Konfiguration von BGP über routenbasiertes VPN auf von FDM verwaltetem FTD

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration des BGP über ein routenbasiertes Site-to-Site-VPN auf dem vom FirePOWER Device Manager (FDM) verwalteten FTDv beschrieben.

Voraussetzungen

Anforderungen

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

- Grundlegendes Verständnis von VPN
- BGP-Konfigurationen auf FTDv
- Erfahrung mit FDM

Verwendete Komponenten

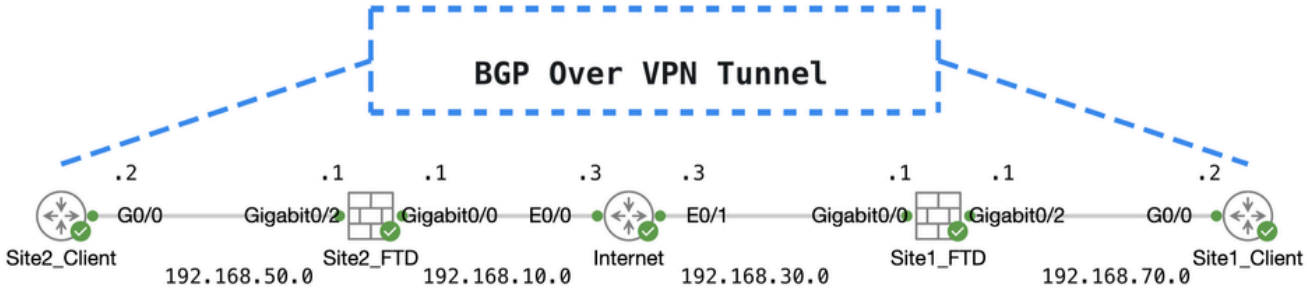
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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.

Konfigurieren

Netzwerkdiagramm



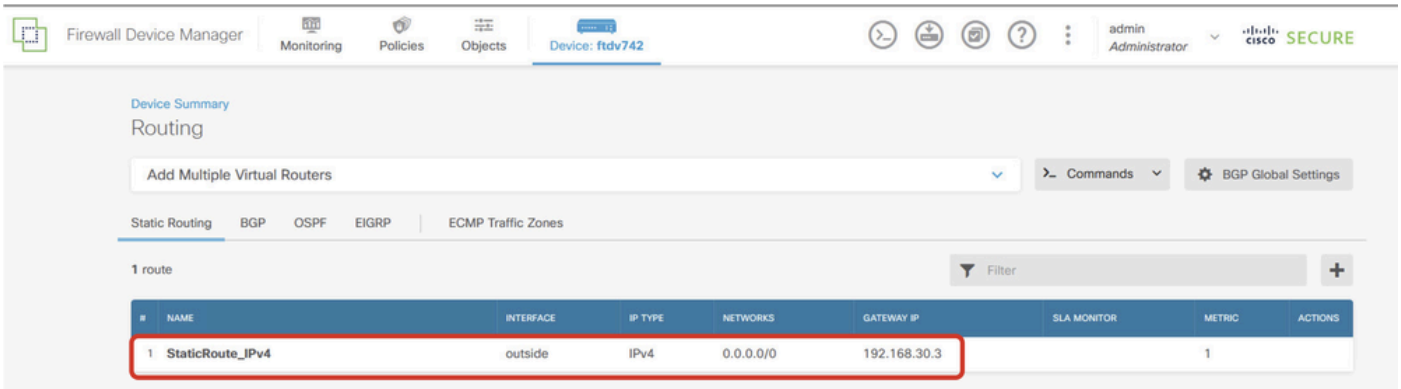
Topo

VPN-Konfigurationen

Schritt 1: Stellen Sie sicher, dass die IP-Verbindungen zwischen den Knoten betriebsbereit und stabil sind. Die Smart-Lizenz auf FDM wurde erfolgreich beim Smart-Konto registriert.

Schritt 2: Das Gateway des Site1 Client wird mit der internen IP-Adresse von Site1 FTD (192.168.70.1) konfiguriert. Das Gateway des Site2-Clients wird mit der internen IP-Adresse von Site2 FTD (192.168.50.1) konfiguriert. Stellen Sie außerdem sicher, dass die Standardroute auf beiden FTDs nach der FDM-Initialisierung richtig konfiguriert ist.

Melden Sie sich bei der GUI der einzelnen FDM an. Navigieren Sie zu .Device > Routing Klicken Sie auf .View Configuration Klicken Sie auf die **Static Routing** Registerkarte, um die statische Standardroute zu überprüfen.



Standort1_FTD_Gateway

Standort2_FTD_Gateway

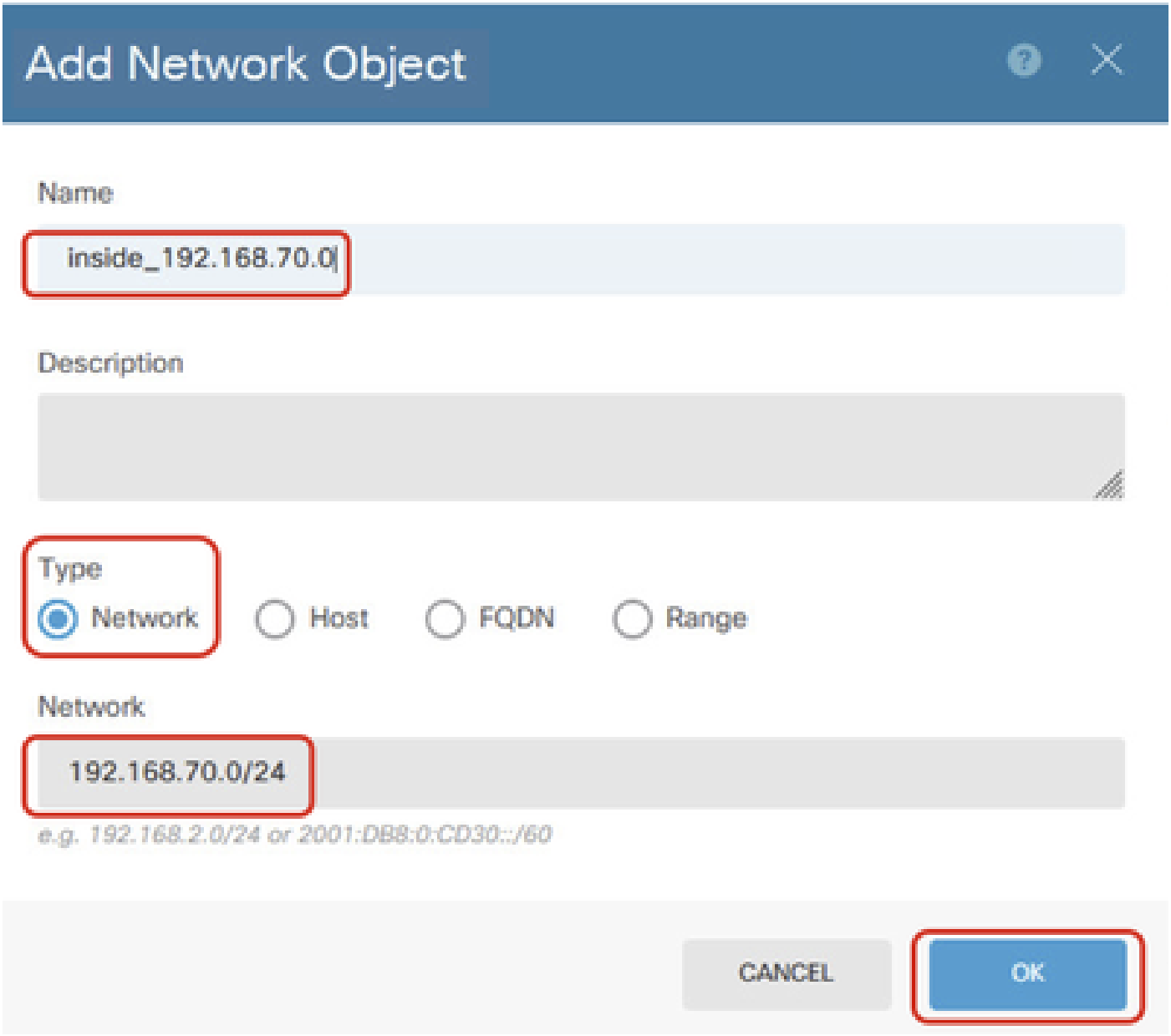
Schritt 3: Konfigurieren Sie ein route-basiertes Site-to-Site-VPN. In diesem Beispiel konfigurieren Sie zuerst Site1 FTD.

Schritt 3.1: Melden Sie sich bei der FDM-GUI von Site1 FTD an. Erstellen Sie ein neues Netzwerkobjekt für das interne Netzwerk von Site1 FTD. Navigieren Sie zu **Objects** > **Networks**, und klicken Sie auf die Schaltfläche +.

Create_Network_Object

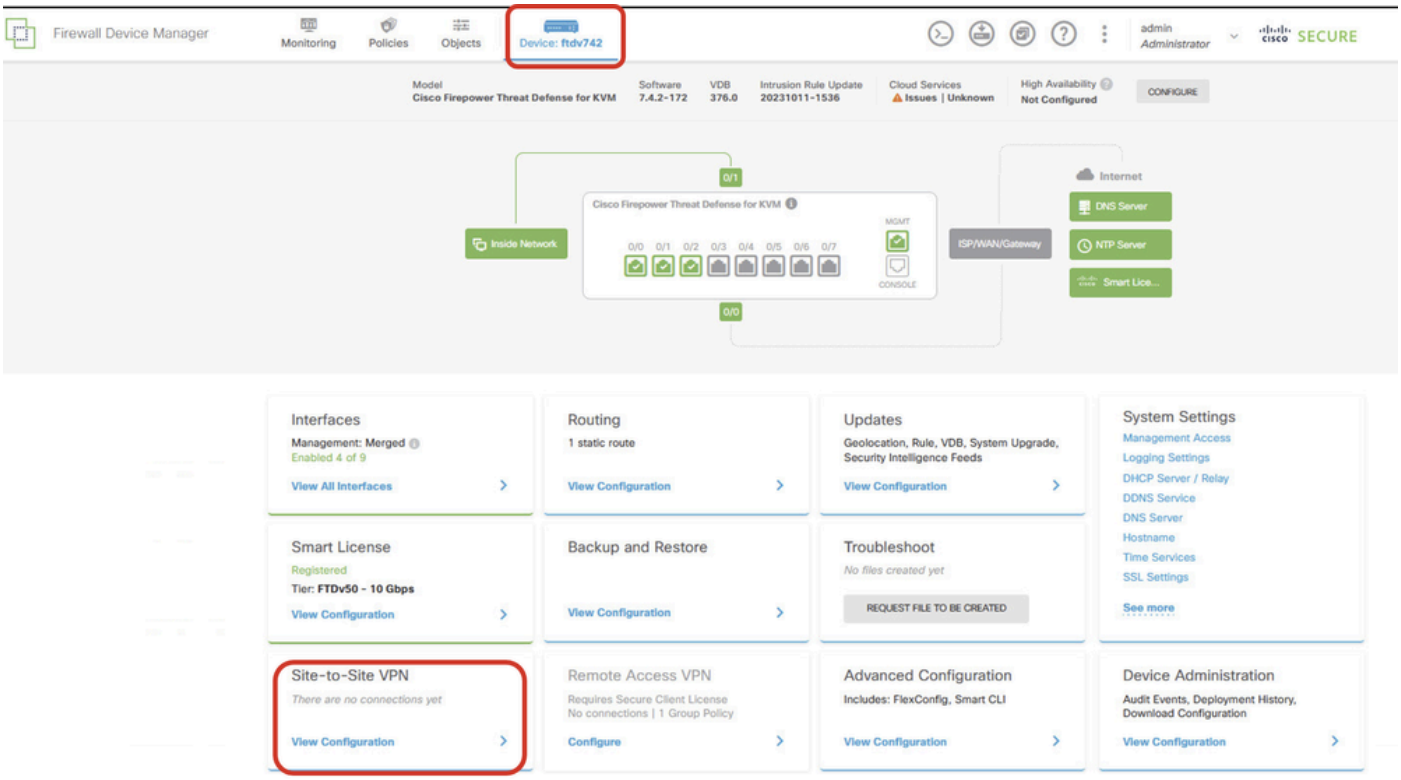
Schritt 3.2: Geben Sie die erforderlichen Informationen ein. Klicken Sie auf die OK Schaltfläche.

- Name: inside_192.168.70.0
- Typ: Netzwerk
- Netzwerk: 192.168.70.0/24



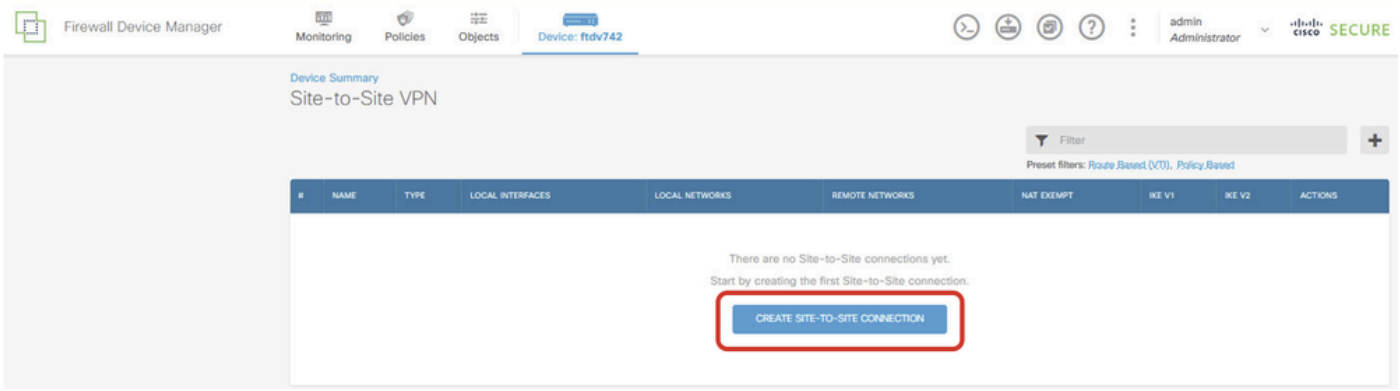
Site1_Inside_Netzwerk

Schritt 3.3: Navigieren Sie zu **.Device > Site-to-Site VPN** Klicken Sie auf **.View Configuration**



