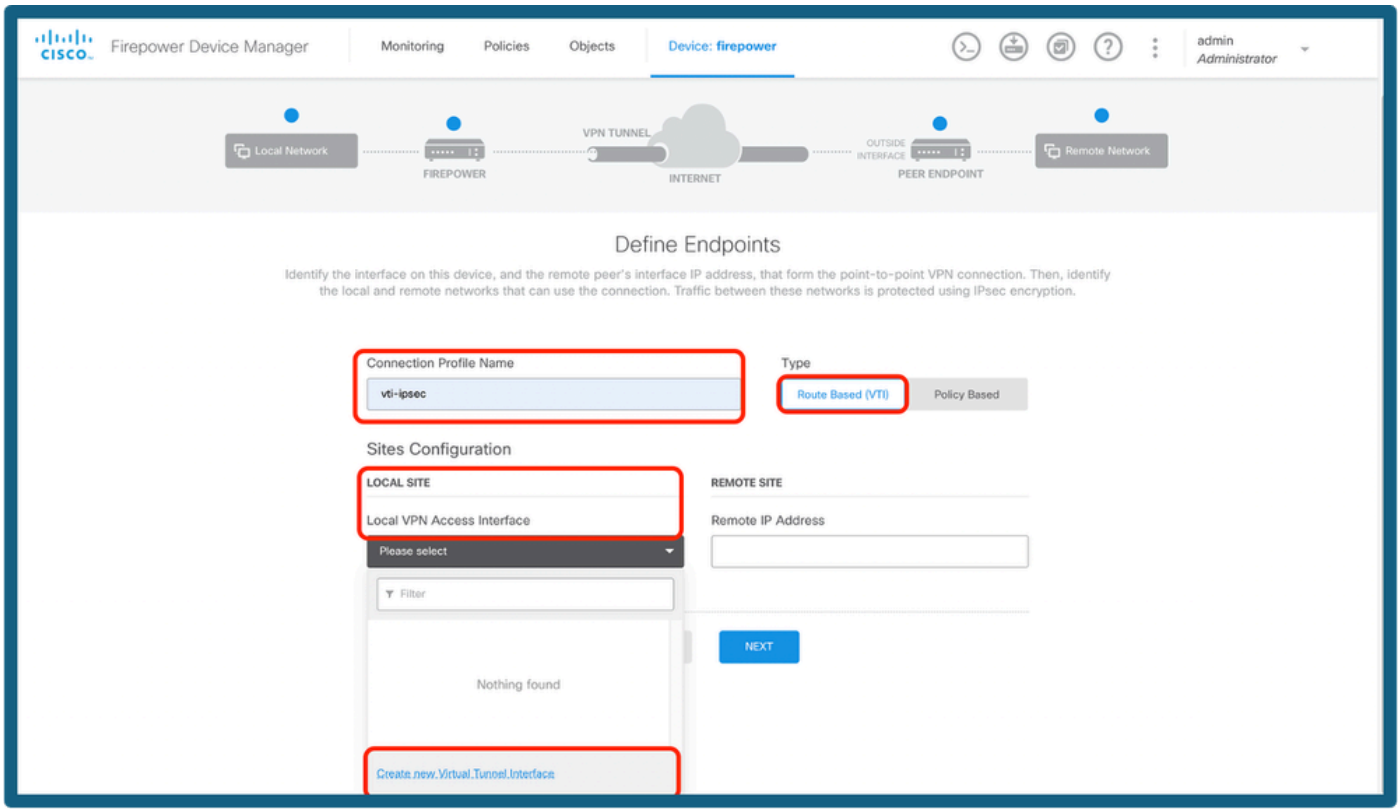
Schritt 2: Klicken Sie auf das +-Symbol, um eine neue Site zur Site-Verbindung hinzuzufügen.



S2S-Verbindung hinzufügen

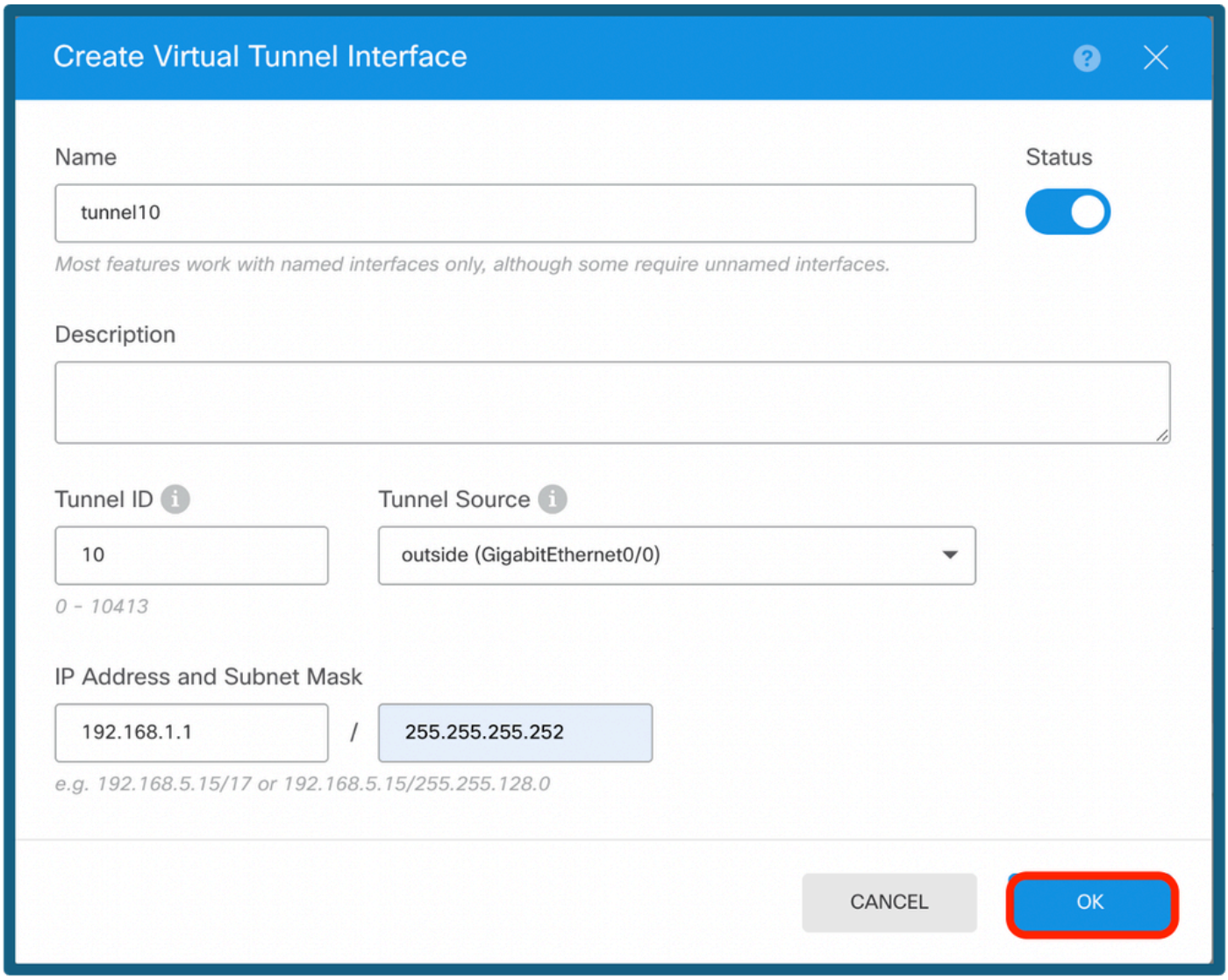
Schritt 3: Geben Sie einen Topologienamen an, und wählen Sie den VPN-Typ als routenbasiert (VTI) aus.

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.



