Konfigurieren eines Dual Active Route-basierten Site-to-Site-VPN mit PBR auf einem von FDM verwalteten FTD

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration eines dualen, aktiven, routenbasierten Site-to-Site-VPN mit PBR auf einem durch FDM verwalteten FTD beschrieben.

Voraussetzungen

Anforderungen

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

- Grundlegendes Verständnis von VPN
- Grundlegendes Verständnis von Policy Based Routing (PBR)
- Grundlegendes Verständnis des Internet Protocol Service Level Agreement (IP SLA)
- Erfahrung mit FDM

Verwendete Komponenten

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

- Cisco FTDv Version 7.4.2
- Cisco FDM Version 7.4.2

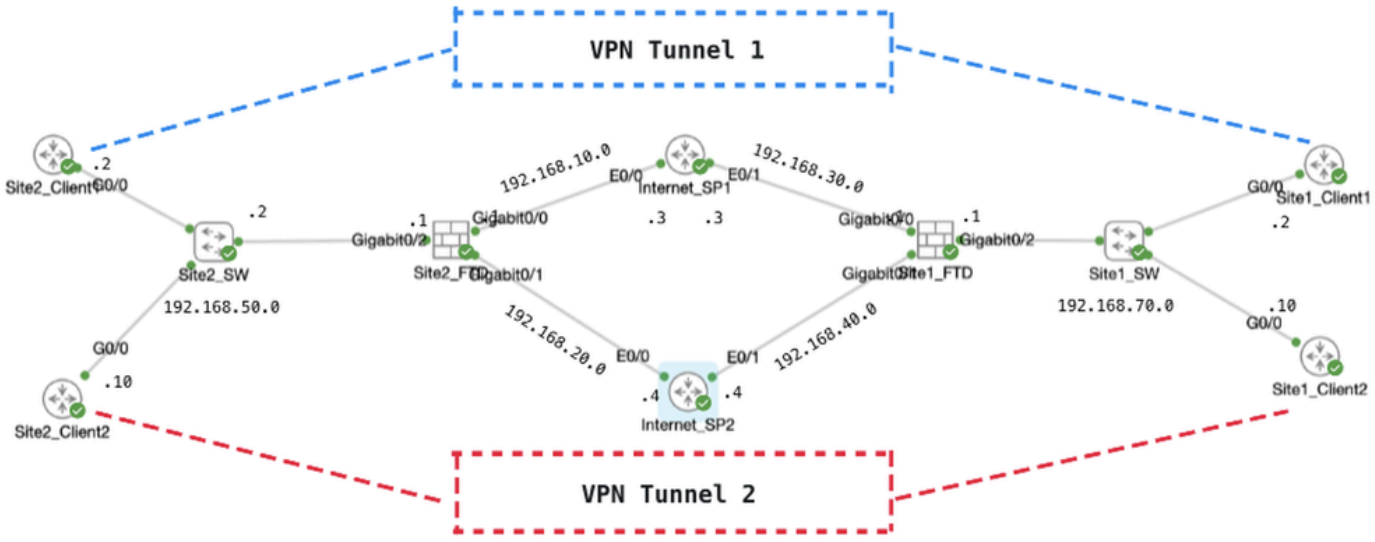
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

In diesem Dokument wird die Konfiguration eines dualen, aktiven, routenbasierten Site-to-Site-VPN auf FTD erläutert. In diesem Beispiel haben FTDs am Standort 1 und am Standort 2 zwei aktive ISP-Verbindungen, die das Site-to-Site-VPN mit beiden ISPs gleichzeitig herstellen. Standardmäßig durchläuft der VPN-Datenverkehr Tunnel 1 über ISP1 (blaue Linie). Bei bestimmten Hosts wird der Datenverkehr über Tunnel 2 und ISP2 geleitet (rote Linie). Wenn auf ISP1 eine Unterbrechung auftritt, wechselt der Datenverkehr als Backup auf ISP2. Umgekehrt: Wenn auf dem ISP2 eine Unterbrechung auftritt, wechselt der Datenverkehr als Backup auf den ISP1. Richtlinienbasiertes Routing (Policy-Based Routing, PBR) und Internet Protocol Service Level Agreement (IP SLA) werden in diesem Beispiel verwendet, um diese Anforderungen zu erfüllen.

Konfigurieren

Netzwerkdiagramm



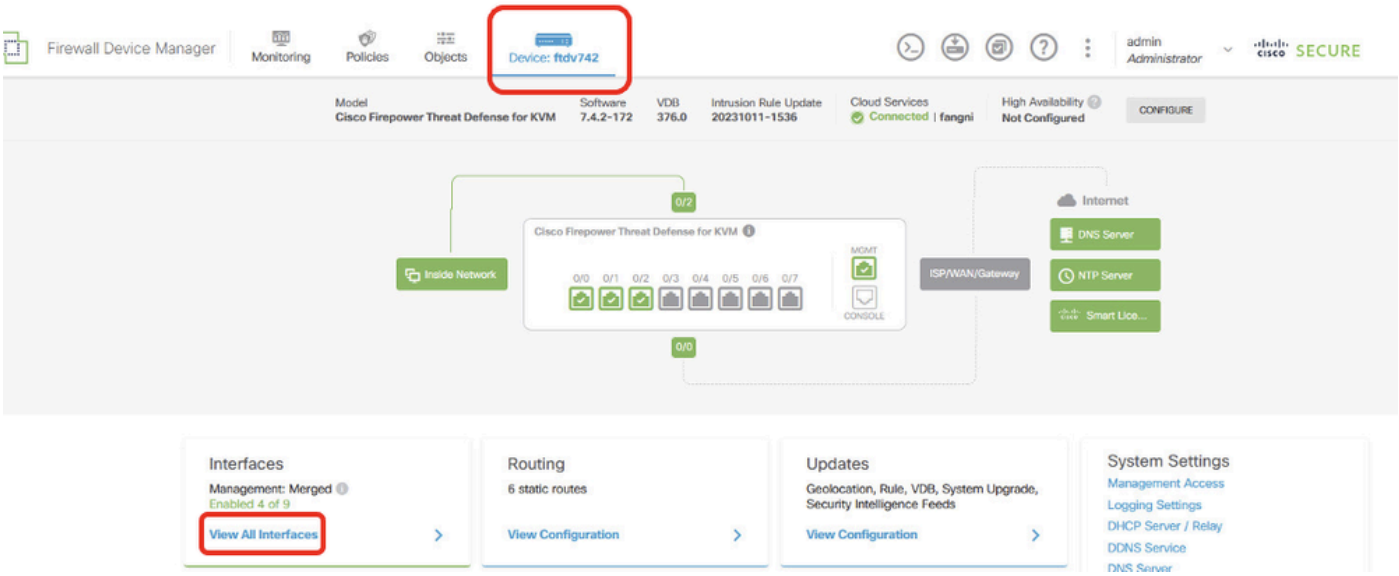
Topologie

VPN-Konfigurationen

Es muss unbedingt sichergestellt werden, dass die vorläufige Konfiguration der IP-Interkonnektivität zwischen den Knoten ordnungsgemäß abgeschlossen wurde. Die Clients an Standort 1 und 2 verfügen über eine FTD innerhalb der IP-Adresse als Gateway.

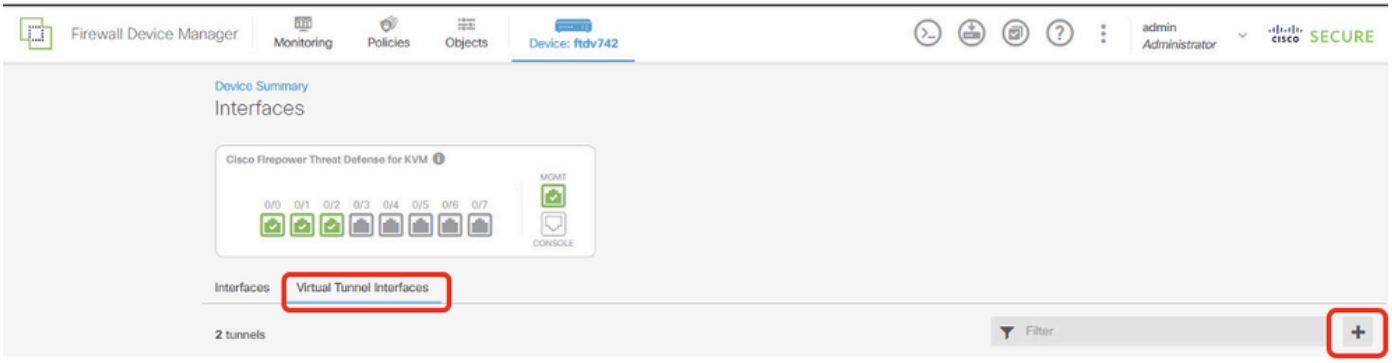
FTD-VPN-Konfiguration für Standort 1

Schritt 1: Erstellen Sie virtuelle Tunnelschnittstellen für ISP1 und ISP2. Melden Sie sich in der FDM-GUI von Site1 FTD an. Navigieren Sie zu Gerät > Schnittstellen. Klicken Sie auf Alle Schnittstellen anzeigen.



Site1FTD_View_All_Interfaces

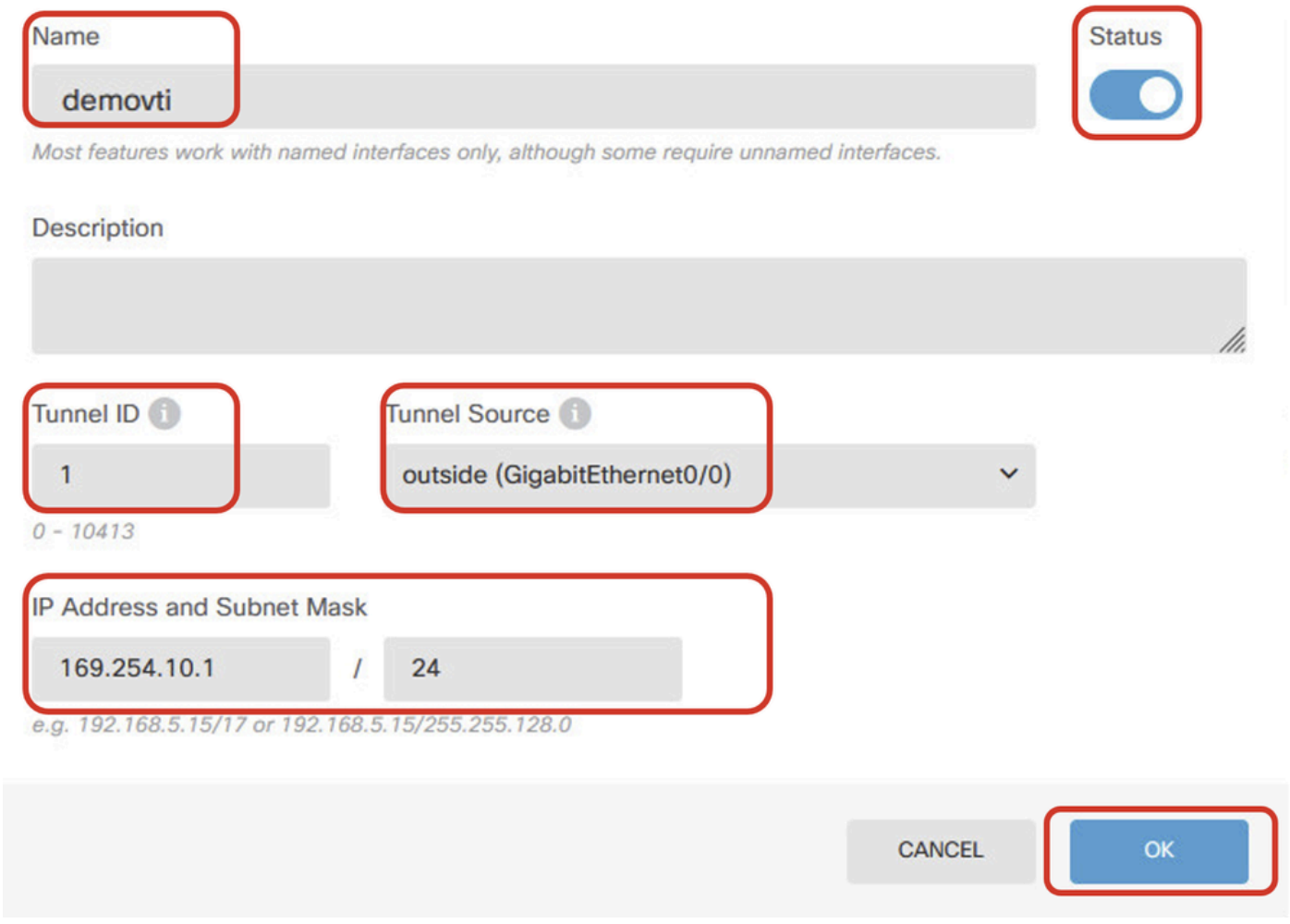
Schritt 2: Klicken Sie auf Virtual Tunnel Interfaces (Virtuelle Tunnelschnittstellen) und dann auf die +-Schaltfläche.



Site1FTD_Create_VTI

Schritt 3: Stellen Sie die erforderlichen Informationen zum VTI bereit. Klicken Sie auf OK.

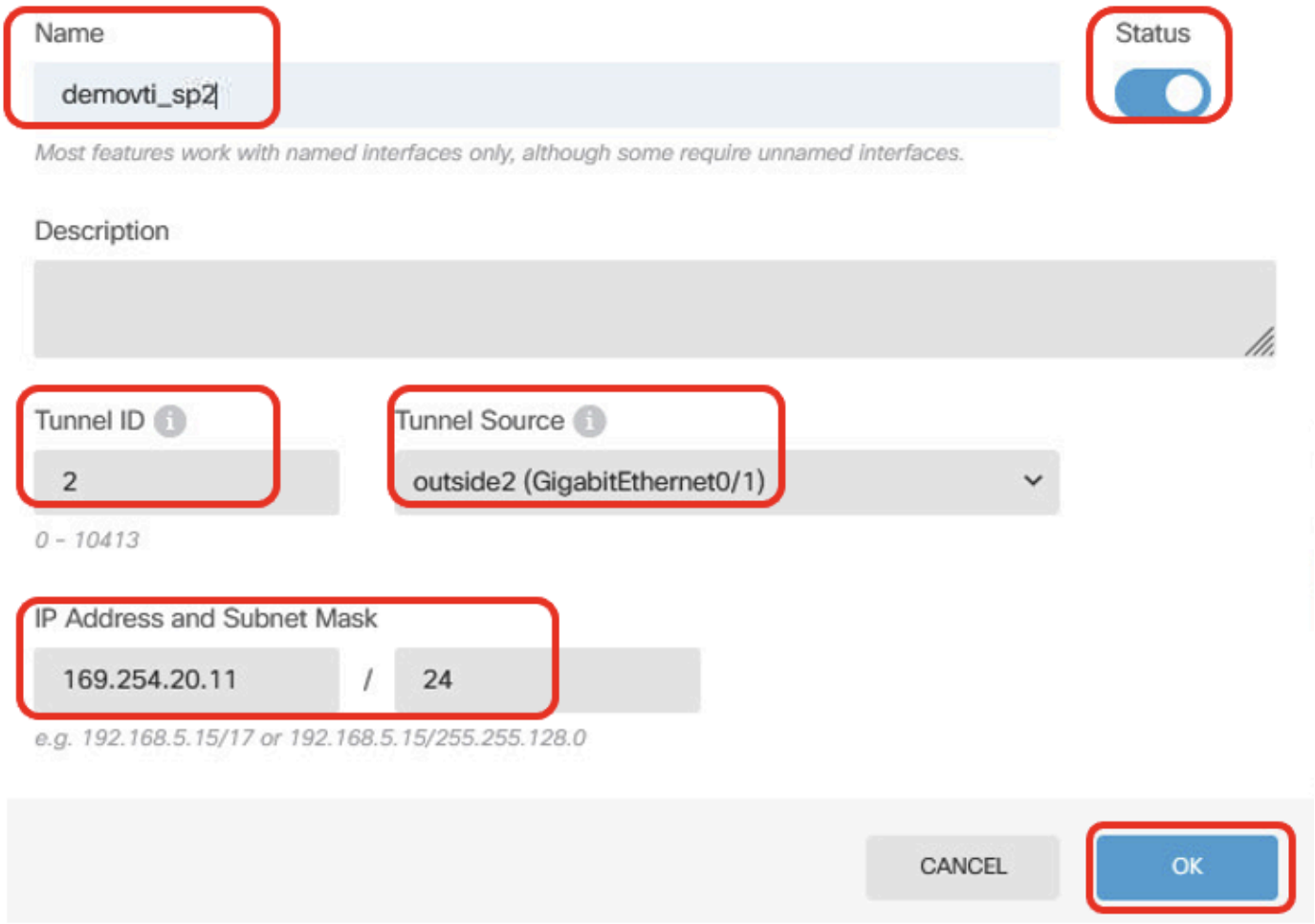
- Name: demovti
- Tunnel-ID: 1
- Tunnelquelle: Extern (GigabitEthernet0/0)
- IP-Adresse und Subnetzmaske: 169.254.10.1/24
- Status: Klicken Sie auf den Schieberegler für die Position Aktiviert.



Standort1FTD_VTI_Details_Tunnel1_ISP1

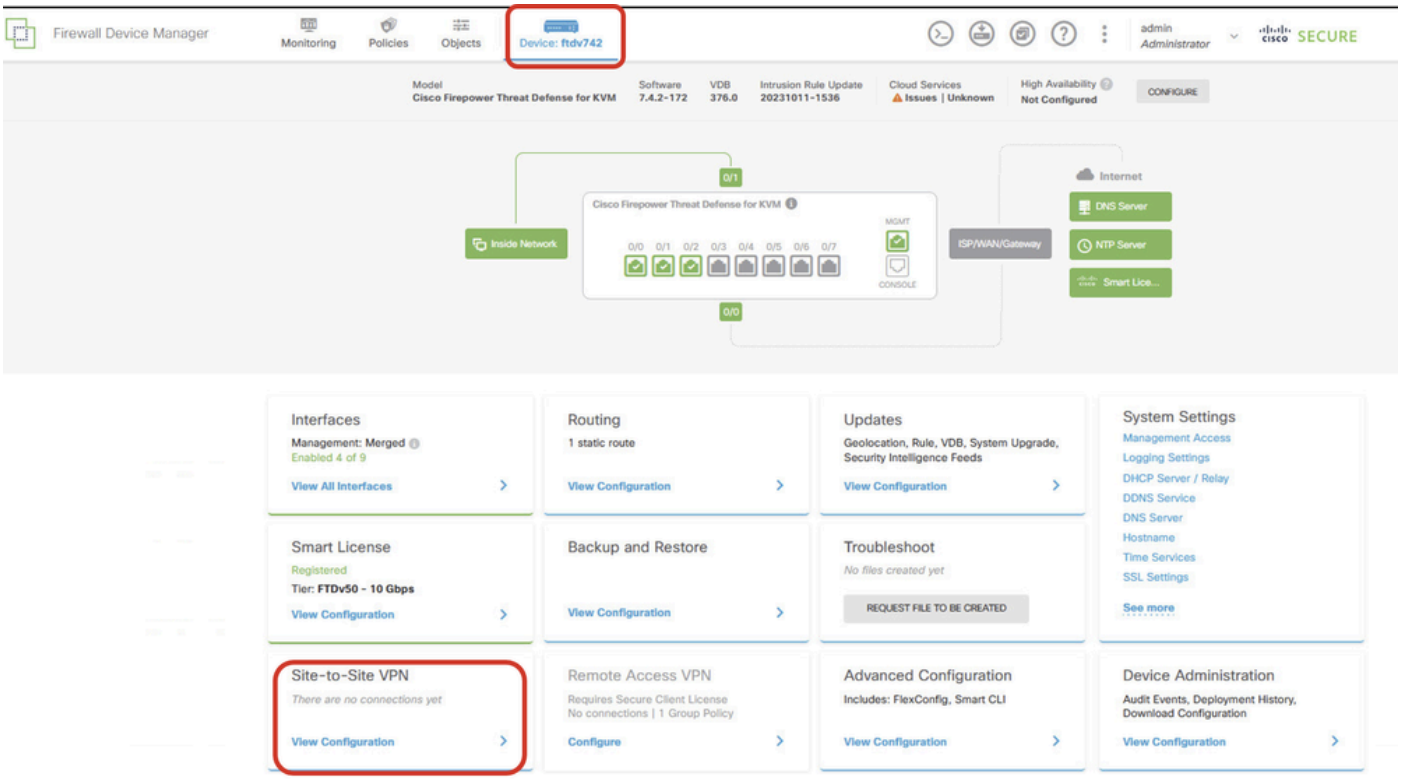
- Name: demovti_sp2
- Tunnel-ID: 2

- Tunnelquelle: outside2 (GigabitEthernet0/1)
- IP-Adresse und Subnetzmaske: 169.254.20.11/24
- Status: Klicken Sie auf den Schieberegler für die Position Aktiviert.



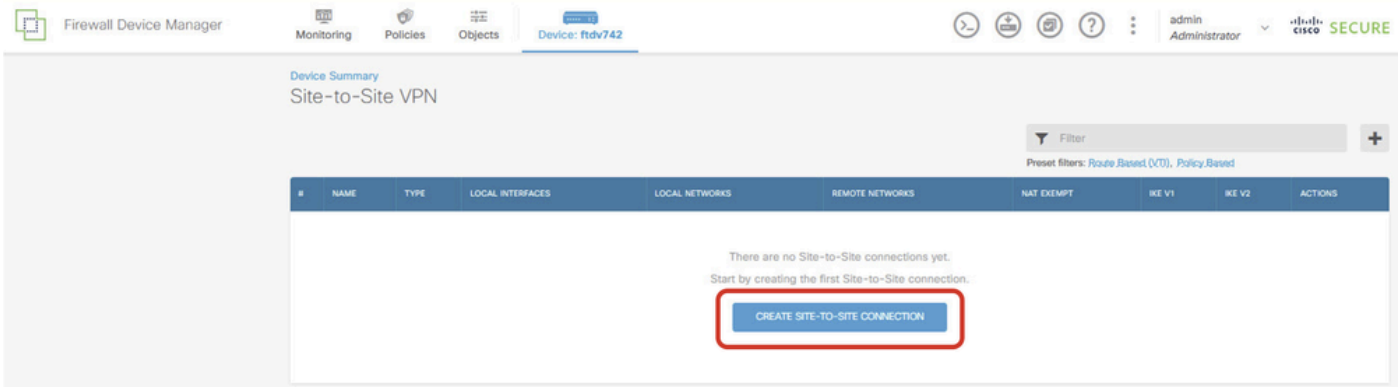
Standort1FTD_VTI_Details_Tunnel2_ISP2

Schritt 4: Navigieren Sie zu Device > Site-to-Site VPN (Gerät > Site-to-Site-VPN). Klicken Sie auf die Schaltfläche Konfiguration anzeigen.



Site1FTD_View_Site2Site_VPN

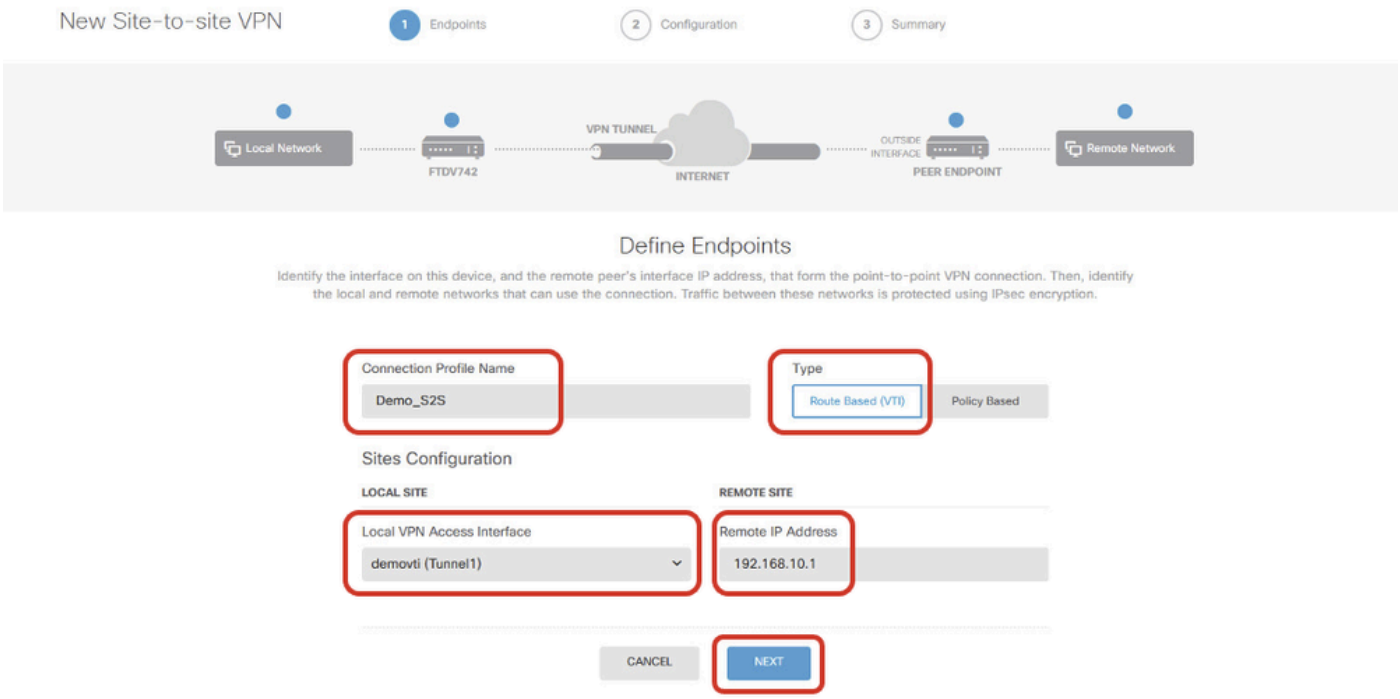
Schritt 5. Starten Sie mit dem Erstellen eines neuen Site-to-Site-VPN über ISP1. Klicken Sie auf SITE-TO-SITE-VERBINDUNG ERSTELLEN, oder klicken Sie auf die + Schaltfläche.



Site1FTD_Create_Site-to-Site_Connection

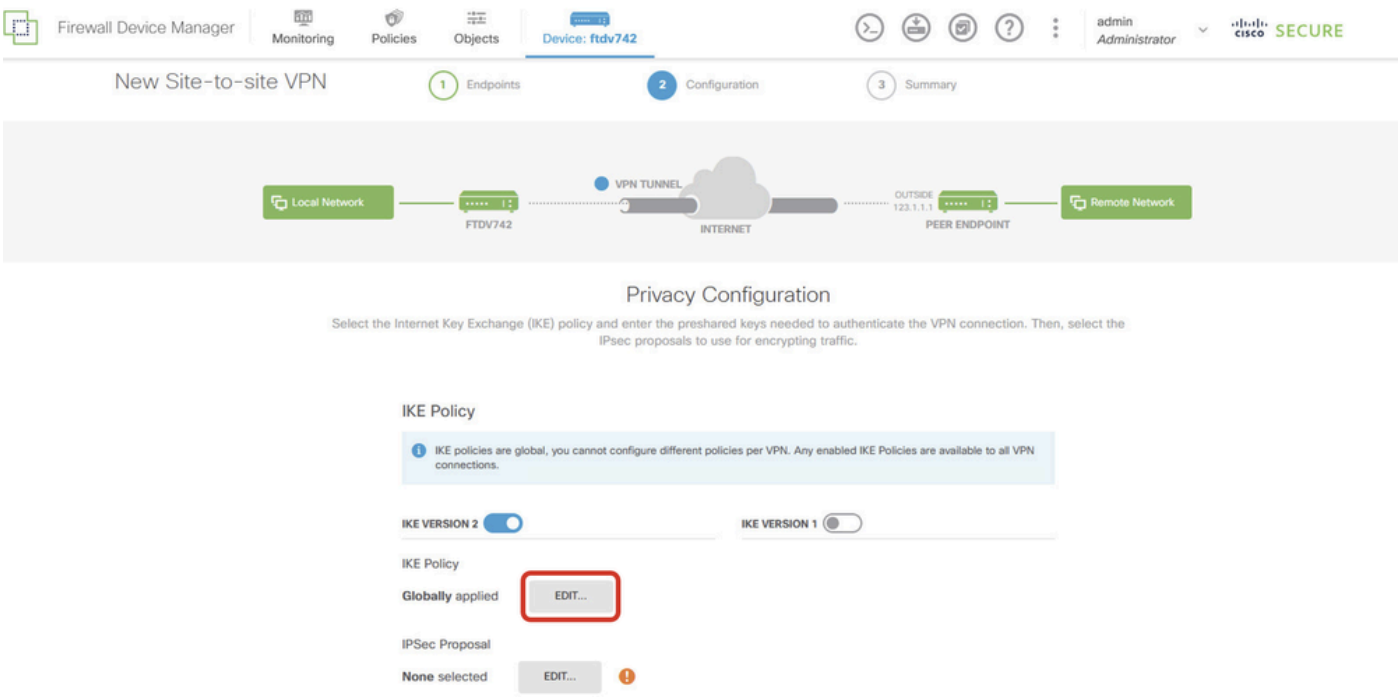
Schritt 5.1: Bereitstellen der erforderlichen Informationen zu Endpunkten Klicken Sie auf die Schaltfläche Weiter.

