Konfigurieren eines Site-to-Site-VPNs auf einem von FDM verwalteten FTD

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von Site-to-Site-VPN auf Firepower Threat Defense (FTD) beschrieben, die vom FirePOWER Device Manager (FDM) verwaltet wird.

Voraussetzungen

Anforderungen

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

- Grundlegendes Verständnis von VPN
- Erfahrung mit FDN
- Erfahrung mit der Adaptive Security Appliance (ASA) Befehlszeile

Verwendete Komponenten

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

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

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.

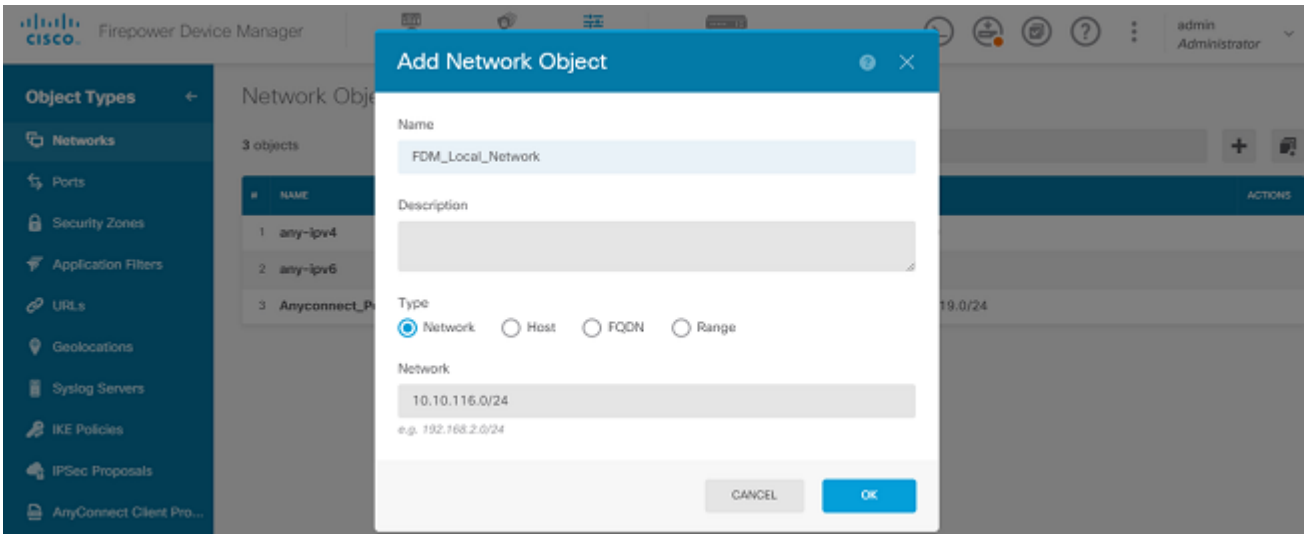
Konfigurieren

Beginnen Sie mit der Konfiguration auf FTD mit FDM.