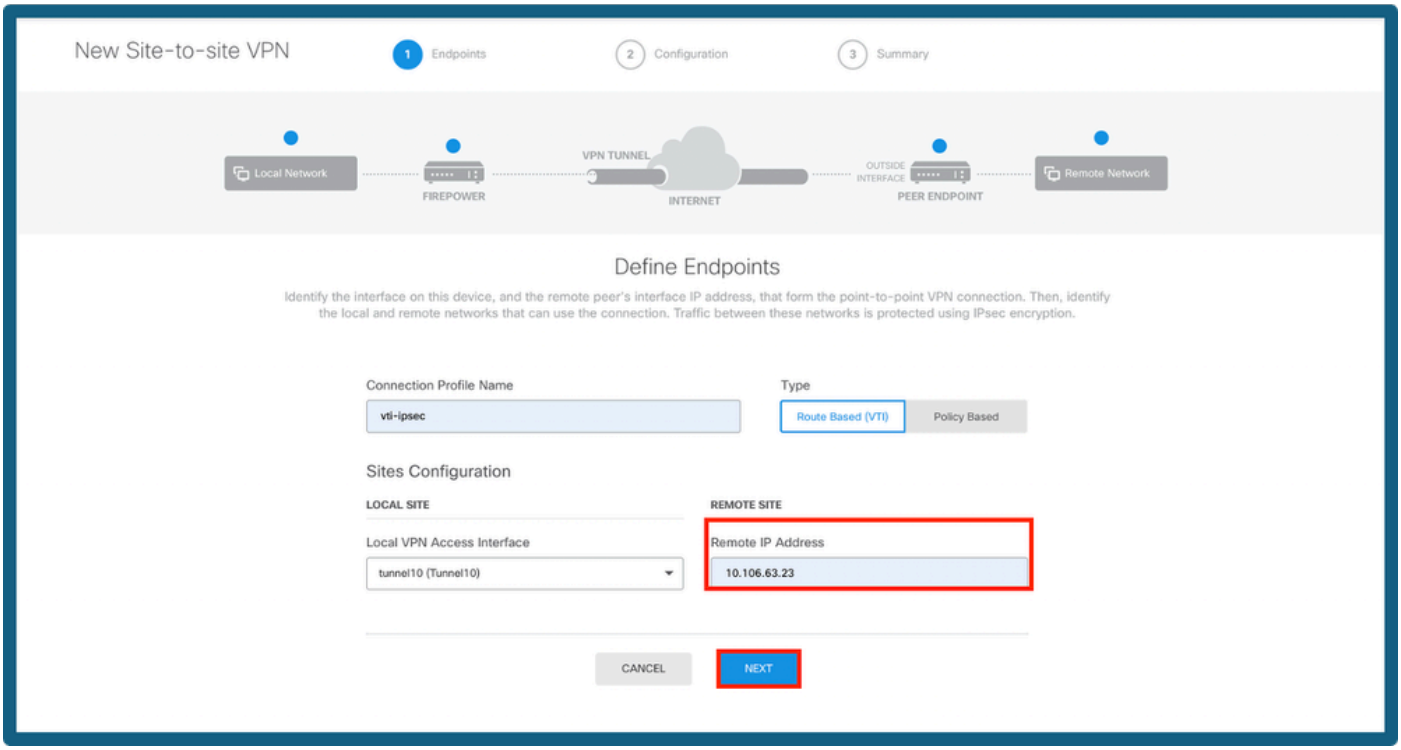
Tunnelschnittstelle hinzufügen

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



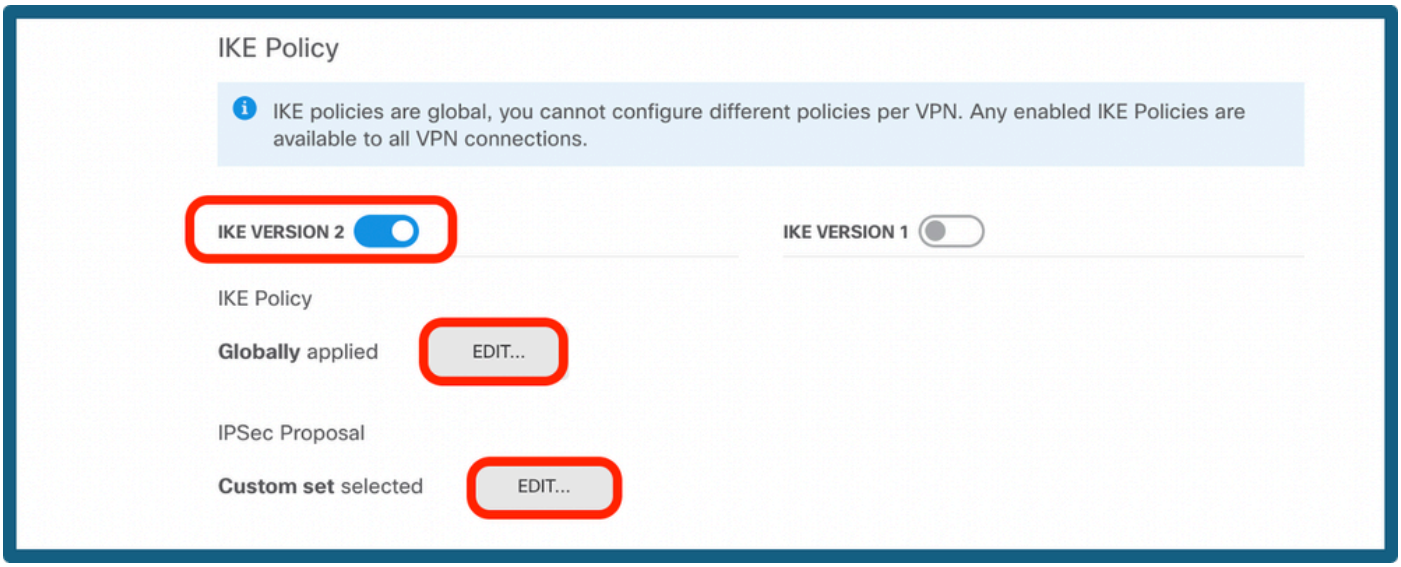
VTI-Konfiguration

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.