- Verbindungsprofilname: Demo S2S
- Typ: Routenbasiert (VTI)
- Local VPN Access Interface (Lokale VPN-Zugriffsschnittstelle): demovti (erstellt in Schritt 3)
- Remote-IP-Adresse: 192.168.10.1 (dies ist die IP-Adresse von Site2 FTD ISP1)



Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

Schritt 5.2: Navigieren Sie zur IKE-Richtlinie. Klicken Sie auf die Schaltfläche BEARBEITEN.

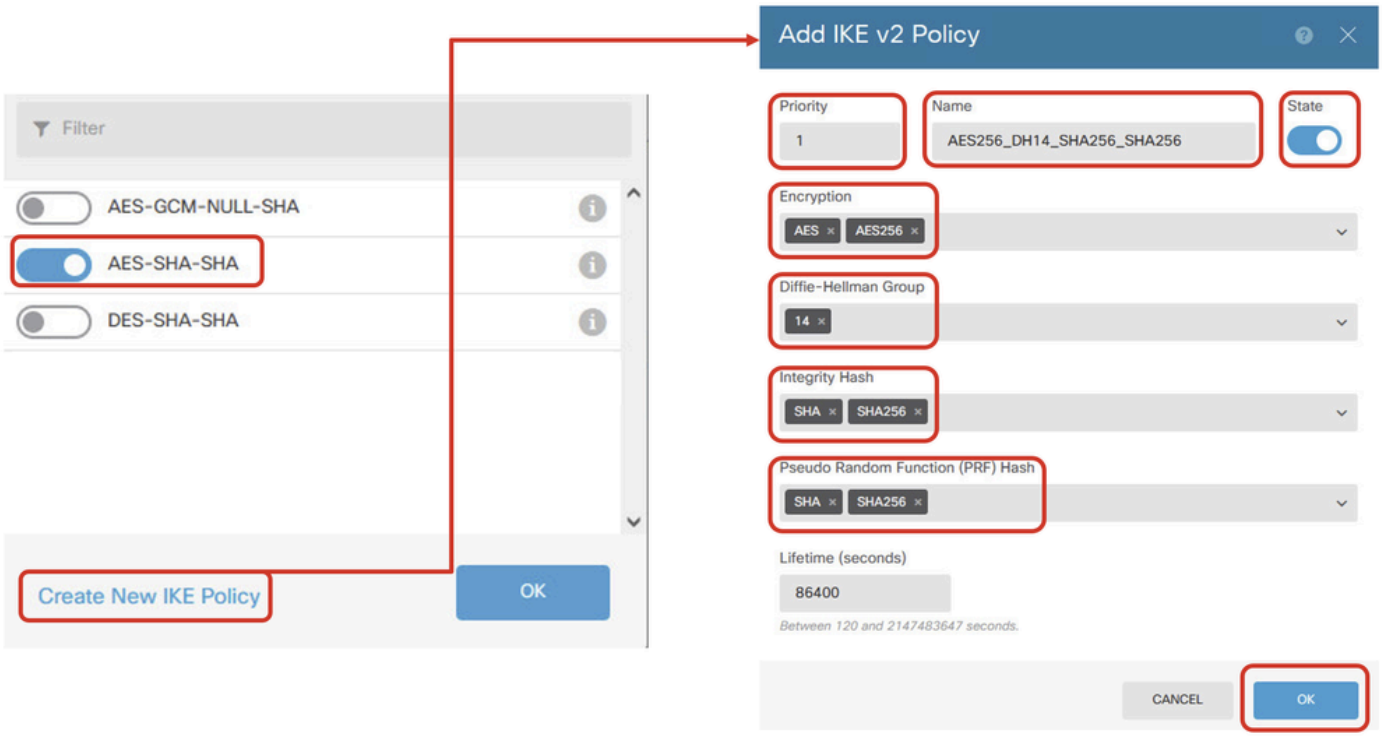


Site1FTD_Edit_IKE_Policy

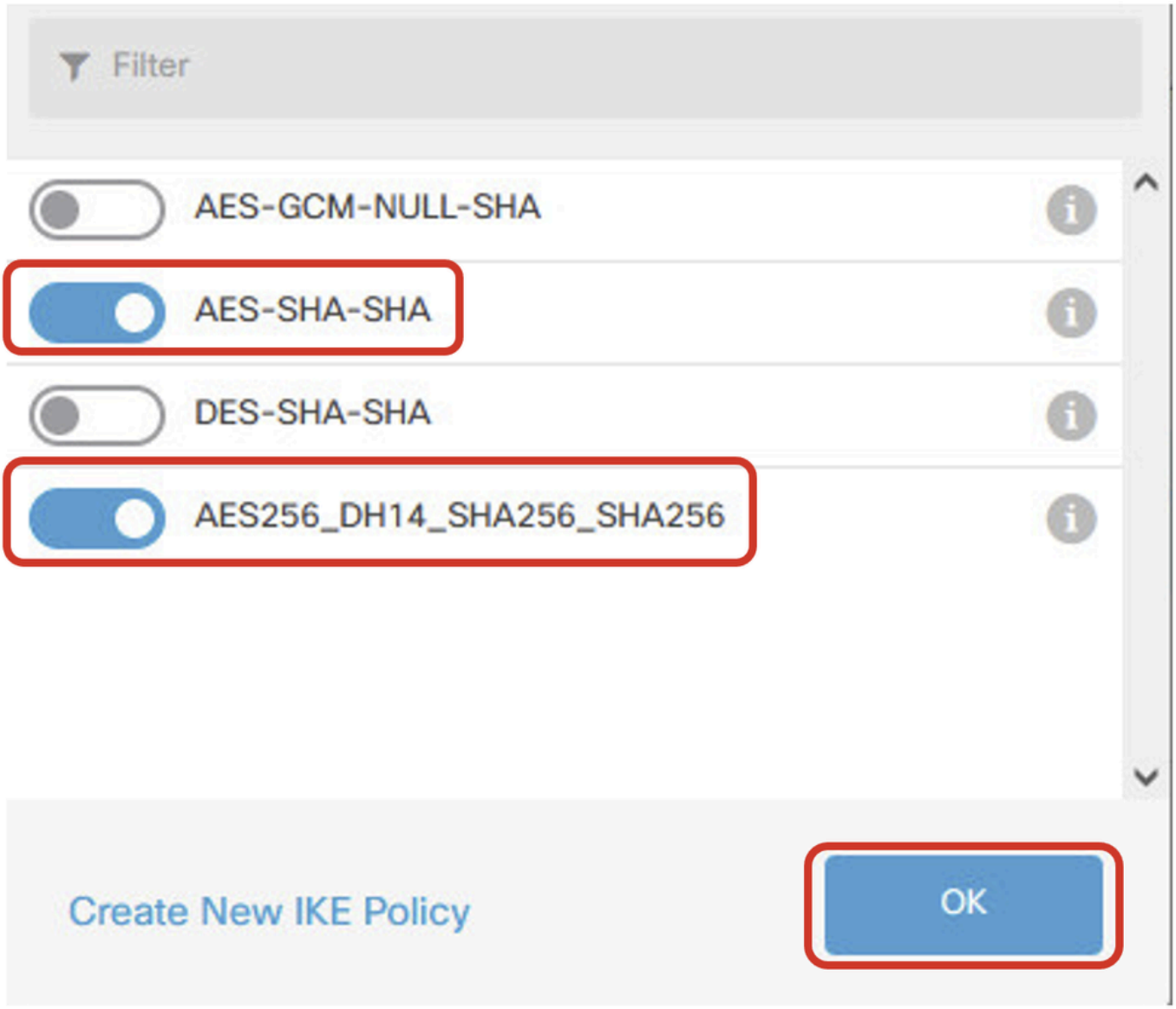
Schritt 5.3: Für die IKE-Richtlinie können Sie eine vordefinierte Richtlinie verwenden oder eine neue erstellen, indem Sie auf "Neue IKE-Richtlinie erstellen" klicken.

Schalten Sie in diesem Beispiel eine vorhandene IKE-Richtlinie AES-SHA-SHA um, und erstellen Sie eine neue Richtlinie für Demozwecke. Klicken Sie auf OK, um zu speichern.

- Name: AES256_DH14_SHA256_SHA256
- Verschlüsselung: AES, AES256
- DH-Gruppe: 14
- Integritätshash: SHA, SHA256
- PRF-Hash: SHA, SHA256
- Lebenszeit: 86400 (Standard)

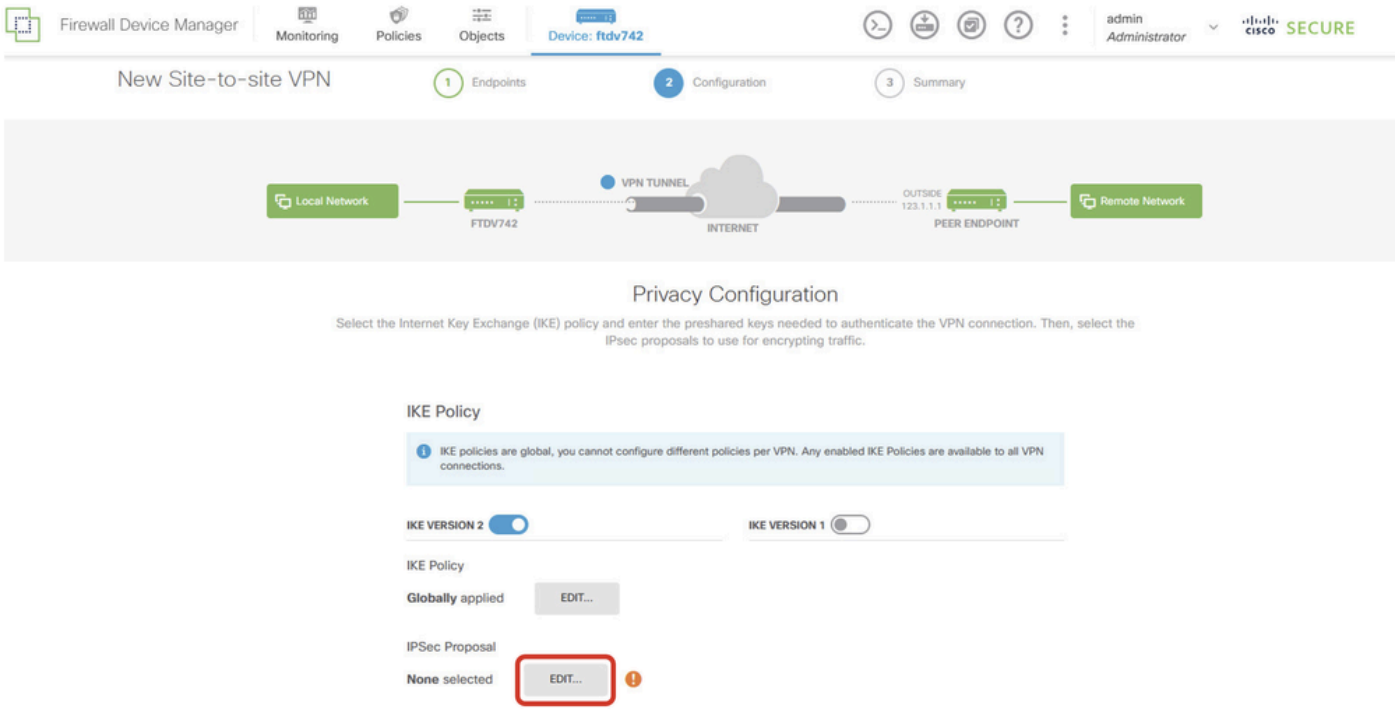


Site1FTD_Add_New_IKE_Policy



Site1FTD_Enable_New_IKE_Policy

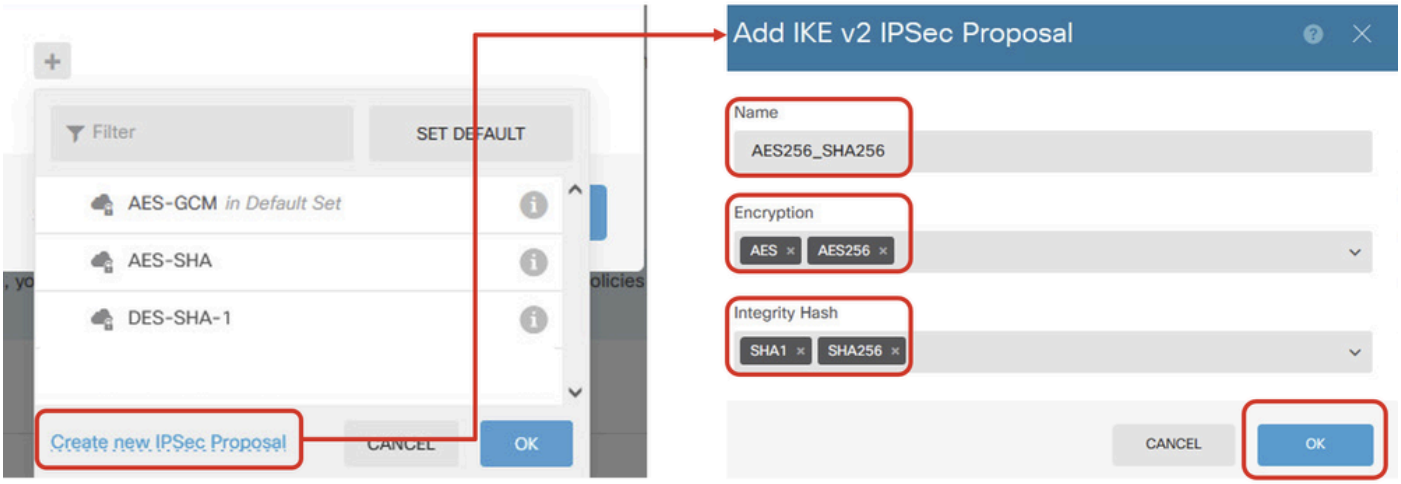
Schritt 5.4: Navigieren Sie zu IPSec-Angebot. Klicken Sie auf die Schaltfläche BEARBEITEN.



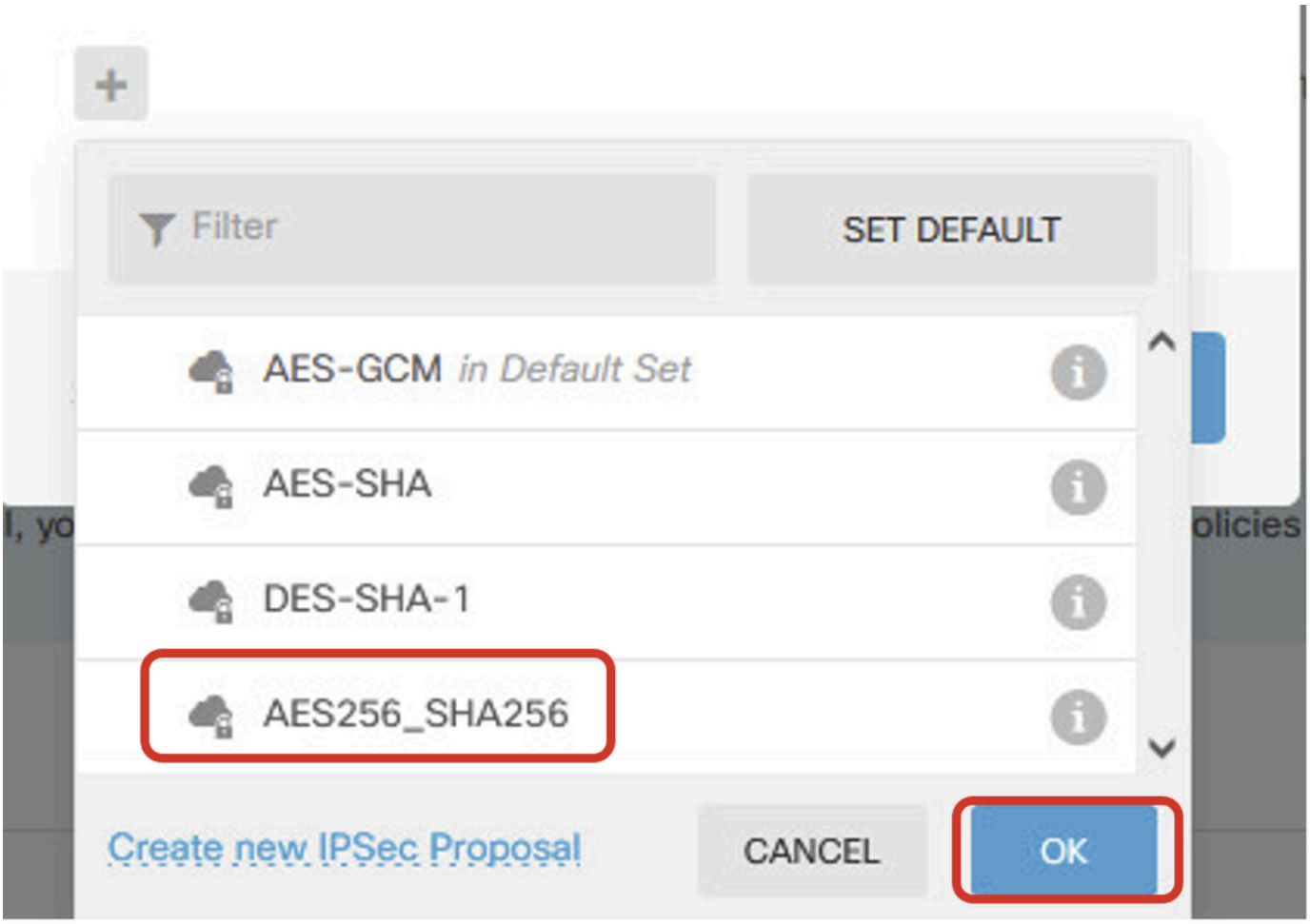
Site1FTD_Edit_IKE_Proposal

Schritt 5.5. Für ein IPSec-Angebot können Sie das vordefinierte verwenden oder ein neues erstellen, indem Sie auf Neues IPSec-Angebot erstellen klicken. In diesem Beispiel erstellen Sie eine neue Version für Demozwecke. Klicken Sie auf OK, um zu speichern.

- Name: AES 256 SHA 256
- Verschlüsselung: AES, AES256
- Integritätshash: SHA1, SHA256



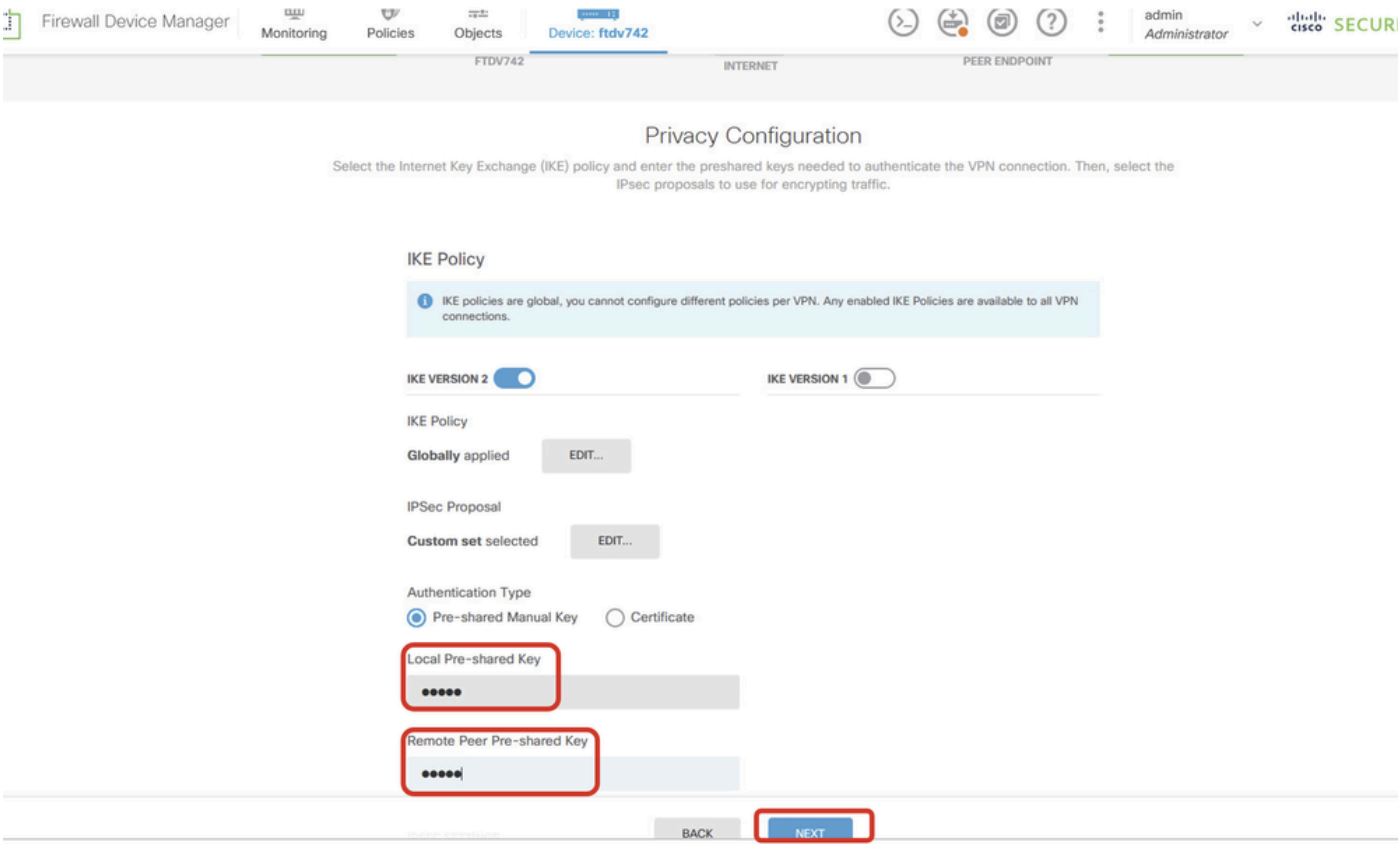
Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

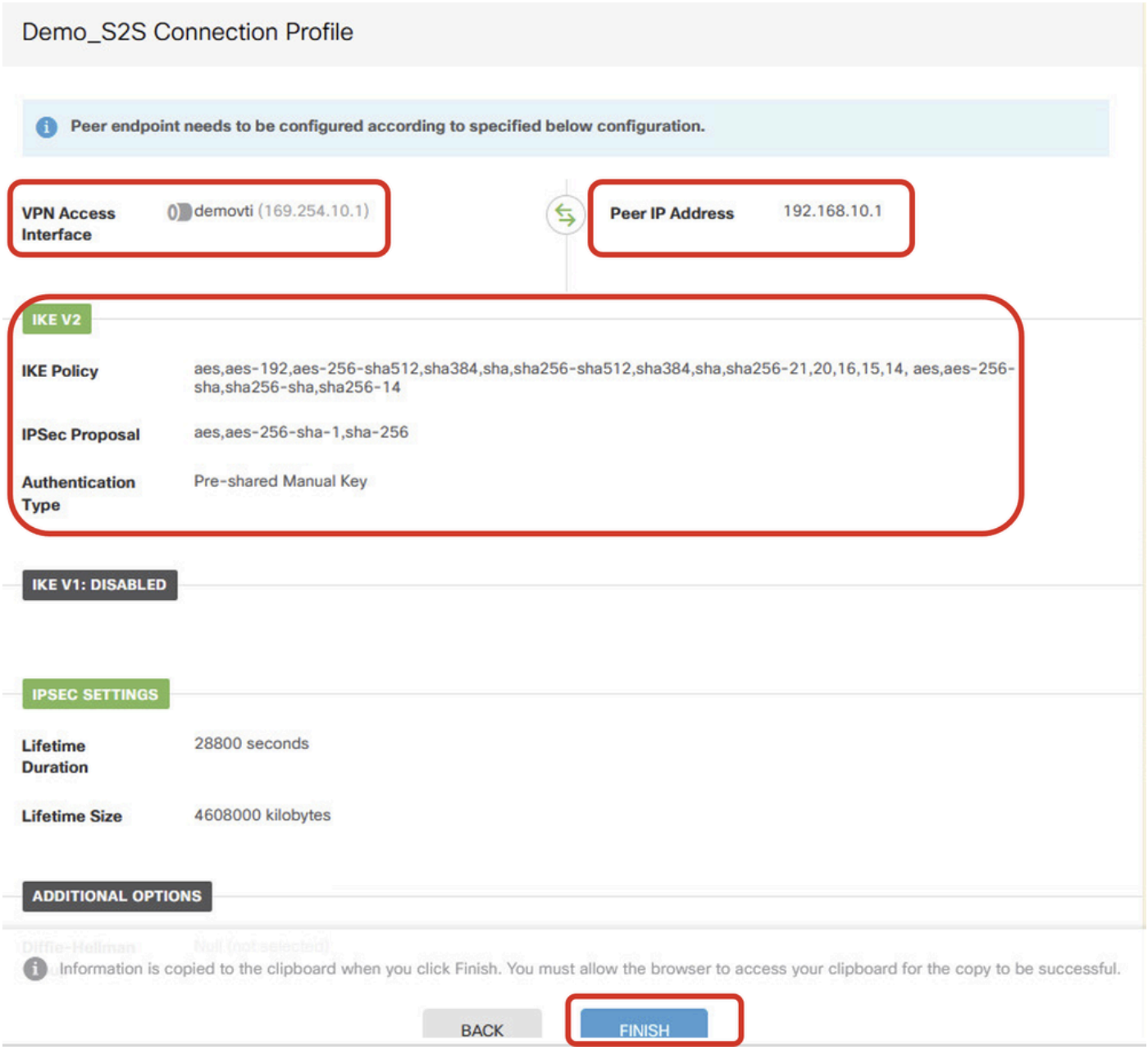
Schritt 5.6: Blättern Sie auf der Seite nach unten, und konfigurieren Sie den vorinstallierten Schlüssel. Klicken Sie auf die Schaltfläche NEXT.

Notieren Sie sich diesen vorinstallierten Schlüssel, und konfigurieren Sie ihn später auf Site2 FTD.



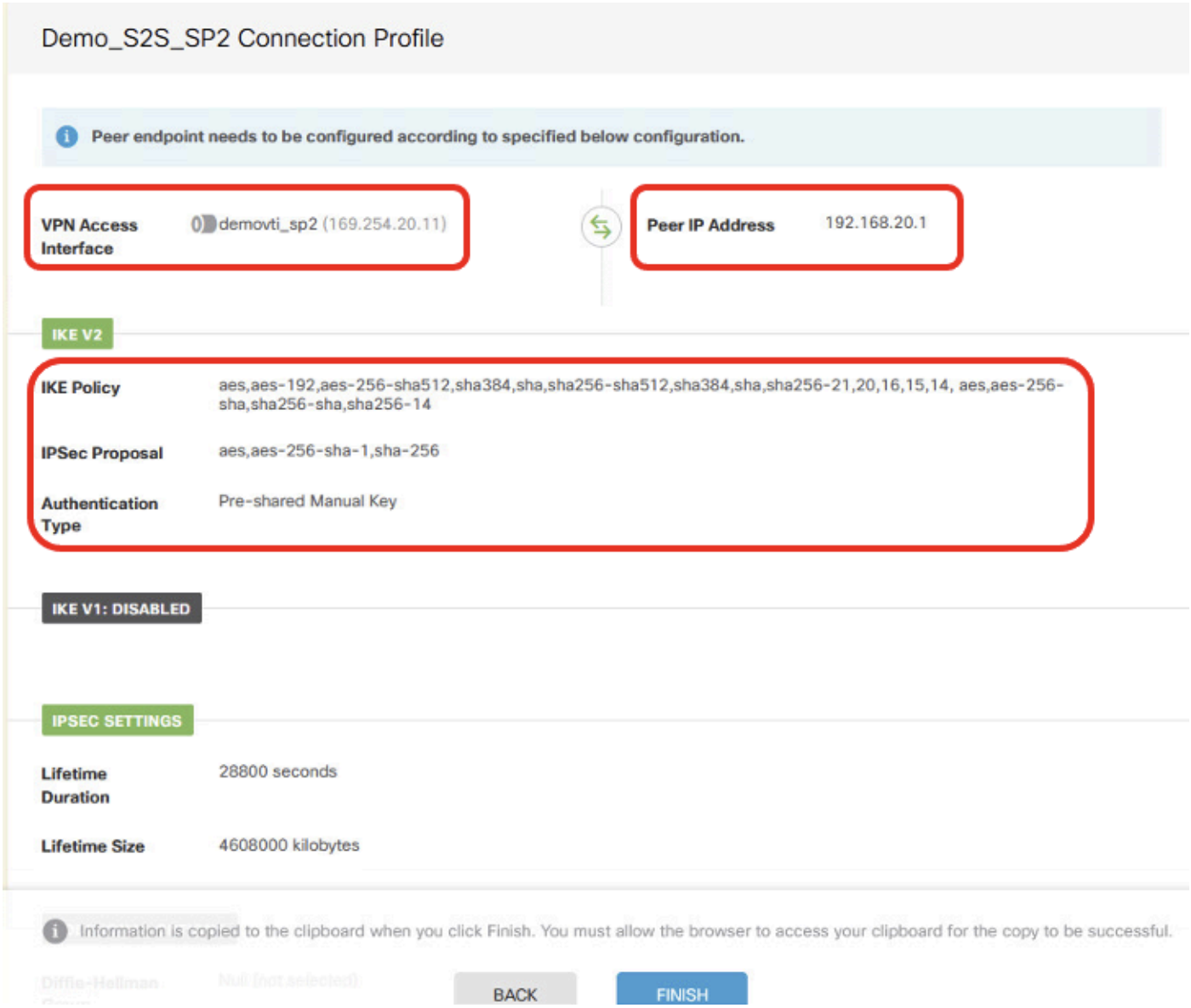
Site1FTD_Configure_Pre_Shared_Key

Schritt 5.7: Überprüfen der VPN-Konfiguration Wenn Sie Änderungen vornehmen möchten, klicken Sie auf die Schaltfläche Zurück. Wenn alles in Ordnung ist, klicken Sie auf die Schaltfläche FERTIG stellen.