Standortübergreifendes VPN anzeigen

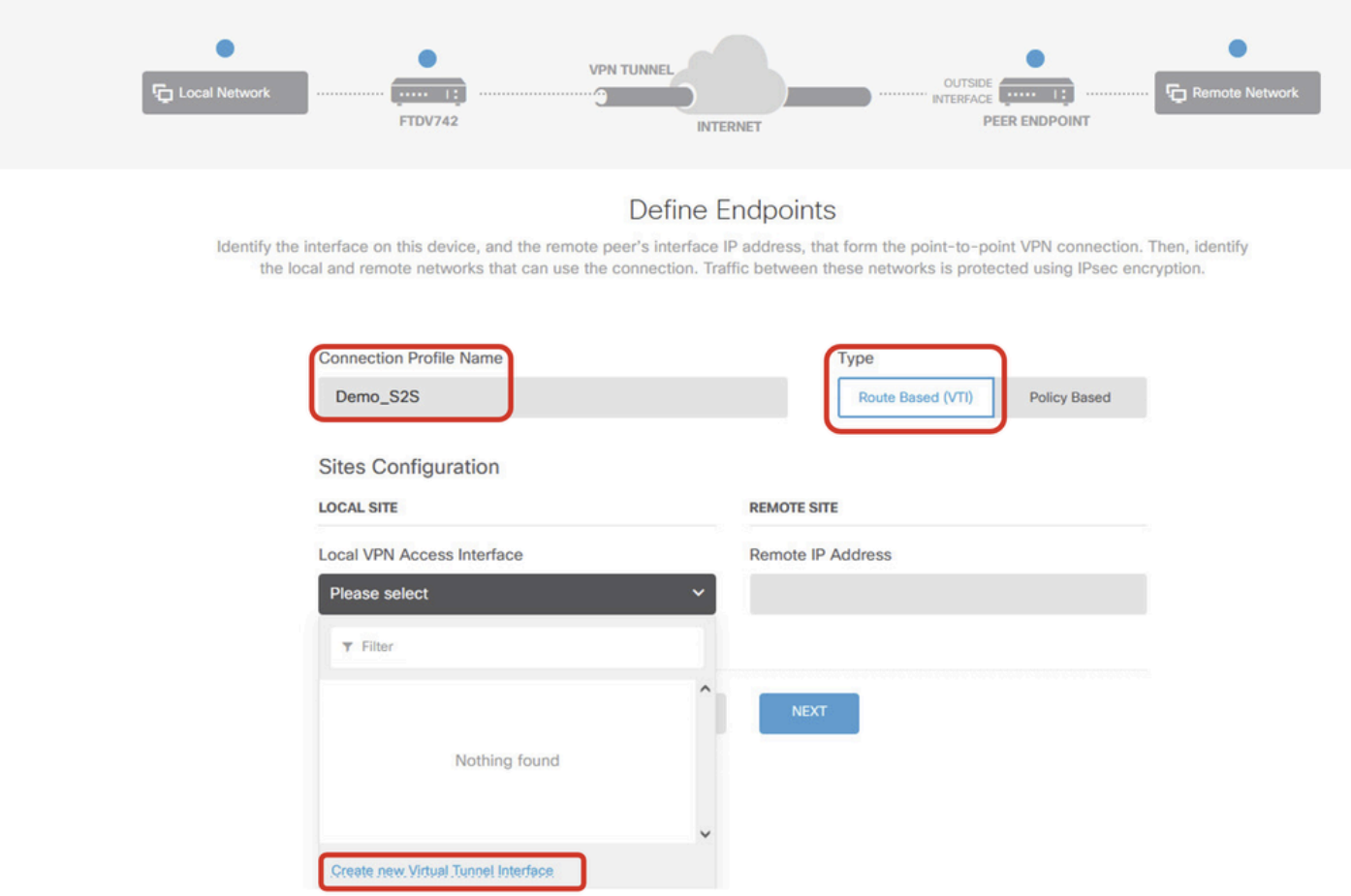
Schritt 3.4: Erstellen Sie ein neues Site-to-Site-VPN. Klicken Sie auf .**CREATE SITE-TO-SITE CONNECTION**



Site-to-Site_Verbindung erstellen

Schritt 3.5: Geben Sie die erforderlichen Informationen ein.

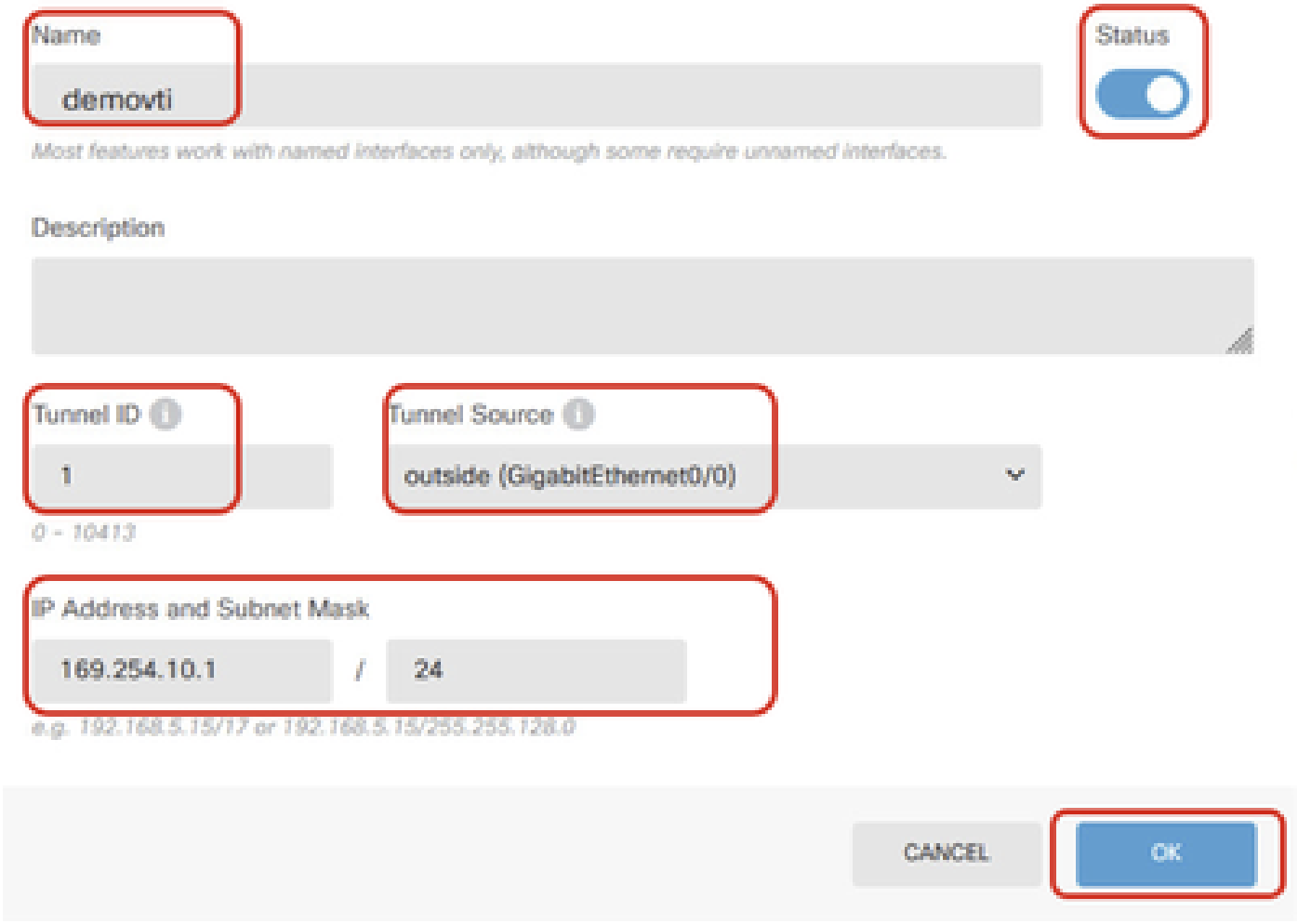
- Verbindungsprofilname: Demo_S2S
- Typ: routenbasiert (VTI)
- Local VPN Access Interface (Lokale VPN-Zugriffsschnittstelle): Klicken Sie auf die Dropdown-Liste, und klicken Sie dann auf **Create new Virtual Tunnel Interface** .



Create_VTI_in_VPN_Wizard

Schritt 3.6: Stellen Sie die erforderlichen Informationen bereit, um einen neuen VTI zu erstellen. Klicken Sie auf die Schaltfläche OK.

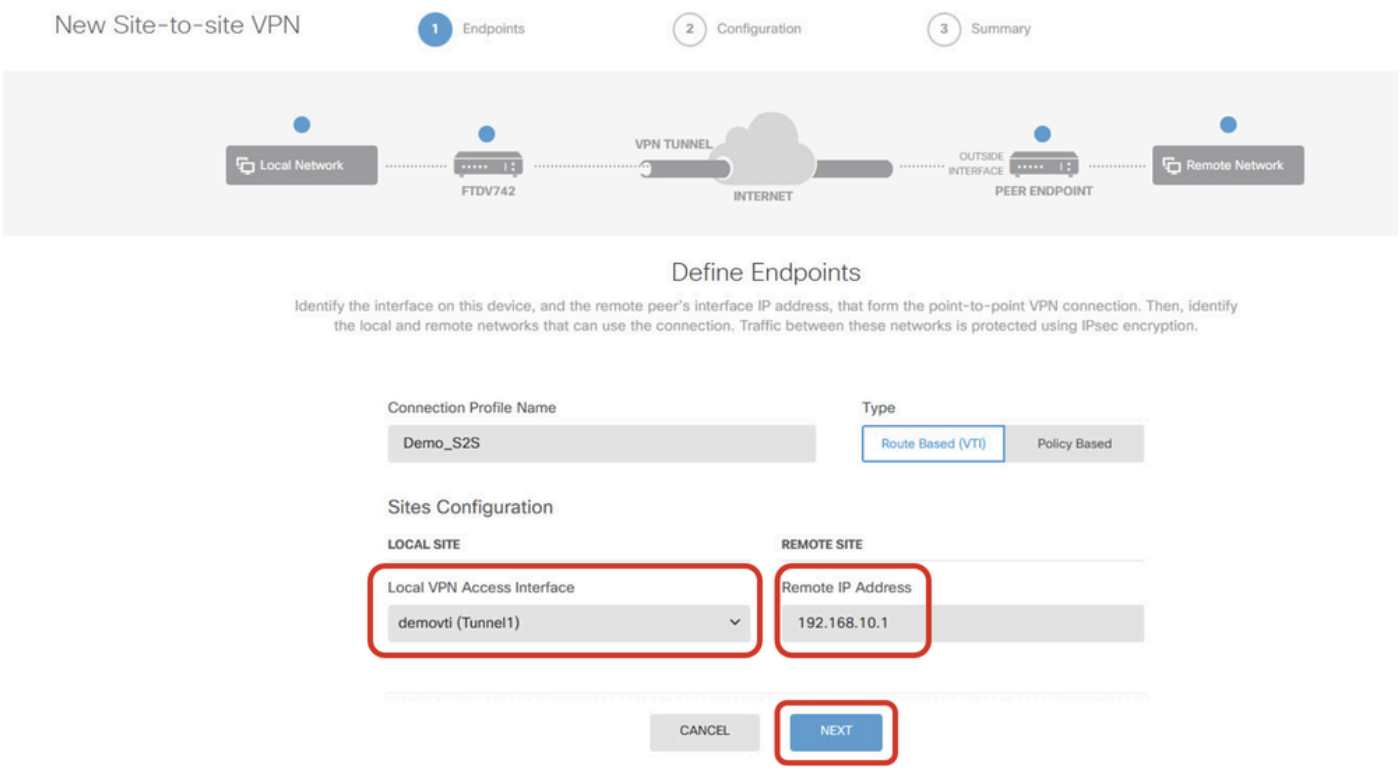
- Name: demovti
- Tunnel-ID: 1
- Tunnelquelle: außen (GigabitEthernet0/0)
- IP-Adresse und Subnetzmaske: 169.254.10.1/24
- Status: Klicken Sie auf den Schieberegler für die Position Aktiviert.



_VTI_Details

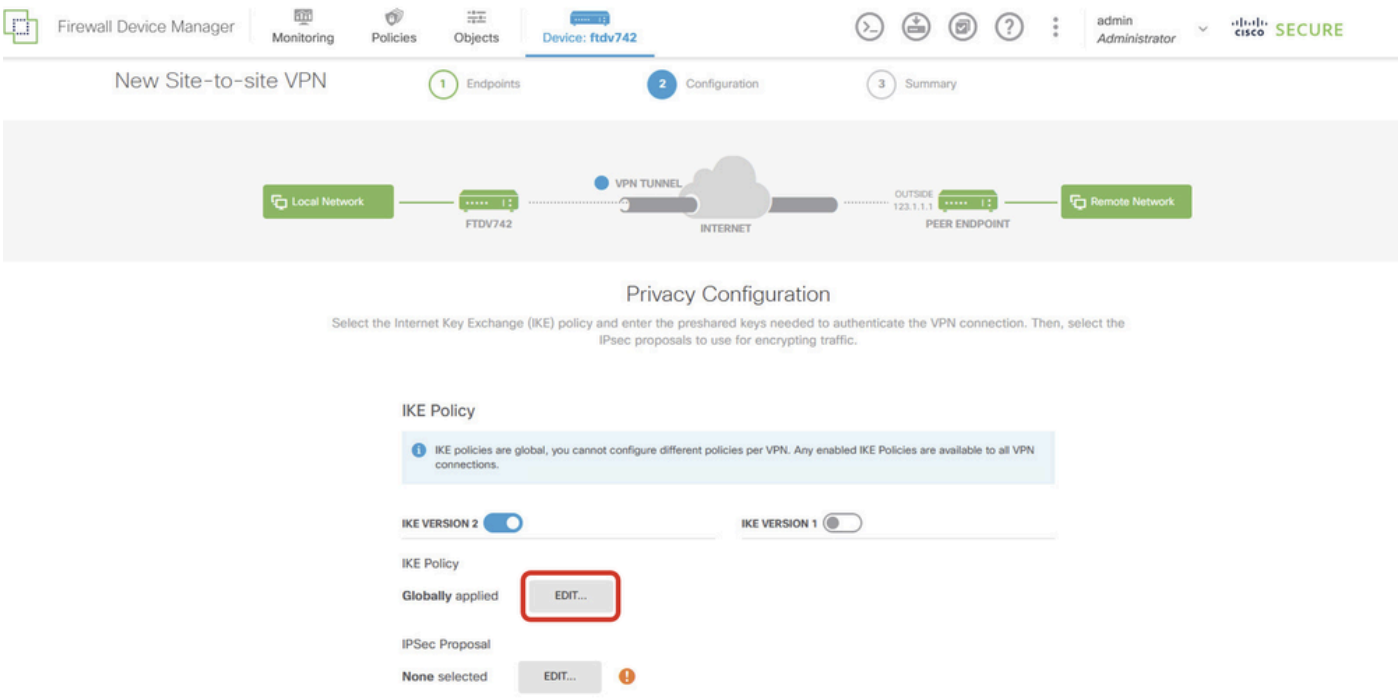
Schritt 3.7: Geben Sie weiterhin die erforderlichen Informationen ein. Klicken Sie auf die Schaltfläche WEITER.

- Schnittstelle für lokalen VPN-Zugriff: demovti (erstellt in Schritt 3.6)
- Remote-IP-Adresse: 192.168.10.1



VPN-Assistent_Endpunkte_Schritt1

Schritt 3.8: Navigieren Sie zur IKE-Richtlinie. Klicken Sie auf die Schaltfläche BEARBEITEN.