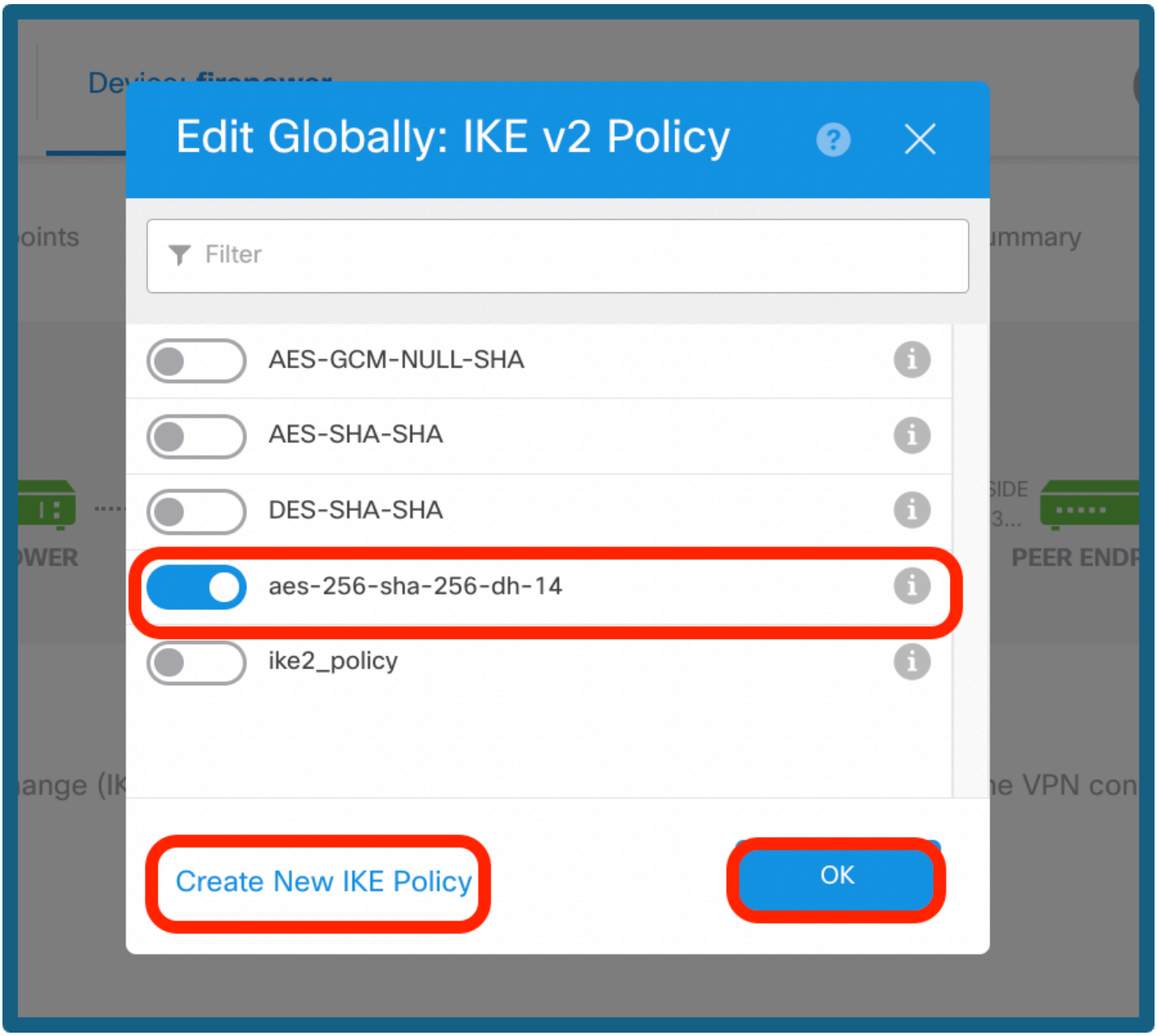
Peer-IP hinzufügen

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

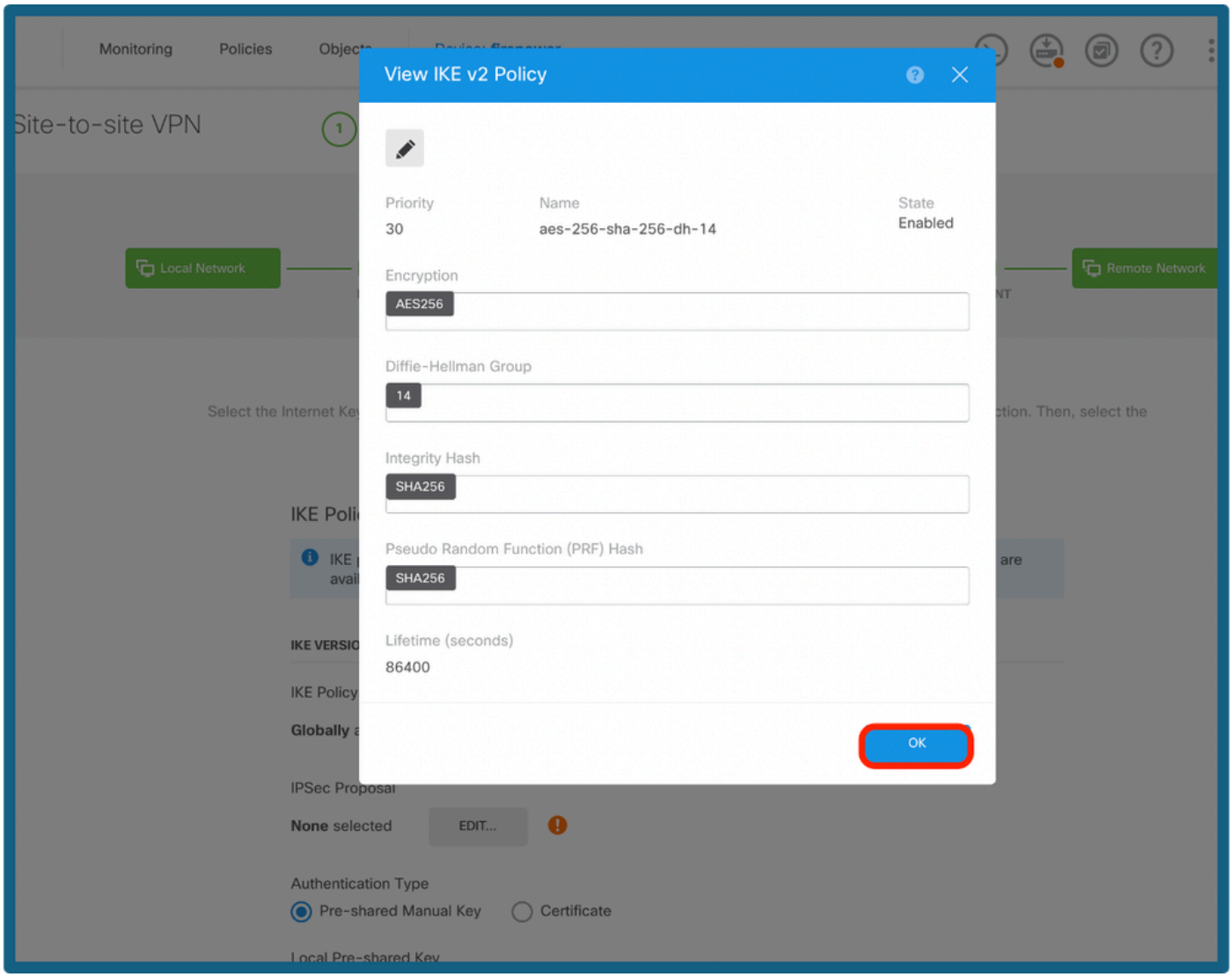


IKE-Version konfigurieren

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.

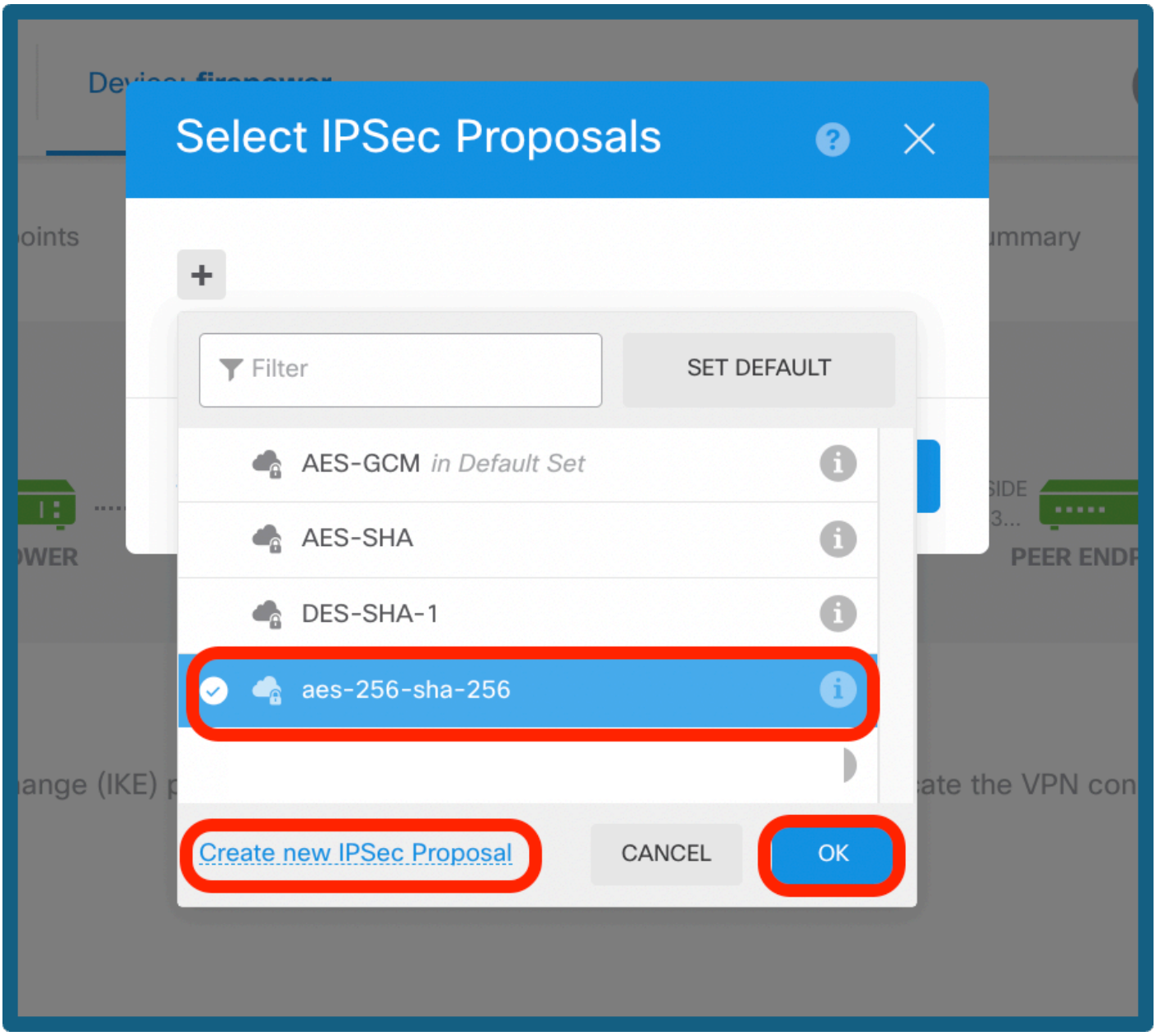


IKE-Richtlinie auswählen

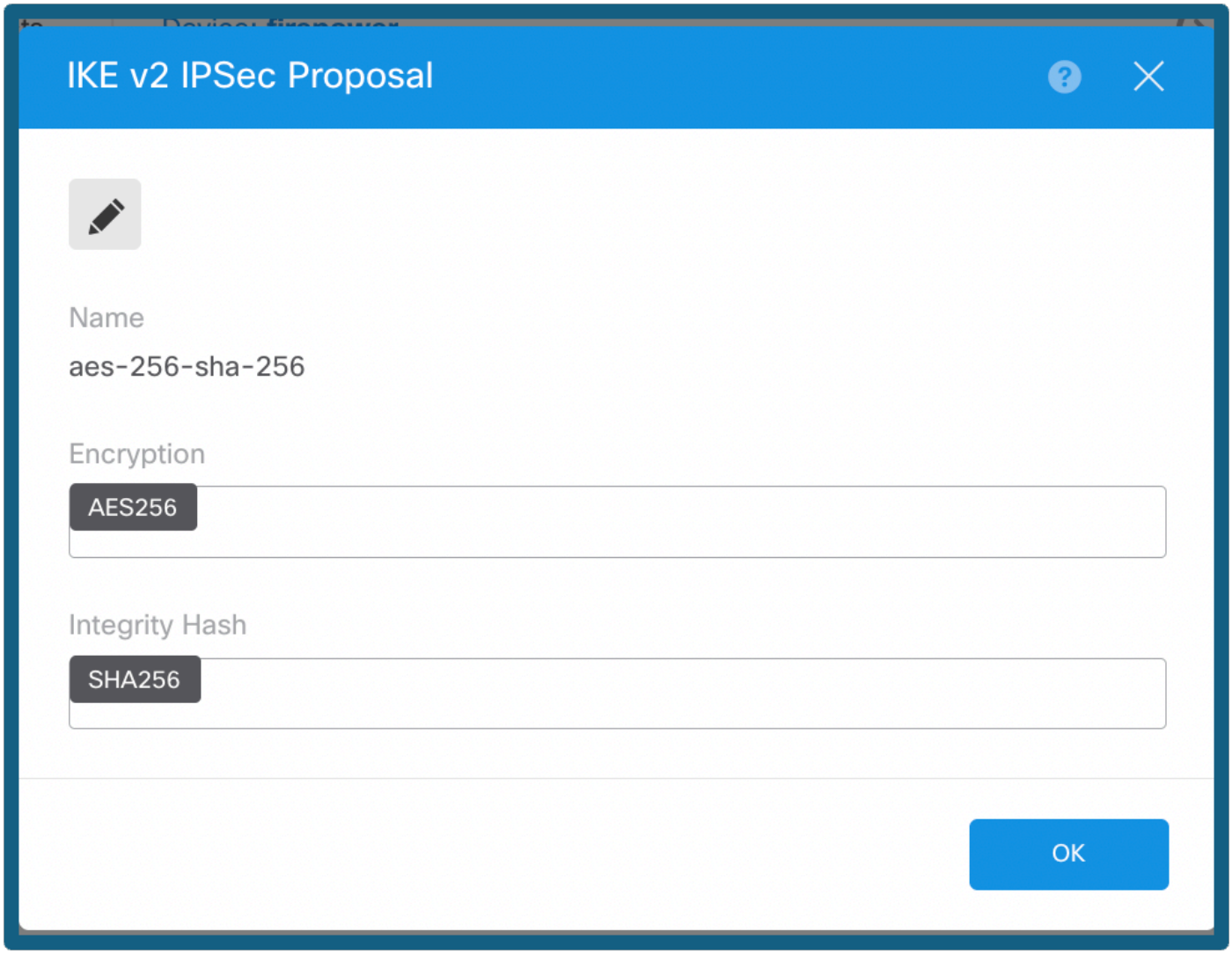


Konfiguration der IKE-Richtlinie

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.