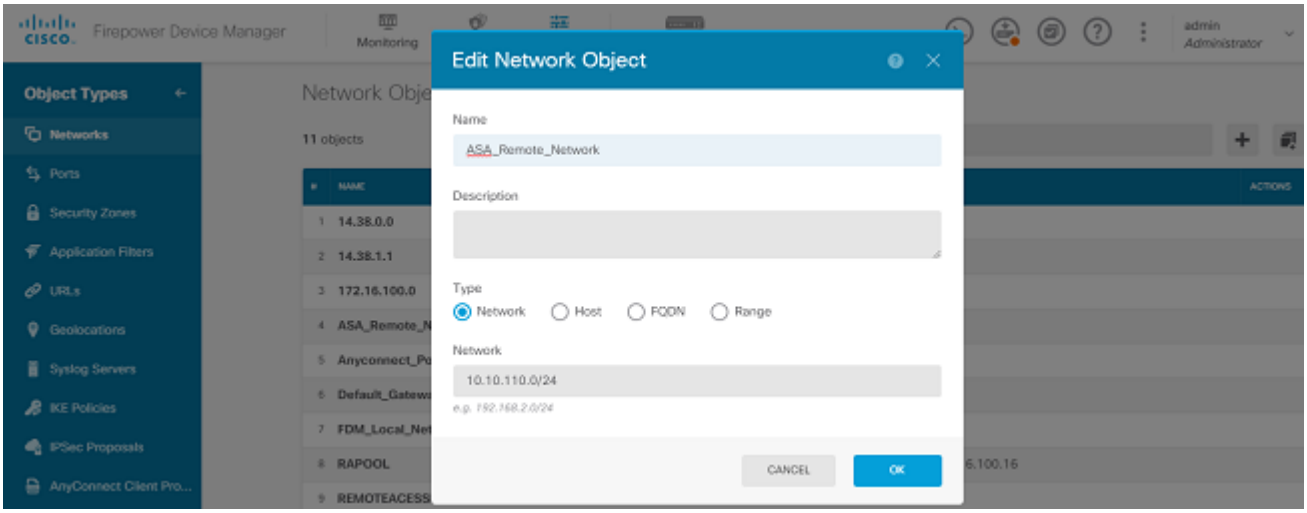
Geschützte Netzwerke definieren

Navigieren Sie zu **Objekte > Netzwerke > Neues Netzwerk hinzufügen**.

Konfigurieren von Objekten für die LAN-Netzwerke über die FDM-GUI Erstellen Sie ein Objekt für das lokale Netzwerk hinter dem FDM-Gerät, wie im Bild gezeigt.



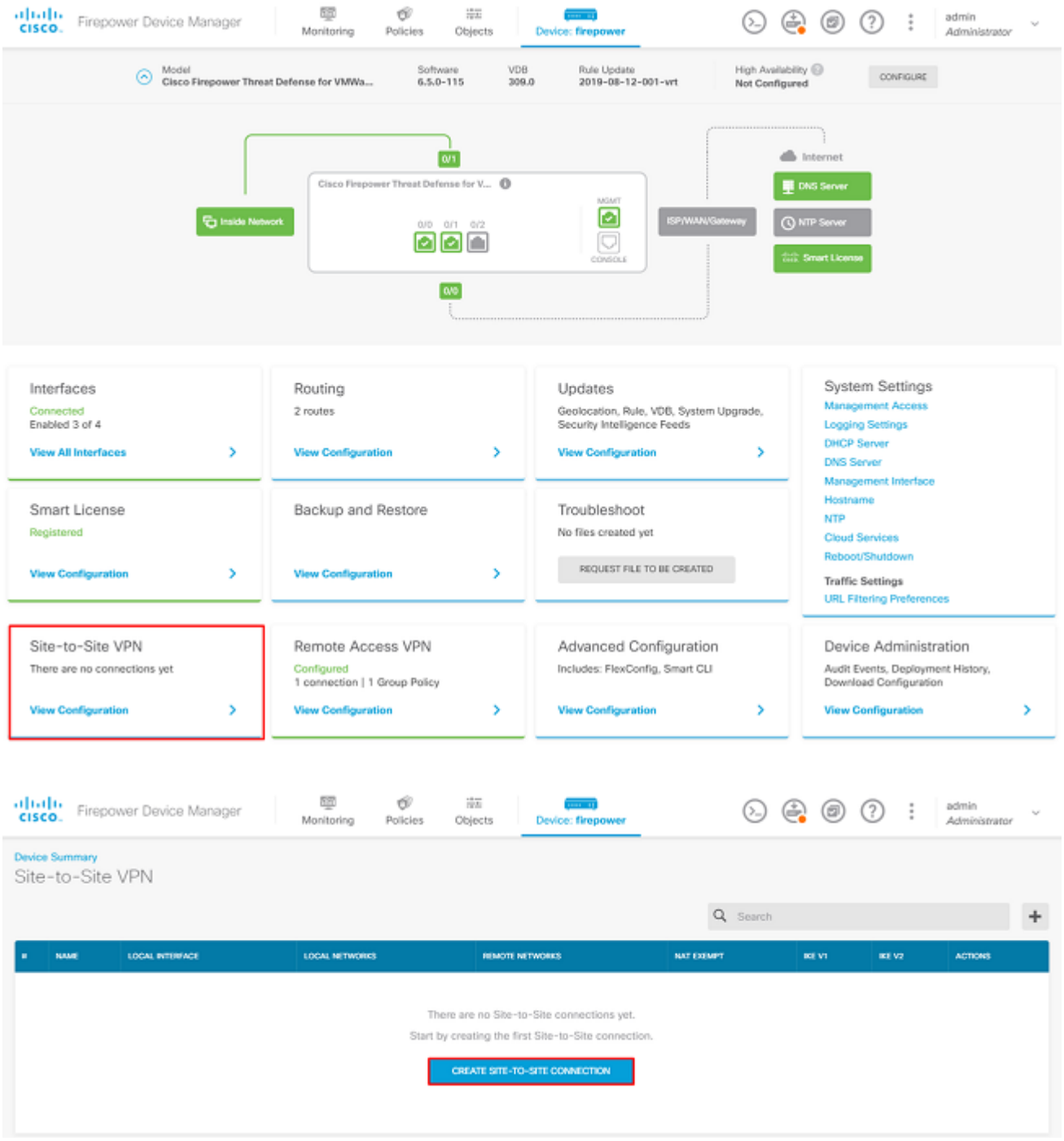
Erstellen Sie ein Objekt für das Remote-Netzwerk hinter dem ASA-Gerät, wie im Bild dargestellt.