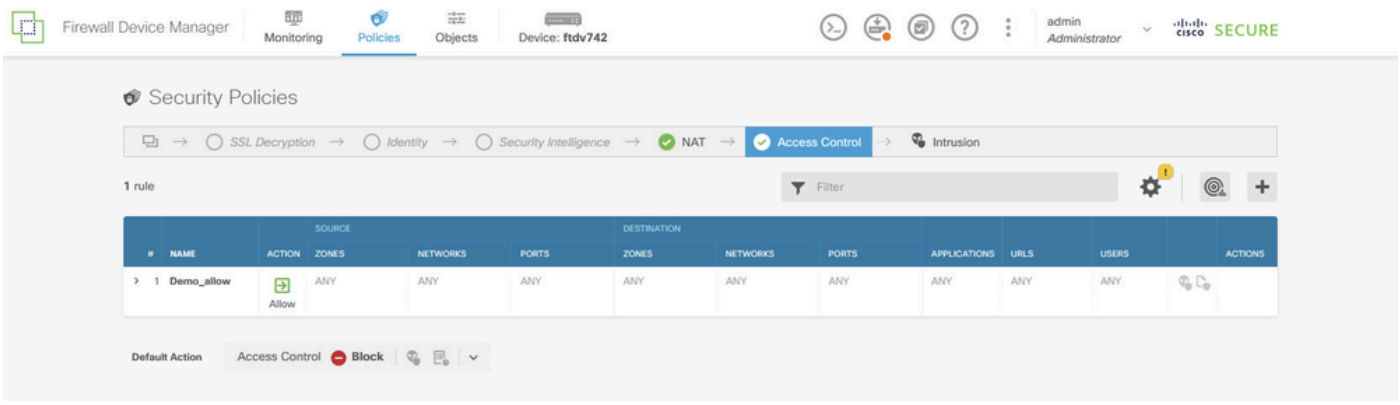
Site1FTD_ISP1_Review_VPN_Config_Summary

Schritt 6: Wiederholen Sie Schritt 5, um über ISP2 ein neues Site-to-Site-VPN zu erstellen.



Site1FTD_ISP2_Review_VPN_Config_Summary

Schritt 7: Erstellen Sie eine Zugriffskontrollregel, um den Datenverkehr durch das FTD passieren zu lassen. In diesem Beispiel alle für Demozwecke zulassen. Ändern Sie Ihre Richtlinie entsprechend Ihren tatsächlichen Anforderungen.



Site1FTD_Allow_Access_Control_Rule_Example

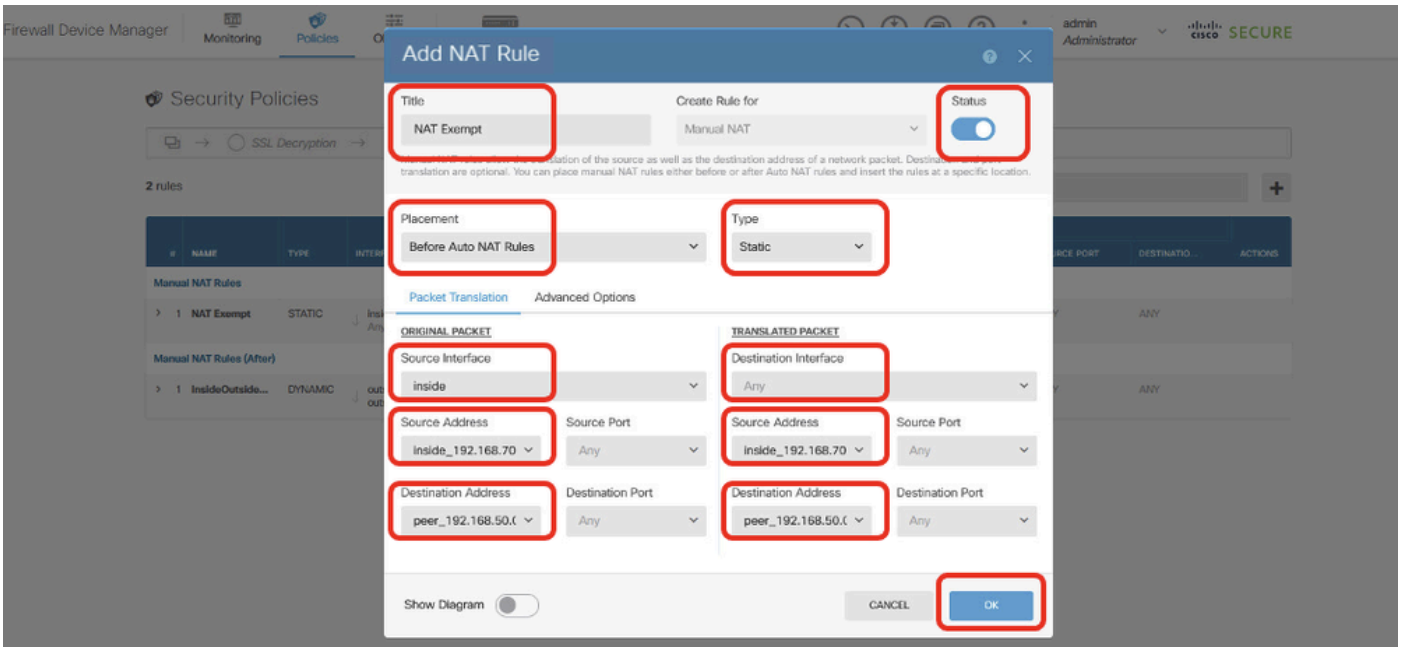
Schritt 8: (Optional) Konfigurieren Sie die NAT-Ausschlussregel für den Client-Datenverkehr auf

FTD, wenn für den Client eine dynamische NAT für den Zugriff auf das Internet konfiguriert wurde.

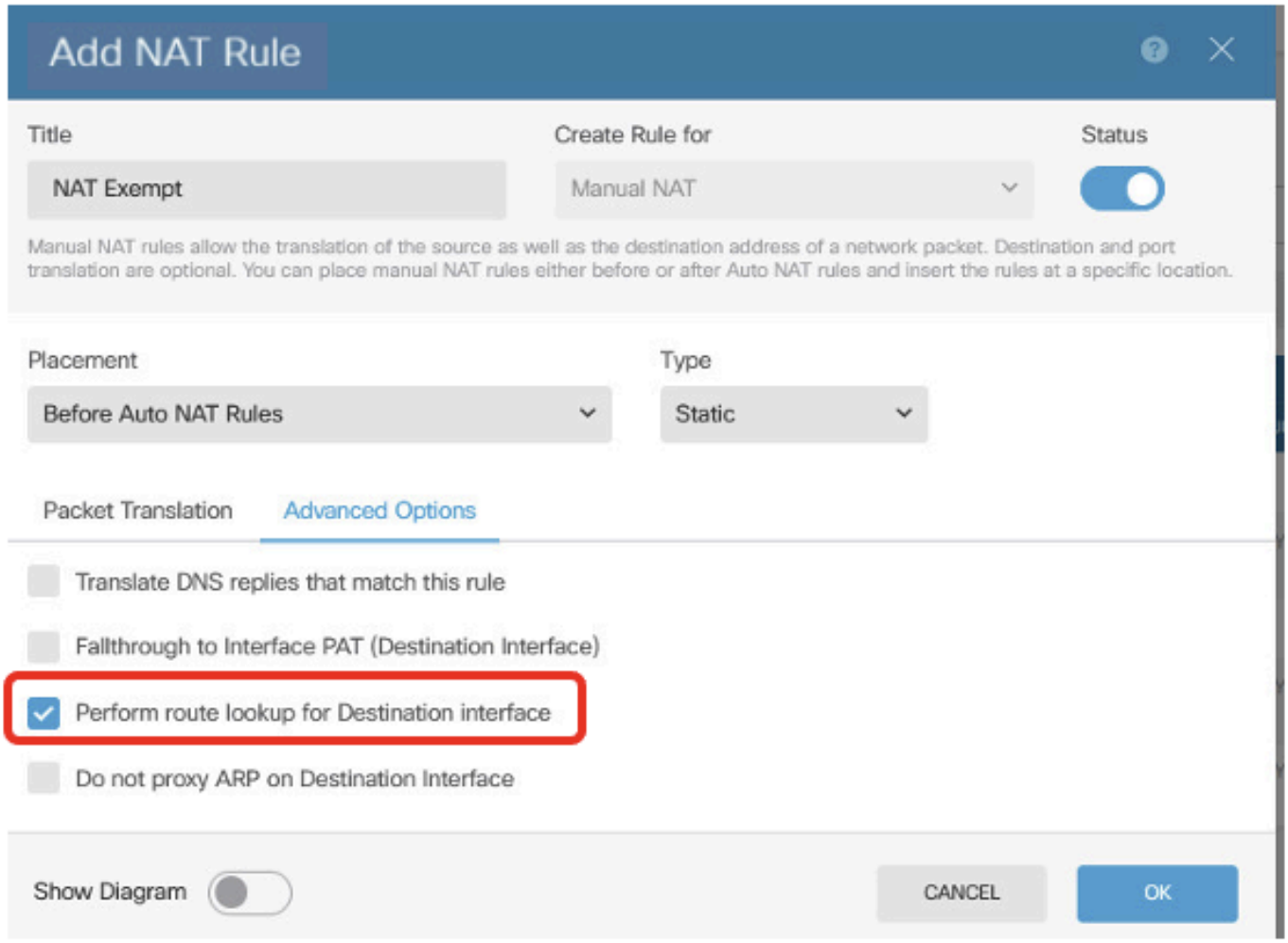
Für Demozwecke wird dynamische NAT für Clients konfiguriert, um in diesem Beispiel auf das Internet zuzugreifen. Daher ist eine NAT-Ausschlussregel erforderlich.

Navigieren Sie zu Richtlinien > NAT. Klicken Sie auf +. Geben Sie die Details an, und klicken Sie auf OK.

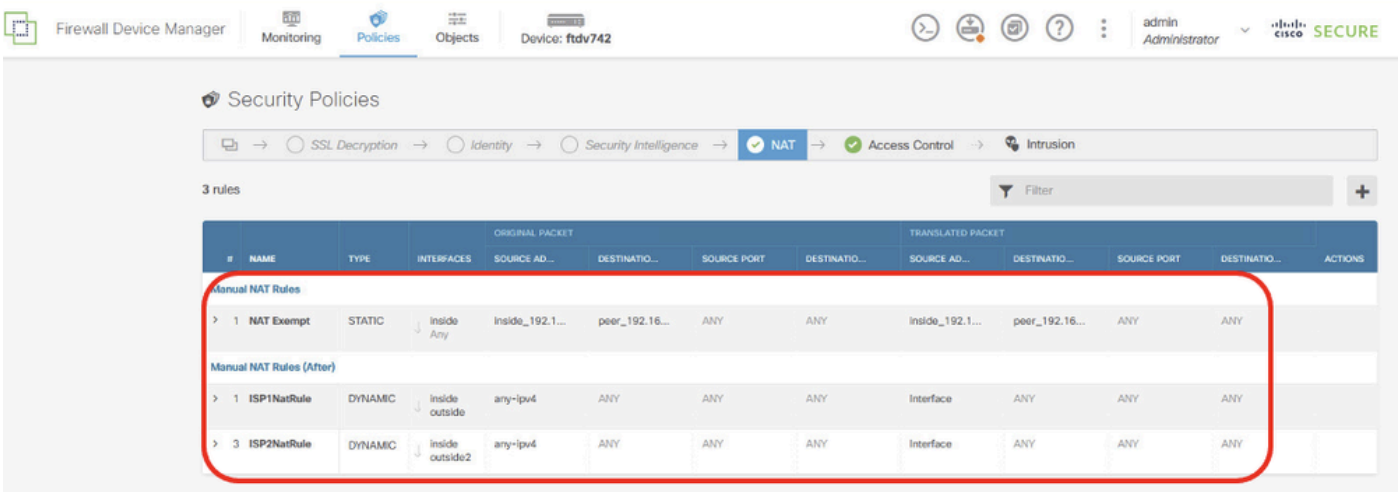
- Title: NAT-Ausnahme
- Anordnung: Vor Auto NAT-Regeln
- Typ: Statisch
- Quellschnittstelle: Intern
- Ziel: Beliebig
- Originalquelladresse: 192.168.70.0/24
- Übersetzte Quelladresse: 192.168.70.0/24
- Originalzieladresse: 192.168.50.0/24
- Übersetzte Zieladresse: 192.168.50.0/24
- Routensuche aktiviert



Site1FTD_NAT_Exempt_Rule



Site1FTD_NAT_Exempt_Rule_2



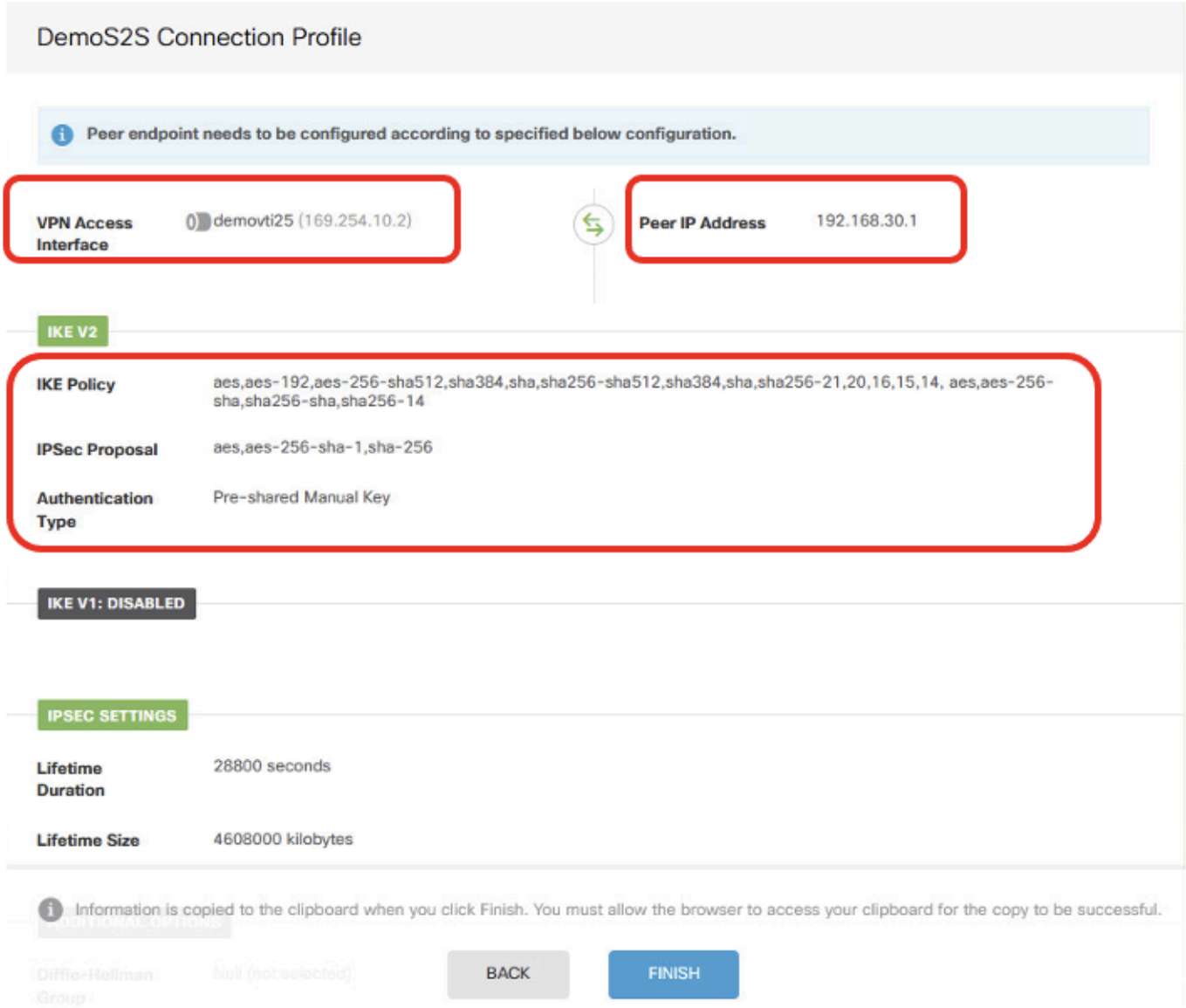
Site1FTD_NAT_Rule_Overview

Schritt 9: Bereitstellen der Konfigurationsänderungen

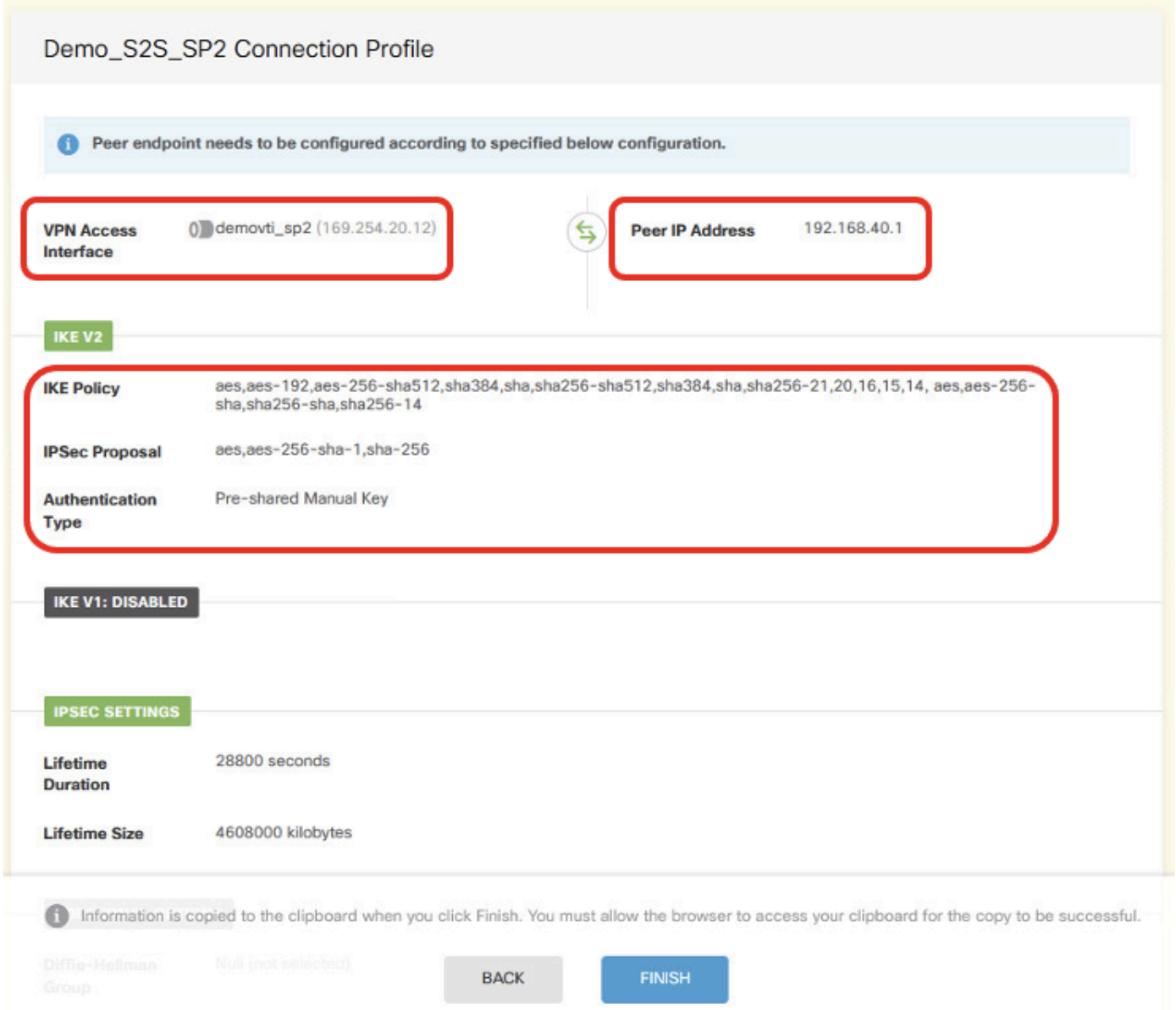
Site1FTD_Deployment_Changes

FTD-VPN-Konfiguration für Standort 2

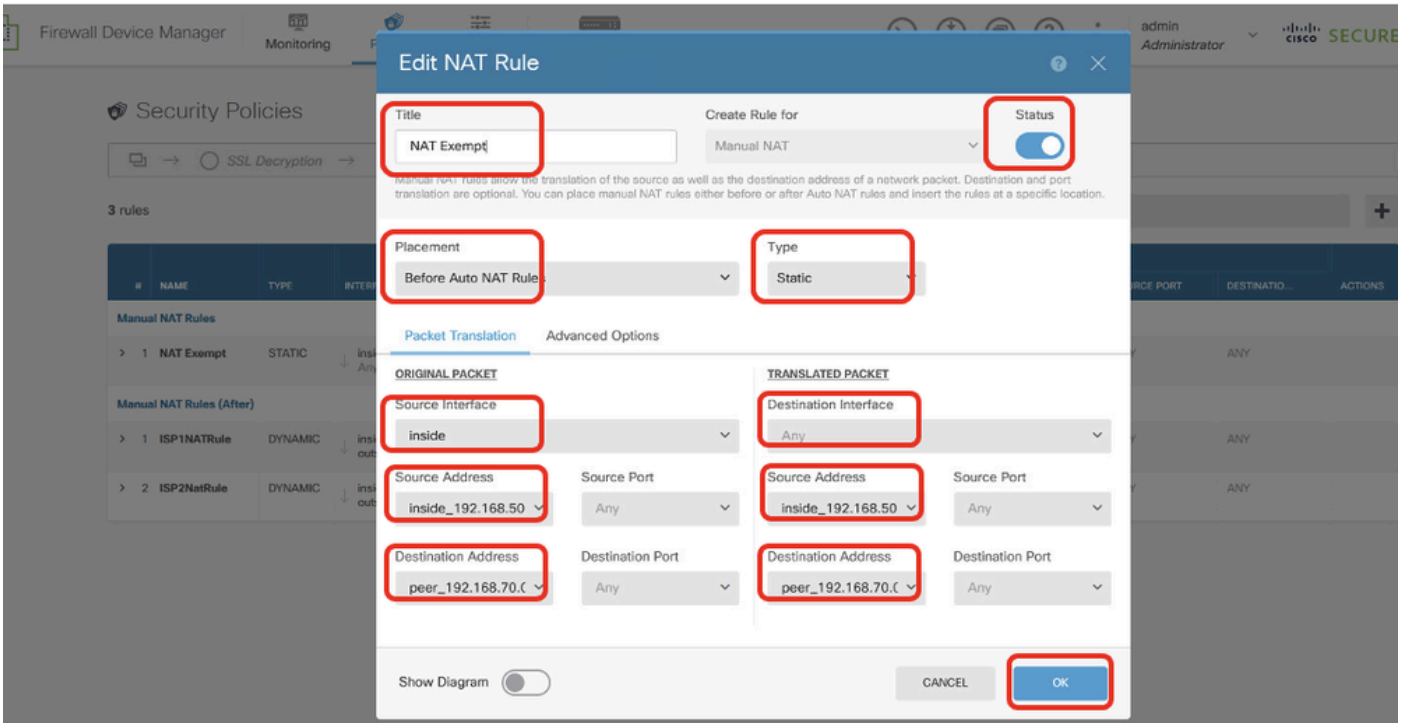
Schritt 10: Wiederholen Sie die Schritte 1 bis 9 mit den entsprechenden Parametern für Site2 FTD.



Site2FTD_ISP1_Review_VPN_Config_Summary



Site2FTD_ISP2_Review_VPN_Config_Summary

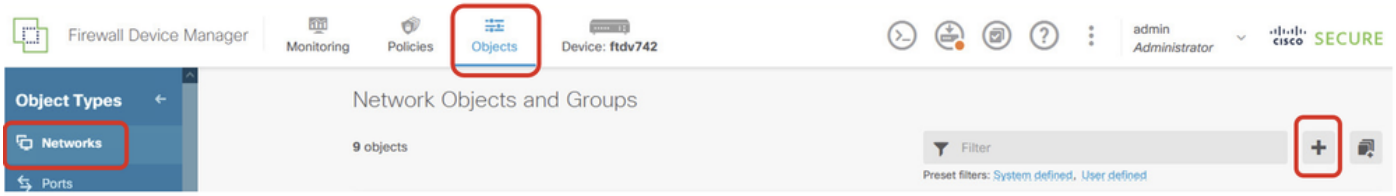


Site2FTD_NAT_Exempt_Rule

Konfigurationen auf PBR

PBR-Konfiguration für Standort 1 FTD

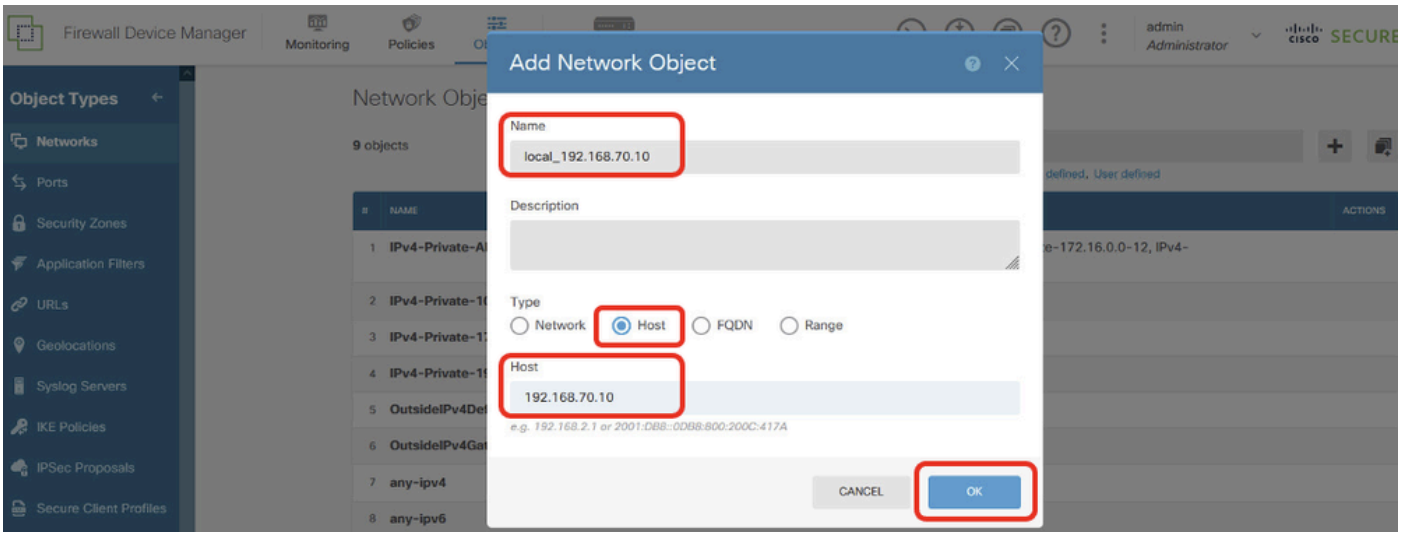
Schritt 11. Erstellen Sie neue Netzwerkobjekte, die von der PBR-Zugriffsliste für Site1 FTD verwendet werden sollen. Navigieren Sie zu Objekte > Netzwerke, und klicken Sie auf +.



Site1FTD_Create_Network_Object

Schritt 11.1: Erstellen Sie das Objekt der IP-Adresse von Site1 Client2. Geben Sie die erforderlichen Informationen an. Klicken Sie auf die Schaltfläche OK.