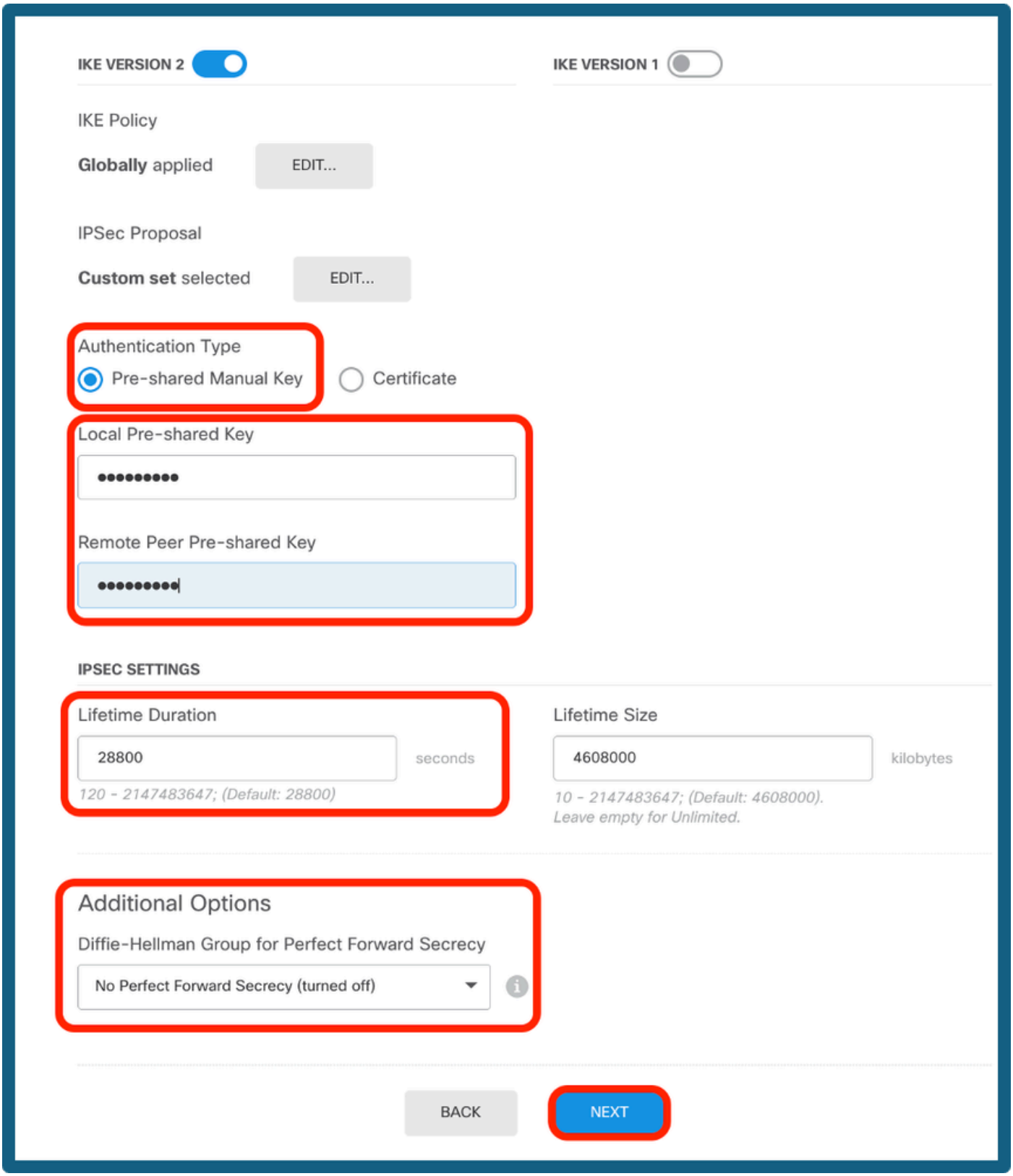
IPsec-Angebot auswählen



Konfiguration des IPsec-Angebots

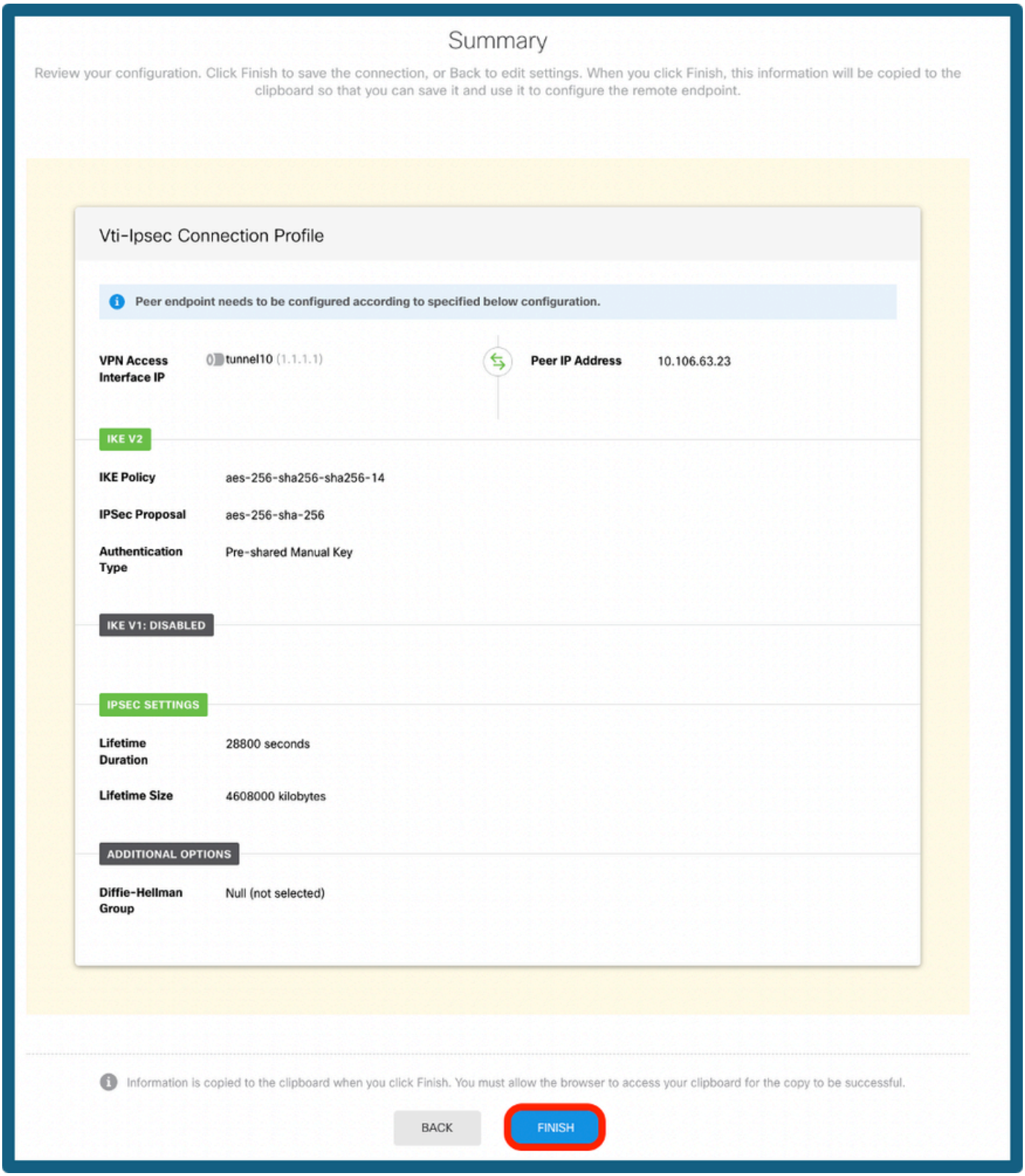
Schritt 8a: Wählen Sie den Authentifizierungstyp aus. Wenn ein vorinstallierter manueller Schlüssel verwendet wird, geben Sie den vorinstallierten lokalen und Remote-Schlüssel an.

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.