Site-to-Site-VPN konfigurieren

Navigieren Sie zu **Site-to-Site-VPN > Site-to-Site-Verbindung erstellen**.

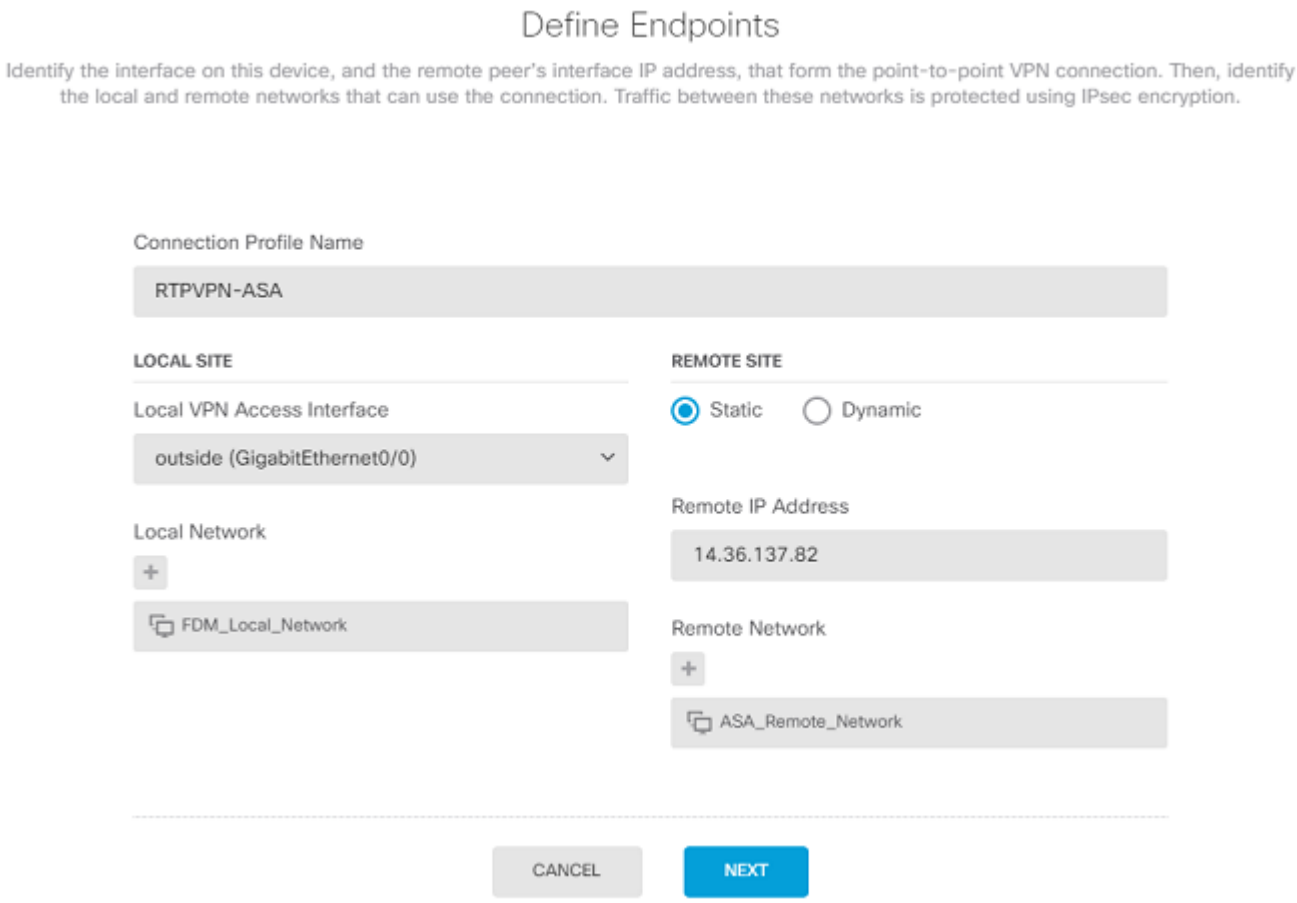
Gehen Sie durch den Site-to-Site-Assistenten auf FDM, wie im Bild gezeigt.