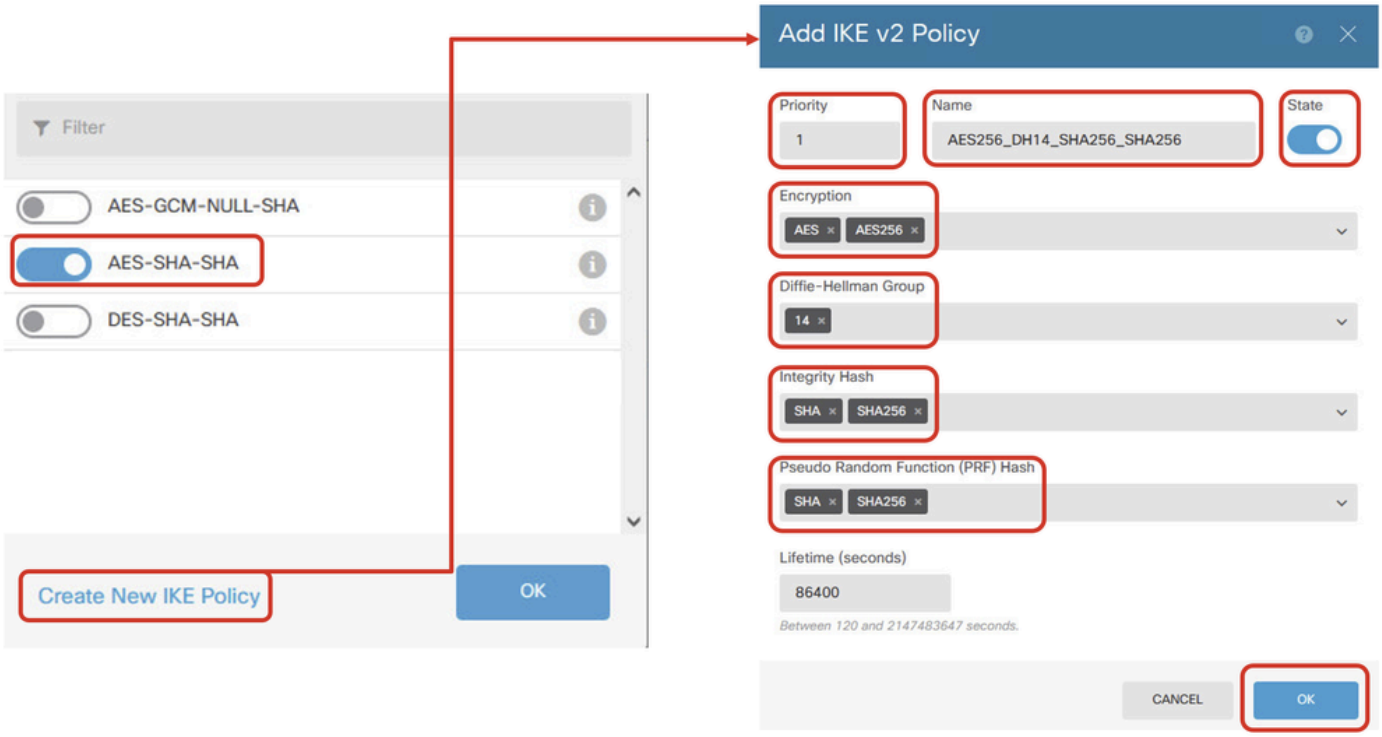
Bearbeiten_IKE_Richtlinie

Schritt 3.9: Für die IKE-Richtlinie können Sie eine vordefinierte IKE-Richtlinie verwenden oder eine neue erstellen, indem Sie auf Neue IKE-Richtlinie erstellen klicken.

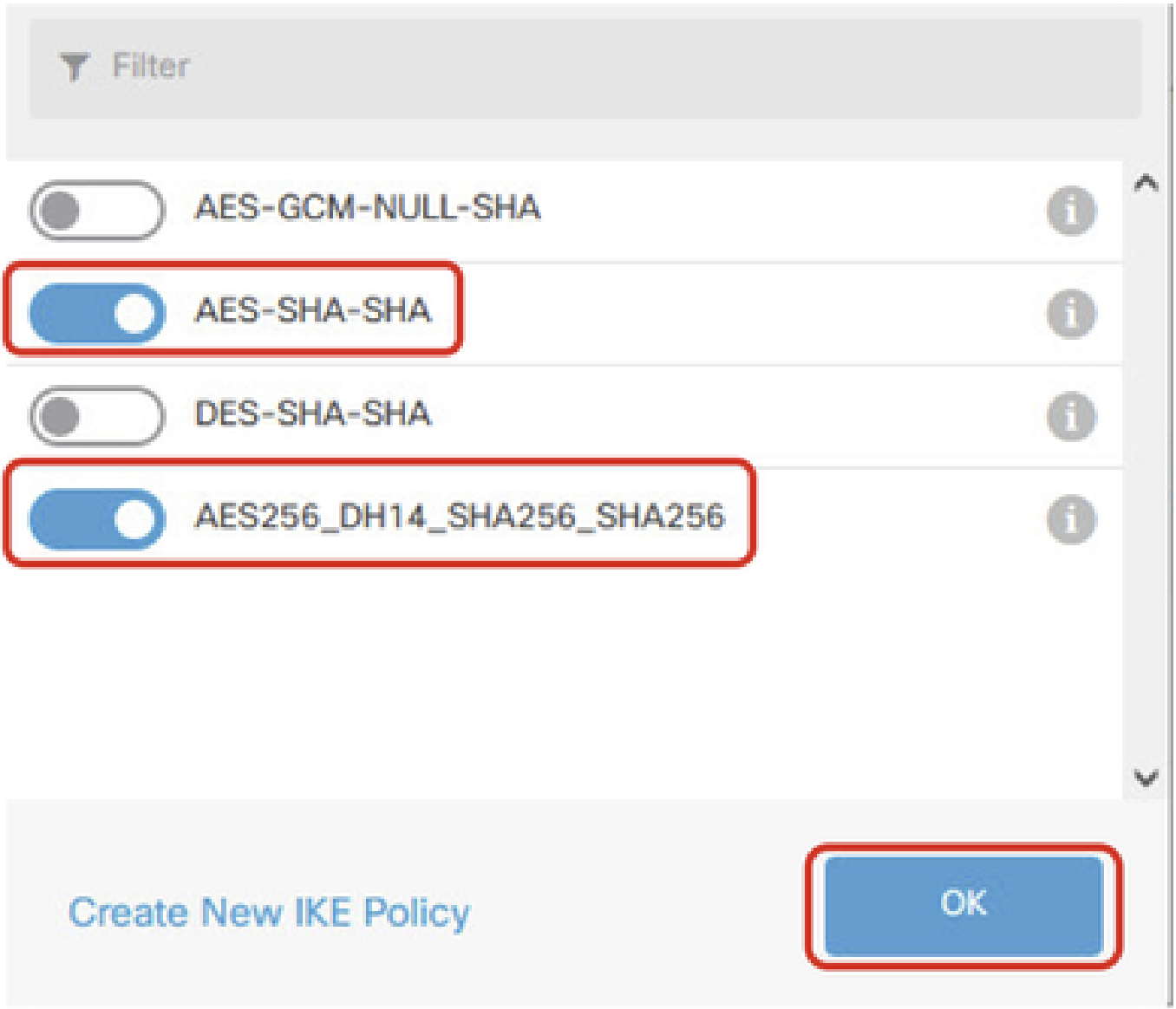
Schalten Sie in diesem Beispiel eine vorhandene IKE-Richtlinie AES-SHA-SHA um, und erstellen

Sie eine neue Richtlinie für Demozwecke. Klicken Sie auf die Schaltfläche OK, um zu speichern.

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

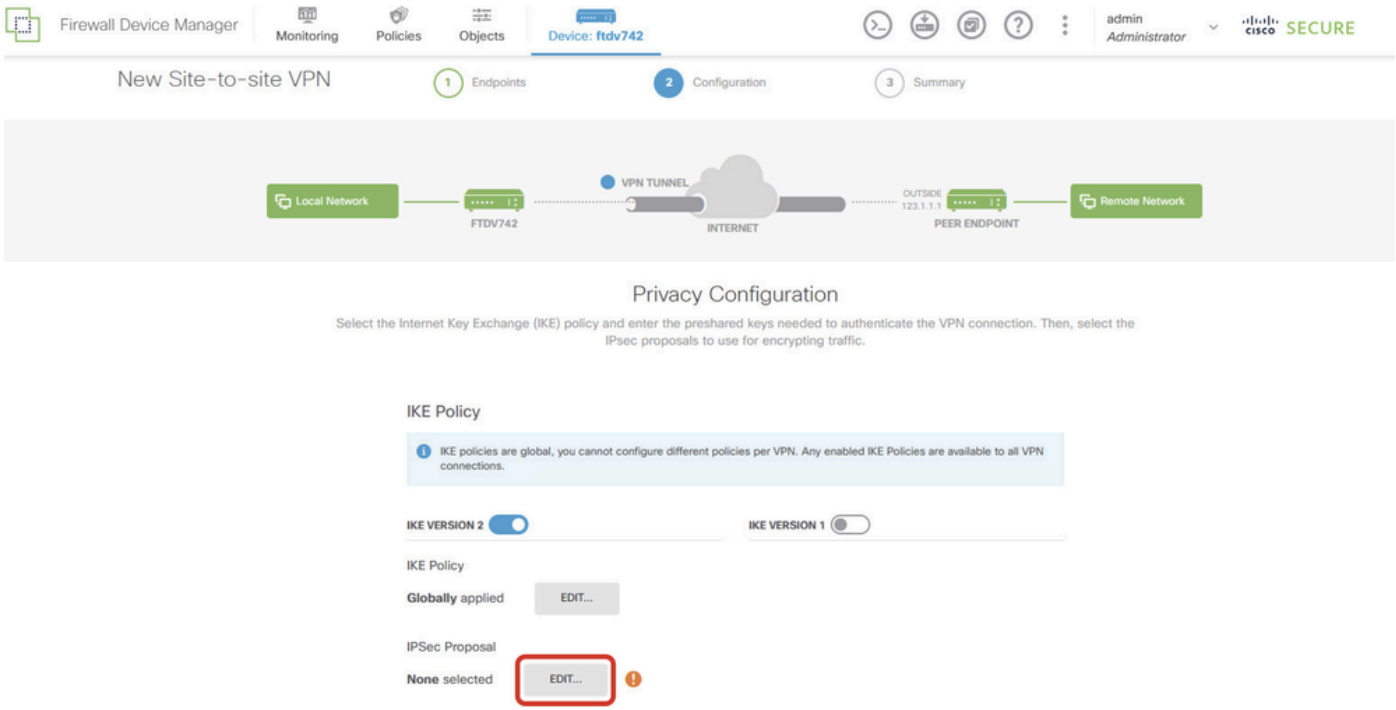


Neue_IKE_Richtlinie hinzufügen



Enable_New_IKE_Policy

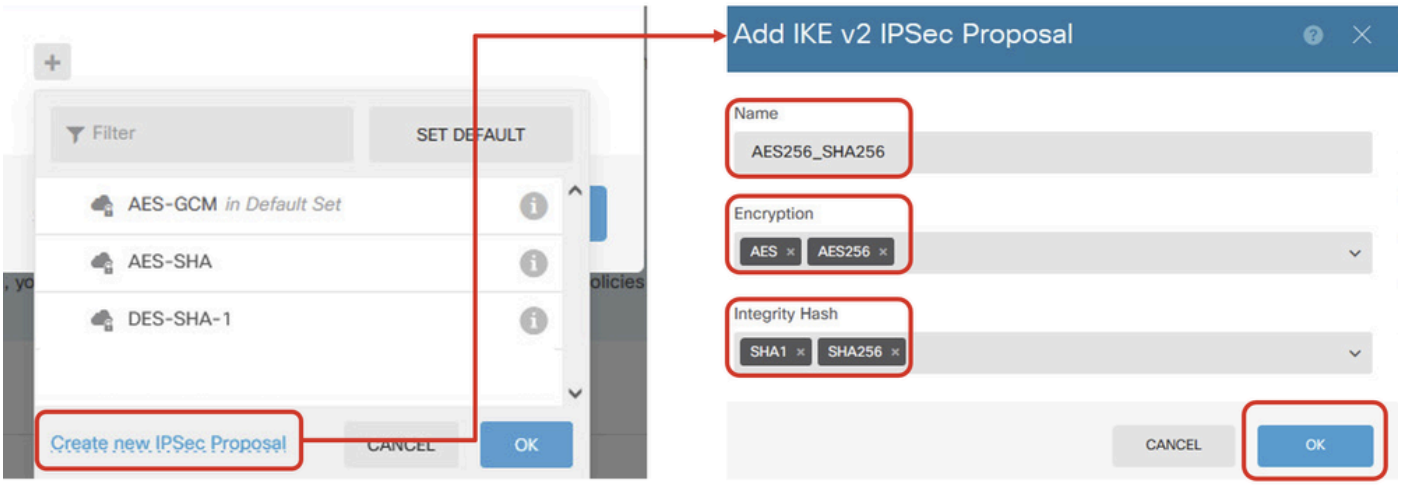
Schritt 3.10: Navigieren Sie zum IPSec-Angebot. Klicken Sie auf die Schaltfläche BEARBEITEN.



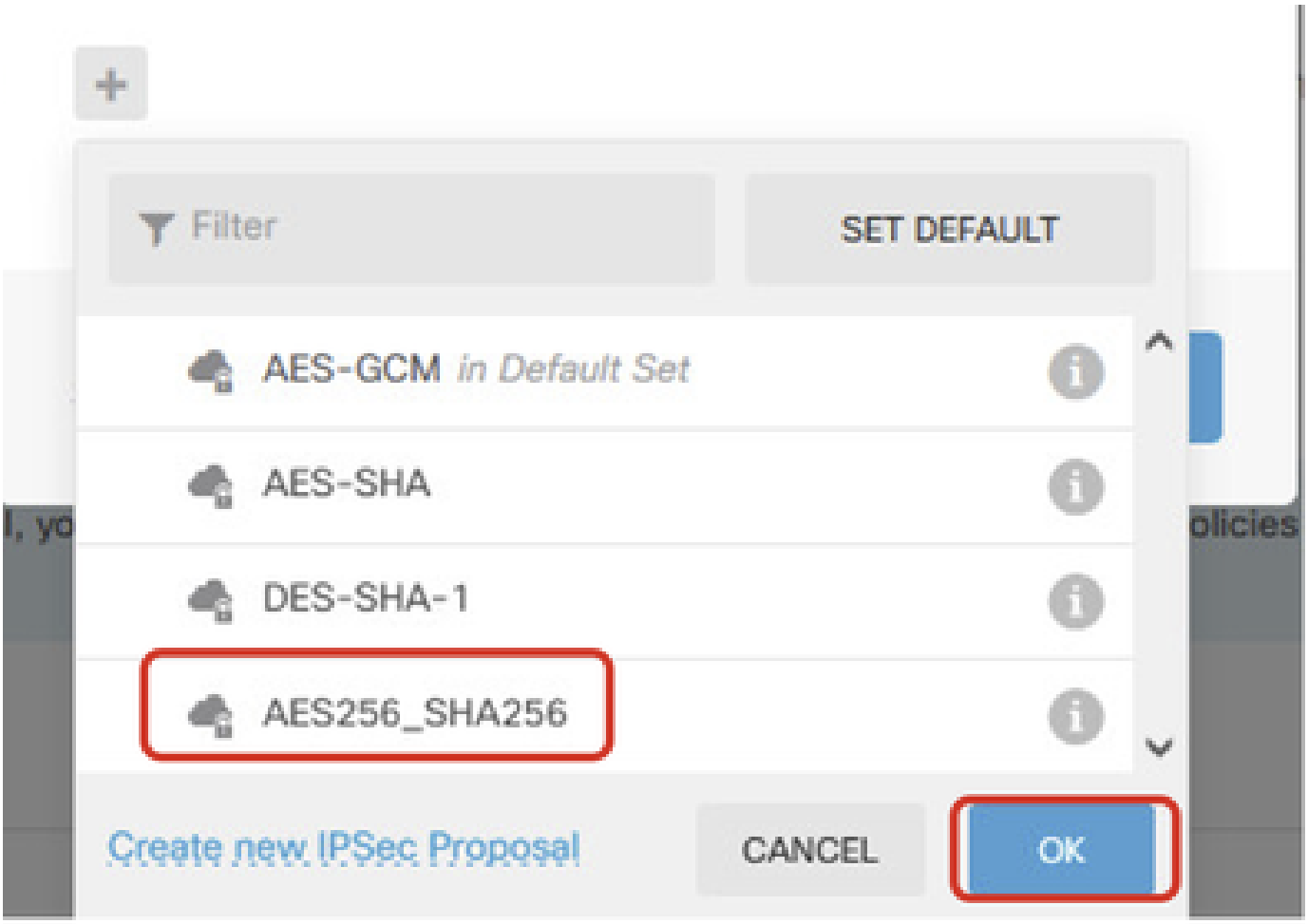
Bearbeiten_IKE_Angebot

Schritt 3.11: Für das IPSec-Angebot können Sie ein vordefiniertes verwenden oder ein neues erstellen, indem Sie auf Neues IPSec-Angebot erstellen klicken. Erstellen Sie in diesem Beispiel eine neue Anwendung für Demozwecke. Geben Sie die erforderlichen Informationen ein. Klicken Sie auf die Schaltfläche OK, um zu speichern.