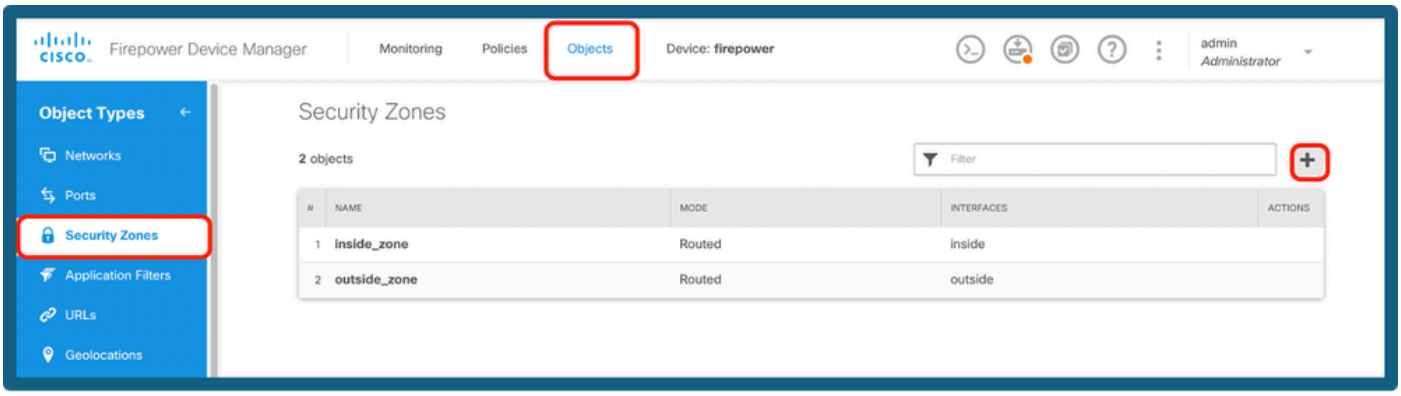
PSK- und Lebenszeitkonfiguration

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



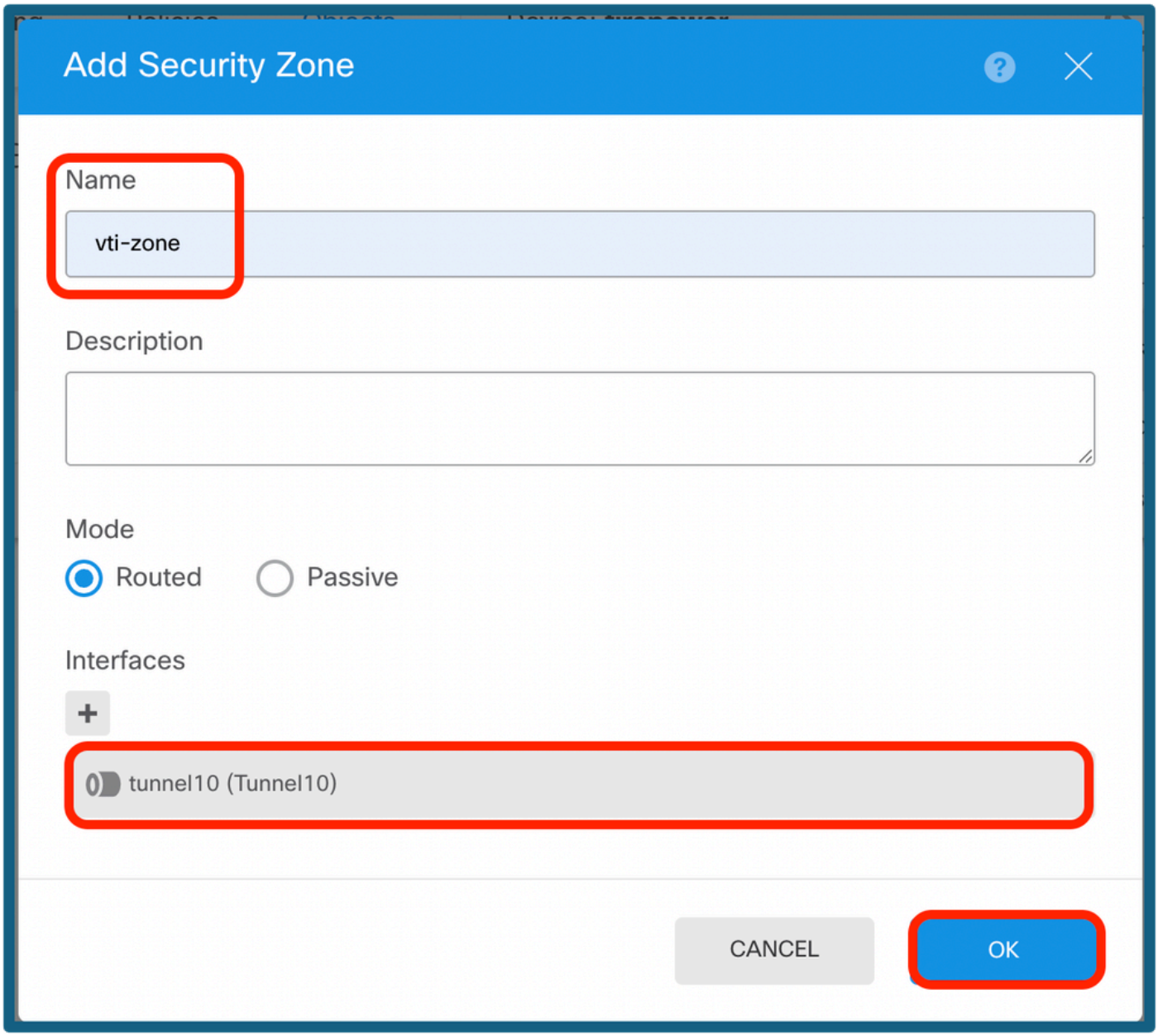
Konfigurationszusammenfassung

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



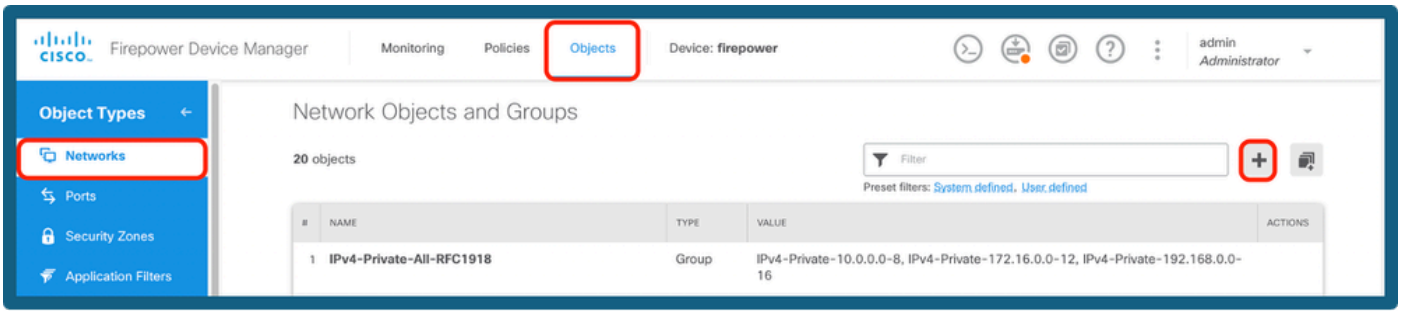
Hinzufügen einer Sicherheitszone

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



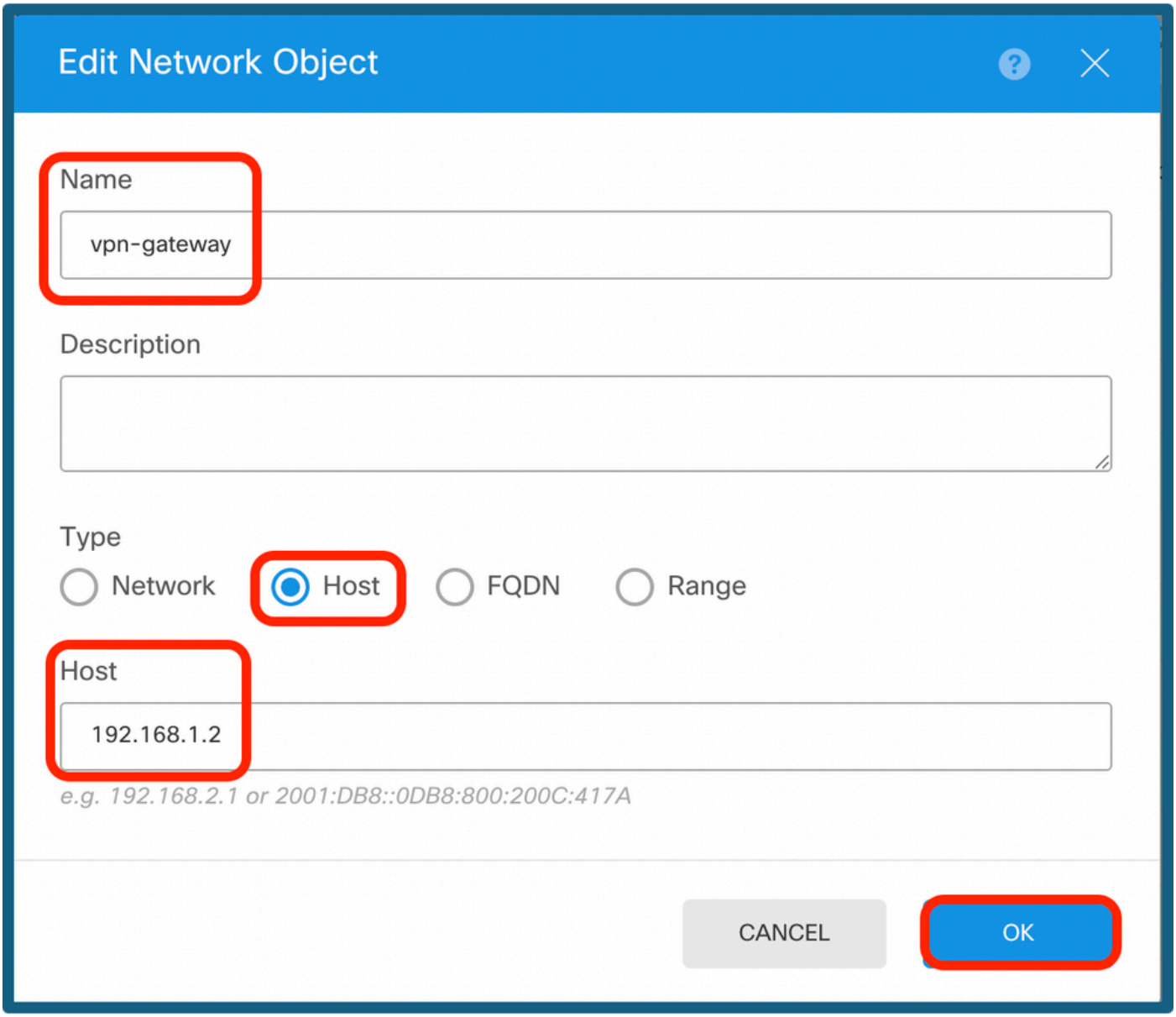