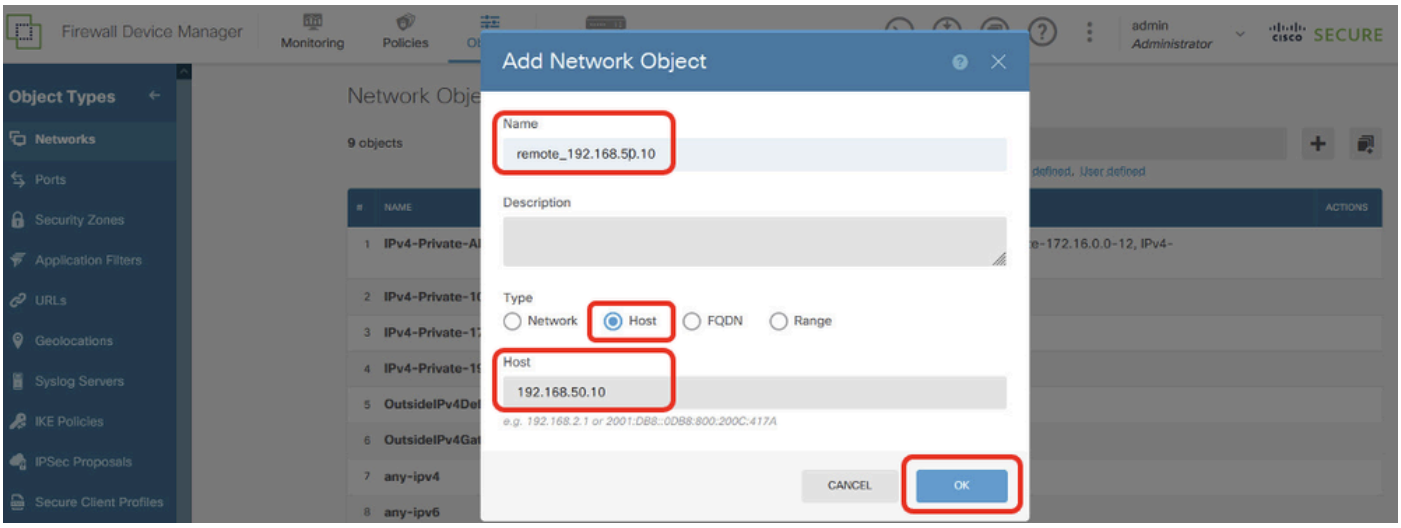
- Name: local_192,168,70,10
- Typ: Host
- Gastgeber: 192.168.70.10



Site1FTD_Site1FTD_PBR_LokalesObjekt

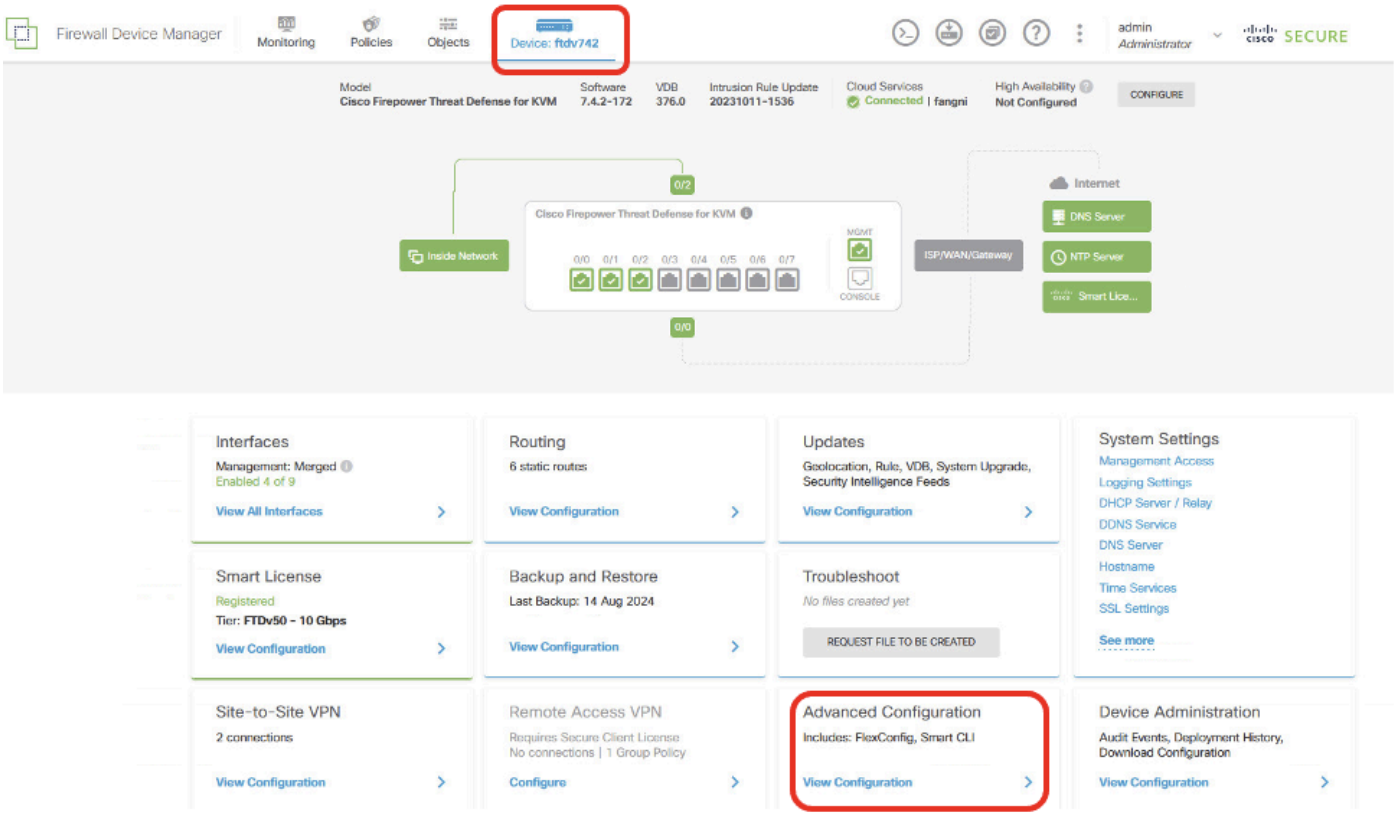
Schritt 11.2. Erstellen Sie das Objekt der IP-Adresse von Site2 Client2. Geben Sie die erforderlichen Informationen an. Klicken Sie auf OK.

- Name: remote_192,168.50,10
- Typ: Host
- Gastgeber: 192.168.50.10



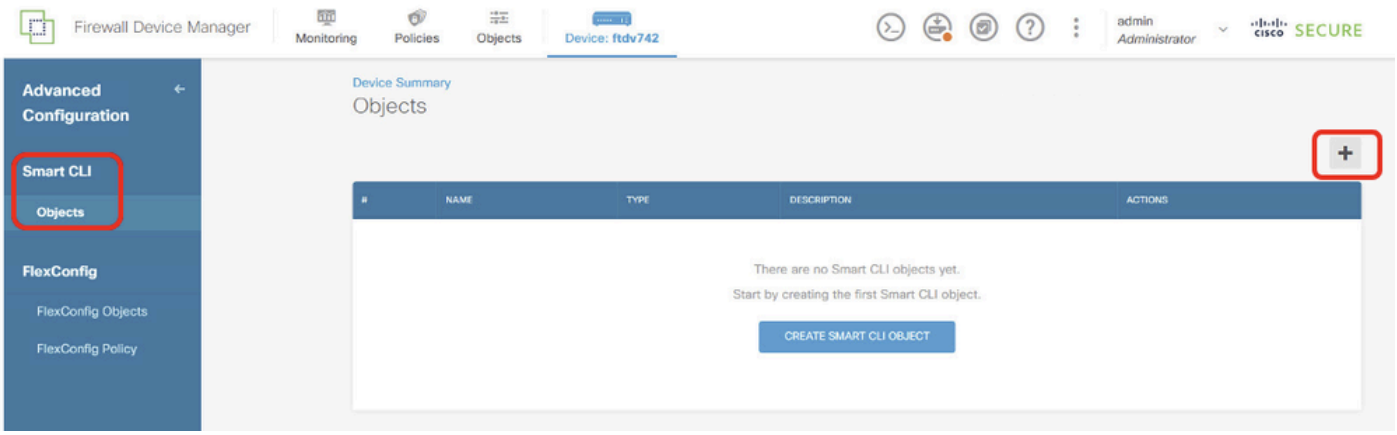
Standort1FTD_PBR_Remote-Objekt

Schritt 12: Erstellen einer erweiterten Zugriffsliste für PBR Navigieren Sie zu Gerät > Erweiterte Konfiguration. Klicken Sie auf Konfiguration anzeigen.



Site1FTD_View_Advanced_Configuration

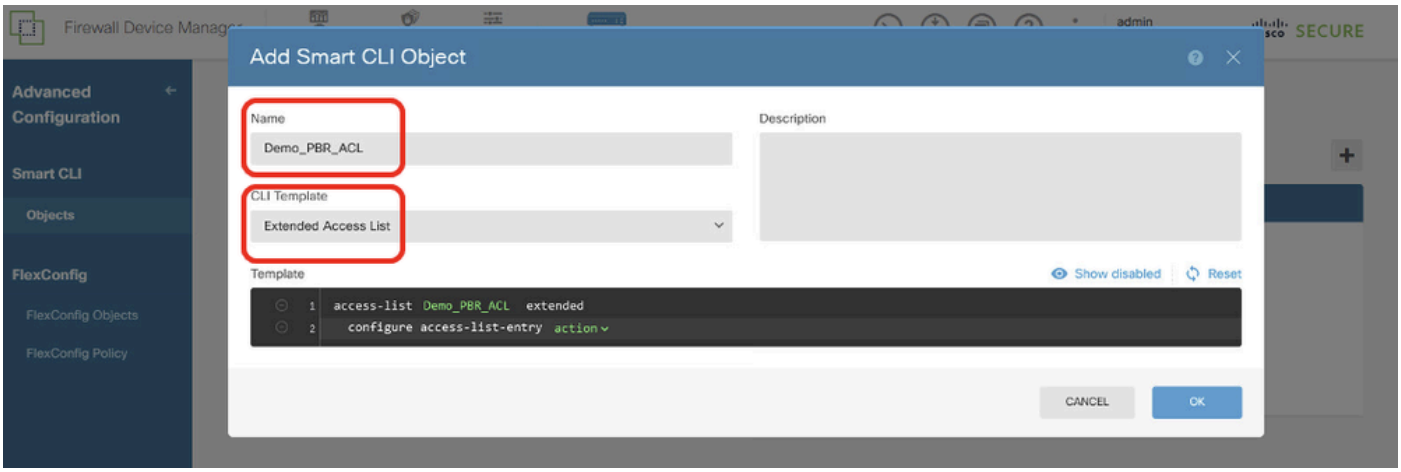
Schritt 12.1. Navigieren Sie zu Smart CLI > Objects. Klicken Sie auf +.



Site1FTD_Add_SmartCLI_Object

Schritt 12.2. Geben Sie einen Namen für das Objekt ein, und wählen Sie die CLI-Vorlage aus.

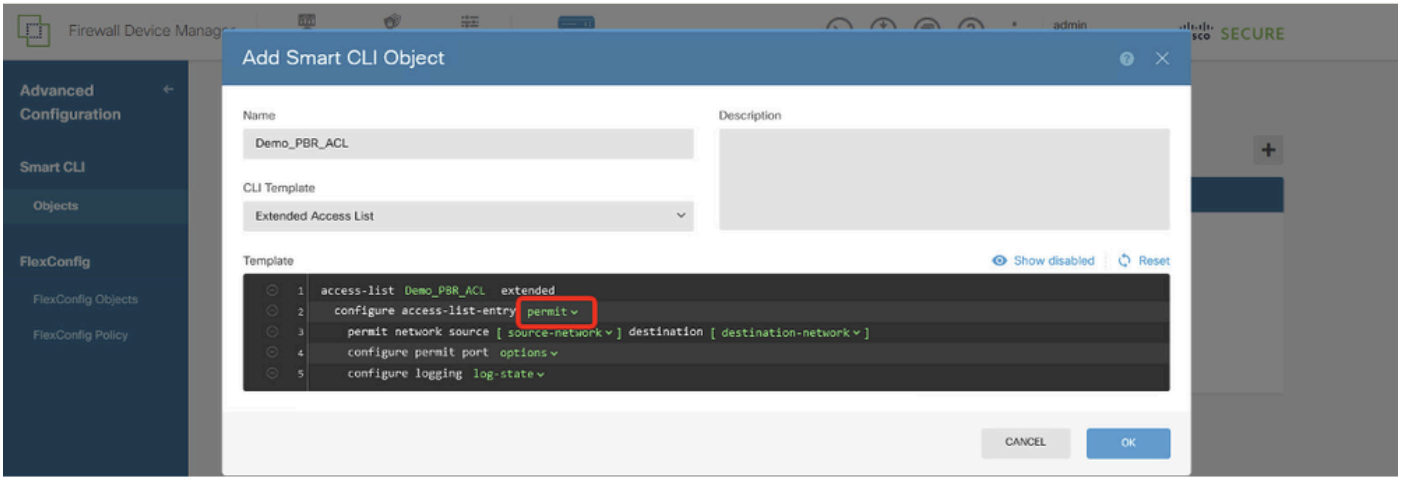
- Name: Demo_PBR_ACL
- CLI-Vorlage: Erweiterte Zugriffsliste



Standort1FTD_Erstellen_PBR_ACL_1

Schritt 12.3: Navigieren Sie zu Vorlage und konfigurieren. Klicken Sie auf die Schaltfläche OK, um zu speichern.

Zeile 2, klicken Sie auf Aktion. Wählen Sie Zulassen.

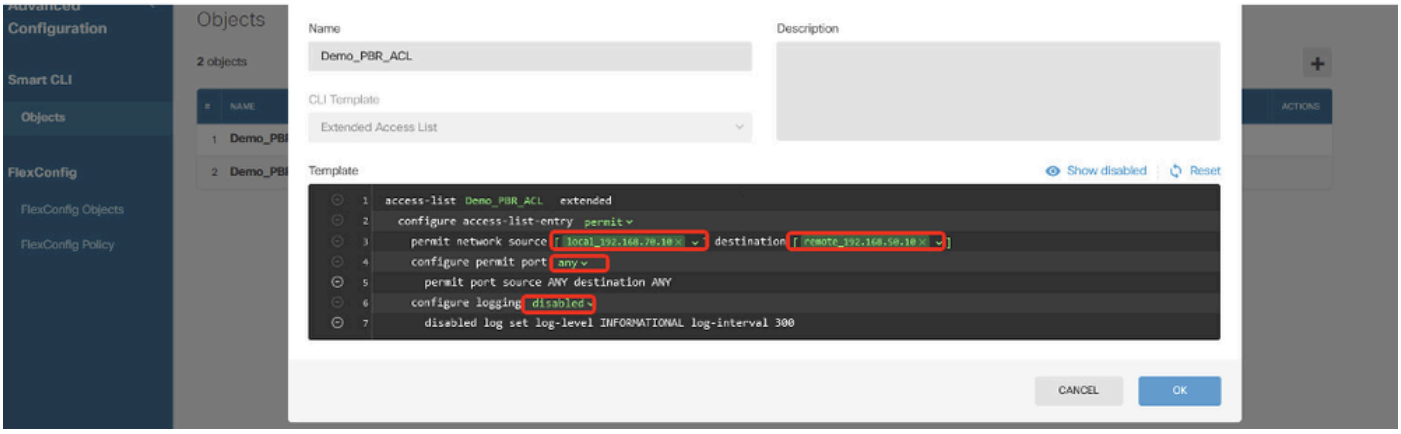


Standort1FTD_Create_PBR_ACL_2

Leitung 3, auf Quellnetzwerk klicken. Wählen Sie local_192.168.70.10 aus. Klicken Sie auf destination-network. Wählen Sie remote_192.168.50.10 aus.

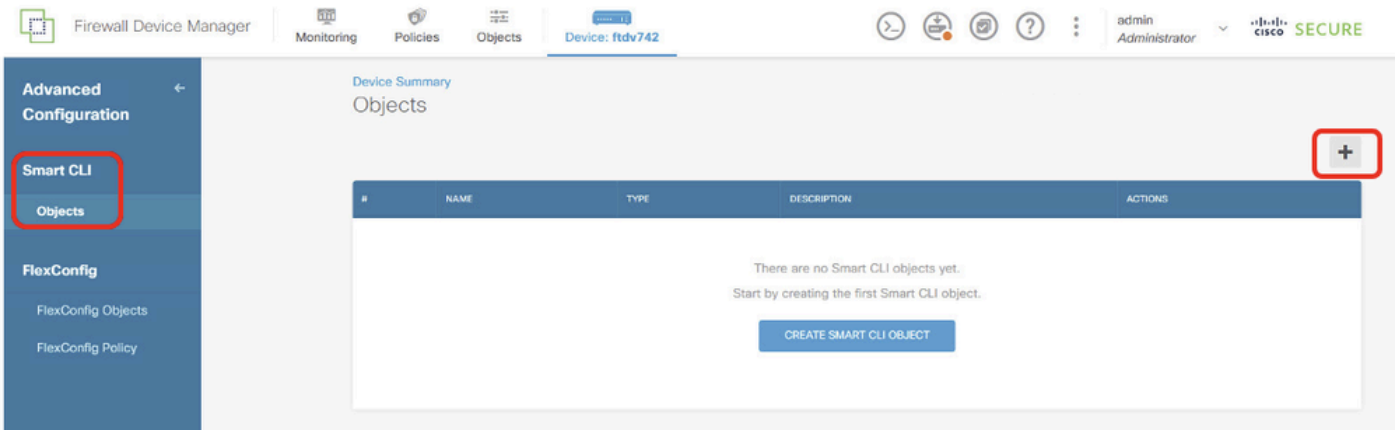
Zeile 4: Klicken Sie auf Optionen, und wählen Sie eine Option aus.

Leitung 6, klicken Sie auf Log-state und wählen Sie disabled (Deaktiviert).



Standort1FTD_Create_PBR_ACL_3

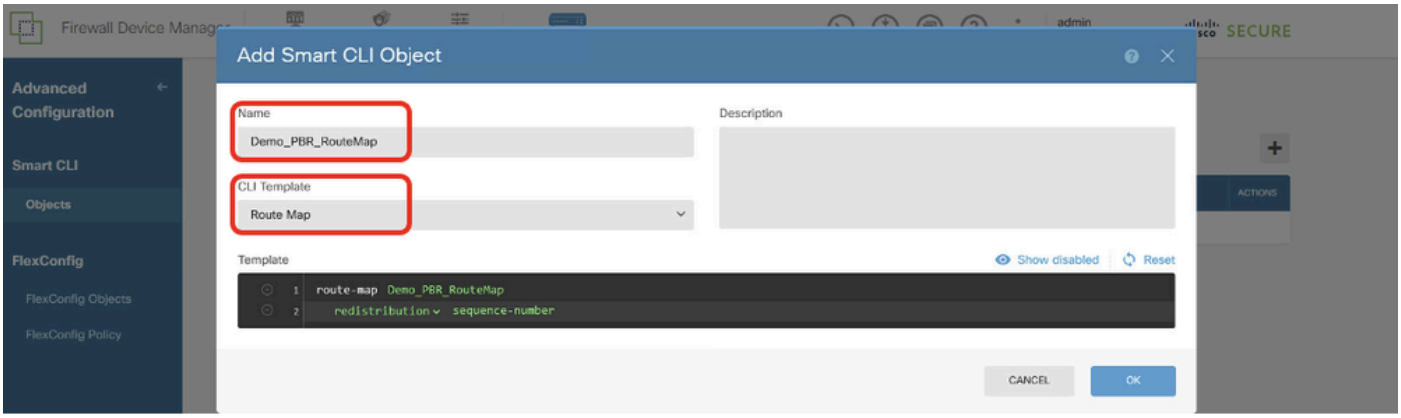
Schritt 13: Erstellen Sie eine Routenübersicht für PBR. Navigieren Sie zu Gerät > Erweiterte Konfiguration > Smart CLI > Objekte. Klicken Sie auf +.



Site1FTD_Add_SmartCLI_Object

Schritt 13.1. Geben Sie einen Namen für das Objekt ein, und wählen Sie die CLI-Vorlage aus.

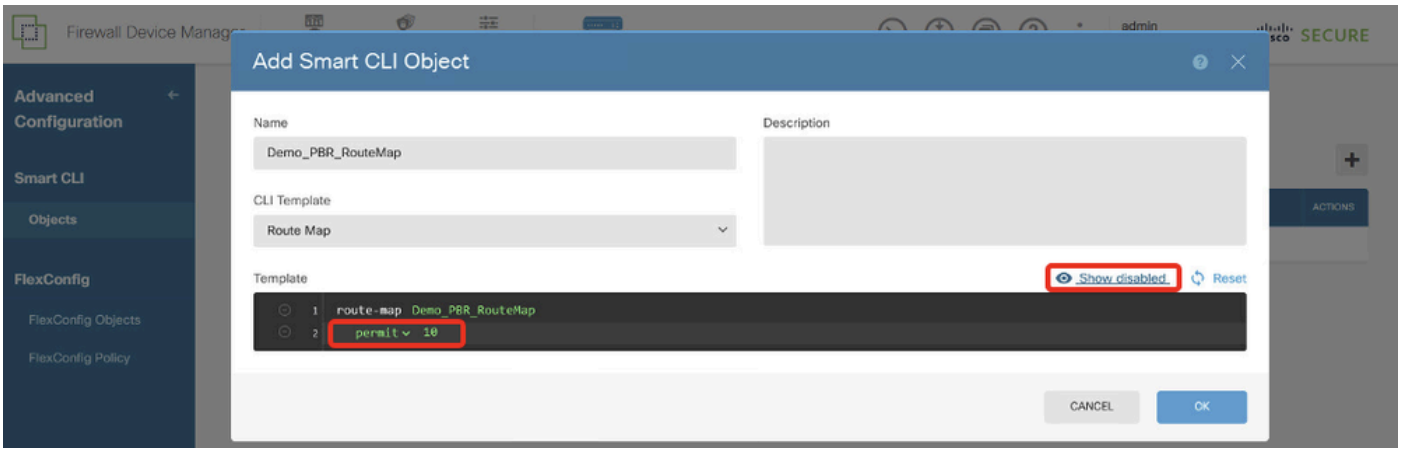
- Name: Demo_PBR_RouteMap
- CLI-Vorlage: Routenübersicht



Site1FTD_Create_PBR_RouteMap_1

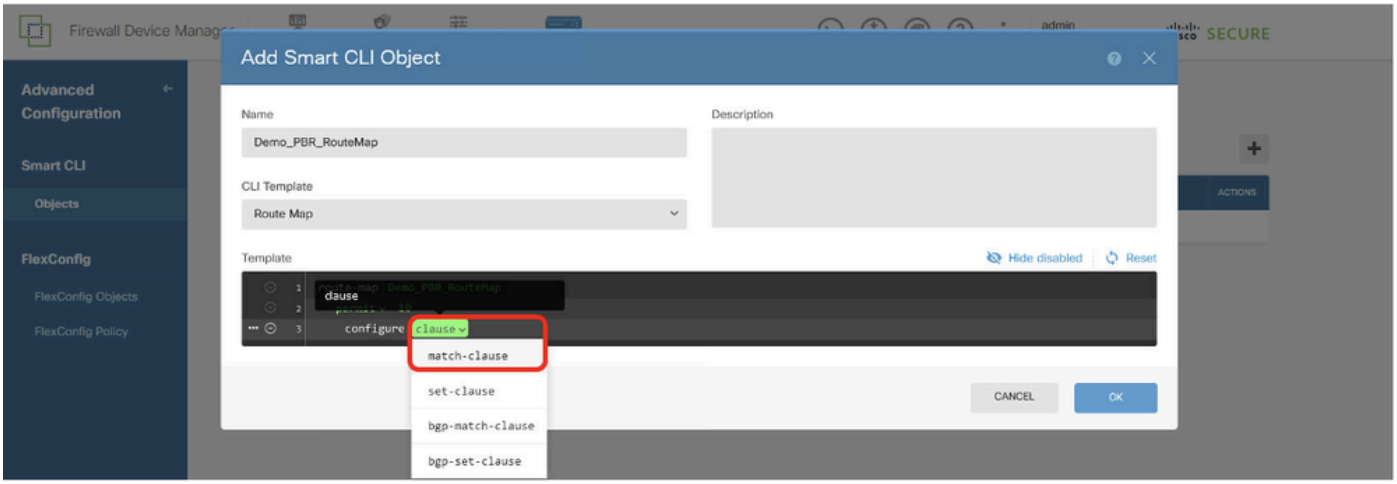
Schritt 13.2: Navigieren Sie zu Vorlage, und konfigurieren Sie sie. Klicken Sie zum Speichern auf OK.

Leitung 2, klicken Sie auf Neuverteilung. Wählen Sie Zulassen. Klicken Sie auf Sequenznummer, manuelle Eingabe 10. Klicken Sie auf Show disabled (Deaktiviert).



Site1FTD_Create_PBR_RouteMap_2

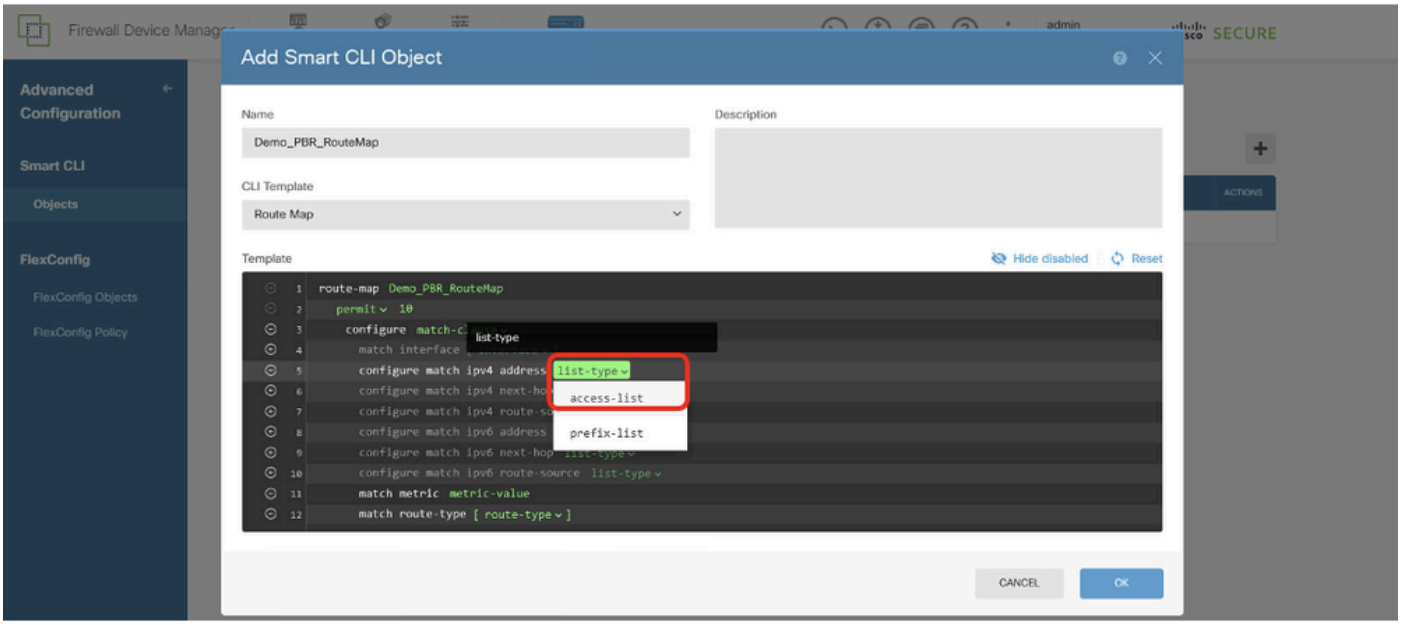
Zeile 3: Klicken Sie auf +, um die Zeile zu aktivieren. Click-Klausel. Wählen Sie eine Übereinstimmungsklausel aus.



Site1FTD_Create_PBR_RouteMap_3

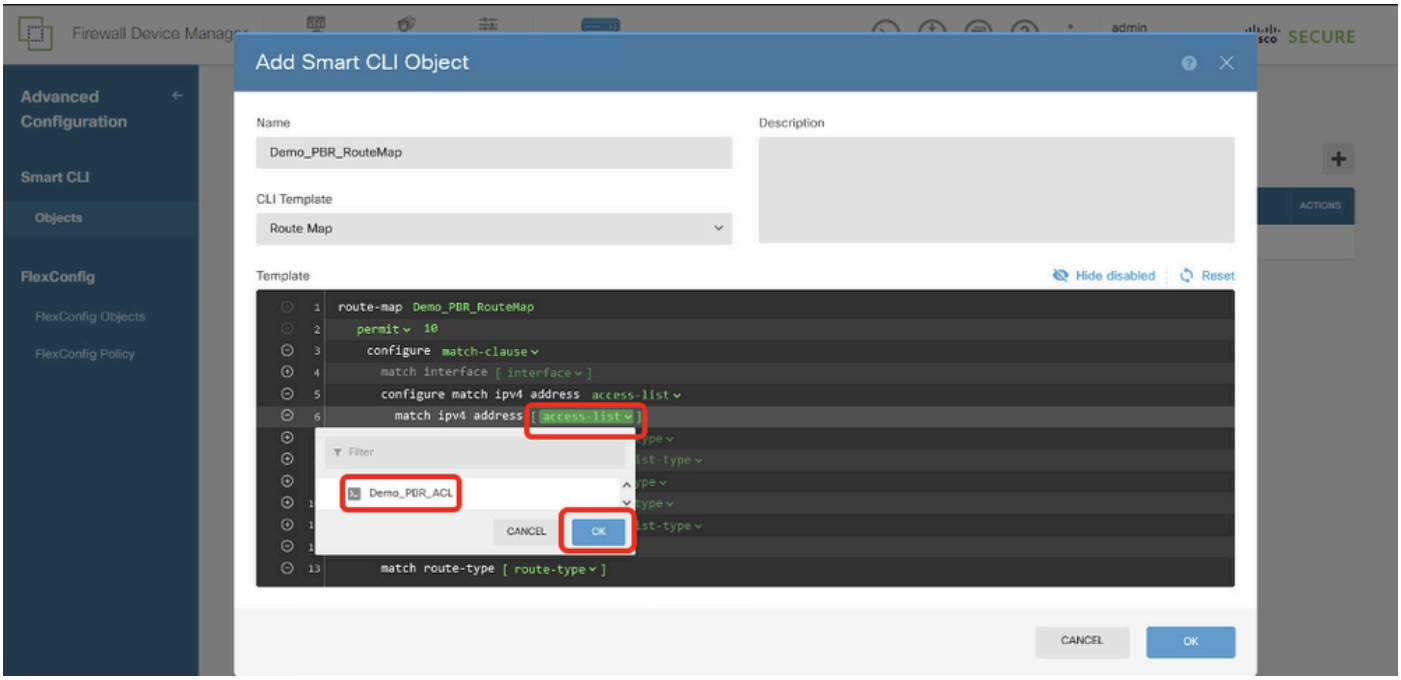
Leitung 4, klicken Sie - um die Leitung zu deaktivieren.