- Name: AES256_SHA256
- Verschlüsselung: AES, AES256
- Integritätshash: SHA1, SHA256



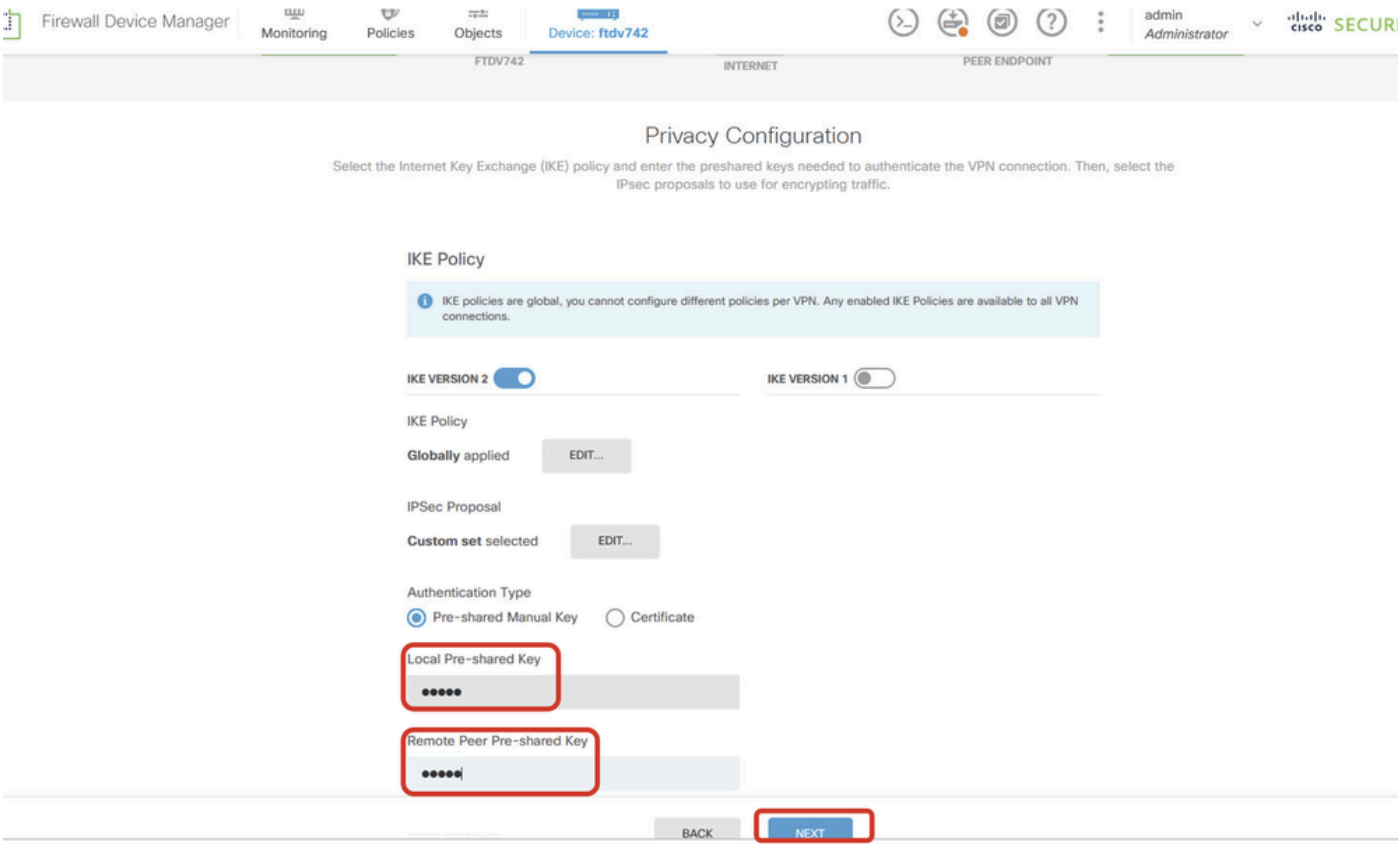
Add_New_IPSec_Proposal



Enable_New_IPSec_Proposal

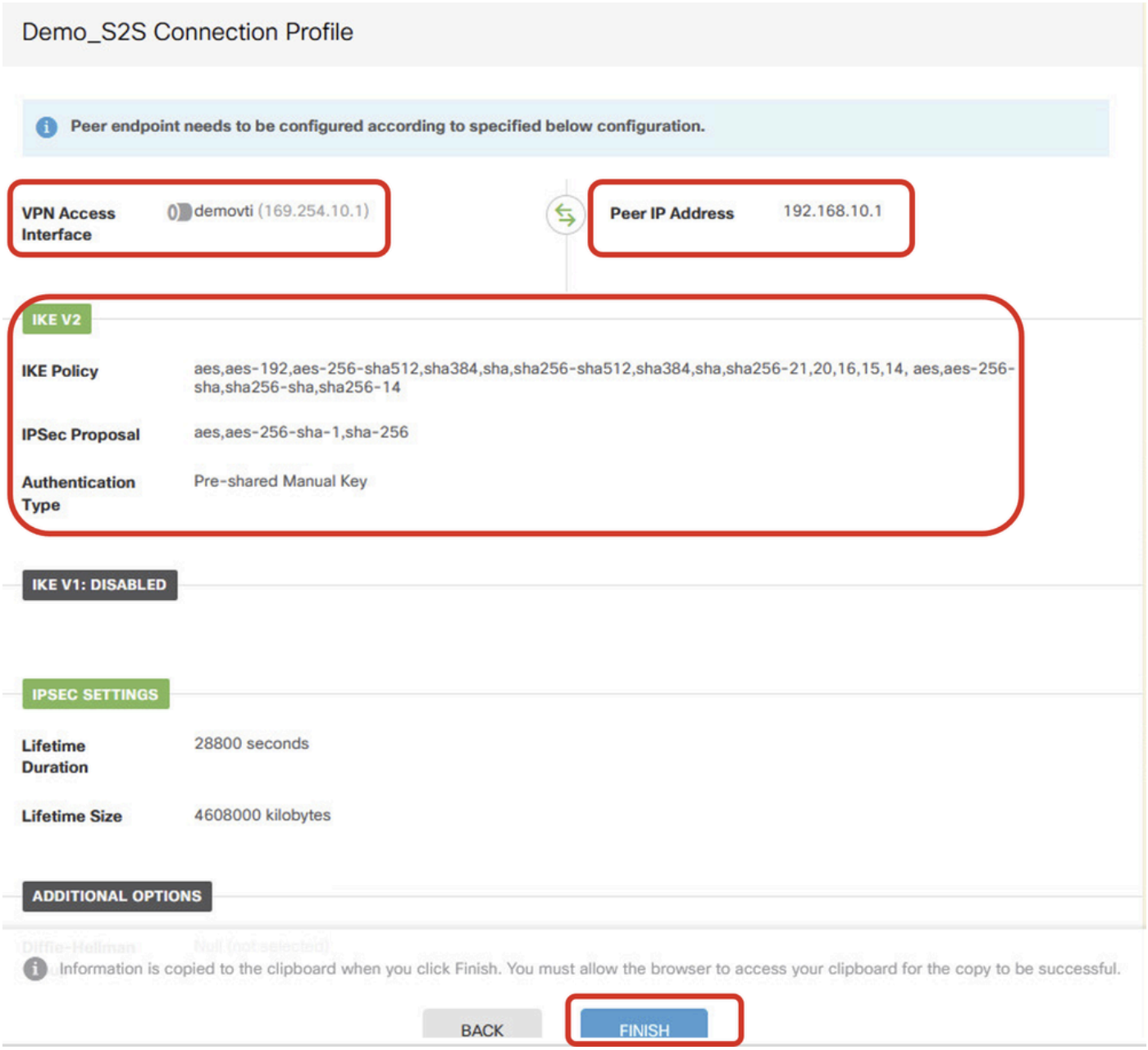
Schritt 3.12: Konfigurieren Sie den vorinstallierten Schlüssel. Klicken Sie auf die Schaltfläche WEITER.

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



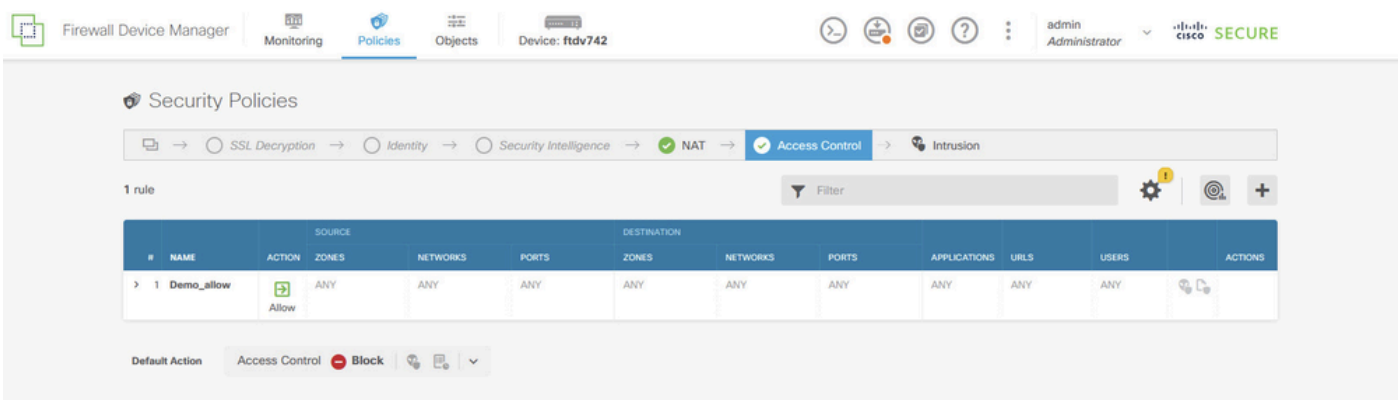
Configure_Pre_Shared_Key

Schritt 3.13: 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.



VPN_Assistent_Abgeschlossen

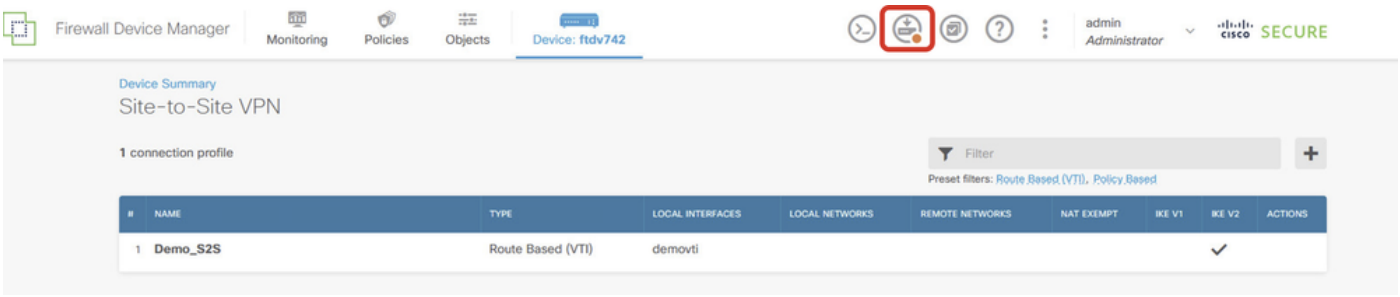
Schritt 3.14: Erstellen Sie eine Zugriffskontrollregel, um den Datenverkehr durch das FTD passieren zu lassen. In diesem Beispiel alle zu Demonstrationszwecken zulassen. Ändern Sie Ihre Richtlinie entsprechend Ihren tatsächlichen Anforderungen.



Beispiel für Zugriffskontrolle_Regel

Schritt 3.15: (Optional) Konfigurieren Sie die NAT-Ausschlussregel für den Client-Datenverkehr auf FTD, wenn für den Client eine dynamische NAT konfiguriert wurde, um auf das Internet zuzugreifen. In diesem Beispiel ist es nicht erforderlich, eine NAT-Ausschlussregel zu konfigurieren, da für jedes FTD keine dynamische NAT konfiguriert ist.

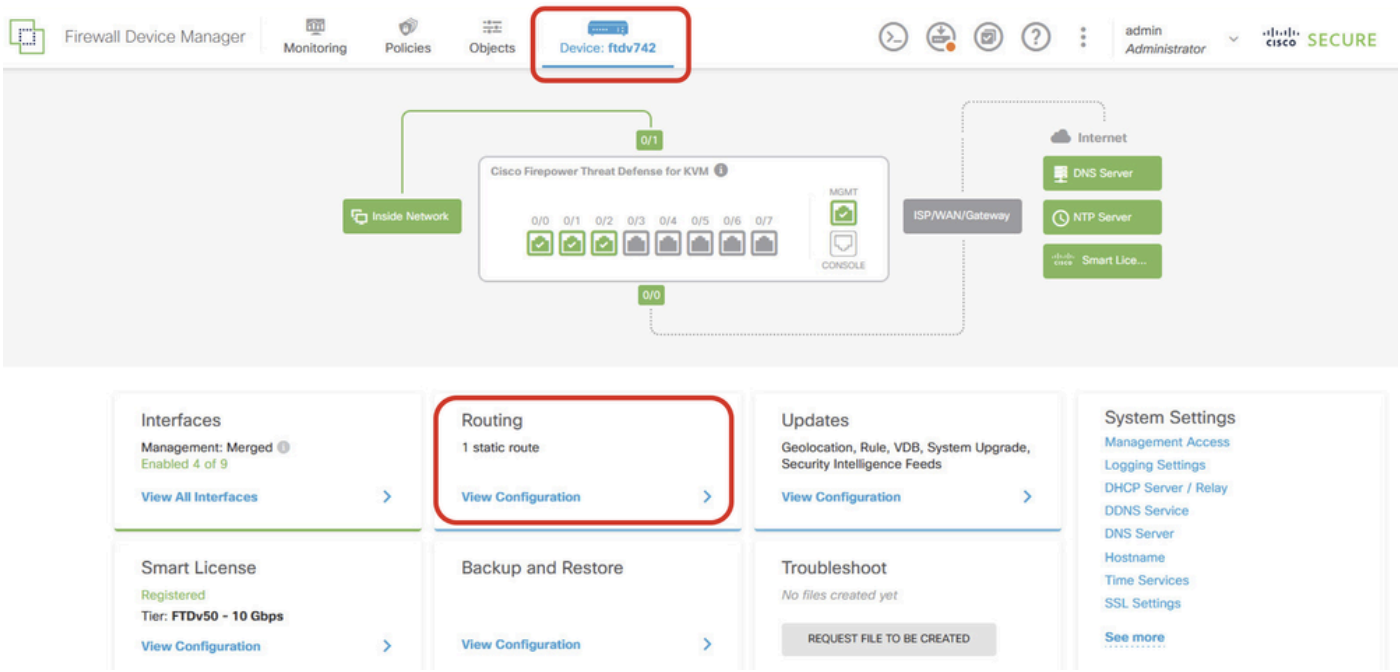
Schritt 3.16: Bereitstellen der Konfigurationsänderungen



Bereitstellen_VPN_Konfiguration

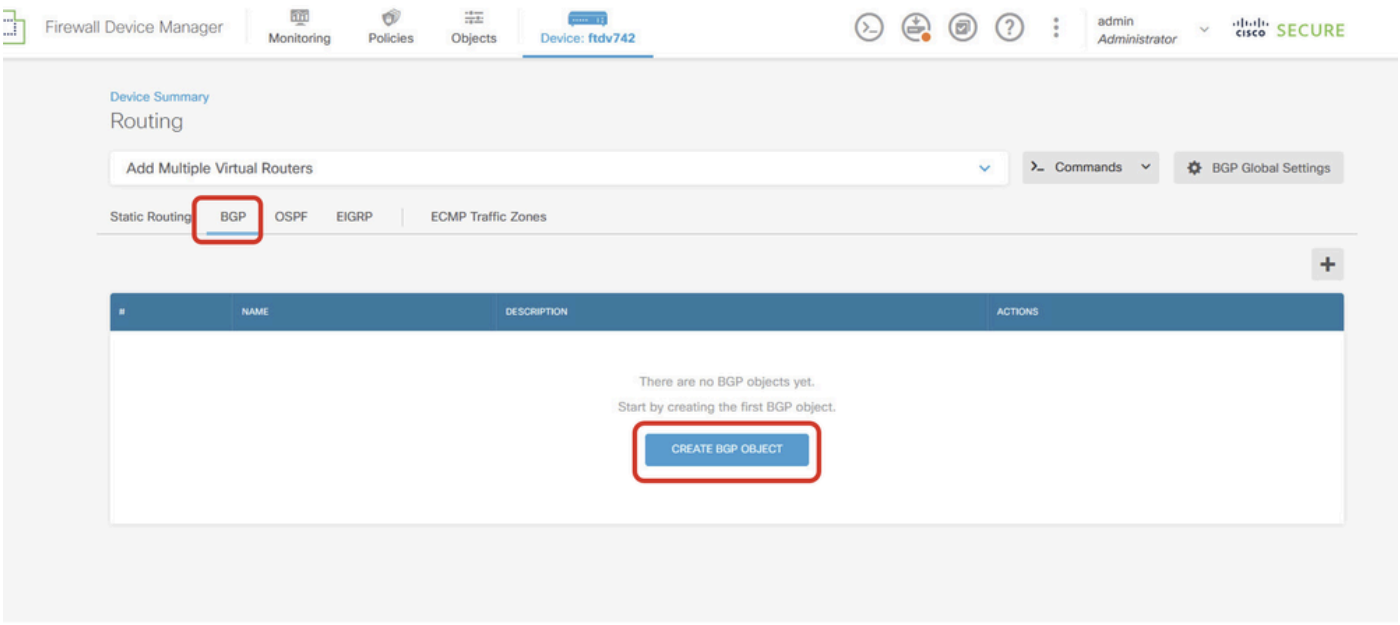
Konfigurationen im BGP

Schritt 4: Navigieren Sie zu Gerät > Routing. Klicken Sie auf Konfiguration anzeigen.