Konfiguration der Sicherheitszone

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



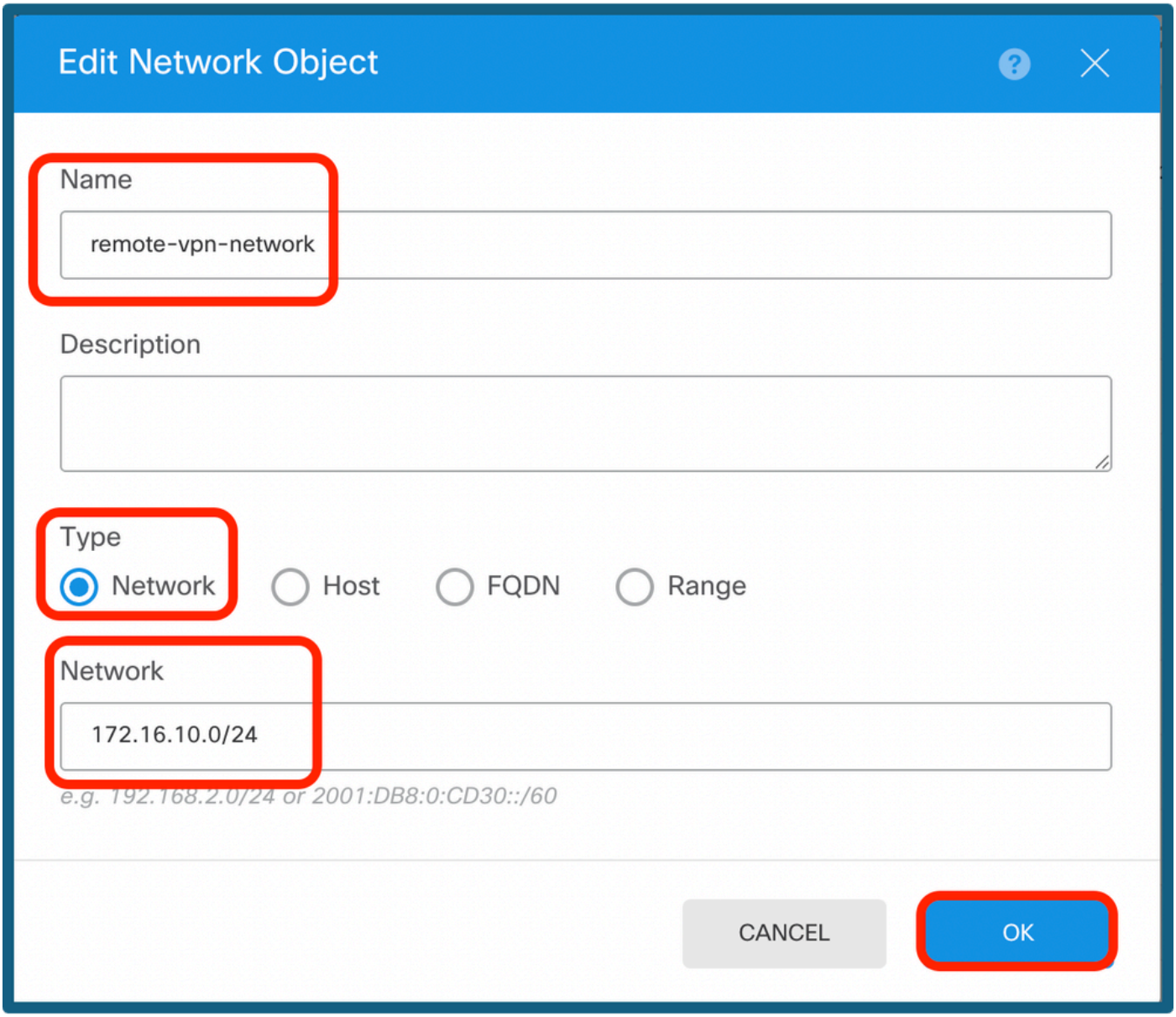
Netzwerkobjekte hinzufügen

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

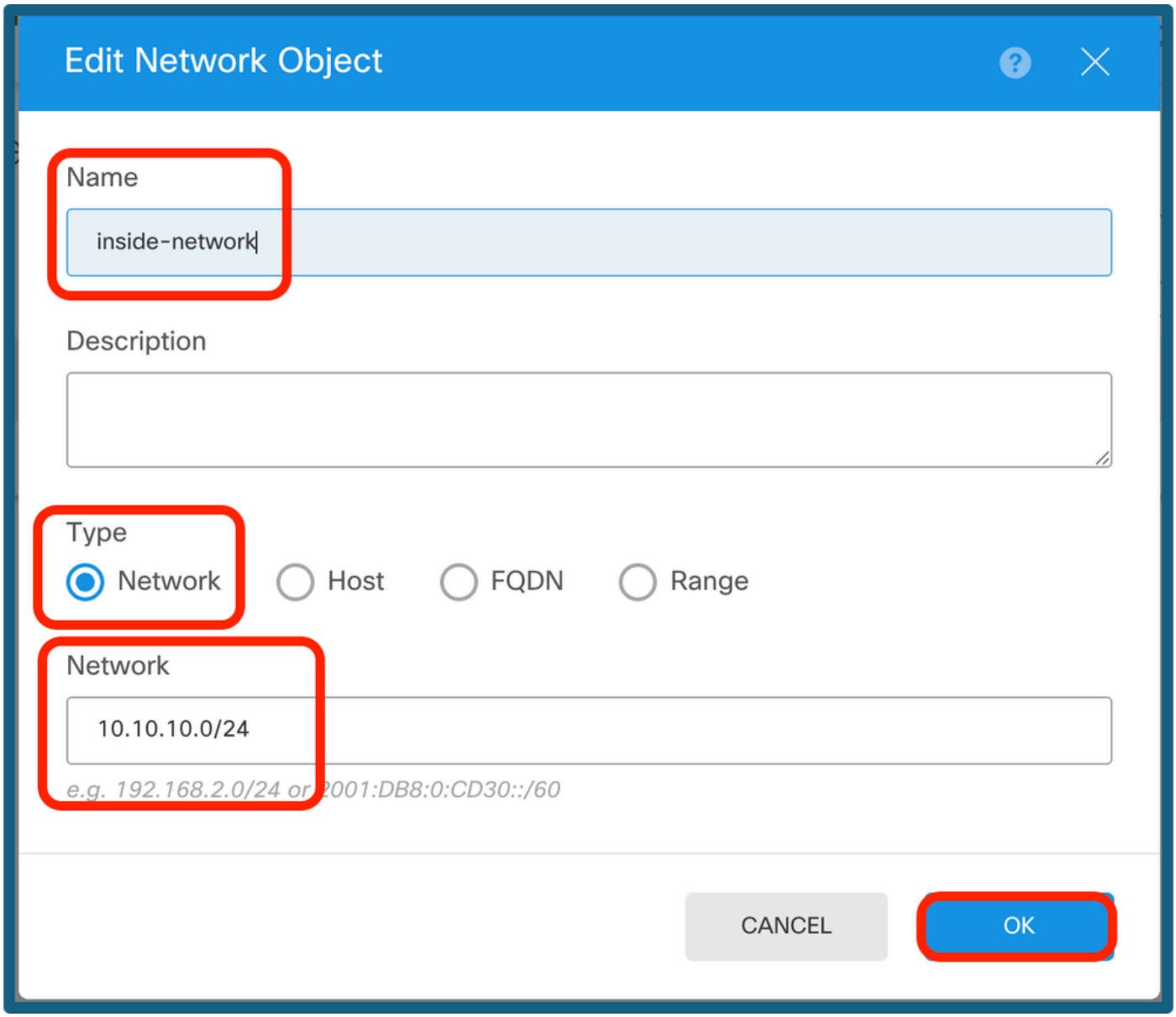


VPN-Gateway konfigurieren

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

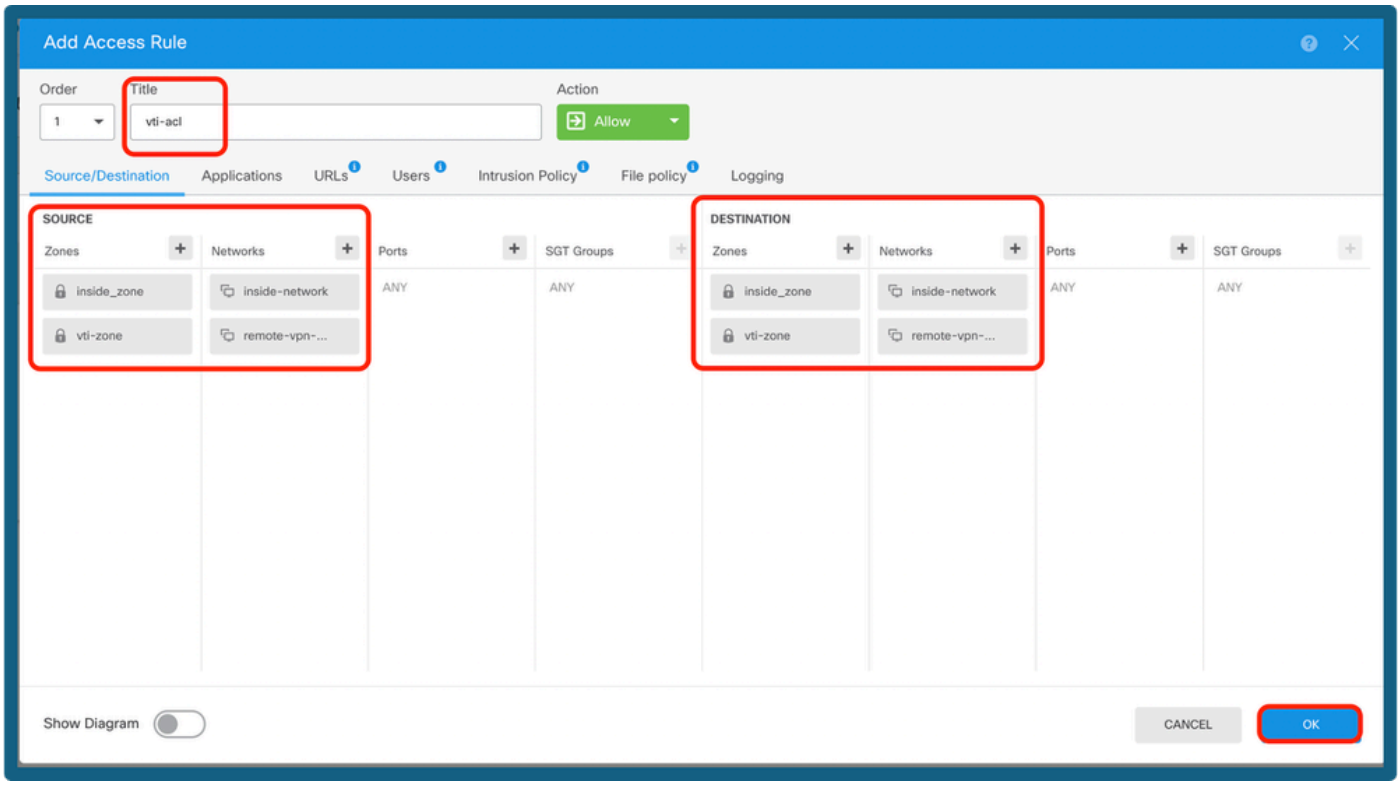


Remote-IP-Konfiguration