Zeile 5: Klicken Sie auf +, um die Zeile zu aktivieren. Klicken Sie auf Listentyp. Wählen Sie Zugriffsliste aus.



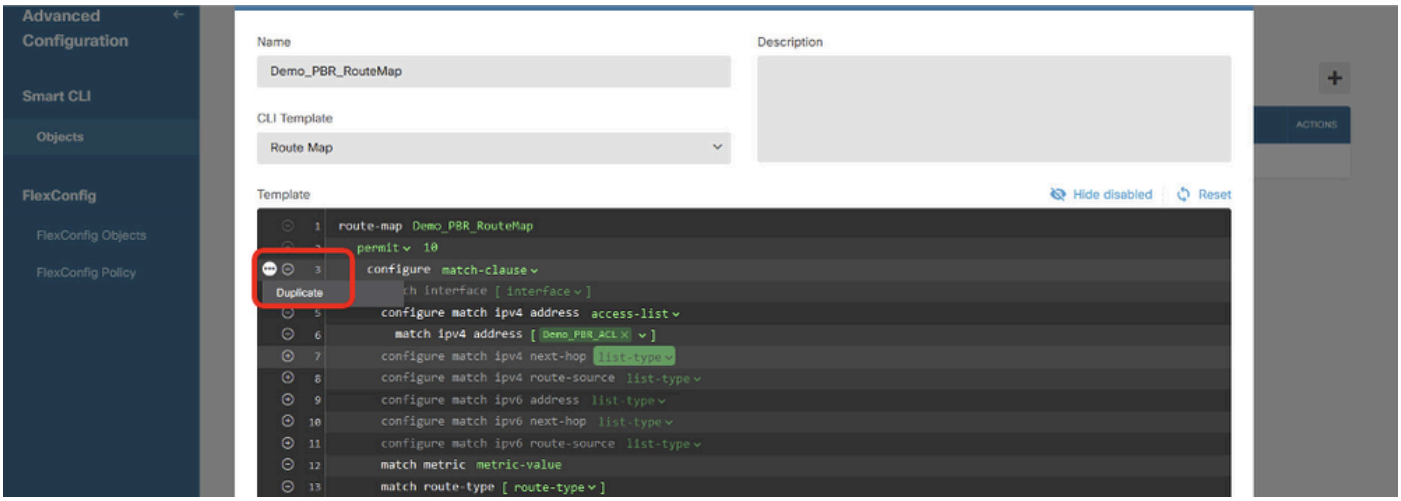
Site1FTD_Create_PBR_RouteMap_4

Leitung 6, klicken Sie auf access-list. Wählen Sie den ACL-Namen, der in Schritt 12 erstellt wird. In diesem Beispiel lautet der Name Demo_PBR_ACL.



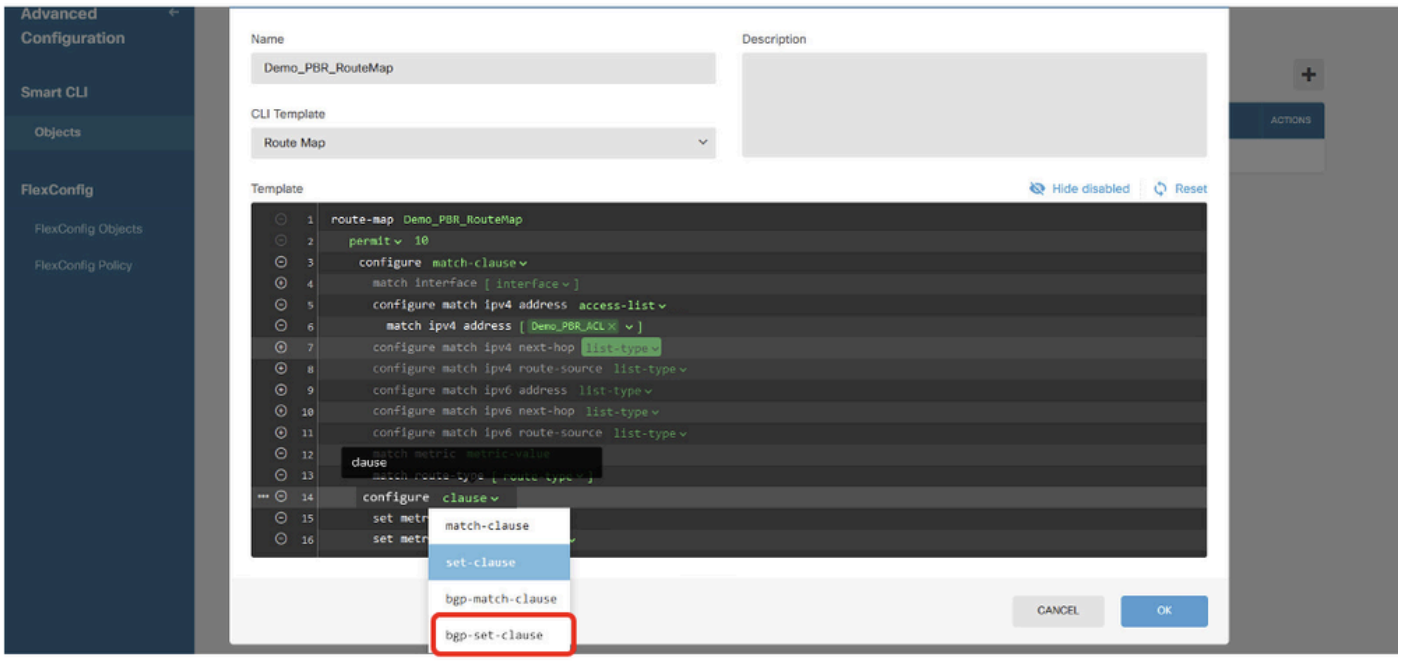
Site1FTD_Create_PBR_RouteMap_5

Zurück zu Zeile 3. Klicken Sie auf die Optionen ... , und wählen Sie Duplizieren.



Site1FTD_Create_PBR_RouteMap_6

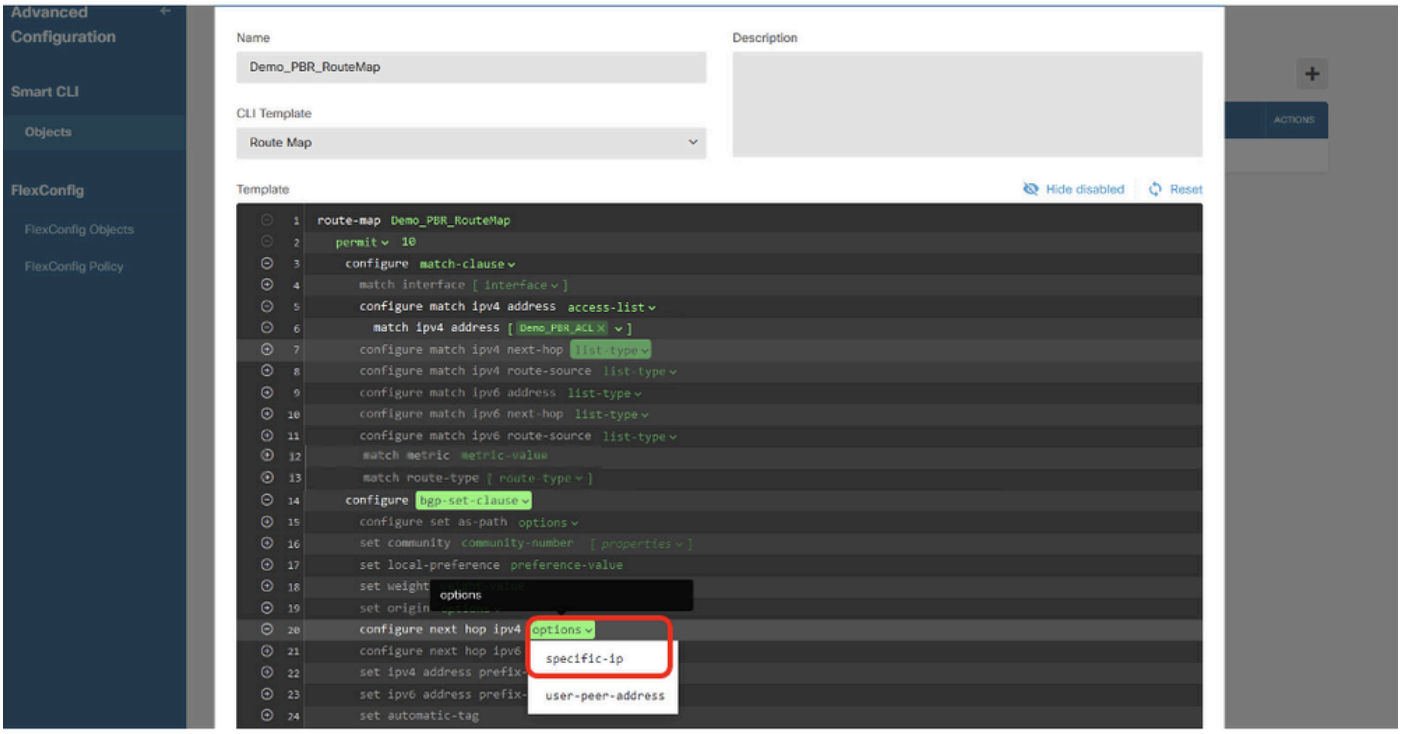
Zeile 14, klicken Sie auf clause und wählen Sie bgp-set-clause.



Standort1FTD_Create_PBR_RouteMap_7

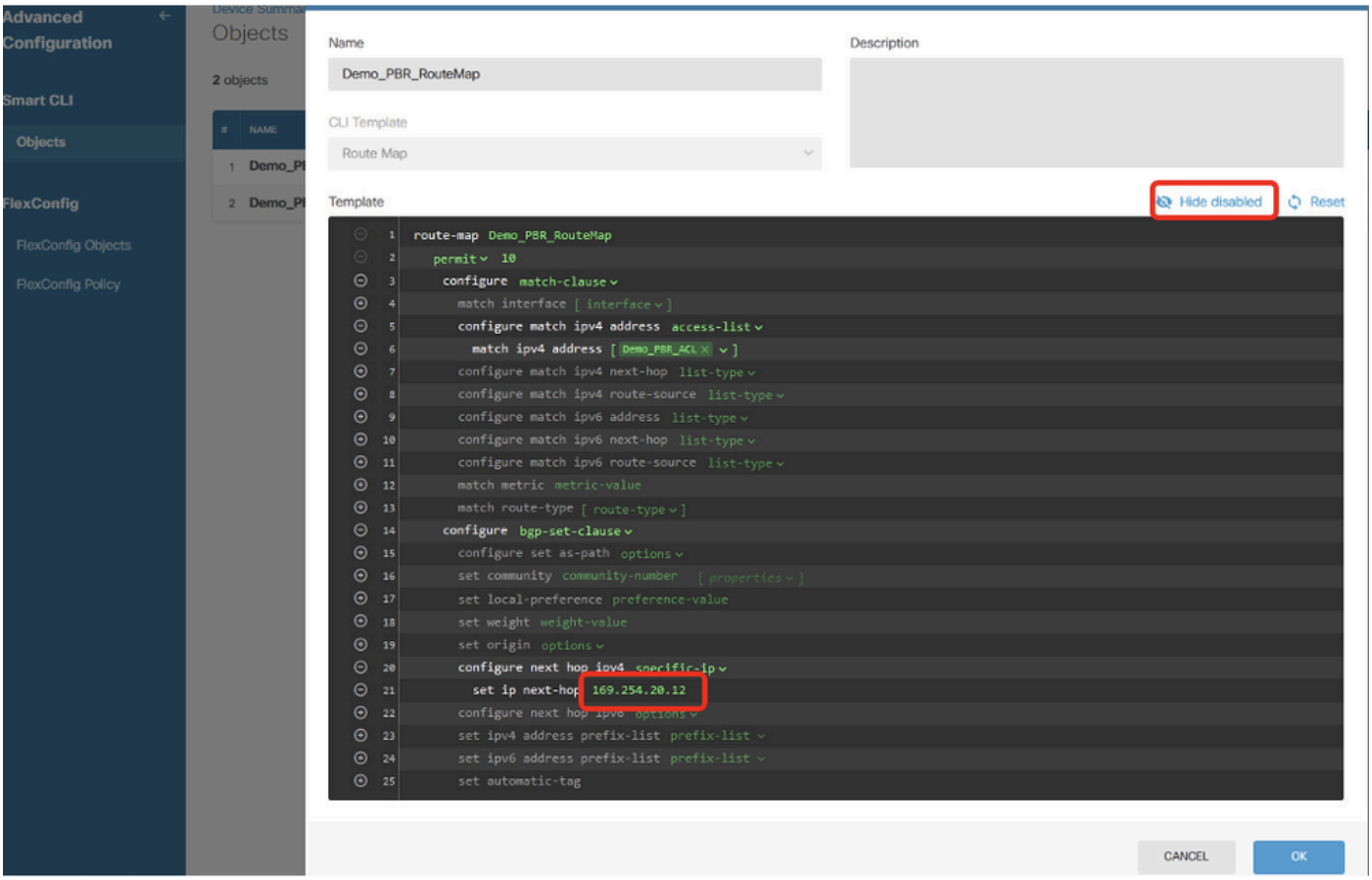
Klicken Sie in den Zeilen 12, 13, 15, 16, 17, 18, 19, 21, 22, 23, 24 auf - button, um die Deaktivierung vorzunehmen.

Zeile 20, klicken Sie auf Optionen und wählen Sie specific-ip aus.



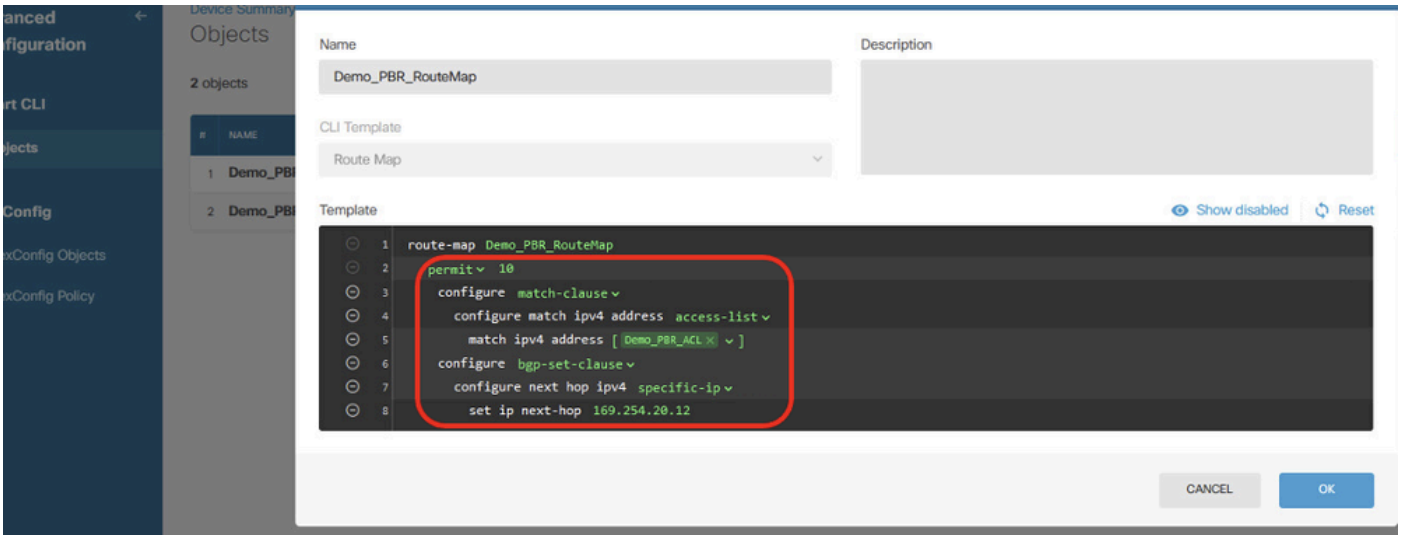
Standort1FTD_Create_PBR_RouteMap_8

Leitung 21, klicken Sie auf IP-Adresse. Next-Hop-IP-Adresse manuell eingeben In diesem Beispiel ist es die IP-Adresse des Peer-Standorts2 FTD VTI tunnel2 (169.254.20.12). Klicken Sie auf Ausblenden deaktiviert.



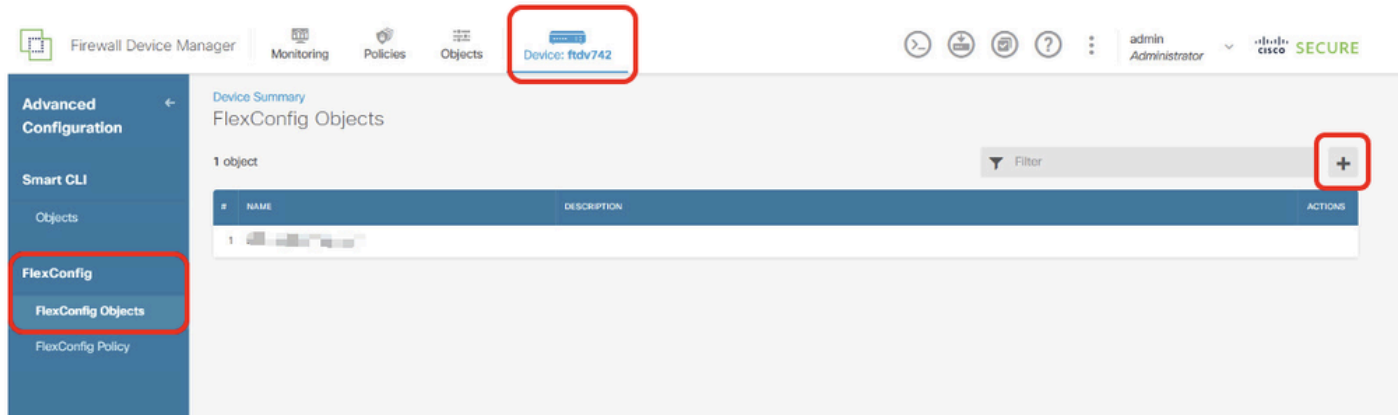
Site1FTD_Create_PBR_RouteMap_9

Überprüfen der Konfiguration der Routenübersicht



Standort1FTD_Create_PBR_RouteMap_10

Schritt 14: Erstellen eines FlexConfig-Objekts für PBR Navigieren Sie zu Device > Advanced Configuration > FlexConfig Objects, und klicken Sie auf +.



Standort1FTD_Create_PBR_FlexObj_1

Schritt 14.1: Geben Sie einen Namen für das Objekt ein. In diesem Beispiel lautet Demo_PBR_FlexObj. Geben Sie im Editor für Vorlagen und Negate Vorlagen die Befehlszeilen ein.

- Vorlage:

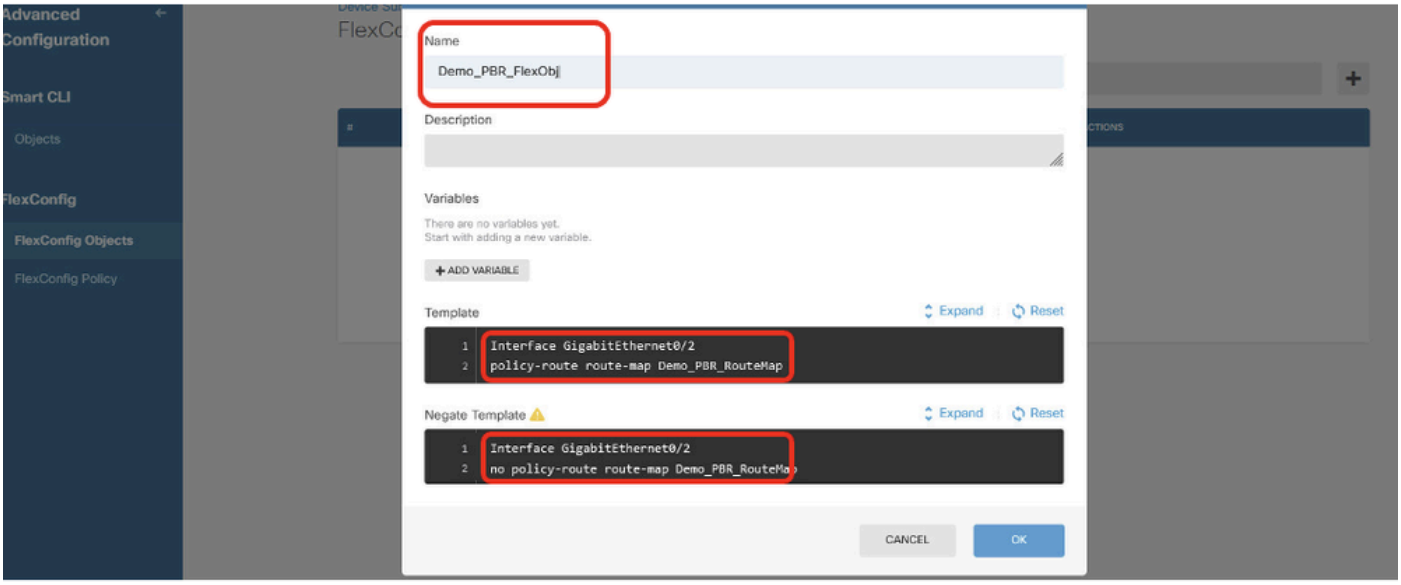
interface GigabitEthernet0/2

policy-route-route-map Demo_PBR_RouteMap_Site2

- Negative-Vorlage:

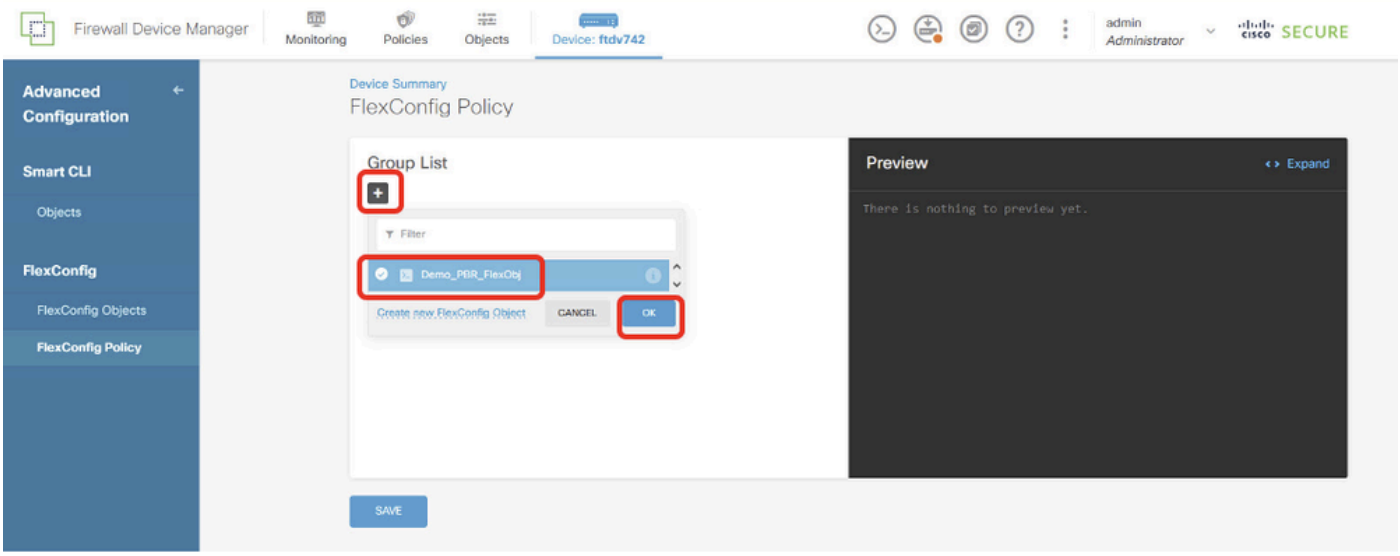
interface GigabitEthernet0/2

no policy-route-route-map Demo_PBR_RouteMap_Site2



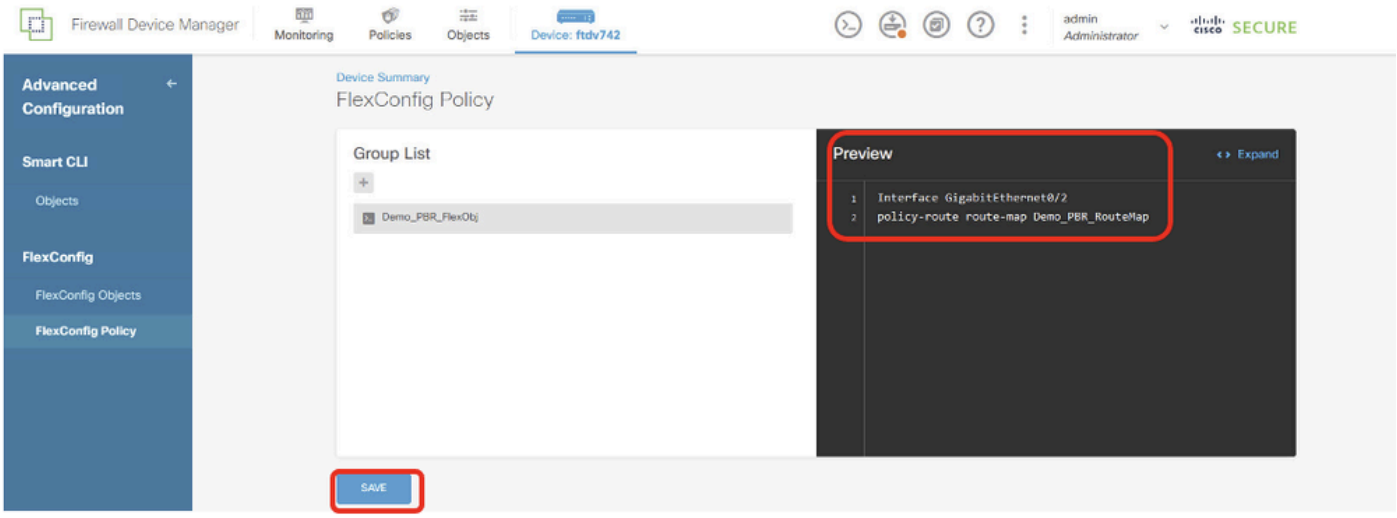
Standort1FTD_Create_PBR_FlexObj_2

Schritt 15: Erstellen einer FlexConfig-Richtlinie für PBR Navigieren Sie zu Gerät > Erweiterte Konfiguration > FlexConfig-Richtlinie. Klicken Sie auf +. Wählen Sie den in Schritt 14 erstellten FlexConfig-Objektnamen aus. Klicken Sie auf die Schaltfläche OK.



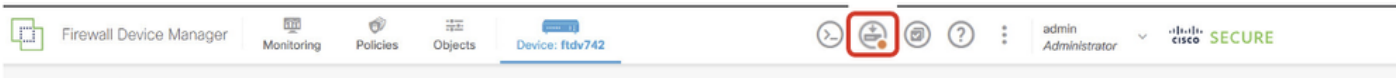
Site1FTD_Create_PBR_FlexPolicy_1

Schritt 15.1. Überprüfen Sie den Befehl im Fenster Vorschau. Klicken Sie in diesem Fall auf Speichern.