View_Routing_Konfiguration

Schritt 5: Klicken Sie auf die Registerkarte BGP und dann auf BGP-OBJEKT ERSTELLEN.



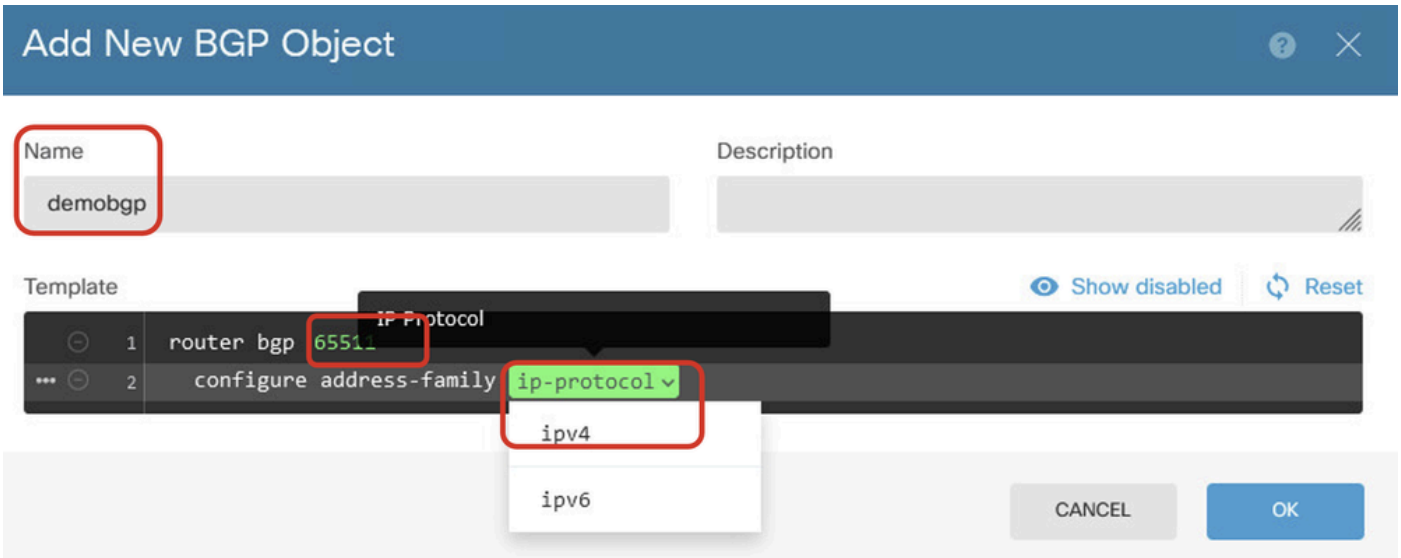
Erstellen_BGP_Objekt

Schritt 6: Geben Sie den Namen des Objekts an. Navigieren Sie zu Vorlage, und konfigurieren Sie sie. Klicken Sie auf die Schaltfläche OK, um zu speichern.

Name: demobgp

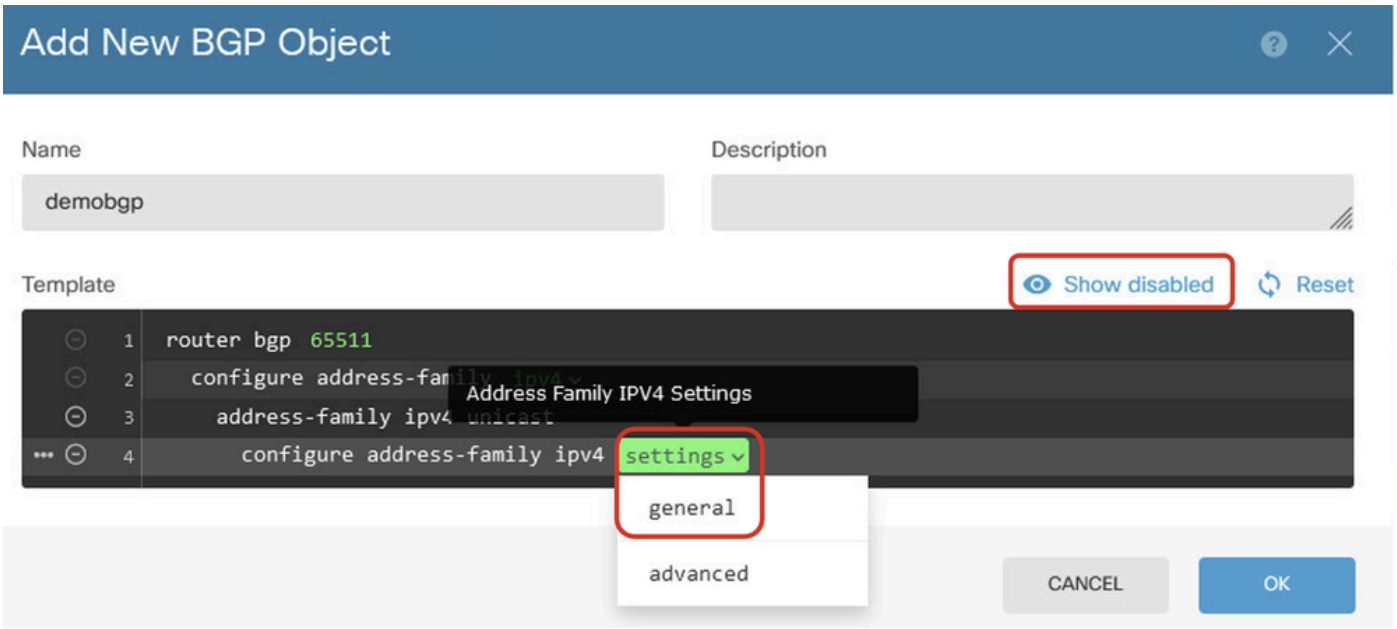
Zeile 1: Konfigurieren der AS-Nummer Klicken Sie auf as-number. Manuelle Eingabe der lokalen AS-Nummer In diesem Beispiel ist AS-Nummer 65511 für Site1 FTD.

Leitung 2: Konfigurieren des IP-Protokolls Klicken Sie auf ip-protocol. Wählen Sie ipv4 aus.



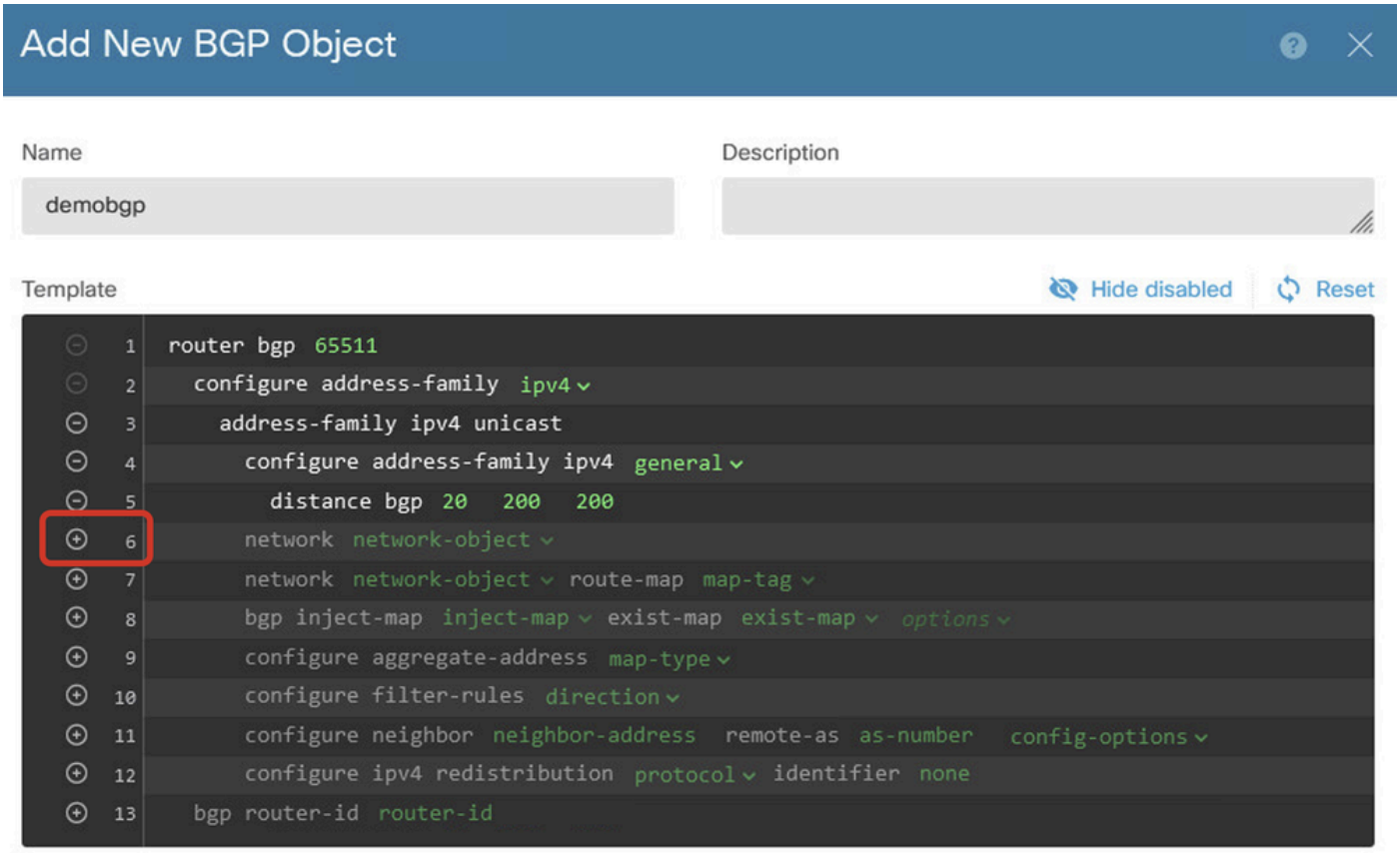
Create_BGP_Object_ASNumber_Protocol

Zeile 4: Konfigurieren weiterer Einstellungen Klicken Sie auf Einstellungen, wählen Sie Allgemein aus, und klicken Sie dann auf Deaktivieren anzeigen.

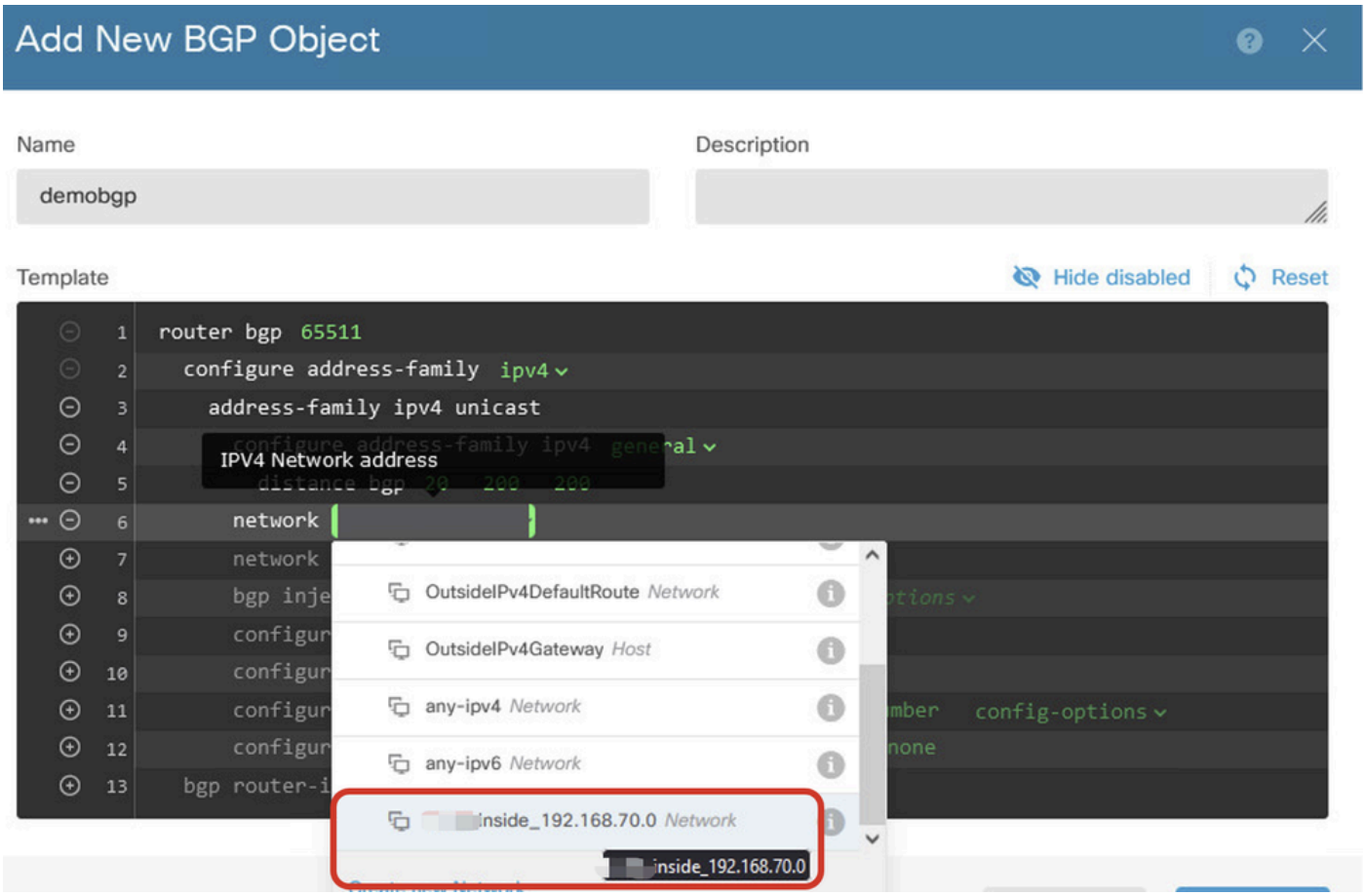


Create_BGP_Object_AddressSetting

Leitung 6: Klicken Sie auf das Symbol +, um die Leitung für die Konfiguration des BGP-Netzwerks zu aktivieren. Klicken Sie auf Netzwerkobjekt. Sie können die vorhandenen Objekte sehen und eines auswählen. Wählen Sie in diesem Beispiel den Objektnamen inside_192.168.70.0 (erstellt in Schritt 3.2).