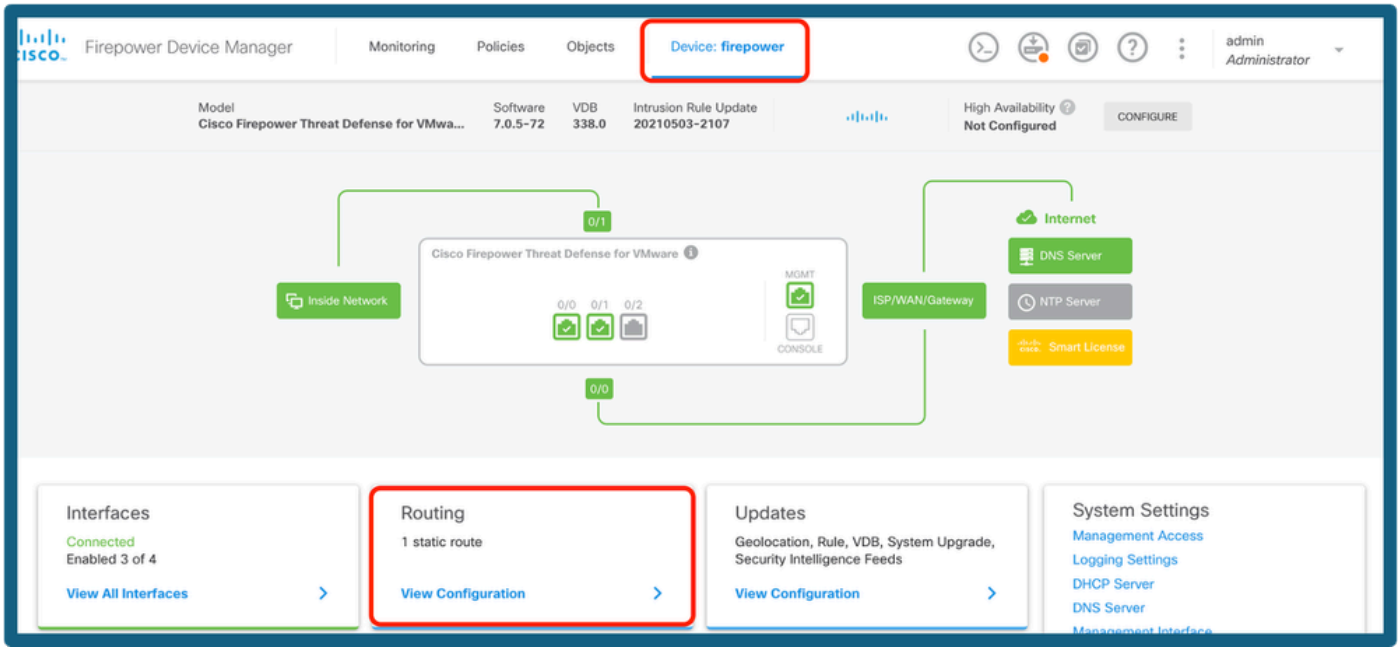
Lokale IP-Konfiguration

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



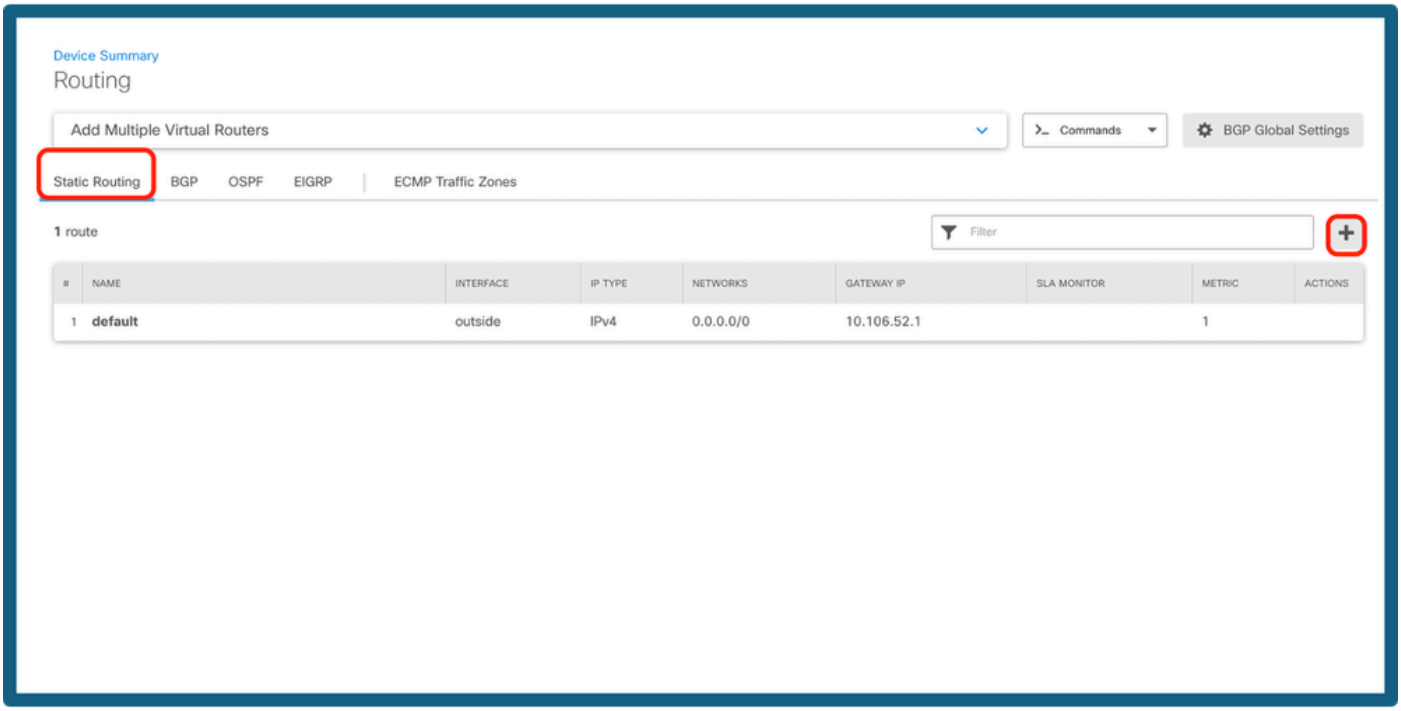
Zugriffskontrollrichtlinie hinzufügen

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



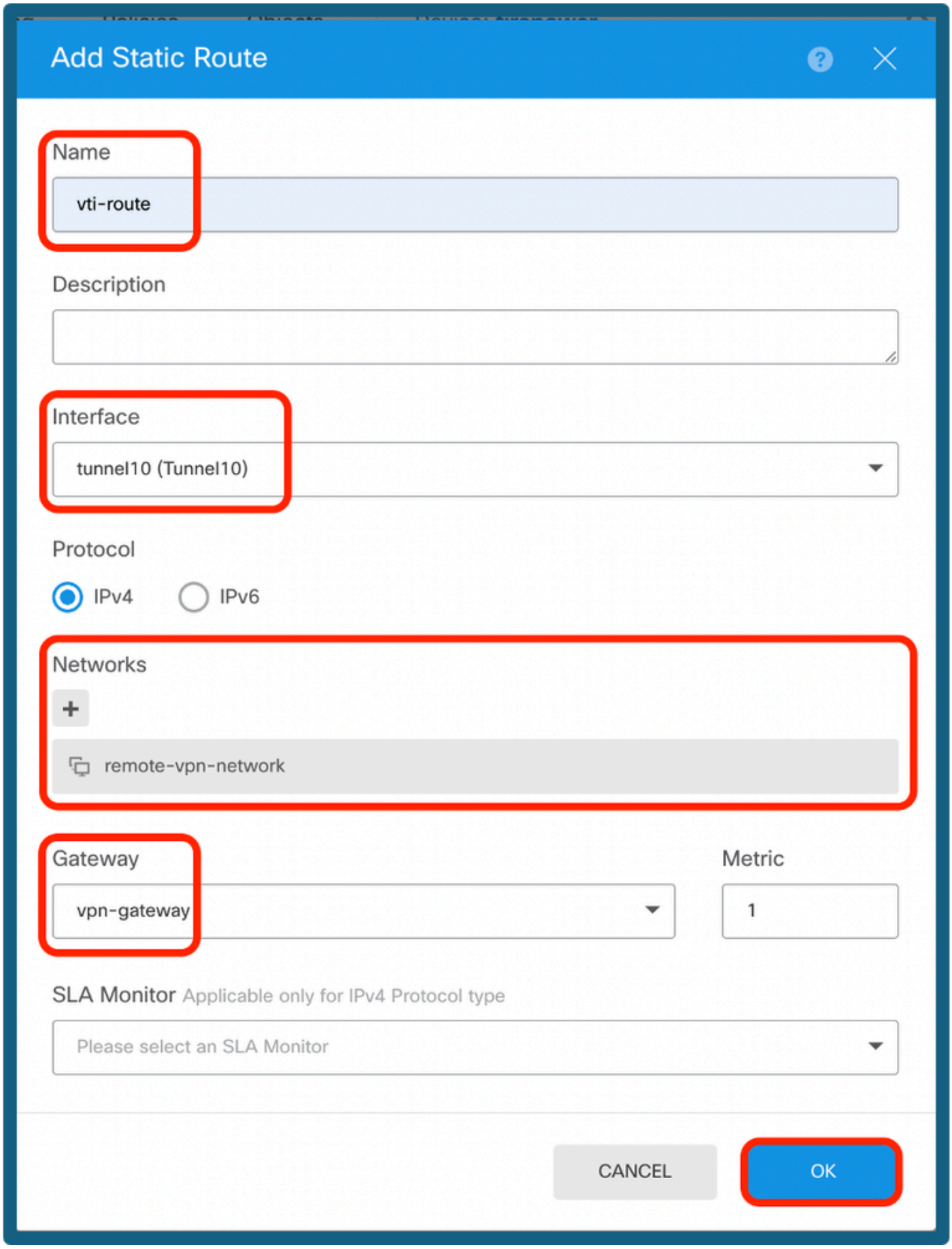
Routing auswählen

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



Route hinzufügen

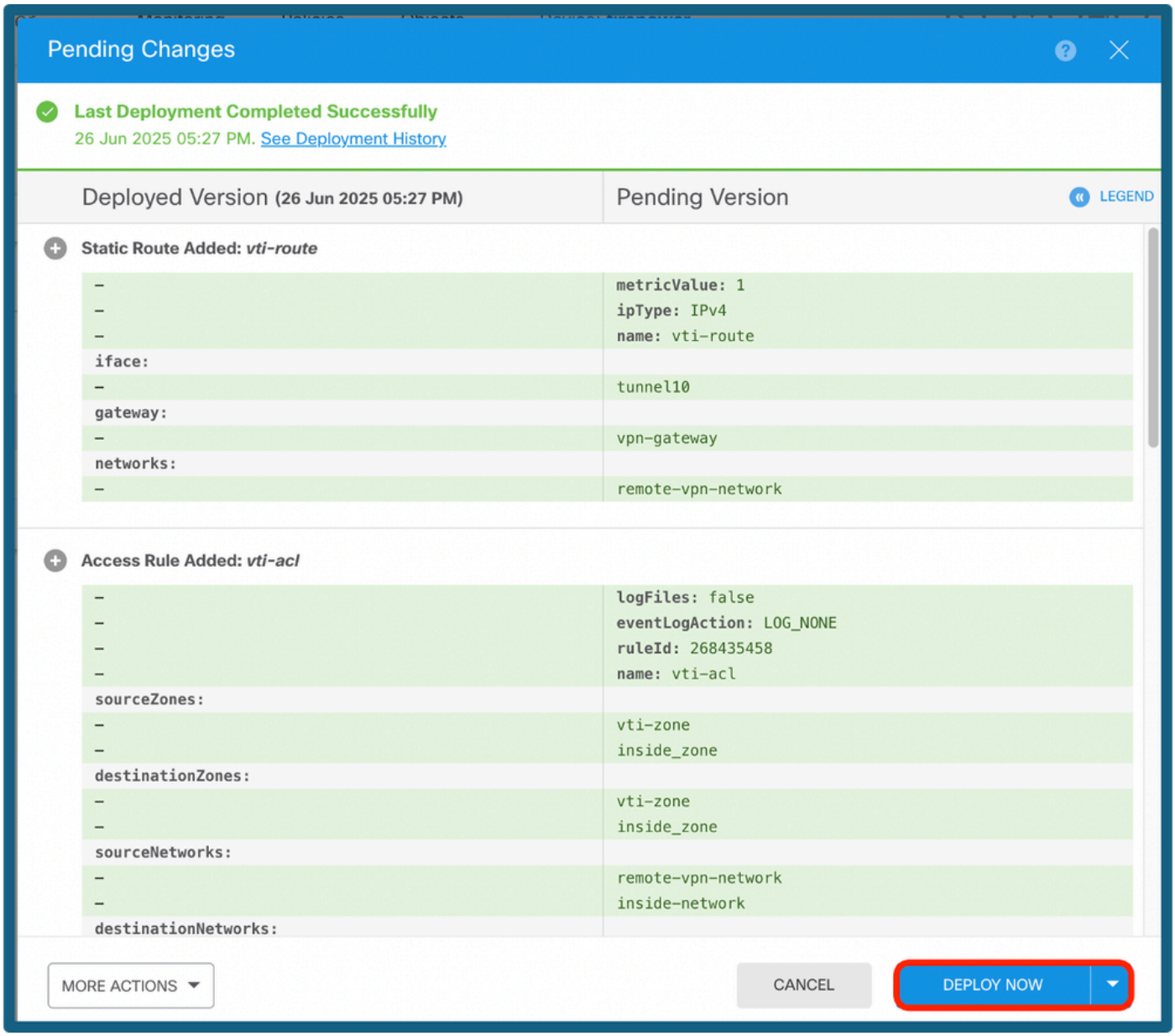