Site1FTD_Create_PBR_FlexPolicy_2

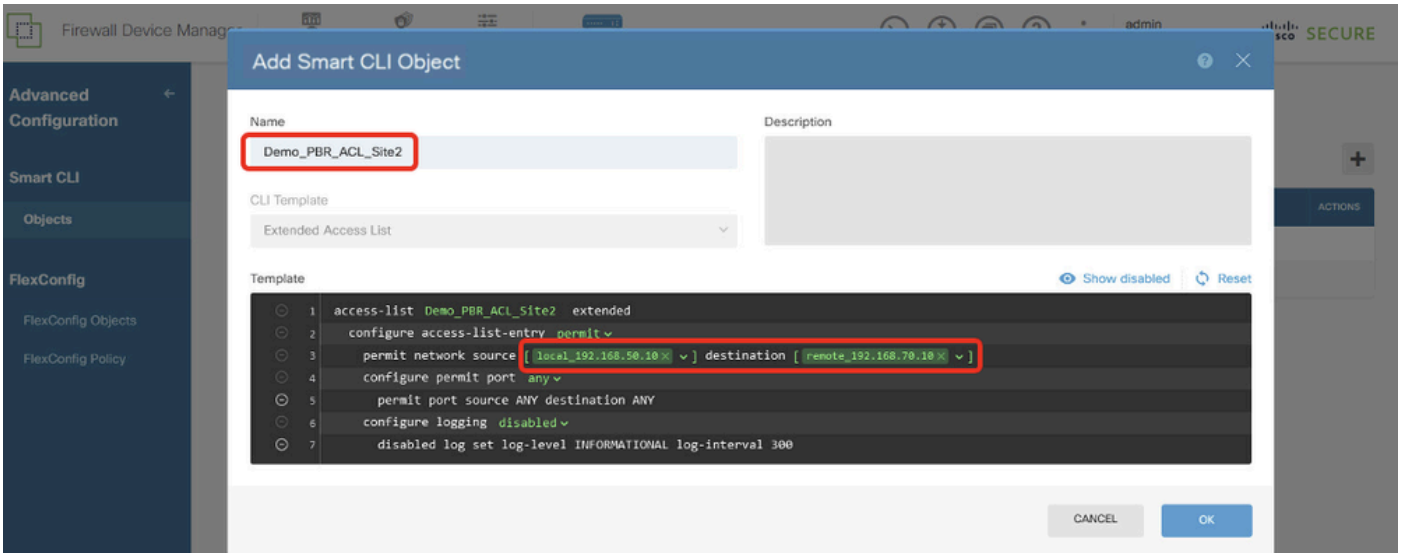
Schritt 16: Bereitstellen der Konfigurationsänderungen



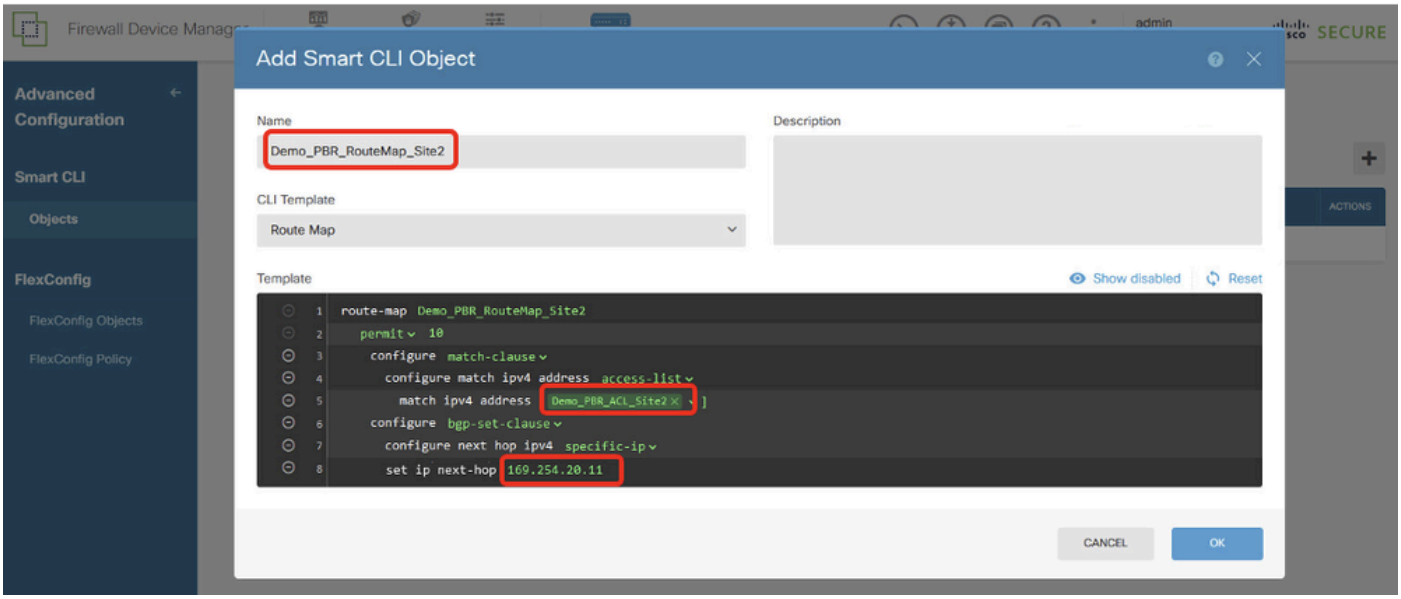
Site1FTD_Deployment_Changes

PBR-Konfiguration für Site2 FTD

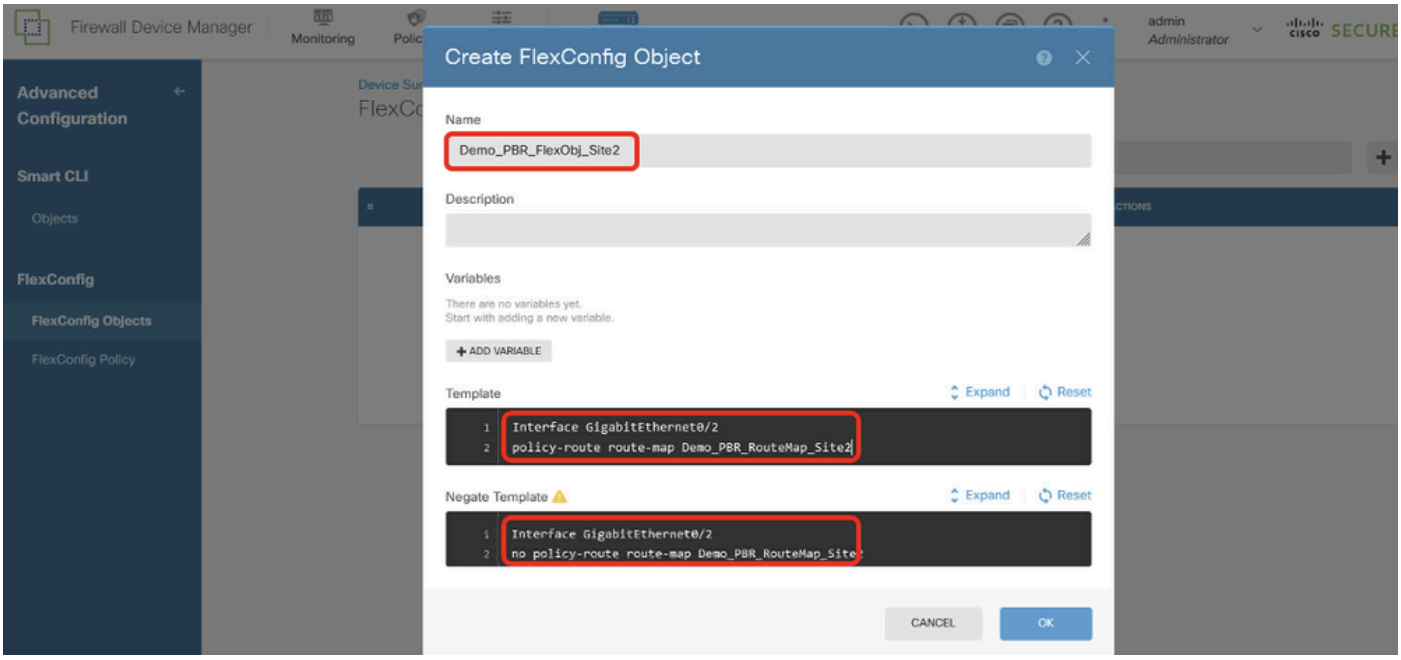
Schritt 17: Wiederholen Sie Schritt 11 bis Schritt 16, um PBR mit den entsprechenden Parametern für Site2 FTD zu erstellen.



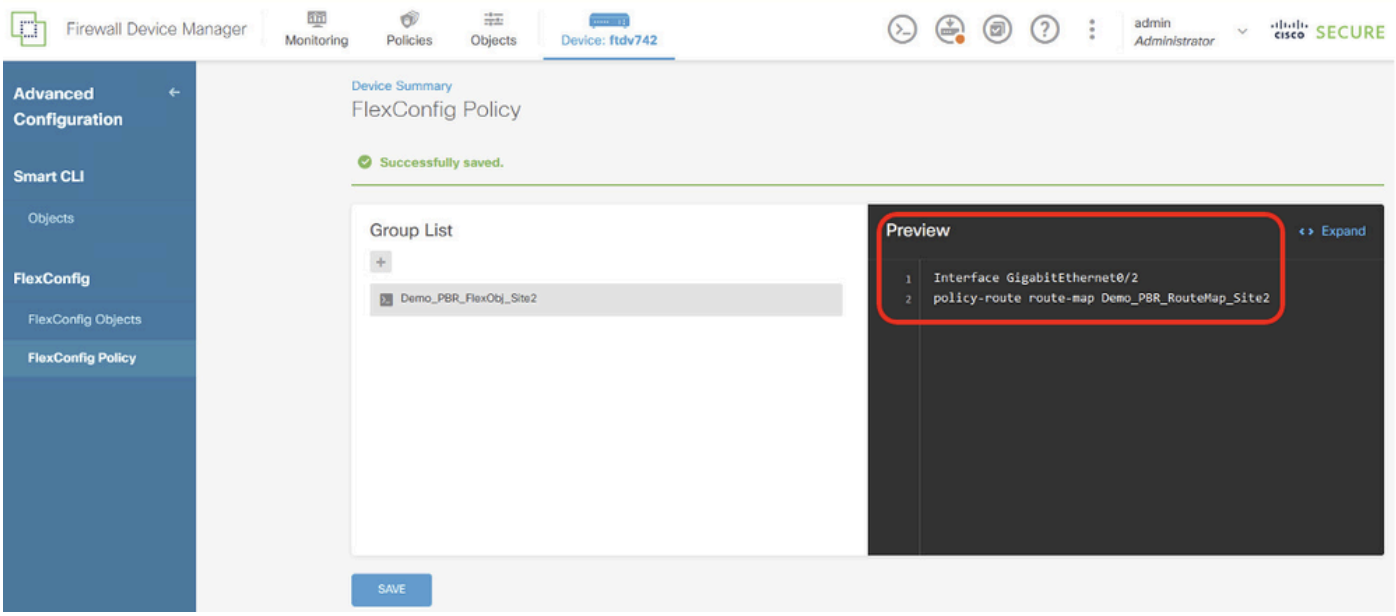
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

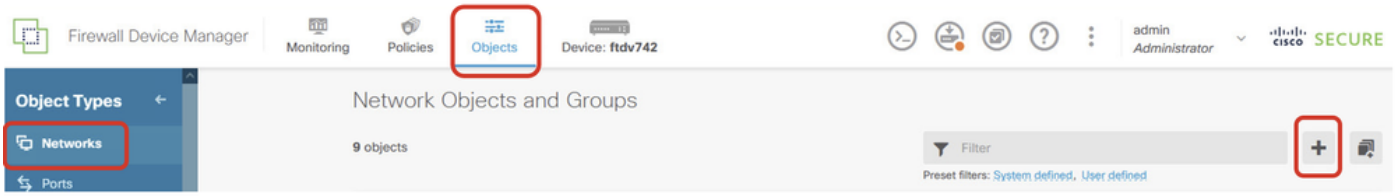


Site2FTD_Create_PBR_FlexPolicy

Konfigurationen auf SLA Monitor

Site1 FTD SLA-Überwachungskonfiguration

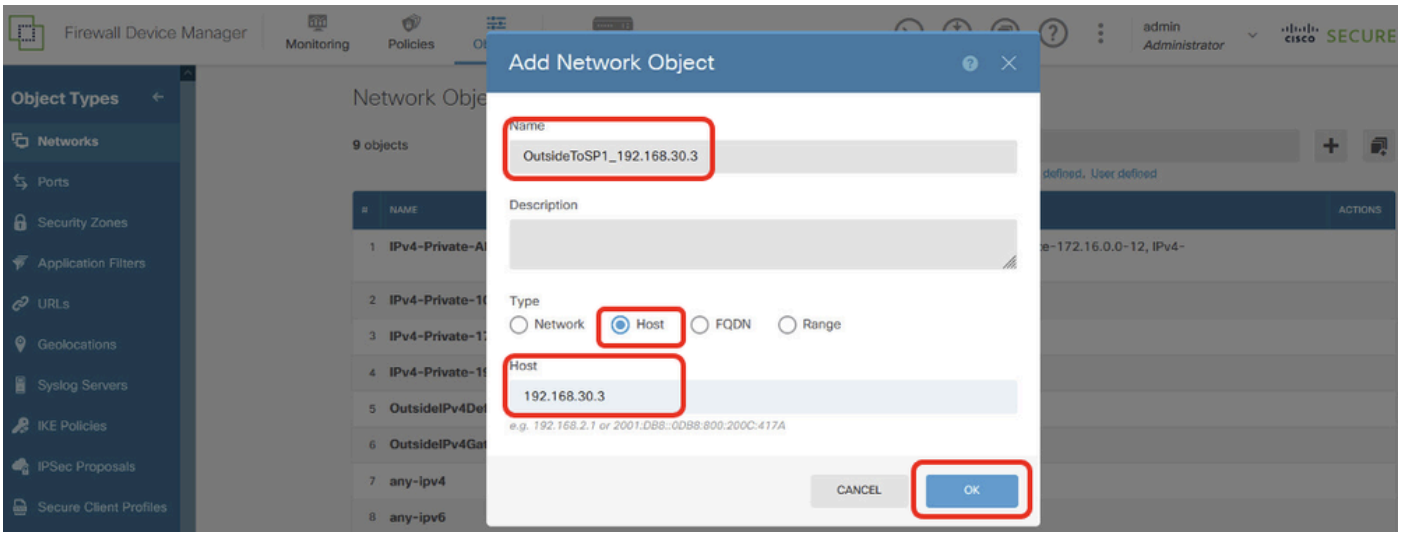
Schritt 18. Erstellen Sie neue Netzwerkobjekte, die von SLA Monitors für Site1 FTD verwendet werden sollen. Navigieren Sie zu Objekte > Netzwerke, und klicken Sie auf +.



Site1FTD_Create_Network_Object

Schritt 18.1. Erstellen Sie ein Objekt für die IP-Adresse des ISP1-Gateways. Geben Sie die erforderlichen Informationen an. Klicken Sie auf OK.

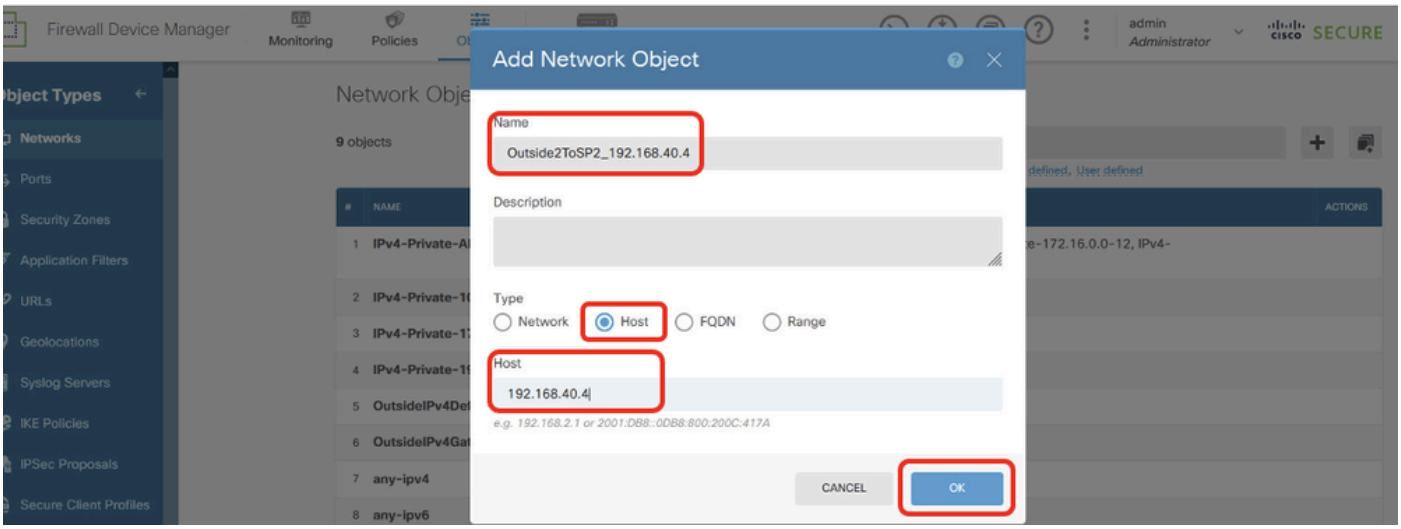
- Name: ExternZuSP1_192.168.30.3
- Typ: Host
- Gastgeber: 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

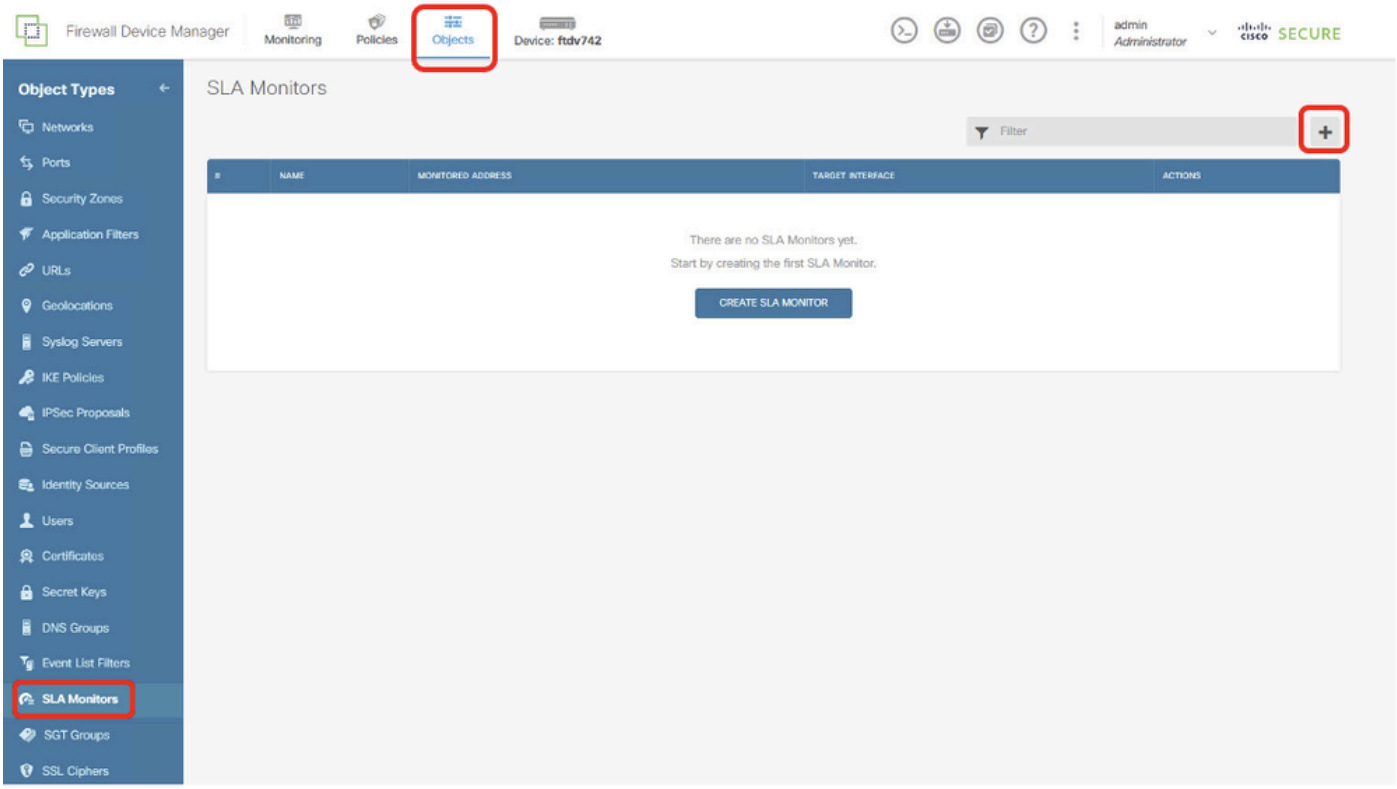
Schritt 18.2. Erstellen Sie ein Objekt für die IP-Adresse des ISP2-Gateways. Geben Sie die erforderlichen Informationen an. Klicken Sie auf OK.

- Name: Extern2ZuSP2_192,168,40,4
- Typ: Host
- Gastgeber: 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

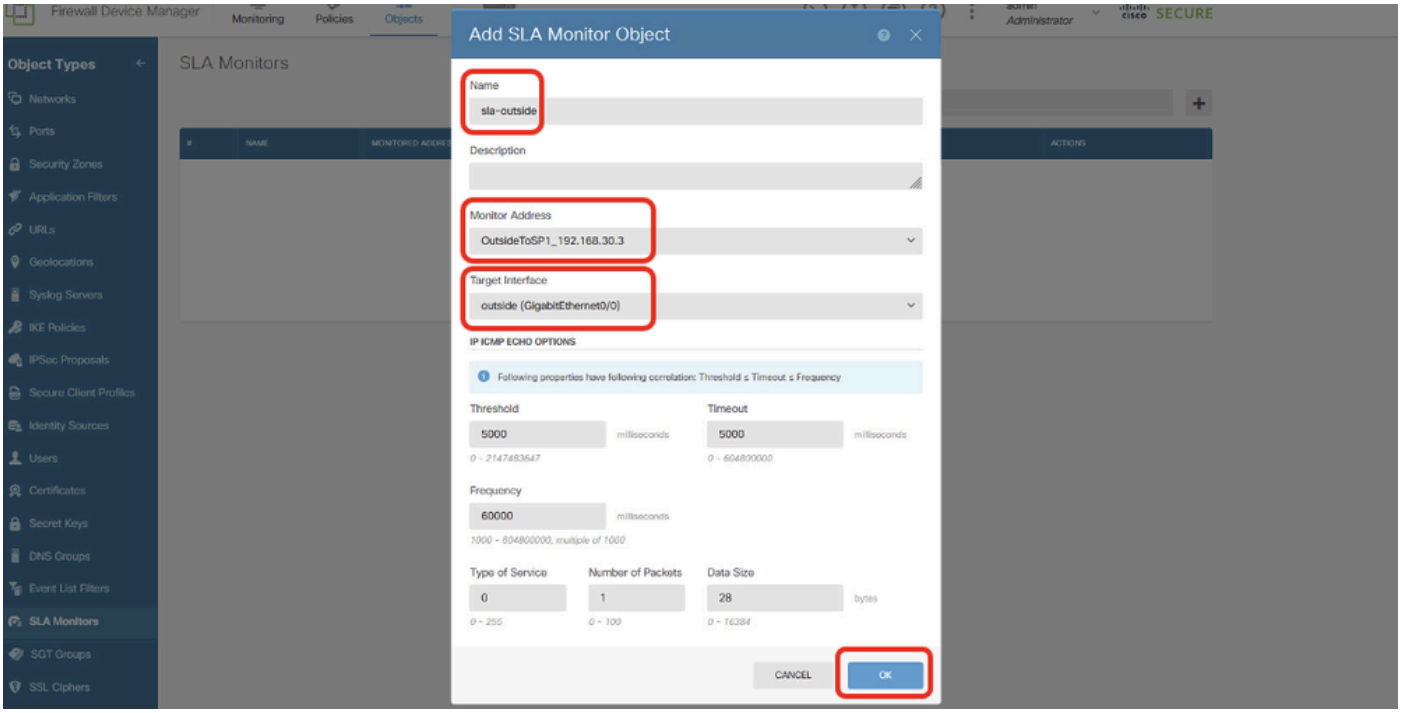
Schritt 19: Erstellen der SLA-Überwachung Navigieren Sie zu Objekte > Objekttypen > SLA-Monitore. Klicken Sie auf +, um einen neuen SLA-Monitor zu erstellen.



Site1FTD_Create_SLAMonitor

Schritt 19.1: Geben Sie im Fenster Add SLA Monitor Object (SLA-Überwachungsobjekt hinzufügen) die erforderlichen Informationen für das ISP1-Gateway an. Klicken Sie zum Speichern auf OK.

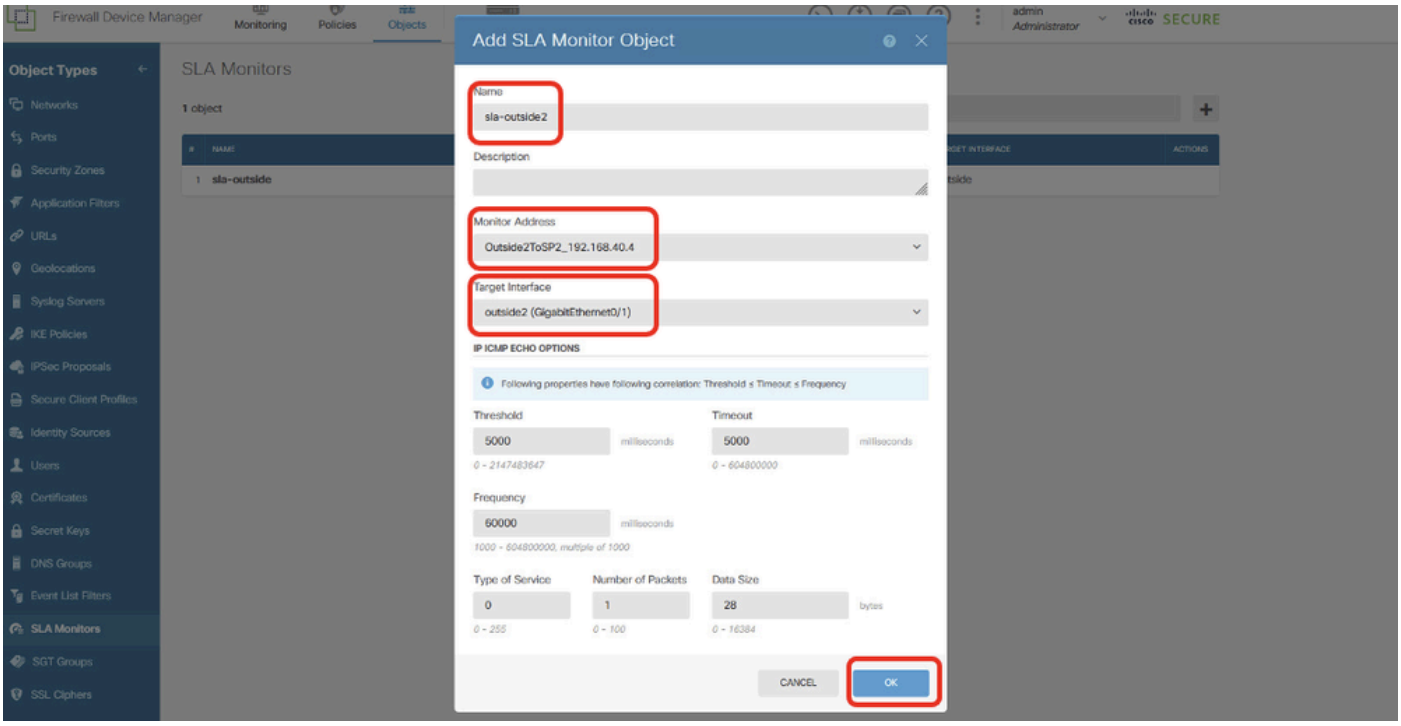
- Name: sla-extern
- Überwachungsadresse: ExternZuSP1_192.168.30.3
- Zielschnittstelle: outside(GigabitEthernet0/0)
- IP ICMP ECHO-OPTIONEN: standard



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

Schritt 19.2. Klicken Sie weiterhin auf +, um einen neuen SLA-Monitor für das ISP2-Gateway zu erstellen. Geben Sie im Fenster Add SLA Monitor Object (SLA-Überwachungsobjekt hinzufügen) die erforderlichen Informationen für das ISP2-Gateway ein. Klicken Sie zum Speichern auf OK.