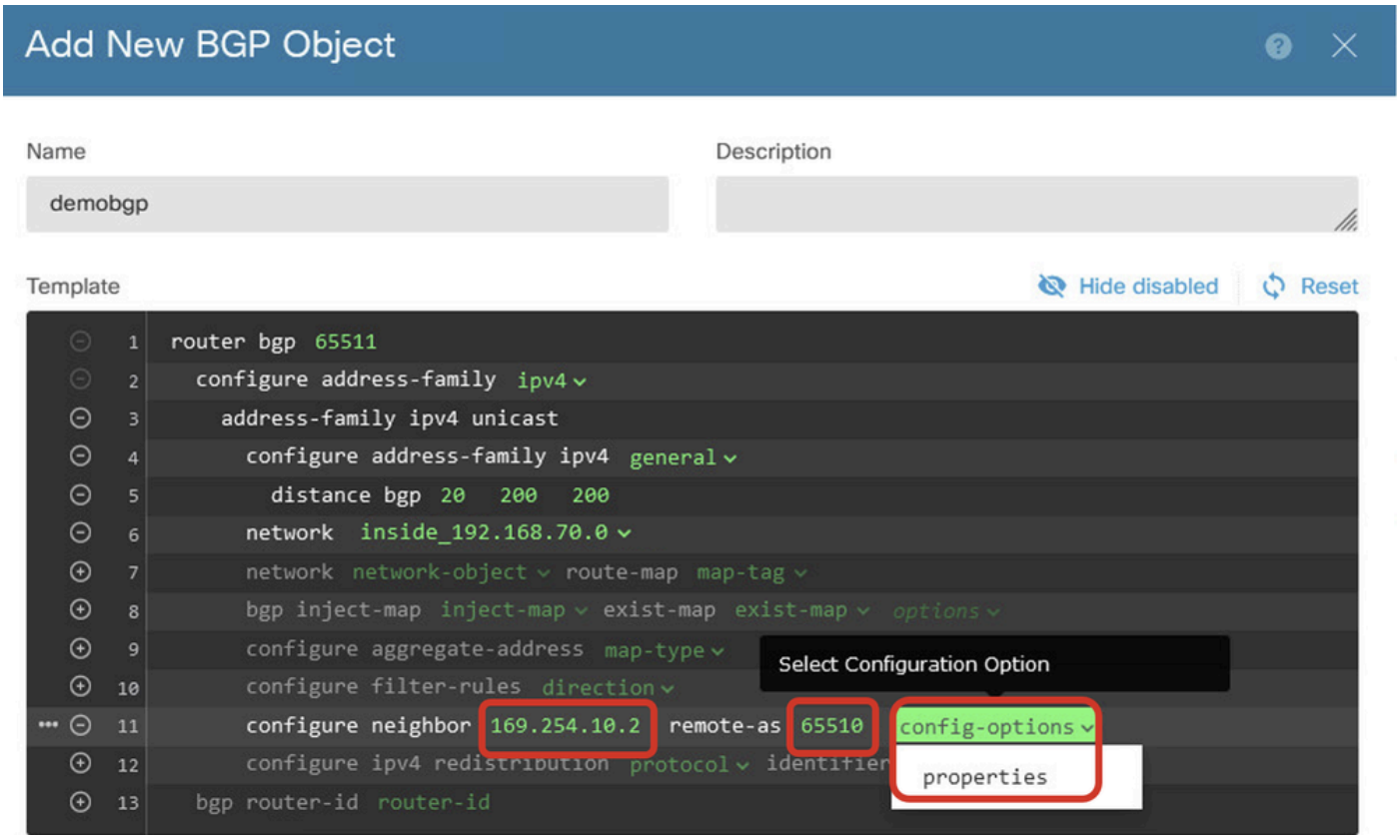


Create_BGP_Object_Add_Network



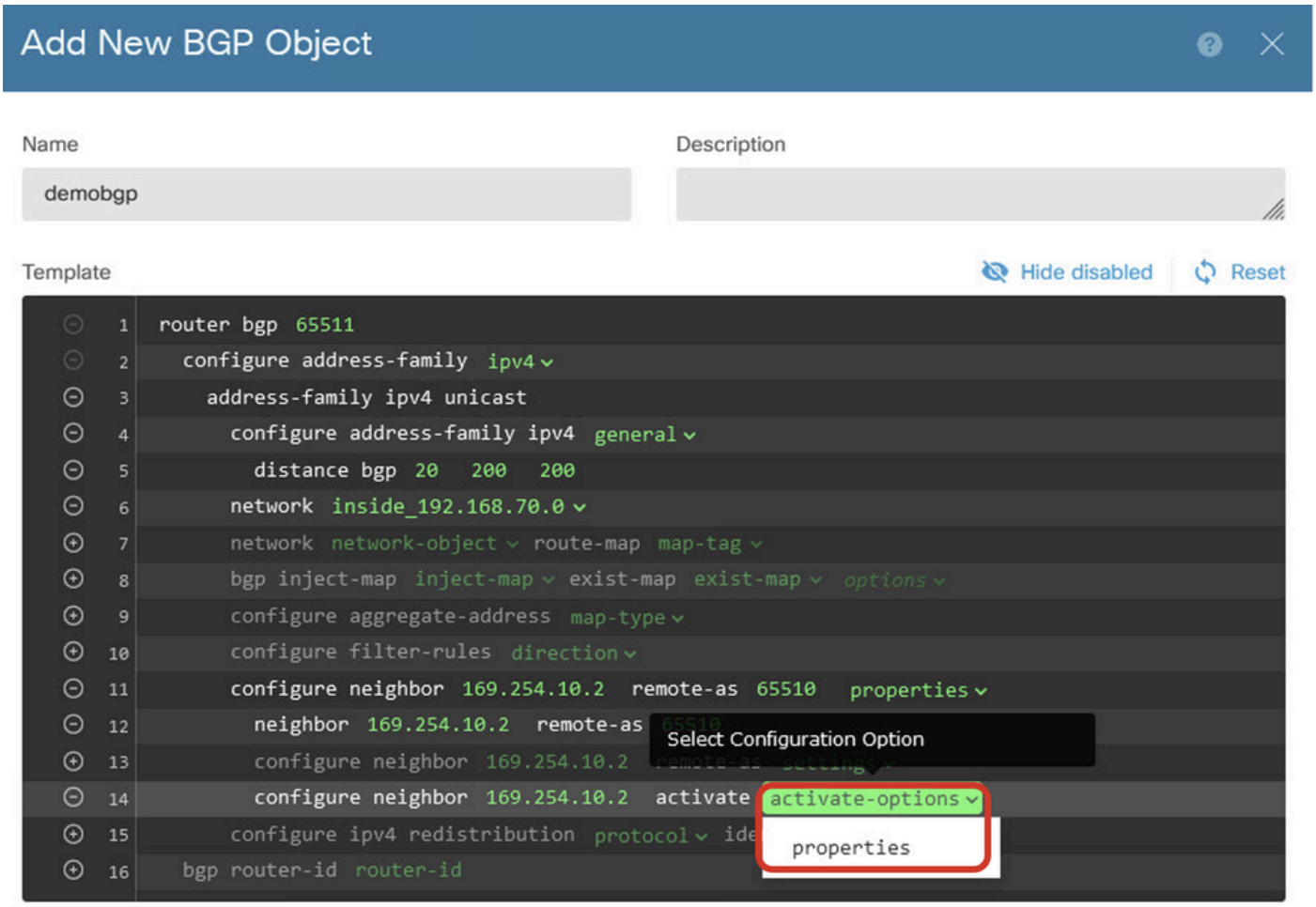
Create_BGP_Object_Add_Network2

Zeile 11: Klicken Sie auf das +-Symbol, um die Leitung zur Konfiguration der Informationen zu den BGP-Nachbarn zu aktivieren. Klicken Sie auf Neighbor-Adresse, und geben Sie die BGP-Nachbaradresse des Peers manuell ein. In diesem Beispiel ist dies 169.254.10.2 (VTI-IP-Adresse von Site2 FTD). Klicken Sie auf AS-Nummer, und geben Sie die AS-Nummer des Peers manuell ein. In diesem Beispiel ist 65510 für Site2 FTD. Klicken Sie auf Konfigurationsoptionen, und wählen Sie Eigenschaften aus.



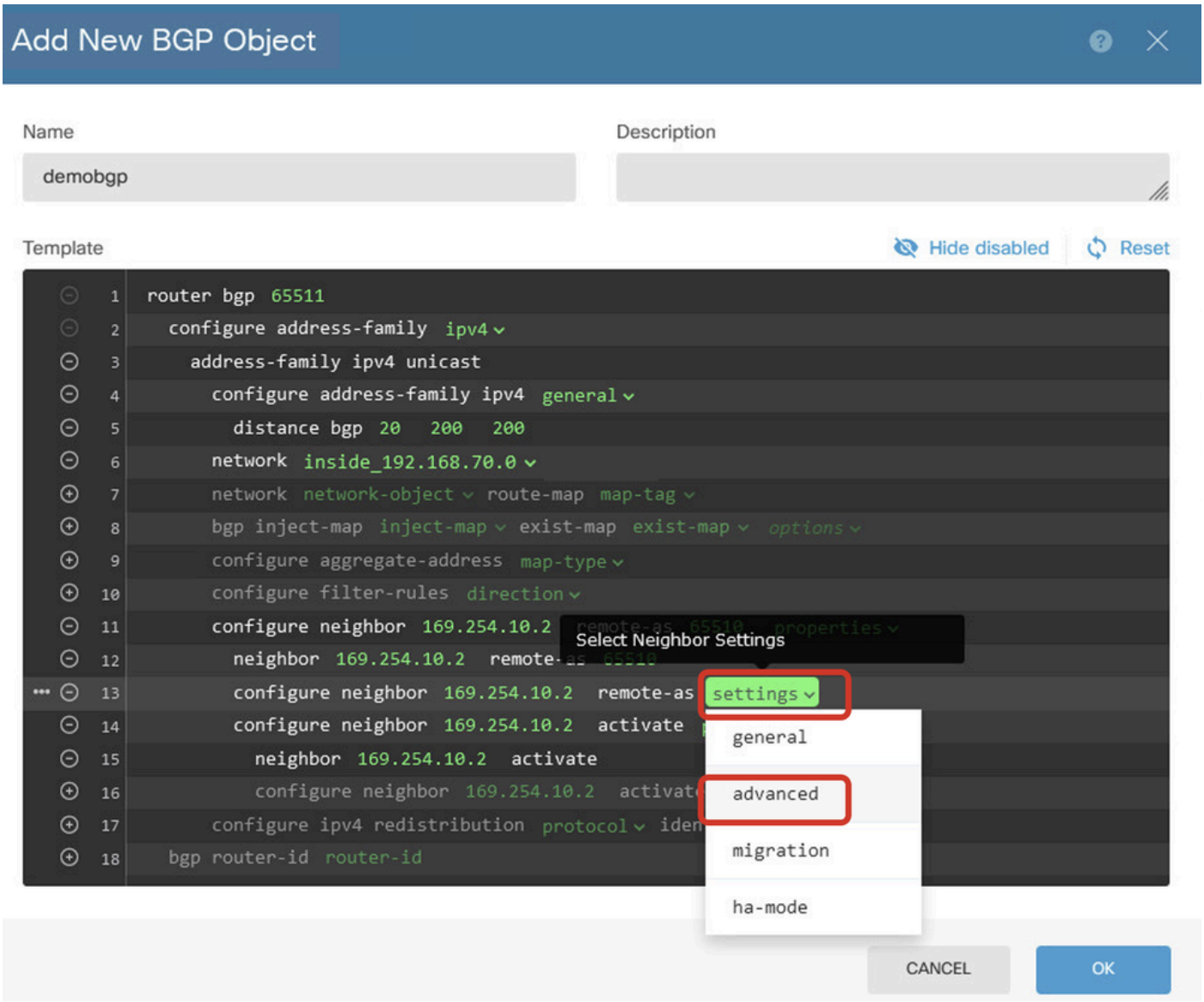
Create_BGP_Object_NeighborEinstellung

Zeile 14: Klicken Sie auf das Symbol +, um die Leitung zum Konfigurieren einiger Eigenschaften des Nachbarn zu aktivieren. Klicken Sie auf activate-options und wählen Sie Eigenschaften.



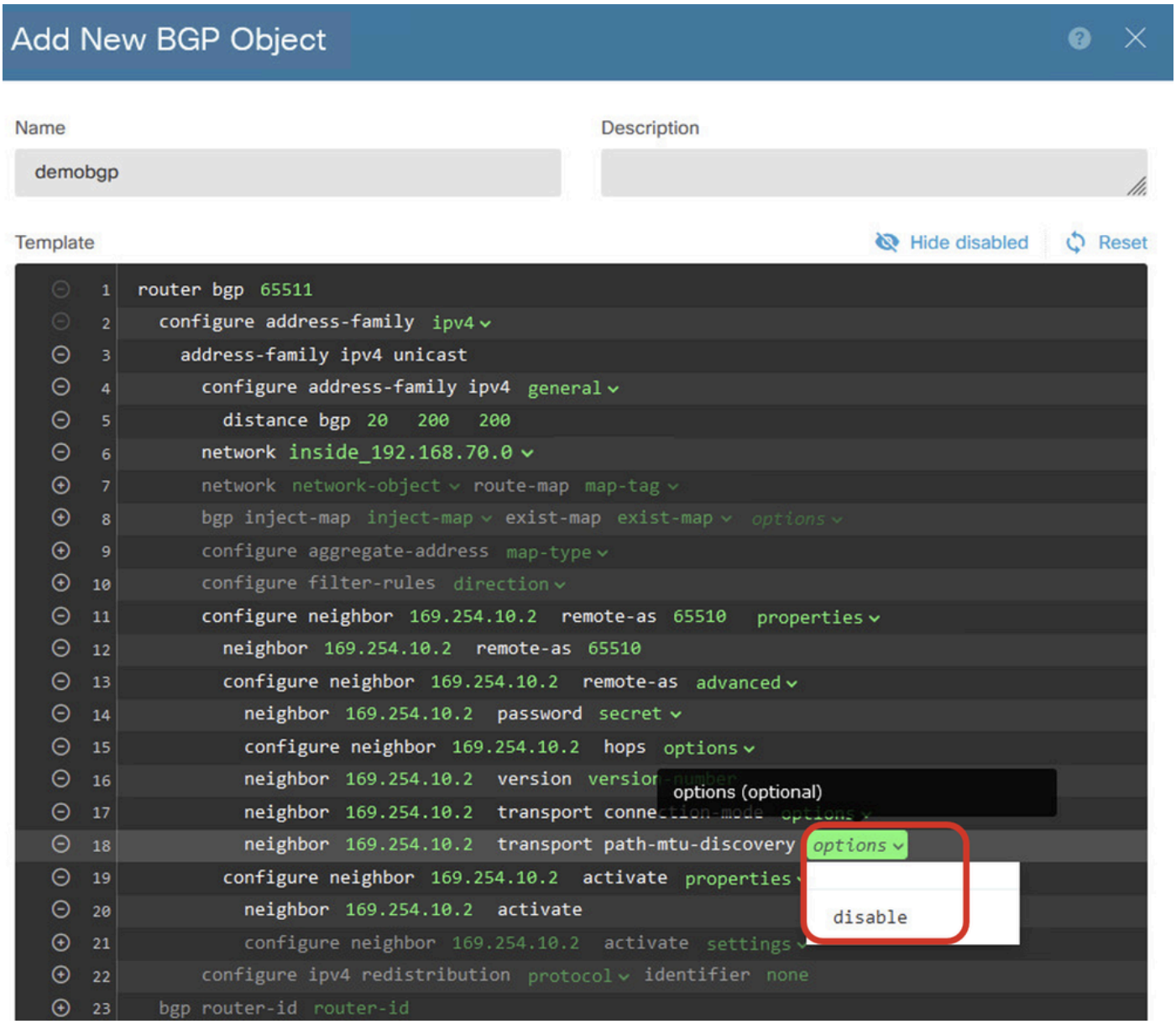
Create_BGP_Object_NeighborSetting_Properties

Zeile 13: Klicken Sie auf das Symbol +, damit für den Posten erweiterte Optionen angezeigt werden. Klicken Sie auf Einstellungen, und wählen Sie Erweitert aus.