Schritt 13c: Stellen Sie die Schnittstelle bereit, wählen Sie das Netzwerk, und stellen Sie das Gateway bereit. Klicken Sie auf OK.



Statische Route konfigurieren

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

auf Jetzt bereitstellen.

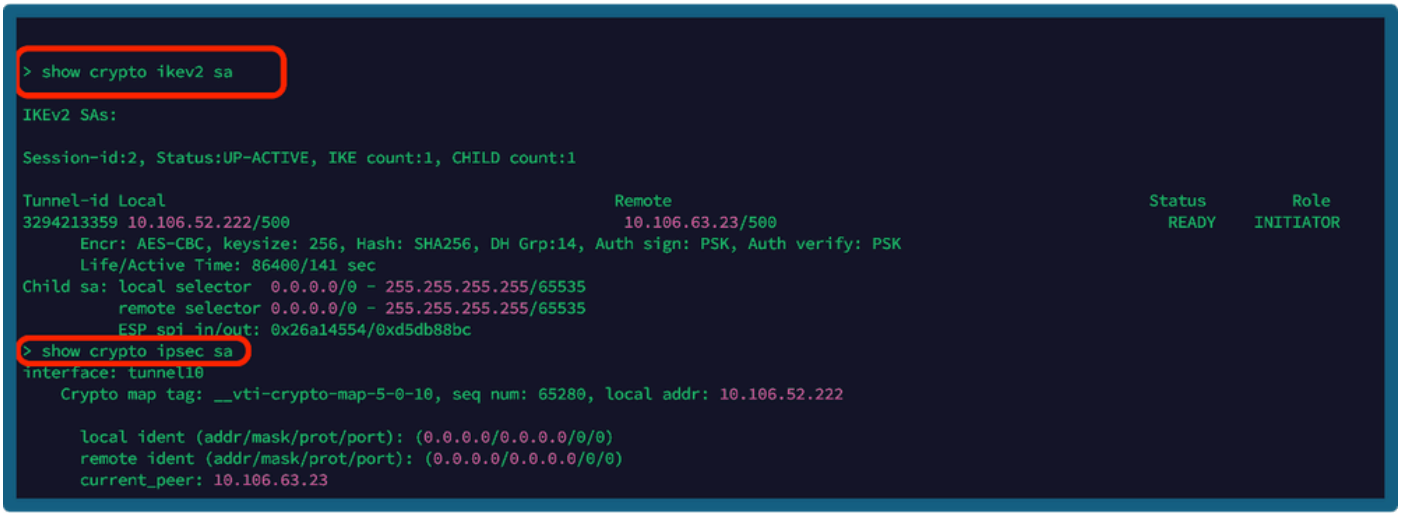


Konfig. bereitstellen

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-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.