- Name: sla-extern2
- Überwachungsadresse: Extern2ZuSP2_192,168,40,4
- Zielschnittstelle: outside2(GigabitEthernet0/1)
- IP ICMP ECHO-OPTIONEN: standard



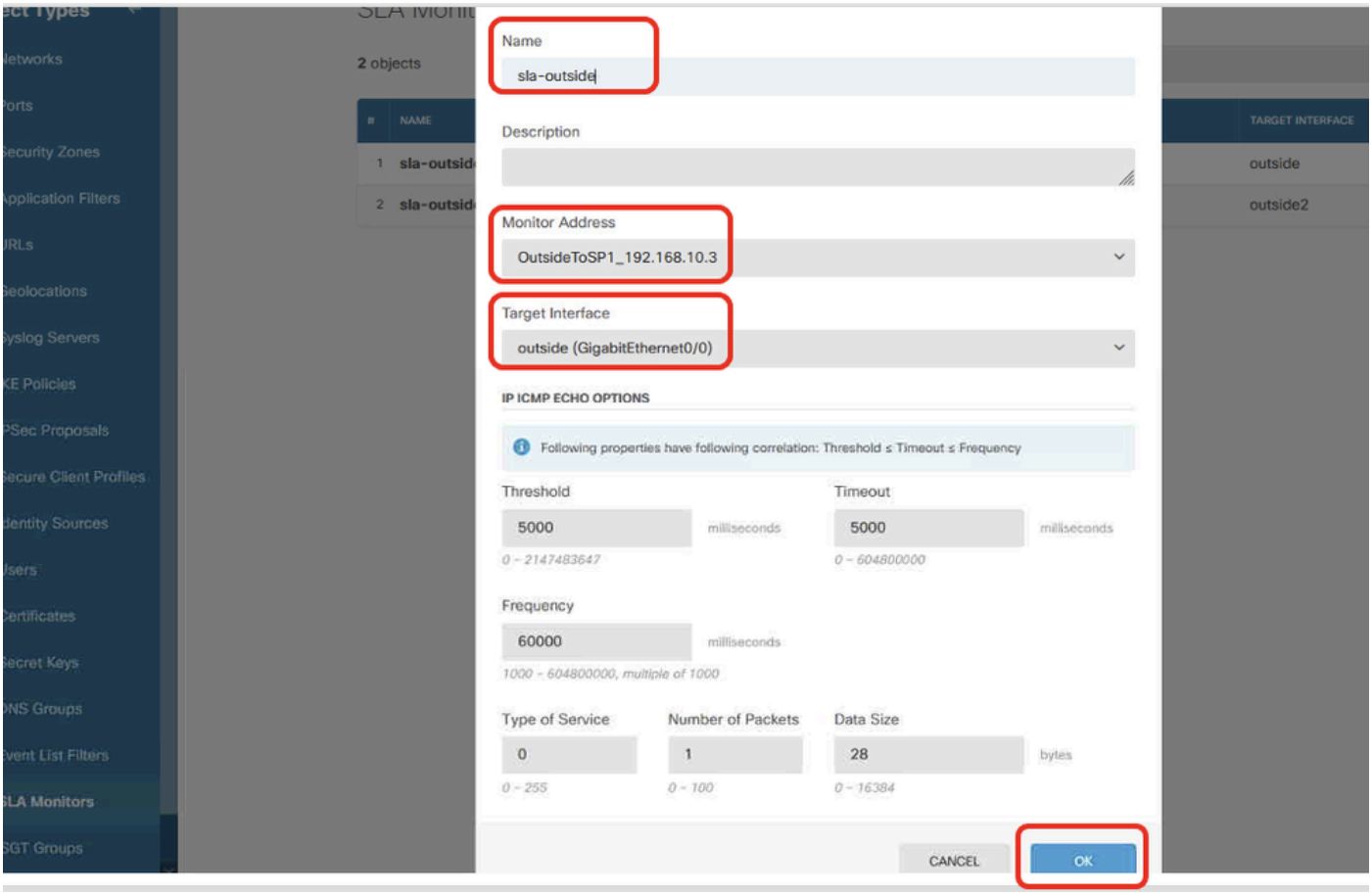
Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

Schritt 20: Bereitstellen der Konfigurationsänderungen

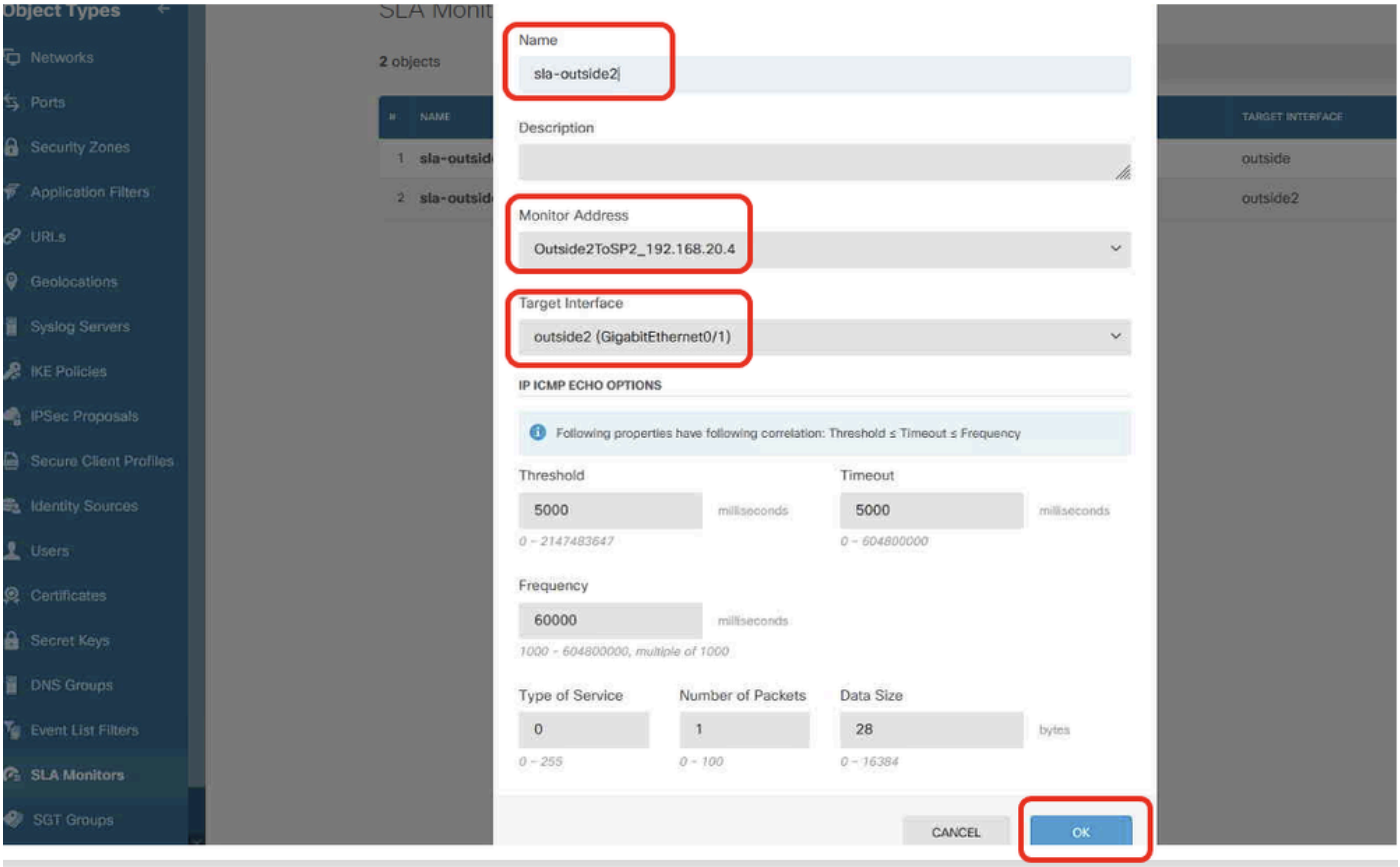
Site1FTD_Deployment_Changes

Site2 FTD SLA-Überwachungskonfiguration

Schritt 21. Wiederholen Sie Schritt 18. bis Schritt 20. Erstellen Sie einen SLA-Monitor mit den entsprechenden Parametern auf Site2 FTD.



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

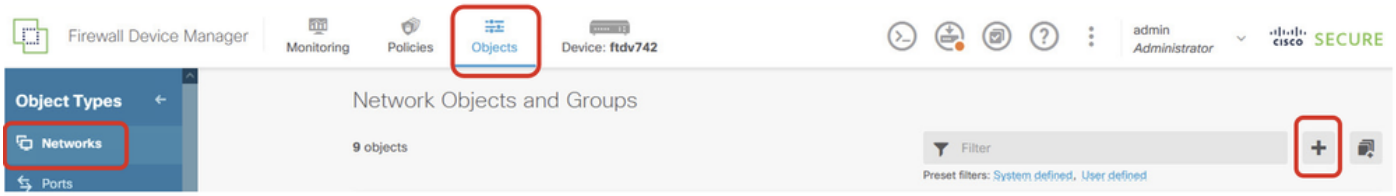


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

Konfigurationen auf statischer Route

Statische FTD-Routenkonfiguration für Standort 1

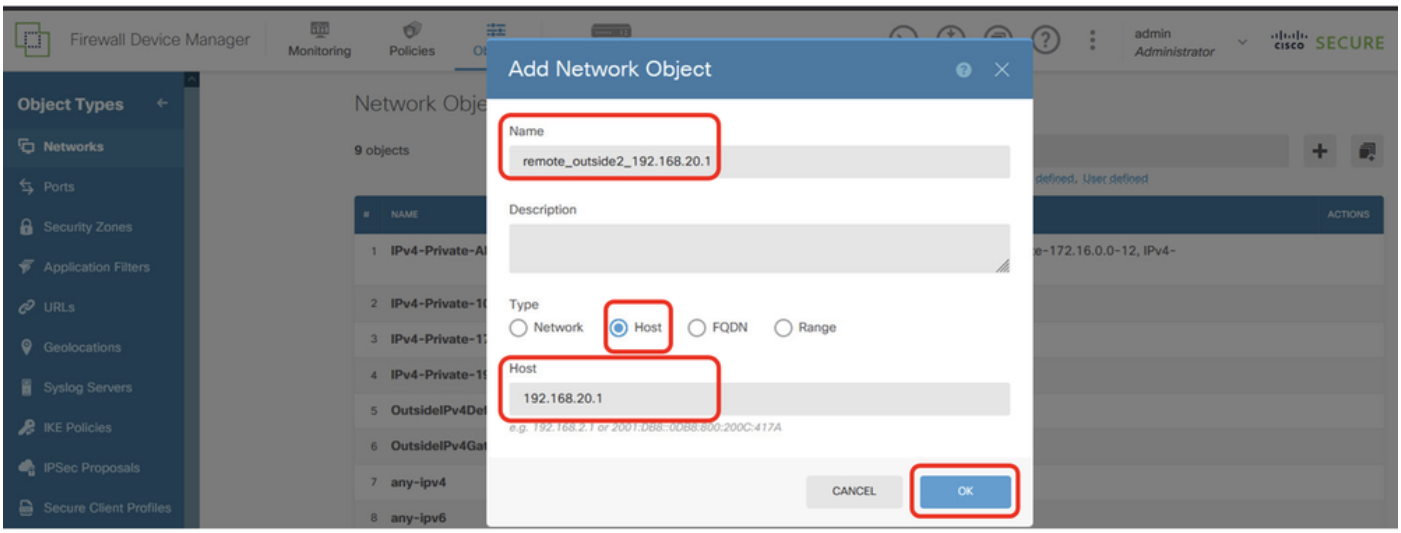
Schritt 22. Erstellen Sie neue Netzwerkobjekte, die von der statischen Route für Site1 FTD verwendet werden sollen. Navigieren Sie zu Objekte > Netzwerke, klicken Sie auf + Schaltfläche.



Standort1FTD_Create_Obj

Schritt 22.1. Objekt für externe 2 IP-Adresse des Peer-Standorts erstellen2 FTD. Geben Sie die erforderlichen Informationen ein. Klicken Sie auf OK.

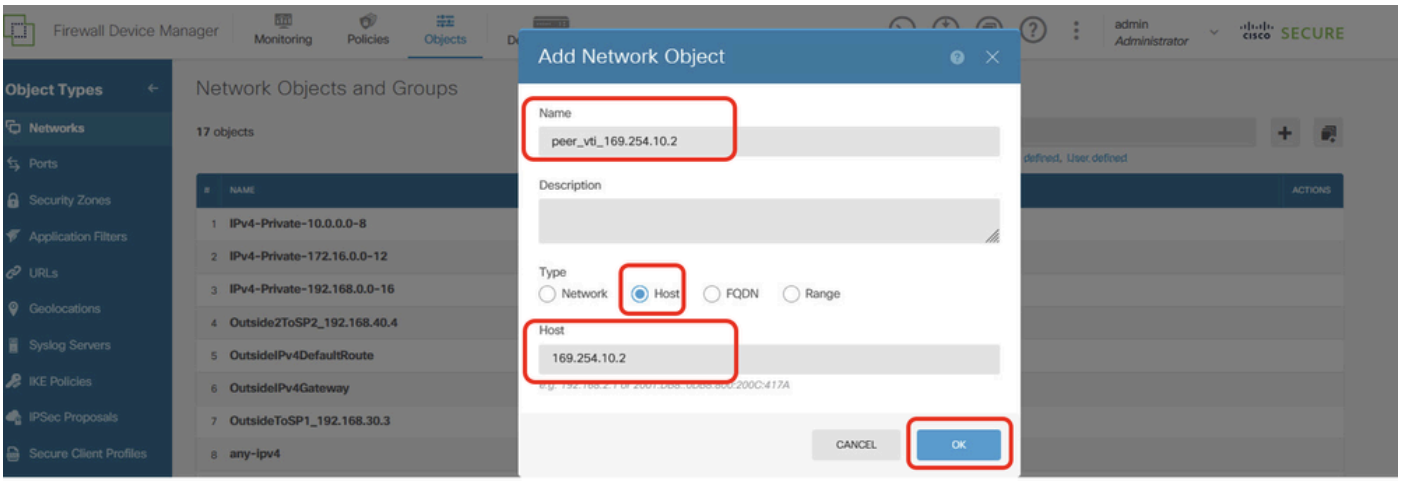
- Name: remote_outside2_192.168.20.1
- Typ: GASTGEBER
- Netzwerk: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

Schritt 22.2. Erstellen Sie das Objekt für die IP-Adresse von VTI Tunnel1 des Peer-Standorts2 FTD. Geben Sie die erforderlichen Informationen an. Klicken Sie auf OK.

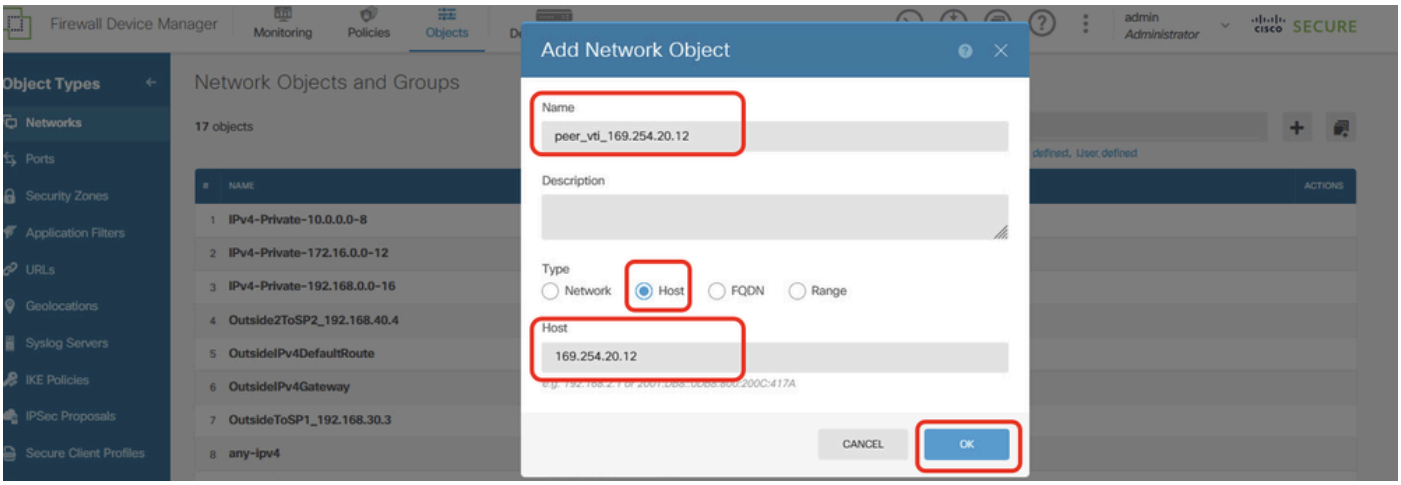
- Name: peer_vti_169.254.10.2
- Typ: GASTGEBER
- Netzwerk:169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

Schritt 22.3. Erstellen Sie das Objekt für die IP-Adresse des VTI Tunnel2 des Peer-Standorts2 FTD. Geben Sie die erforderlichen Informationen an. Klicken Sie auf OK.

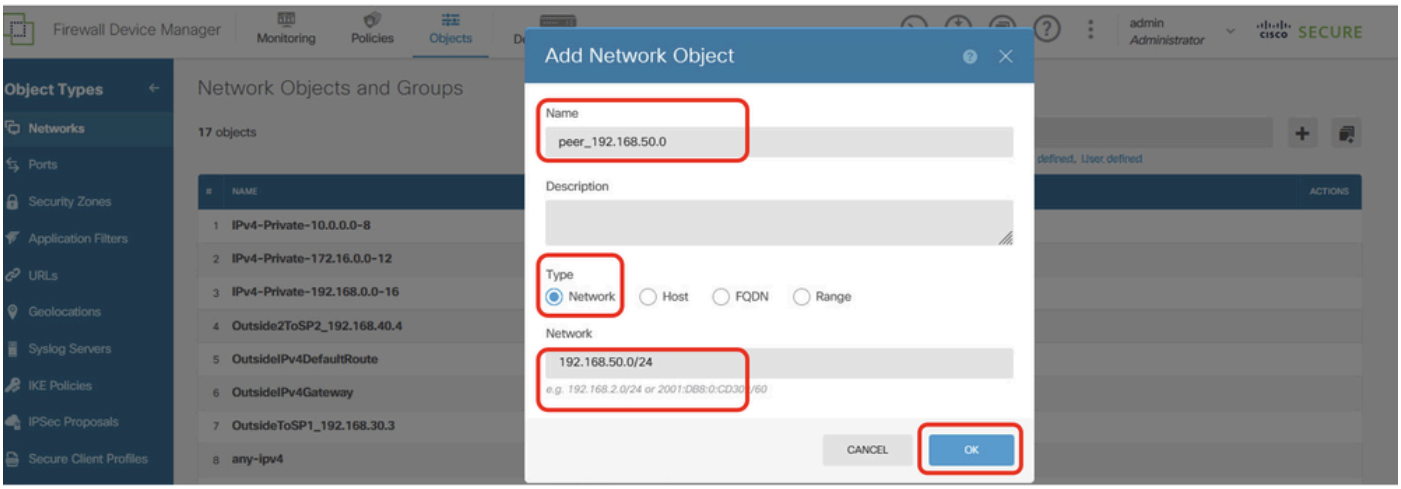
- Name: peer_vti_169,254.20,12
- Typ: GASTGEBER
- Netzwerk:169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

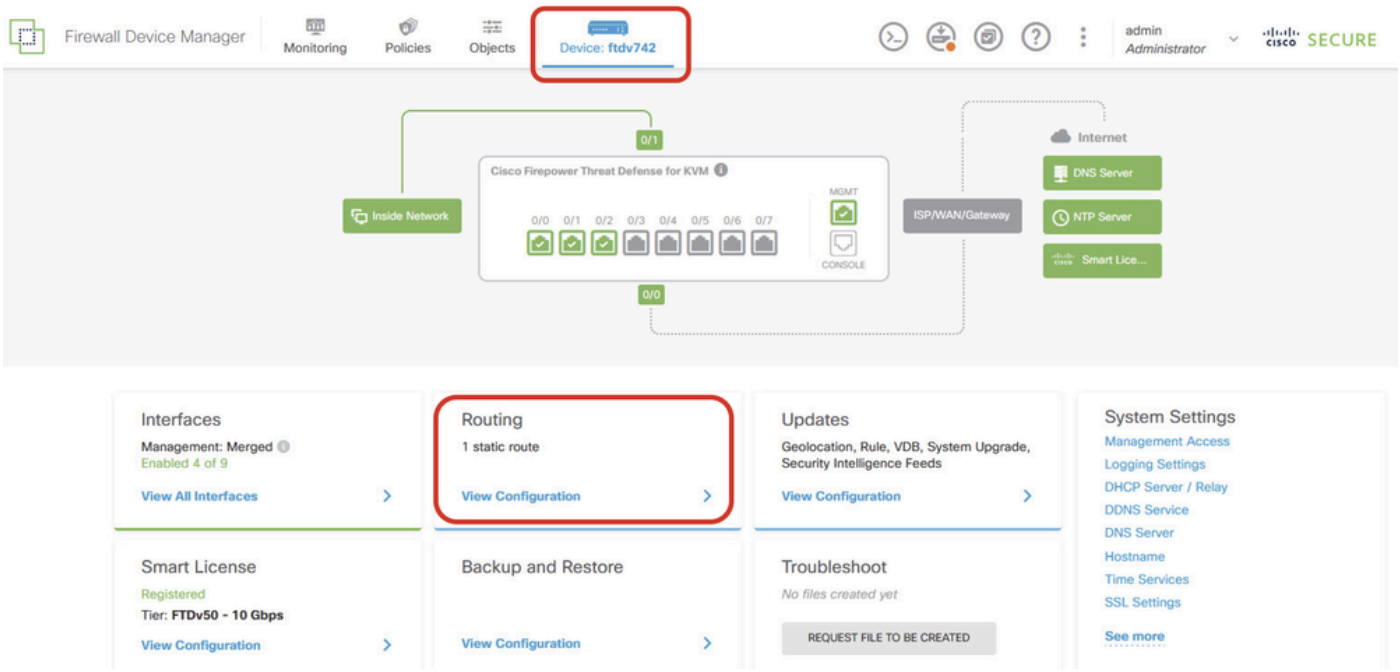
Schritt 22.4. Erstellen Sie ein Objekt für das interne Netzwerk des Peer-Site2 FTD. Geben Sie die erforderlichen Informationen an. Klicken Sie auf OK.

- Name: peer_192,168,50,0
- Typ: NETZWERK
- Netzwerk:192.168.50.0/24

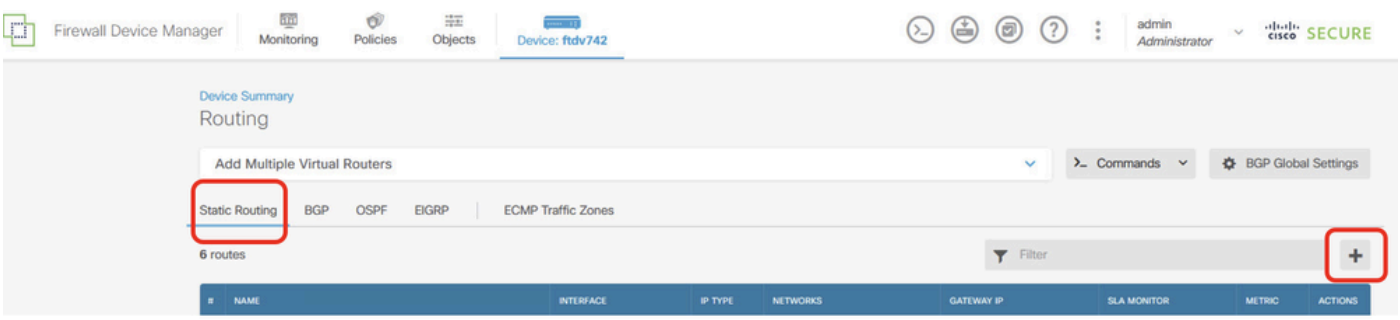


Site1FTD_Create_NetObj_StaticRoute_4

Schritt 23: Navigieren Sie zu Gerät > Routing. Klicken Sie auf Konfiguration anzeigen. Klicken Sie auf die Registerkarte "Statisches Routing". Klicken Sie auf +, um eine neue statische Route hinzuzufügen.



Standort1FTD_View_Route_Configuration

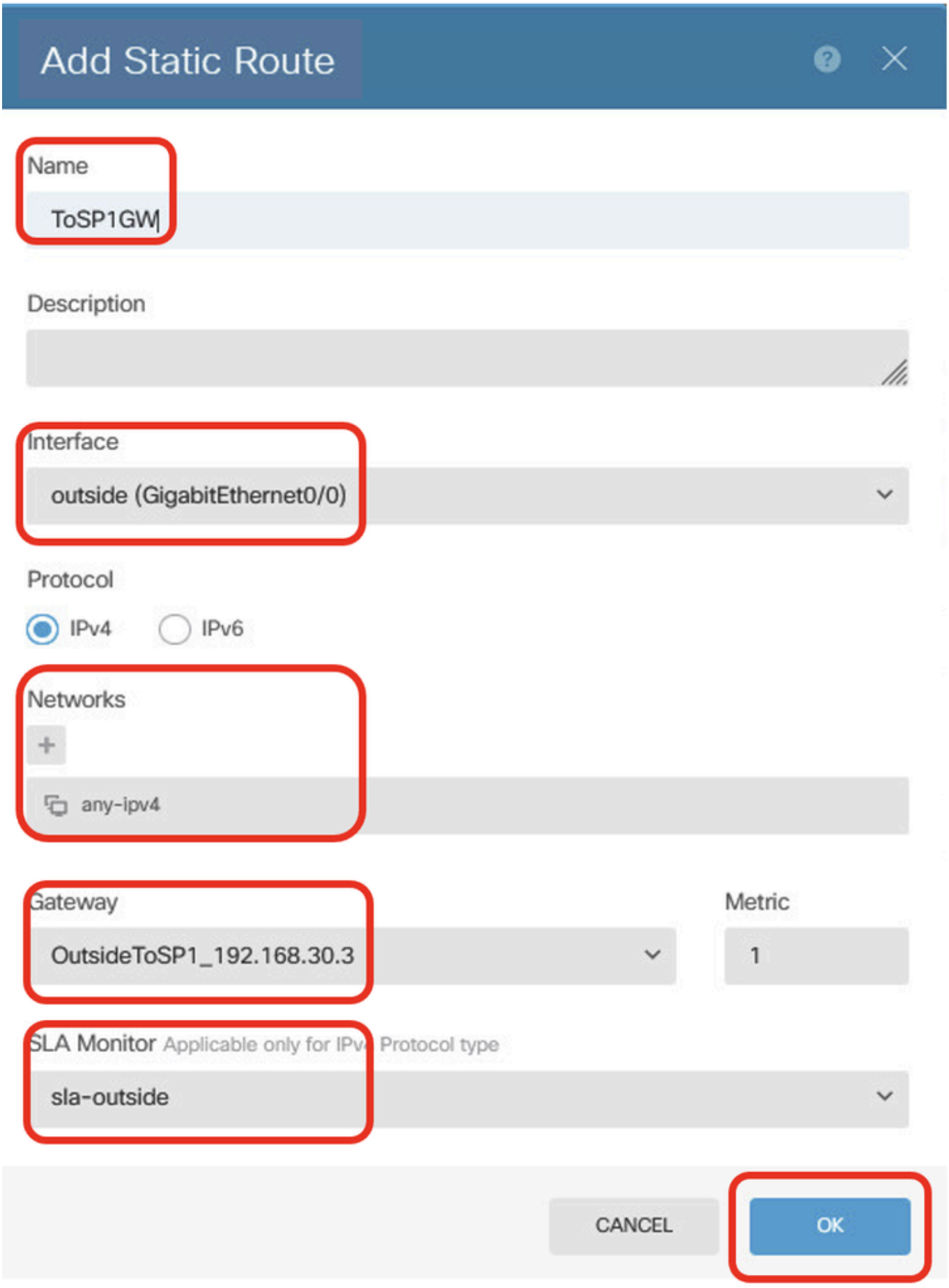


Standort1FTD_Add_Static_Route

Schritt 23.1: Erstellen Sie eine Standardroute über das ISP1-Gateway mit SLA-Überwachung.

Wenn das ISP1-Gateway unterbrochen wird, wechselt der Datenverkehr über ISP2 zur Backup-Standardroute. Sobald ISP1 wiederhergestellt ist, wird der Datenverkehr wieder über ISP1 geleitet. Geben Sie die erforderlichen Informationen an. Klicken Sie zum Speichern auf OK.

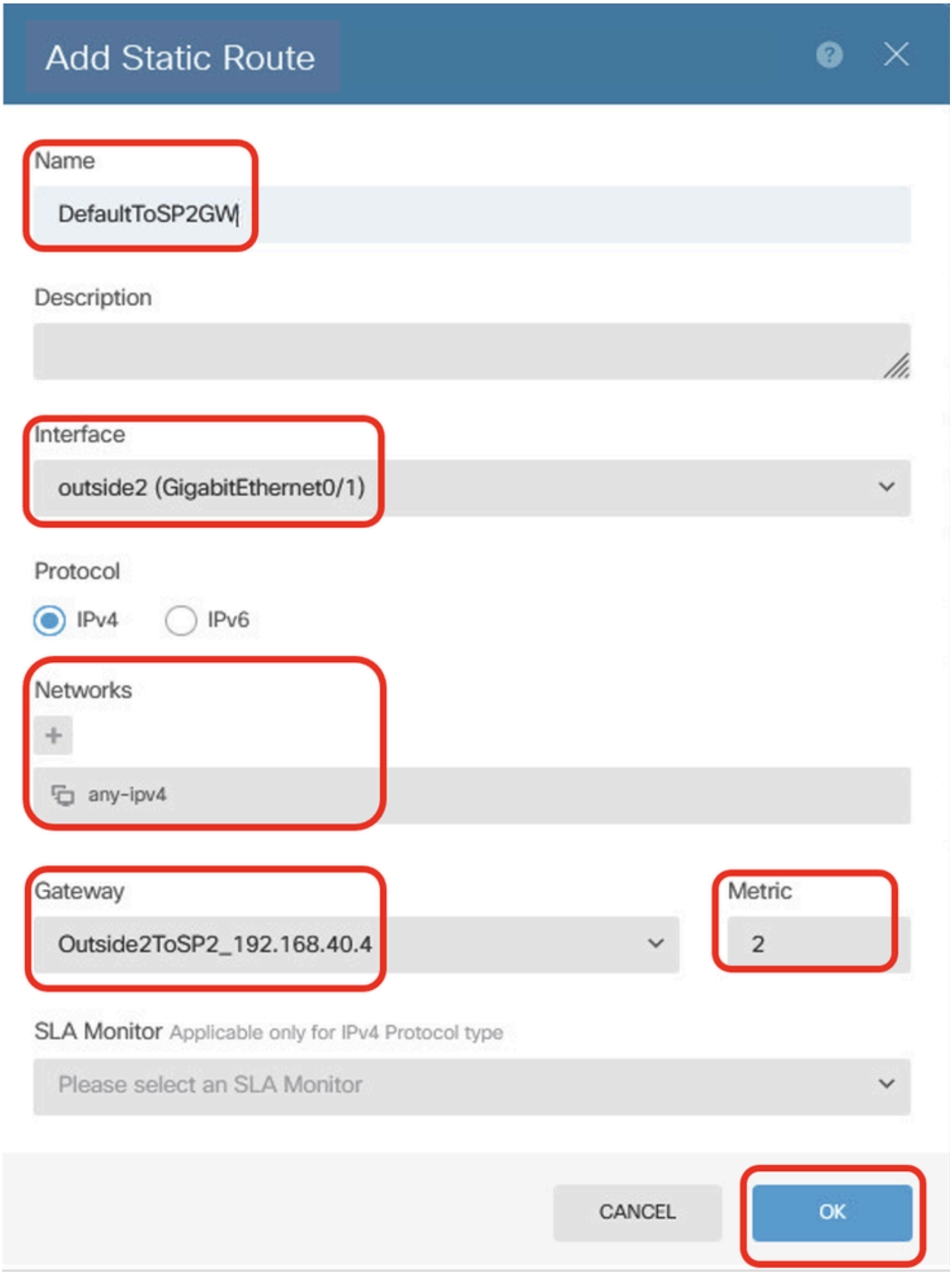
- Name: AnSP1GW
- Schnittstelle: outside(GigabitEthernet0/0)
- Protokolle: IPv4
- Netzwerke: any-ipv4
- Gateway: ExternZuSP1_192.168.30.3
- Kennzahl: 1
- SLA-Monitor: sla-extern



Site1FTD_Create_StaticRoute_1

Schritt 23.2: Erstellen Sie eine Backup-Standardroute über das Gateway ISP2. Metrik muss größer als 1 sein. In diesem Beispiel ist Metrik 2. Geben Sie die erforderlichen Informationen ein. Klicken Sie zum Speichern auf OK.