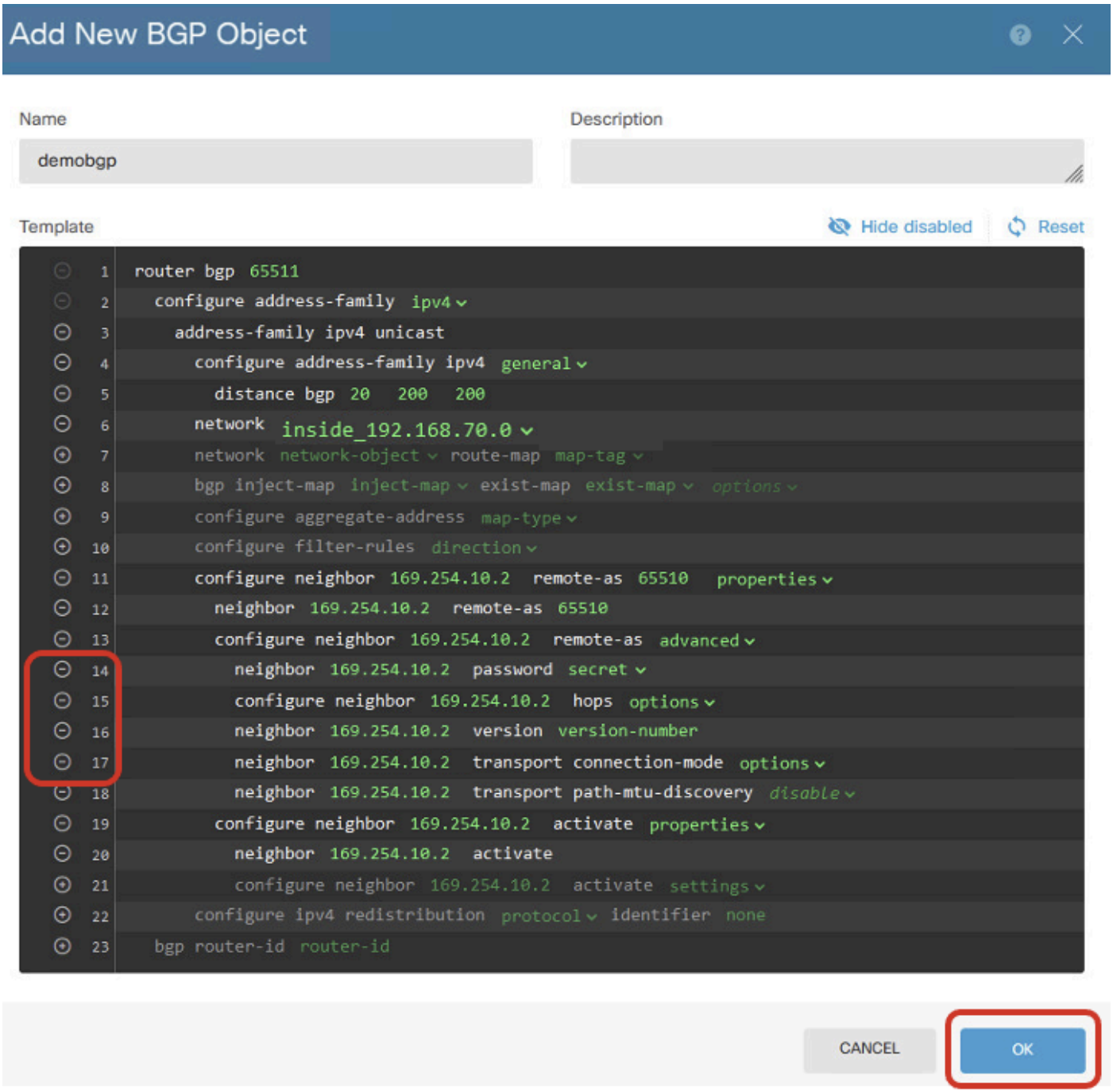
Create_BGP_Object_NeighborSetting_Properties_Advanced

Zeile 18: Klicken Sie auf Options (Optionen), und wählen Sie disable aus, um die MTU-Pfaderkennung zu deaktivieren.



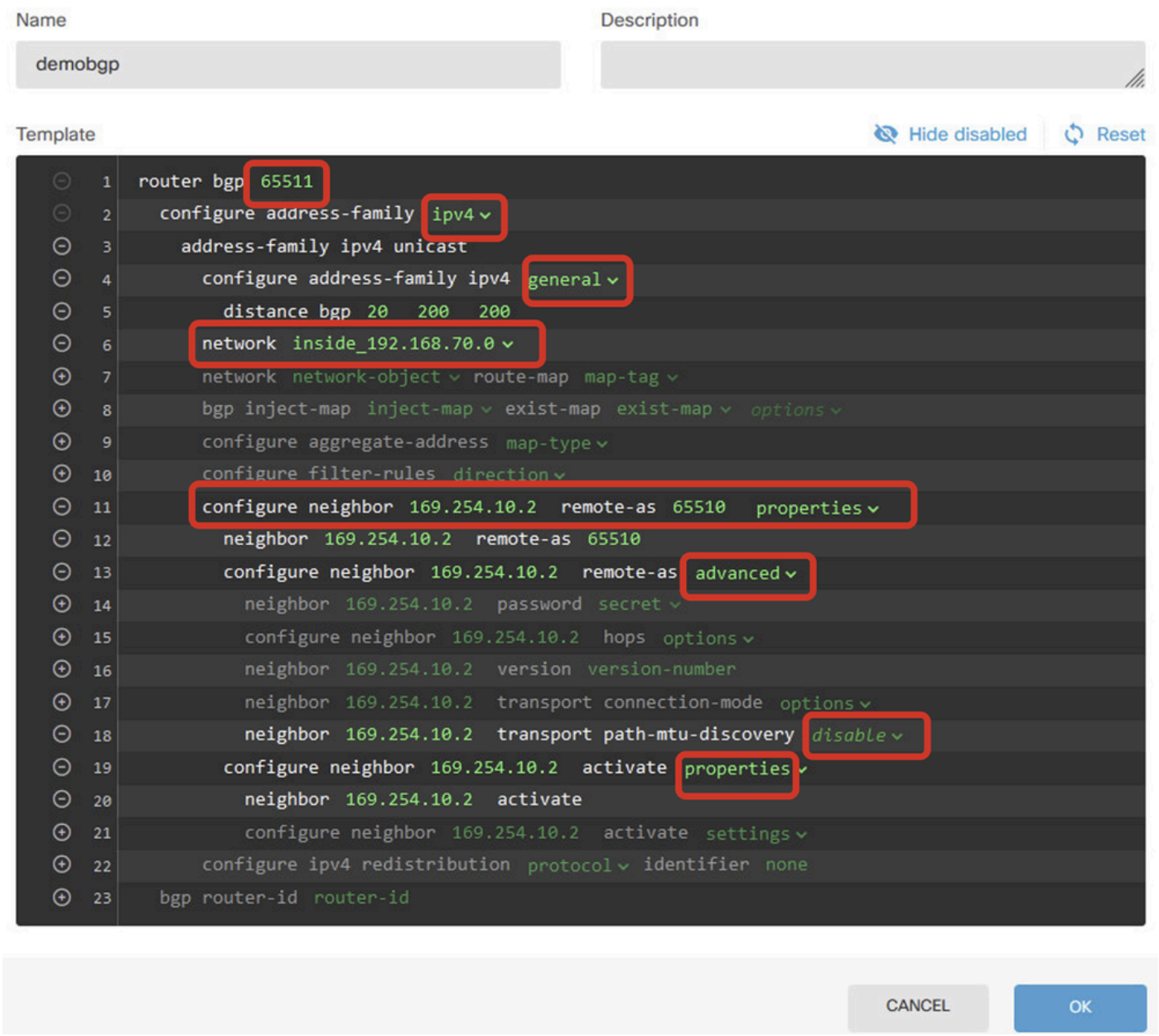
Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

Leitung 14, 15, 16, 17: Klicken Sie auf die - Taste, um die Leitungen zu deaktivieren. Klicken Sie anschließend auf die Schaltfläche OK, um das BGP-Objekt zu speichern.



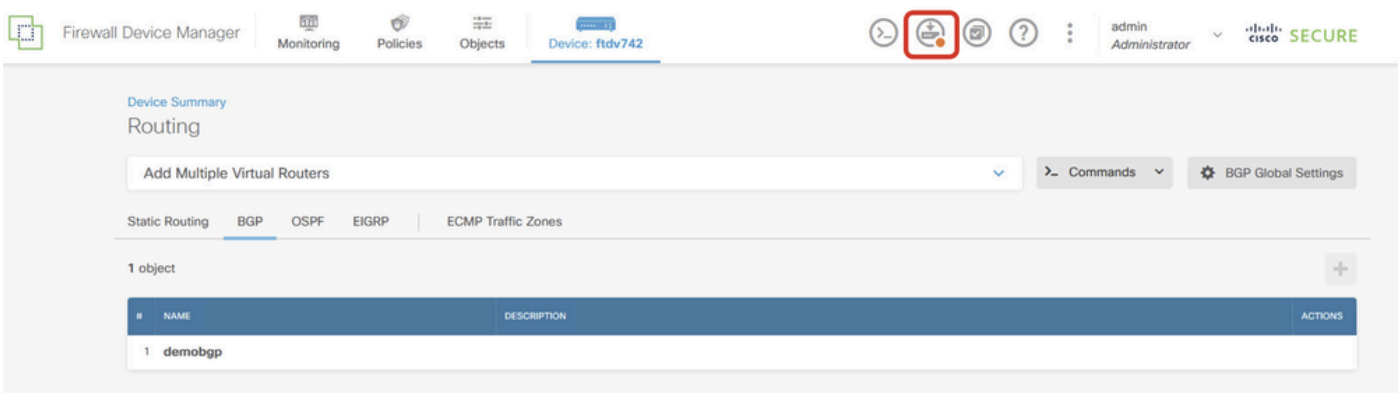
Create_BGP_Object_DisableLines

Dies ist eine Übersicht über die BGP-Einstellung in diesem Beispiel. Sie können die anderen BGP-Einstellungen entsprechend Ihren tatsächlichen Anforderungen konfigurieren.



Create_BGP_Object_Final_Overview

Schritt 7. Bereitstellen der BGP-Konfigurationsänderungen



Bereitstellen_BGP_Konfiguration

Schritt 8: Nun ist die Konfiguration für Site1 FTD abgeschlossen.

Um Site2 FTD VPN und BGP zu konfigurieren, wiederholen Sie Schritt 3 bis Schritt 7 mit den entsprechenden Parametern von Site2 FTD.

Konfigurationsübersicht für Site1 FTD und Site2 FTD in CLI.

Standort1 FTD	Standort2 FTD
NGFW-Version 7.4.2 interface GigabitEthernet0/0 nameif extern CTS-Handbuch Weitergeben sgt serve untag Richtlinie statisches sgt deaktiviert Vertrauenswürdig Sicherheitsstufe 0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside Sicherheitsstufe 0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 Nameleif demovti ip address 169.254.10.1 255.255.255.0 Tunnelquellenschnittstelle außen Tunnelziel 192.168.10.1 Tunnelmodus IPsec IPv4 tunnel protection ipsec-profil ipsec_profile|e4084d322d Objektnetzwerk OutsideIPv4Gateway Host 192.168.30.3 Objektnetzwerk inside_192.168.70.0 Subnetz 192.168.70.0 255.255.255.0 Zugriffsgruppe NGFW_ONBOX_ACL global Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435457: ZUGRIFFSRICHTLINIE: NGFW_Access_Policy Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435457: L5 REGEL: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc in jeder ifc außerhalb jeder Regel-ID 268435457 Ereignisprotokoll, beide Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435458: ZUGRIFFSRICHTLINIE:	NGFW-Version 7.4.2 interface GigabitEthernet0/0 nameif extern CTS-Handbuch Weitergeben sgt serve untag Richtlinie statisches sgt deaktiviert Vertrauenswürdig Sicherheitsstufe 0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif inside Sicherheitsstufe 0 ip address 192.168.50.1 255.255.255.0 interface Tunnel1 Name eif demovti25 ip address 169.254.10.2 255.255.255.0 Tunnelquellenschnittstelle außen Tunnelziel 192.168.30.1 Tunnelmodus IPsec IPv4 tunnel protection ipsec-profil ipsec_profile|e4084d322d Objektnetzwerk OutsideIPv4Gateway Host 192.168.10.3 Objektnetzwerk inside_192.168.50.0 Subnetz 192.168.50.0 255.255.255.0 Zugriffsgruppe NGFW_ONBOX_ACL global Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435457: ZUGRIFFSRICHTLINIE: NGFW_Access_Policy Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435457: L5 REGEL: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc in jeder ifc außerhalb jeder Regel-ID 268435457 Ereignisprotokoll, beide Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435458: ZUGRIFFSRICHTLINIE: NGFW_Access_Policy

NGFW_Access_Policy	
Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435458: L5 RULE: Demo_allow	Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 268435458: L5 RULE: Demo_allow
access-list NGFW_ONBOX_ACL advanced permit object-Gruppe |acSvcg-268435458 alle Regel-ID 268435458 Ereignisprotokolle, beide	access-list NGFW_ONBOX_ACL advanced permit object-Gruppe |acSvcg-268435458 alle Regel-ID 268435458 Ereignisprotokolle, beide
Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 1: ZUGRIFFSRICHTLINIE: NGFW_Access_Policy	Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 1: ZUGRIFFSRICHTLINIE: NGFW_Access_Policy
Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 1: L5 RULE: DefaultActionRule	Zugriffsliste NGFW_ONBOX_ACL Bemerkung Regel-ID 1: L5 RULE: DefaultActionRule
access-list NGFW_ONBOX_ACL advanced deny ip any rule-id 1	access-list NGFW_ONBOX_ACL advanced deny ip any rule-id 1
Router BGP 65511	Router BGP 65510
bgp log-neighbor-änderungen	bgp log-neighbor-änderungen
bgp router-id vrf automatisch zuweisen	bgp router-id vrf automatisch zuweisen
address-family-IPv4-Unicast	address-family-IPv4-Unicast
neighbor 169.254.10.2 remote-as 65510	neighbor 169.254.10.1 remote-as 65511
neighbor 169.254.10.2 transport path-mtu-discovery disable	neighbor 169.254.10.1 transport path-mtu-discovery disable
Nachbar 169.254.10.2 aktivieren	Nachbar 169.254.10.1 aktivieren
Netzwerk 192.168.70.0	Netzwerk 192.168.50.0
keine automatische Zusammenfassung	keine automatische Zusammenfassung
keine Synchronisierung	keine Synchronisierung
Ausgangsadressenfamilie	Ausgangsadressenfamilie
Route außerhalb 0.0.0.0 0.0.0.0 192.168.30.3 1	Route außerhalb 0.0.0.0 0.0.0.0 192.168.10.3 1
crypto ipsec ikev2 ipsec-vorschlag AES256_SHA256	crypto ipsec ikev2 ipsec-vorschlag AES256_SHA256
Protokoll-ESP-Verschlüsselung AES-256 AES	Protokoll-ESP-Verschlüsselung AES-256 AES
Protokoll esp integrität sha-256 sha-1	Protokoll esp integrität sha-256 sha-1
crypto ipsec-Profil ipsec_profile|e4084d322d	crypto ipsec-Profil ipsec_profile|e4084d322d
set ikev2 ipsec-vorschlag AES256_SHA256	set ikev2 ipsec-vorschlag AES256_SHA256
set security-association lebensdauer kilobyte 4608000	set security-association lebensdauer kilobyte 4608000
Lebensdauer der Sicherheitszuordnung festlegen 28800	Lebensdauer der Sicherheitszuordnung festlegen 28800
crypto ipsec Sicherheitszuordnung pmtu-aging unendlich	crypto ipsec Sicherheitszuordnung pmtu-aging unendlich
crypto ikev2 policy 1	crypto ikev2 policy 1
Verschlüsselung AES-256 AES	Verschlüsselung AES-256 AES
Integrität sha256 sha	Integrität sha256 sha
Gruppe 14	Gruppe 14
prf sha256 sha	prf sha256 sha
Lebensdauersekunden 86400	Lebensdauersekunden 86400
crypto ikev2 policy 20	crypto ikev2 policy 20
Verschlüsselung AES-256 AES-192 AES	Verschlüsselung AES-256 AES-192 AES

Integrität sha512 sha384 sha256 sha Gruppe 21 20 16 15 14 prf sha 512 sha 384 sha 256 sha Lebensdauersekunden 86400 crypto ikev2 außerhalb aktivieren Gruppenpolitik |s2sGP|192.168.10.1 intern Gruppenpolitik |s2sGP|192.168.10.1-Attribute vpn-tunnel-protocol ikev2 tunnel-group 192.168.10.1, Typ ipsec-l2l tunnel-group 192.168.10.1 allgemeine Attribute default-group-policy |s2sGP|192.168.10.1 tunnel-group 192.168.10.1 ipsec-attribute ikev2 Remote-Authentifizierung Pre-Shared-Key ***** ikev2 local-authentication pre-shared-key *****	Integrität sha512 sha384 sha256 sha Gruppe 21 20 16 15 14 prf sha 512 sha 384 sha 256 sha Lebensdauersekunden 86400 crypto ikev2 außerhalb aktivieren Gruppenpolitik |s2sGP|192.168.30.1 intern Gruppenpolitik |s2sGP|192.168.30.1-Attribute vpn-tunnel-protocol ikev2 tunnel-group 192.168.30.1, Typ ipsec-l2l tunnel-group 192.168.30.1 allgemeine Attribute default-group-policy |s2sGP|192.168.30.1 tunnel-group 192.168.30.1 ipsec-attribute ikev2 Remote-Authentifizierung Pre-Shared-Key ***** ikev2 local-authentication pre-shared-key *****

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Navigieren Sie über die Konsole oder SSH zur CLI jedes FTD, um den VPN-Status von Phase 1 und Phase 2 über die Befehle show crypto ikev2 sa und show crypto ipsec sa zu überprüfen.

Standort1 FTD	Standort2 FTD
ftdv742# show crypto ikev2 sa IKEv2-SAs: Session-ID:134, Status:UP-ACTIVE, IKE-Anzahl:1, KINDERZAHL:1 Tunnel-ID Lokale Remote-Rolle "fvrf/ivrf Status" 563984431 192.168.30.1/500 192.168.10.1/500 Global/Global READY RESPONDER Encr: AES-CBC, Keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Lebensdauer/Aktivzeit: 86400/5145 s Untergeordnete SA: lokaler Selektor 0.0.0.0/0 -	ftdv742# show crypto ikev2 sa IKEv2-SAs: Sitzungs-ID:13, Status:UP-ACTIVE, IKE-Anzahl:1, KINDERZAHL:1 Tunnel-ID Lokale Remote-Rolle "fvrf/ivrf Status" 339797985 192.168.10.1/500 192.168.30.1/500 Global/Global READY INITIATOR Encr: AES-CBC, Keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK Lebensdauer/Aktivzeit: 86400/74099 Sek. Untergeordnete SA: lokaler Selektor 0.0.0.0/0 - 255.255.255.255/65535 Remote Selector 0.0.0.0/0 - 255.255.255.255/65535 ESP-Spin/out: 0xb7b5b38b/0xf0c4239d

255.255.255.255/65535 Remote Selector 0.0.0.0/0 - 255.255.255.255/65535 ESP-Spin/out: 0xf0c4239d/0xb7b5b38b	
ftdv742# show crypto ipsec sa Schnittstelle: demovti Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1 Protected VRF (IVRF): global local ident (adr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) remote ident (adr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1 #pkts encaps: 5720, #pkts encrypt: 5720, #pkts digest: 5720 #pkts decaps: 5717, #pkts entschlüsseln: 5717, #pkts verifizieren: 5717 #pkts komprimiert: 0, #pkts dekomprimiert: 0 #pkts nicht komprimiert: 5720, #pkts Comp fehlgeschlagen: 0, #pkts decomp fehlgeschlagen: 0 #pre-frag Erfolge: 0, #pre-frag Misserfolge: 0, #fragments erstellt: 0 #PMTUs gesendet: 0, #PMTUs rcvd: 0, #decapsulated fgs müssen wieder zusammengesetzt werden: 0 #TFC rcvd: 0, #TFC gesendet: 0 #Valid ICMP-Fehler rcvd: 0, #Invalid ICMP-Fehler rcvd: 0 #send Fehler: 0, #recv Fehler: 0 lokales Kryptografieendgerät.: 192.168.30.1/500, entferntes Kryptografieendgerät.: 192.168.10.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Verbleibende PMTU-Zeit (Sek.): 0, DF-Richtlinie: copy-df ICMP-Fehlervalidierung: deaktiviert, TFC-Pakete: deaktiviert	ftdv742# show crypto ipsec sa Schnittstelle: demovti25 Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.10.1 Protected VRF (IVRF): global local ident (adr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) remote ident (adr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1 #pkts encaps: 5721, #pkts encrypt: 5721, #pkts digest: 5721 #pkts decaps: 5721, #pkts entschlüsseln: 5721, #pkts verifizieren: 5721 #pkts komprimiert: 0, #pkts dekomprimiert: 0 #pkts nicht komprimiert: 5721, #pkts Comp fehlgeschlagen: 0, #pkts decomp fehlgeschlagen: 0 #pre-frag Erfolge: 0, #pre-frag Misserfolge: 0, #fragments erstellt: 0 #PMTUs gesendet: 0, #PMTUs rcvd: 0, #decapsulated fgs müssen wieder zusammengesetzt werden: 0 #TFC rcvd: 0, #TFC gesendet: 0 #Valid ICMP-Fehler rcvd: 0, #Invalid ICMP-Fehler rcvd: 0 #send Fehler: 0, #recv Fehler: 0 lokales Kryptografieendgerät.: 192.168.10.1/500, entferntes Kryptografieendgerät.: 192.168.30.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Verbleibende PMTU-Zeit (Sek.): 0, DF-Richtlinie: copy-df ICMP-Fehlervalidierung: deaktiviert, TFC-Pakete: deaktiviert

aktuelle ausgehende Spi: B7B5B38B aktuelle eingehende SPI: F0C4239D Inbound ESP SAS: SPI: 0xF0C4239D (4039386013) SA-Staat: aktiv transformation: esp-aes-256 esp-sha-256-hmac keine Komprimierung In Verwendung: Einstellungen ={L2L, Tunnel, IKEv2, VTI, } Steckplatz: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa-Timing: verbleibende Schlüssellebensdauer (kB/s): (4285389/3722) IV-Größe: 16 Byte Unterstützung für Wiedergabe-Erkennung: Y Anti-Wiedergabe-Bitmap: 0xFFFFFFFF 0xFFFFFFFF Outbound ESP SAS: SPI: 0xB7B5B38B (3082138507) SA-Staat: aktiv transformation: esp-aes-256 esp-sha-256-hmac keine Komprimierung In Verwendung: Einstellungen ={L2L, Tunnel, IKEv2, VTI, } Steckplatz: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa-Timing: verbleibende Schlüssellebensdauer (kB/s): (4147149/3722) IV-Größe: 16 Byte Unterstützung für Wiedergabe-Erkennung: Y Anti-Wiedergabe-Bitmap: 0x00000000 0x00000001	aktuelle ausgehende SPI: F0C4239D aktueller eingehender SPI: B7B5B38B Inbound ESP SAS: SPI: 0xB7B5B38B (3082138507) SA-Staat: aktiv transformation: esp-aes-256 esp-sha-256-hmac keine Komprimierung In Verwendung: Einstellungen ={L2L, Tunnel, IKEv2, VTI, } Steckplatz: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa-Timing: verbleibende Schlüssellebensdauer (kB/s): (3962829/3626) IV-Größe: 16 Byte Unterstützung für Wiedergabe-Erkennung: Y Anti-Wiedergabe-Bitmap: 0xFFFFFFFF 0xFFFFFFFF Outbound ESP SAS: SPI: 0xF0C4239D (4039386013) SA-Staat: aktiv transformation: esp-aes-256 esp-sha-256-hmac keine Komprimierung In Verwendung: Einstellungen ={L2L, Tunnel, IKEv2, VTI, } Steckplatz: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa-Timing: verbleibende Schlüssellebensdauer (kB/s): (4101069/3626) IV-Größe: 16 Byte Unterstützung für Wiedergabe-Erkennung: Y Anti-Wiedergabe-Bitmap: 0x00000000 0x00000001

Schritt 2: Navigieren Sie über die Konsole oder SSH zur CLI der FTD, um den BGP-Status mithilfe der Befehle show bgp neighbors und show route bgp zu überprüfen.

Standort1 FTD	Standort2 FTD
ftdv742# BGP-Nachbarn anzeigen BGP-Nachbar ist 169.254.10.2, vrf single_vf, Remote-AS 65510, externe Verbindung BGP-Version 4, Remote-Router-ID 192.168.50.1 BGP-Status = etabliert, bis zu 1 d20 h Zuletzt gelesen 00:00:25, zuletzt geschrieben	ftdv742# BGP-Nachbarn anzeigen BGP-Nachbar ist 169.254.10.1, vrf single_vf, Remote-AS 65511, externe Verbindung BGP-Version 4, Remote-Router-ID 192.168.70.1 BGP-Status = etabliert, bis zu 1 d20 h Zuletzt gelesen 00:00:11, zuletzt geschrieben

00:00:45, Haltezeit 180, Keepalive-Intervall 60 Sekunden Nachbarsitzungen: 1 aktiv, ist nicht Multisession-fähig (deaktiviert) Funktionen für Nachbarn: Routenaktualisierung: angekündigt und empfangen (neu) 4-Oktett-ASN-Funktion: angekündigt und empfangen Adressfamilie IPv4 Unicast: angekündigt und empfangen Multisession-Funktion: Nachrichtenstatistik: InQ-Tiefe ist 0 OutQ-Tiefe ist 0 Gesendet Empf. Geöffnet: 1 1 Benachrichtigungen: 0 0 Aktualisierungen: 2 2 Keepalive: 2423 2427 Routen-Aktualisierung: 0 0 Gesamt: 2426 2430 Die standardmäßige Mindestdauer zwischen den Anzeigeläufen beträgt 30 Sekunden. Für Adressfamilie: IPv4 Unicast Sitzung: 169.254.10.2 BGP-Tabelle Version 3, Nachbarversion 3/0 Größe der Ausgabewarteschlange: 0 Ziffer 1 1 Mitglied einer Aktualisierungsgruppe Gesendet Empf. Präfixaktivität: ---- ---- Aktuelle Präfixe: 1 1 (80 Byte) Präfixe gesamt: 1 1 Implizit zurückziehen: 0 0 Explizit zurückziehen: 0 0 Als bestmöglicher Pfad verwendet: n/a 1 Als Multipath verwendet: n/a 0 Ausgehender eingehender Datenverkehr Präfixe für abgelehnte lokale Richtlinien: -------- ------ Bester Pfad von diesem Peer: 1 n/a Gesamt: 1 0	00:00:52, Haltezeit 180, Keepalive-Intervall 60 Sekunden Nachbarsitzungen: 1 aktiv, ist nicht Multisession-fähig (deaktiviert) Funktionen für Nachbarn: Routenaktualisierung: angekündigt und empfangen (neu) 4-Oktett-ASN-Funktion: angekündigt und empfangen Adressfamilie IPv4 Unicast: angekündigt und empfangen Multisession-Funktion: Nachrichtenstatistik: InQ-Tiefe ist 0 OutQ-Tiefe ist 0 Gesendet Empf. Geöffnet: 1 1 Benachrichtigungen: 0 0 Aktualisierungen: 2 2 Keepalive: 2424 2421 Routen-Aktualisierung: 0 0 Gesamt: 2427 2424 Die standardmäßige Mindestdauer zwischen den Anzeigeläufen beträgt 30 Sekunden. Für Adressfamilie: IPv4 Unicast Sitzung: 169.254.10.1 BGP-Tabelle Version 9, Nachbarversion 9/0 Größe der Ausgabewarteschlange: 0 Ziffer 4 4 Mitglieder der Aktualisierungsgruppe Gesendet Empf. Präfixaktivität: ---- ---- Aktuelle Präfixe: 1 1 (80 Byte) Präfixe gesamt: 1 1 Implizit zurückziehen: 0 0 Explizit zurückziehen: 0 0 Als bestmöglicher Pfad verwendet: n/a 1 Als Multipath verwendet: n/a 0 Ausgehender eingehender Datenverkehr Präfixe für abgelehnte lokale Richtlinien: -------- ------ Bester Pfad von diesem Peer: 1 n/a Gesamt: 1 0

Anzahl der NLRIs im gesendeten Update: max. 1, min. 0 Die Adressverfolgung ist aktiviert, und die RIB hat eine Route zu 169.254.10.2. Verbindungen hergestellt 1; abgebrochen 0 Letzte Zurücksetzung nie Transport(tcp) path-mtu-discovery ist deaktiviert Ordnungsgemäßer Neustart ist deaktiviert	Anzahl der NLRIs im gesendeten Update: max. 1, min. 0 Die Adressverfolgung ist aktiviert, und die RIB hat eine Route zu 169.254.10.1. Verbindungen hergestellt 4; abgebrochen 3 Letzte Rücksetzung 1d21h, aufgrund Interface-Flapping von Session 1 Transport(tcp) path-mtu-discovery ist deaktiviert Ordnungsgemäßer Neustart ist deaktiviert
ftdv742# Routen-BGP anzeigen Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2 E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, V - VPN i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2 ia - IS-IS interarea, * - candidate default, U - per user static route o - ODR, P - periodische heruntergeladene statische Route, + - replizierte Route SI = Static InterVRF, BI = BGP InterVRF Gateway der letzten Instanz ist 192.168.30.3 zum Netzwerk 0.0.0.0 B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h	ftdv742# Routen-BGP anzeigen Codes: L - lokal, C - verbunden, S - statisch, R - RIP, M - mobil, B - BGP D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea N1 - OSPF NSSA extern Typ 1, N2 - OSPF NSSA extern Typ 2 E1 - externer OSPF-Typ 1, E2 - externer OSPF-Typ 2, V - VPN i - IS-IS, su - IS-IS-Zusammenfassung, L1 - IS-IS-Ebene-1, L2 - IS-IS-Ebene-2 ia - IS-IS interarea, * - candidate default, U - per user static route o - ODR, P - periodische heruntergeladene statische Route, + - replizierte Route SI = Static InterVRF, BI = BGP InterVRF Gateway der letzten Instanz ist 192.168.10.3 zum Netzwerk 0.0.0.0 B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h

Schritt 3: Site1-Client und Site2-Client pingen einander erfolgreich an.

Standort 1-Client:

```
Site1_Client#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 = 31/56/90 ms
```

Standort 2-Client:

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

Fehlerbehebung

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

Sie können diese Debug-Befehle verwenden, um Probleme im 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 BGP-Abschnitt zu beheben.

```
ftdv742# debug ip bgp ?

A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range      BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpnv4      Address family
vpnv6      Address family
vrf        VRF scope
<cr>
```

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.