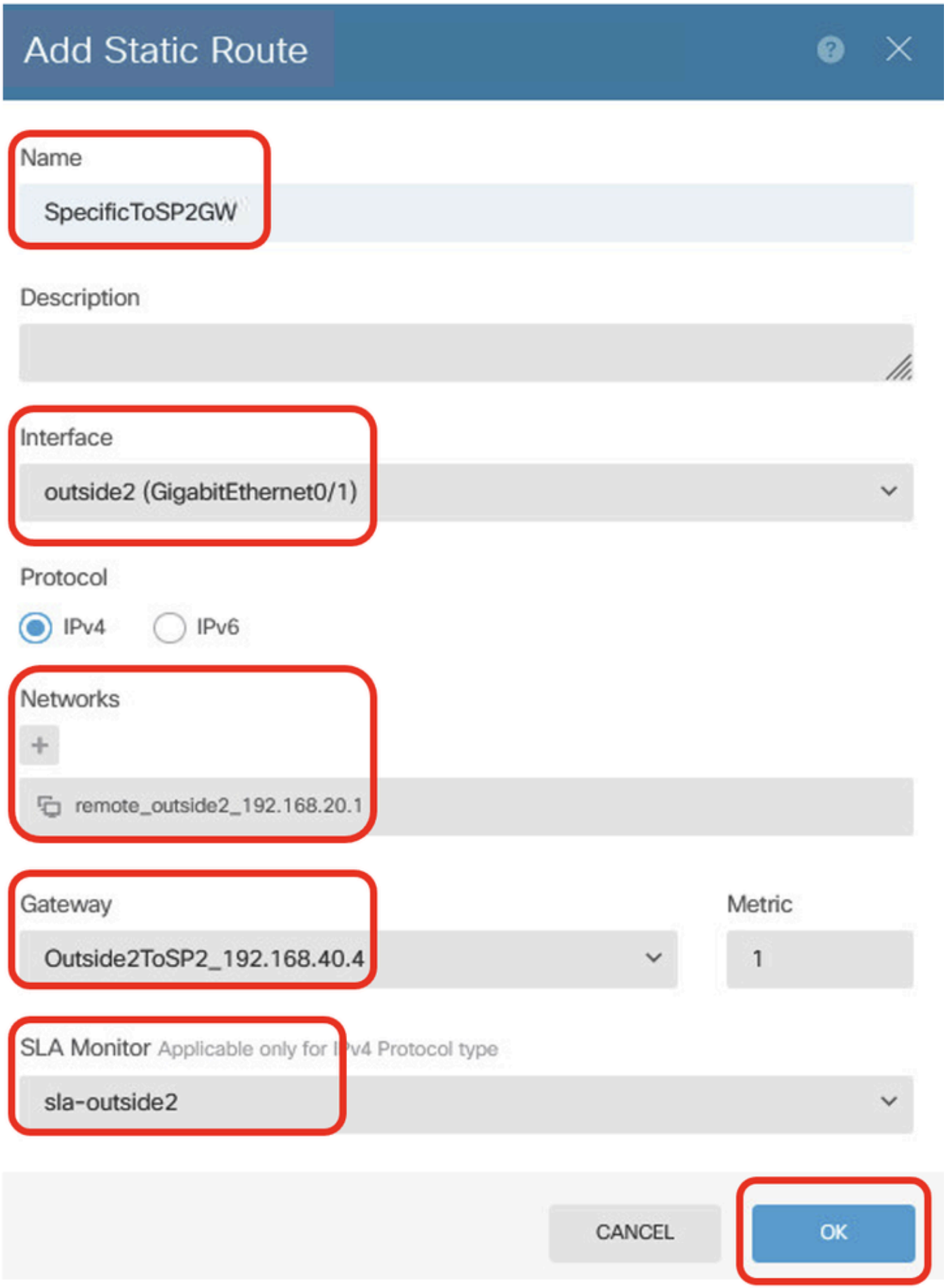
- Name: StandardToSP2GW
- Schnittstelle: outside2(GigabitEthernet0/1)
- Protokolle: IPv4
- Netzwerke: any-ipv4
- Gateway: Extern2ZuSP2_192,168,40,4
- Kennzahl: 2



Site1FTD_Create_StaticRoute_2

Schritt 23.3. Erstellen Sie eine statische Route für den Zielverkehr zu einer externen IP-Adresse2 des Peer-Site2 FTD über ein ISP2-Gateway mit SLA-Überwachung, die für die Einrichtung eines VPN mit einer externen IP-Adresse2 des Peer-Site2 FTD verwendet wird. Geben Sie die erforderlichen Informationen an. Klicken Sie zum Speichern auf OK.

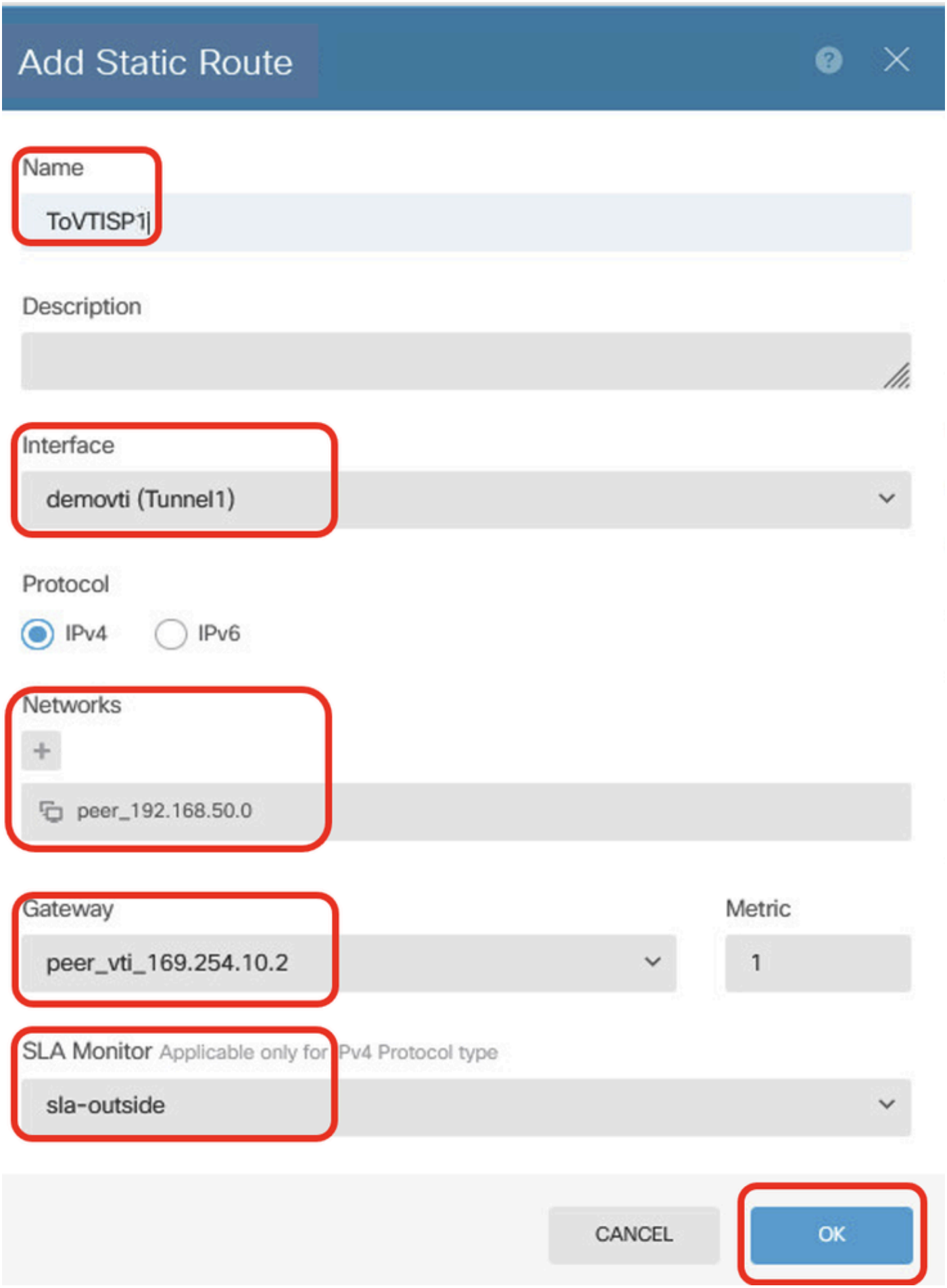
- Name: SpezifischToSP2GW
- Schnittstelle: outside2(GigabitEthernet0/1)
- Protokolle: IPv4
- Netzwerke: remote_outside2_192.168.20.1
- Gateway: Extern2ZuSP2_192,168,40,4
- Kennzahl: 1
- SLA-Monitor: sla-extern2



Site1FTD_Create_StaticRoute_3

Schritt 23.4. Erstellen Sie eine statische Route für den Zieldatenverkehr zum internen Netzwerk des Peer-Standorts 2 FTD über den Peer-VTI-Tunnel 1 von Site 2 FTD als Gateway, mit SLA-Überwachung für die Verschlüsselung des Client-Datenverkehrs über Tunnel 1. Wenn das ISP1-Gateway eine Unterbrechung erfährt, wechselt der VPN-Datenverkehr zum VTI-Tunnel 2 von ISP2. Sobald ISP1 wiederhergestellt ist, wird der Datenverkehr zum VTI-Tunnel zurückgeleitet 1 von ISP1. Geben Sie die erforderlichen Informationen ein. Klicken Sie zum Speichern auf OK.

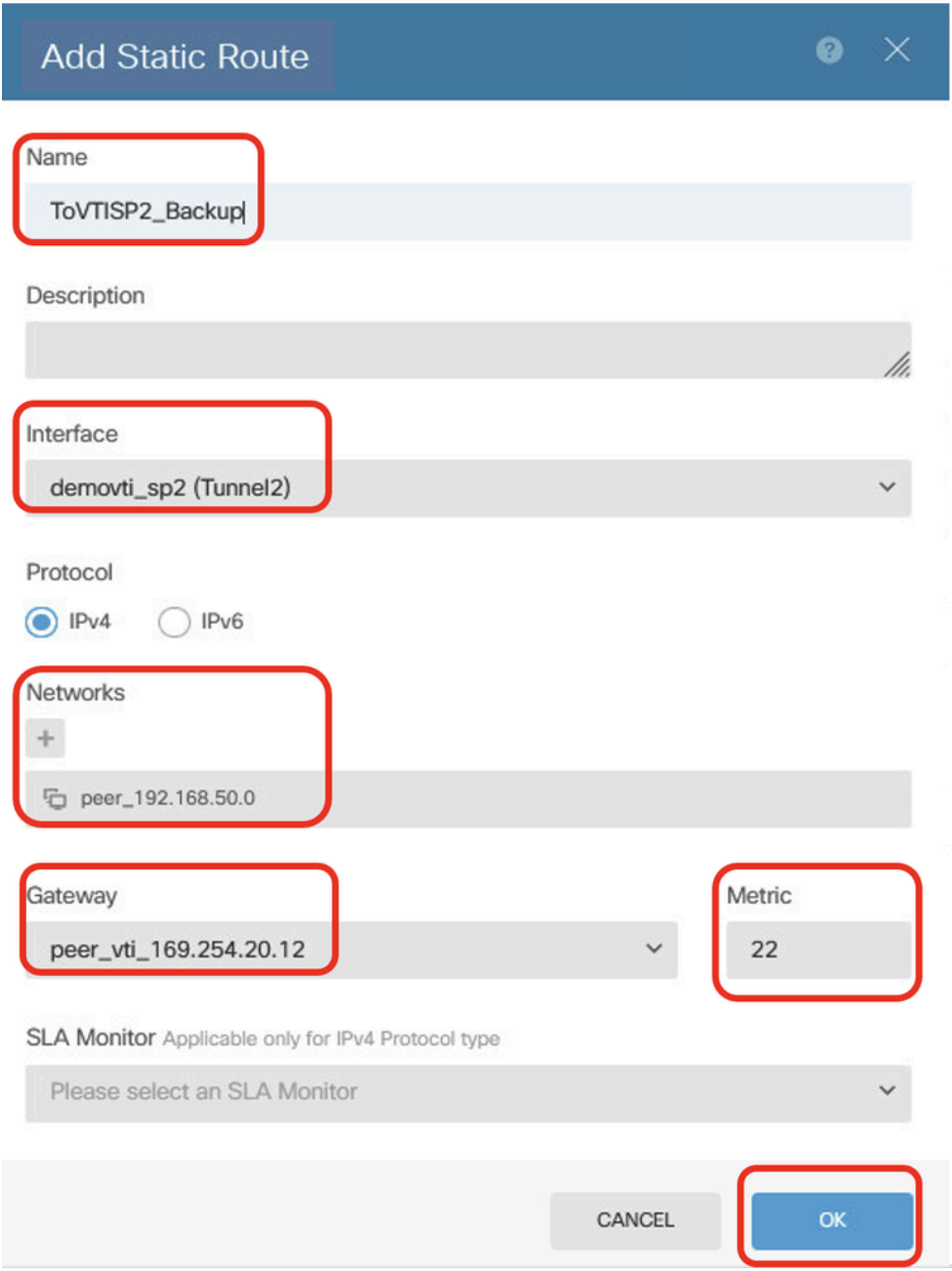
- Name: AnVTISP1
- Schnittstelle: demovti(Tunnel1)
- Protokolle: IPv4
- Netzwerke: peer_192,168,50,0
- Gateway: peer_vti_169.254.10.2
- Kennzahl: 1
- SLA-Monitor: sla-extern



Site1FTD_Create_StaticRoute_4

Schritt 23.5. Erstellen Sie eine statische Backup-Route für den Zielverkehr zum internen Netzwerk des Peer-Standorts 2 FTD über den Peer-VTI-Tunnel 2 von Site 2 FTD als Gateway, der für die Verschlüsselung des Client-Verkehrs über Tunnel 2 verwendet wird. Legen Sie den Wert für die Metrik höher als 1 fest. In diesem Beispiel ist die Metrik 22. Geben Sie die erforderlichen Informationen an. Klicken Sie zum Speichern auf OK.

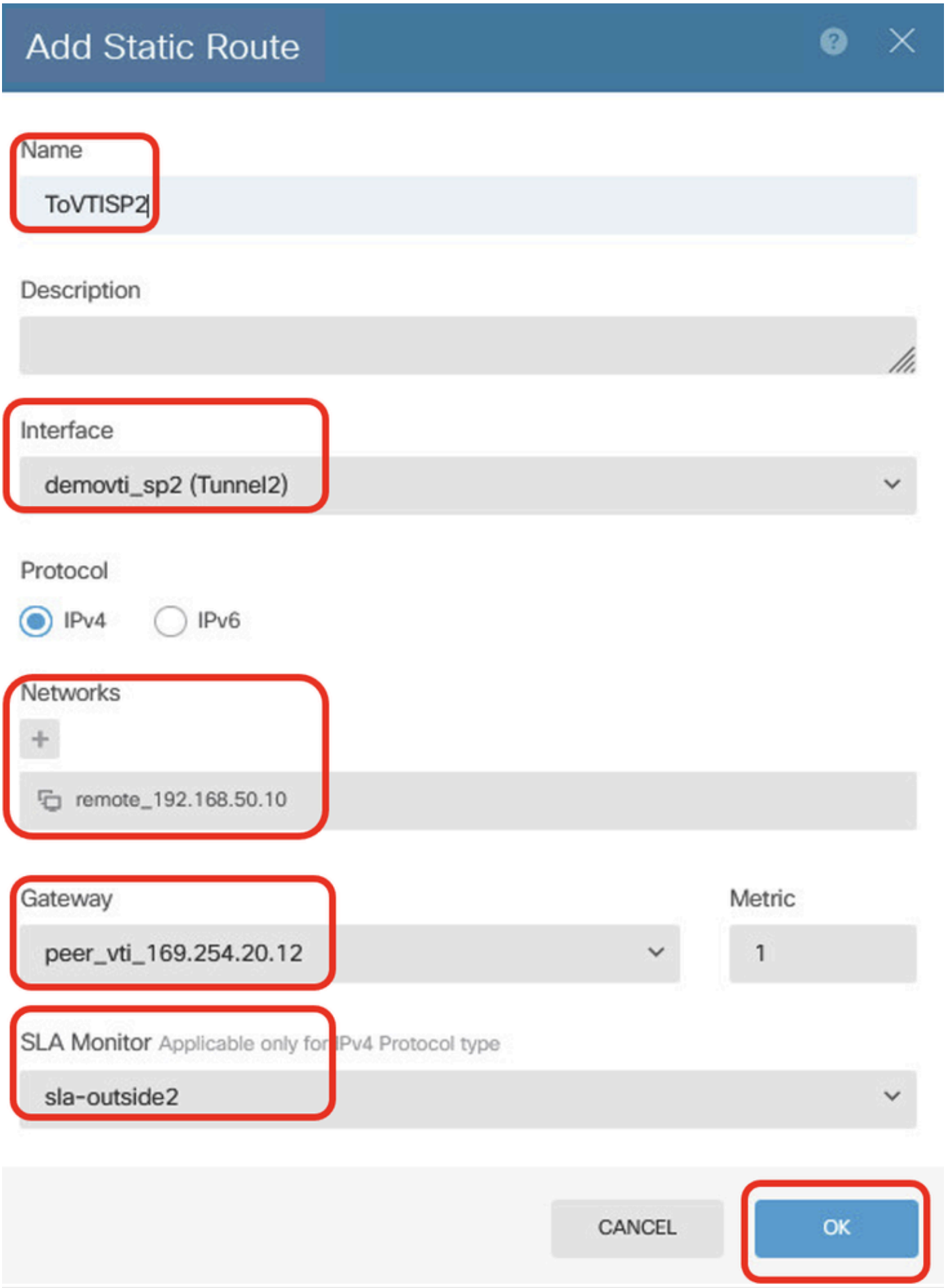
- Name: ToVTISP2_Backup
- Schnittstelle: demovti_sp2 (Tunnel2)
- Protokolle: IPv4
- Netzwerke: peer_192,168,50,0
- Gateway: peer_vti_169,254.20,12
- Kennzahl: 22



Site1FTD_Create_StaticRoute_5

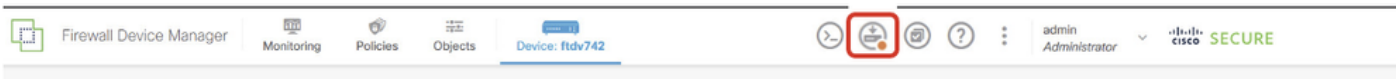
Schritt 23.6: Erstellen einer statischen Route für PBR-Datenverkehr Zieldatenverkehr zu Site2 Client2 über Peer-VTI-Tunnel 2 von Site2 FTD als Gateway mit SLA-Überwachung. Geben Sie die erforderlichen Informationen an. Klicken Sie zum Speichern auf OK.

- Name: AnVTISP2
- Schnittstelle: demovti_sp2 (Tunnel2)
- Protokolle: IPv4
- Netzwerke: remote_192,168.50,10
- Gateway: peer_vti_169,254.20,12
- Kennzahl: 1
- SLA-Monitor: sla-extern2



Site1FTD_Create_StaticRoute_6

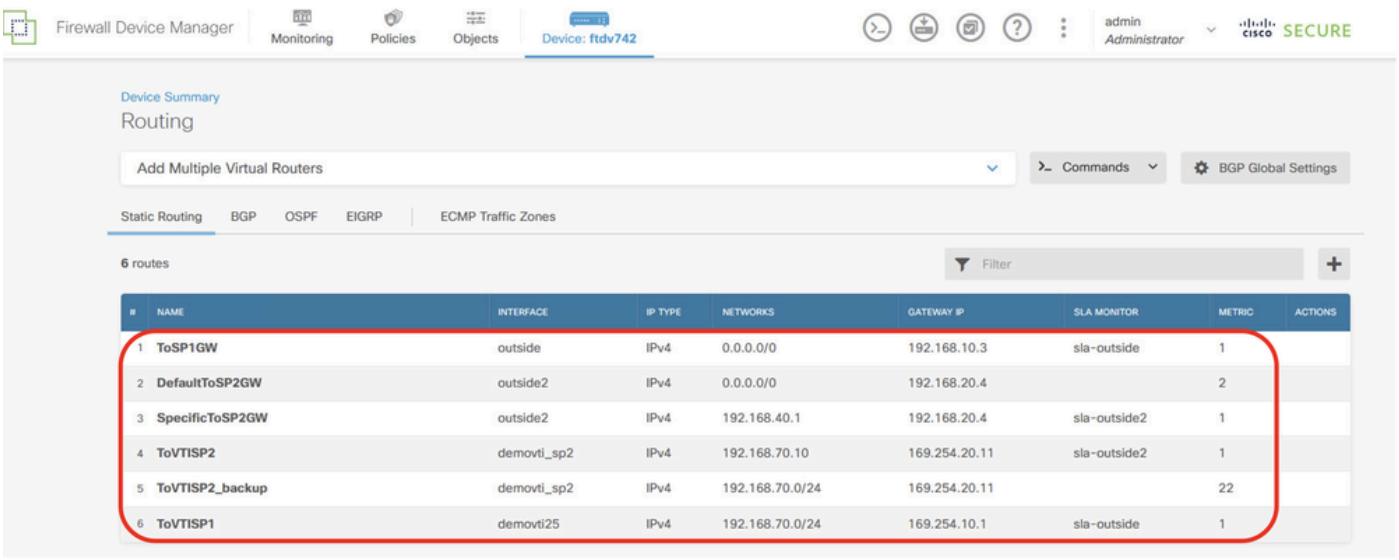
Schritt 24: Bereitstellen der Konfigurationsänderungen



Site1FTD_Deployment_Changes

Statische FTD-Routenkonfiguration für Standort 2

Schritt 25: Wiederholen Sie die Schritte 22 bis 24, um eine statische Route mit den entsprechenden Parametern für Site2 FTD zu erstellen.



Site2FTD_Create_StaticRoute

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert. Navigieren Sie über die Konsole oder SSH zur CLI von Site1 FTD und Site2 FTD.

Sowohl ISP1 als auch ISP2 funktionieren ordnungsgemäß

VPN

```
//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1072332533 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1045734377 192.168.40.1/500                               192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d
```

```
// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
499259237 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607
```

Routing

```
// Site1 FTD:

ftdv742# 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 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside




// Site2 FTD:

ftdv742# 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA-Überwachung

```
// Site1 FTD:
```

```
ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:


ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

```
Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

// Site2 FTD:

```
ftdv742#  show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
```

```
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100

Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Ping-Test

Szenario 1. Standort1 Client1 ping Standort2 Client1.

Überprüfen Sie vor dem Ping die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD.

In diesem Beispiel zeigt Tunnel1 1.497 Pakete für die Kapselung und 1.498 Pakete für die Kapselung.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
```

```
      #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
      #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 erfolgreich.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

Überprüfen Sie die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD after ping successfully.

In diesem Beispiel zeigt Tunnel 1 1.502 Pakete für die Kapselung und 1.503 Pakete für die Entkapselung, wobei beide Zähler um 5 Pakete ansteigen und somit den 5 Ping-Echo-Anforderungen entsprechen. Dies weist darauf hin, dass Pings von Site1 Client1 an Site2 Client1 über ISP1 Tunnel 1 geroutet werden. Tunnel 2 zeigt keine Erhöhung der Kapselungs- oder Entkapselungszähler an und bestätigt, dass es nicht für diesen Datenverkehr verwendet wird.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
      #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Szenario 2. Site1 Client2 pingt Site2 Client2.

Überprüfen Sie vor dem Ping die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD.

In diesem Beispiel zeigt Tunnel2 21 Pakete für die Kapselung und 20 Pakete für die Kapselung an.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2 pingt Site2 Client2 erfolgreich.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/39/87 ms
```

Überprüfen Sie die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD after ping successfully.

In diesem Beispiel zeigt Tunnel 2 26 Pakete für die Kapselung und 25 Pakete für die Entkapselung an, wobei beide Zähler um 5 Pakete ansteigen und somit den 5 Ping-Echo-Anforderungen entsprechen. Dies zeigt an, dass Pings von Site1 Client2 an Site2 Client2 über ISP2 Tunnel 2 geroutet werden. Tunnel 1 zeigt keine Erhöhung der Kapselungs- oder Entkapselungszähler an und bestätigt, dass er nicht für diesen Datenverkehr verwendet wird.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Unterbrechung bei ISP1, während ISP2 einwandfrei funktioniert

In diesem Beispiel wird die Schnittstelle E0/1 auf ISP1 manuell heruntergefahren, um zu simulieren, dass auf ISP1 eine Unterbrechung auftritt.

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

Der Tunnel1 ging unter. Nur Tunnel2 ist mit IKEV2 SA aktiv.

```
// Site1 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.1, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.30.1
    Destination IP address: 192.168.10.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d


ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
1045734377 192.168.40.1/500                                      192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.2, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.10.1
    Destination IP address: 192.168.30.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#

ftdv742# show crypto ikev2 sa
```

```
IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500                      G
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

Routing

In der Routing-Tabelle werden die Backup-Routen übernommen.

```
// Site1 FTD:

ftdv742# 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
Gateway of last resort is 192.168.40.4 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

ftdv742# 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA-Überwachung

Auf Site1 FTD zeigt der SLA-Monitor eine Zeitüberschreitung nach Nummer 855903900 (Zieladresse ist 192.168.30.3) für ISP1 an.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000

Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
```

```
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

ftdv742# show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Down
  7 changes, last change 00:11:03
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Up
  4 changes, last change 13:15:11
  Latest operation return code: OK
  Latest RTT (millisecs) 140
  Tracked by:
    STATIC-IP-ROUTING 0
```

Ping-Test

Überprüfen Sie vor dem Ping die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD.

In diesem Beispiel zeigt Tunnel2 36 Pakete für die Kapselung und 35 Pakete für die Kapselung.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
      #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 erfolgreich.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

Site1 Client2 pingt Site2 Client2 erfolgreich.

```
Site1_Client2#ping 192.168.50.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/56/87 ms
```

Überprüfen Sie die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD after ping successfully.

In diesem Beispiel zeigt Tunnel 2 46 Pakete für die Kapselung und 45 Pakete für die Entkapselung, wobei beide Zähler um 10 Pakete ansteigen und somit den 10 Ping-Echo-Anfragen entsprechen. Dies zeigt an, dass die Ping-Pakete über ISP2 Tunnel 2 geroutet werden.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
      #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Unterbrechung bei ISP2, während ISP1 einwandfrei funktioniert

In diesem Beispiel wird die Schnittstelle E0/1 auf ISP2 manuell heruntergefahren, um zu simulieren, dass auf ISP2 eine Unterbrechung auftritt.

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

Der Tunnel2 ging unter. Nur Tunnel1 ist mit IKEV2 SA aktiv.

```
// Site1 FTD:

ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.40.1
```

```
    Destination IP address: 192.168.20.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1375077093 192.168.30.1/500                               192.168.10.1/500                    (
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc




// Site2 FTD:

ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.12, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.20.1
    Destination IP address: 192.168.40.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1025640731 192.168.10.1/500                               192.168.30.1/500                    (
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

Routing

In der Routing-Tabelle verschwand die ISP2-bezogene Route für den PBR-Verkehr.

```
// Site1 FTD:

ftdv742# 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 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 FTD:

ftdv742# 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

SLA-Überwachung

Auf Site1 FTD zeigt der SLA-Monitor eine Zeitüberschreitung nach Nummer 188426425 (Zieladresse ist 192.168.40.4) für ISP2 an.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
```

```
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100


ftdv742#  show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Up
  8 changes, last change 00:14:37
  Latest operation return code: OK
  Latest RTT (millisecs) 60
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Down
  5 changes, last change 00:09:30
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

Ping-Test

Überprüfen Sie vor dem Ping die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD.

In diesem Beispiel zeigt Tunnel 1 74 Pakete für die Kapselung und 73 Pakete für die Kapselung.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
      #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 erfolgreich.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

Site1 Client2 pingt Site2 Client2 erfolgreich.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/58/143 ms
```

Überprüfen Sie die Zähler von show crypto ipsec sa | inc interface:|encap|decap on Site1 FTD after ping successfully.

In diesem Beispiel zeigt Tunnel 1 84 Pakete für die Kapselung und 83 Pakete für die Entkapselung an, wobei beide Zähler um 10 Pakete ansteigen und somit den 10 Ping-Echo-Anfragen entsprechen. Dies zeigt an, dass die Ping-Pakete über ISP1 Tunnel 1 geroutet werden.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
      #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Sie können diese Befehle zum Debuggen verwenden, um den VPN-Abschnitt zu beheben.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

Sie können diese Befehle verwenden, um Fehler im PBR-Abschnitt zu beheben.

```
debug policy-route
```

Mit diesen Befehlen können Sie Fehler im Abschnitt SLA Monitor beheben.

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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.