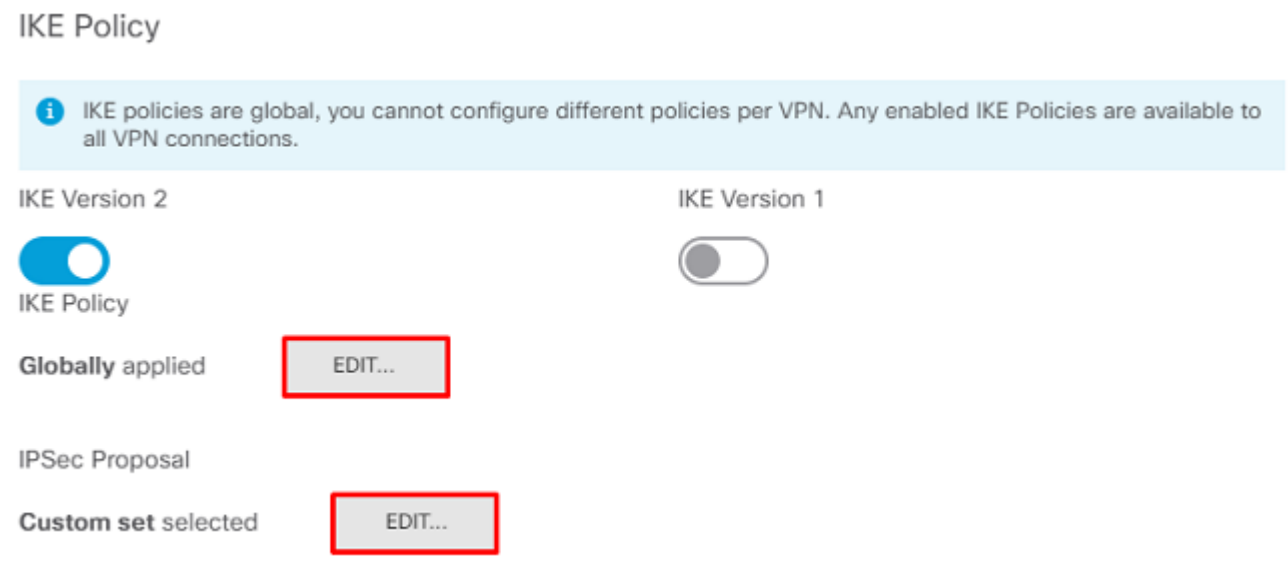
Geben Sie der Site-to-Site-Verbindung einen leicht identifizierbaren Namen für das Verbindungsprofil.

Wählen Sie die richtige externe Schnittstelle für den FTD aus, und wählen Sie dann das lokale Netzwerk aus, das über das Site-to-Site-VPN verschlüsselt werden soll.

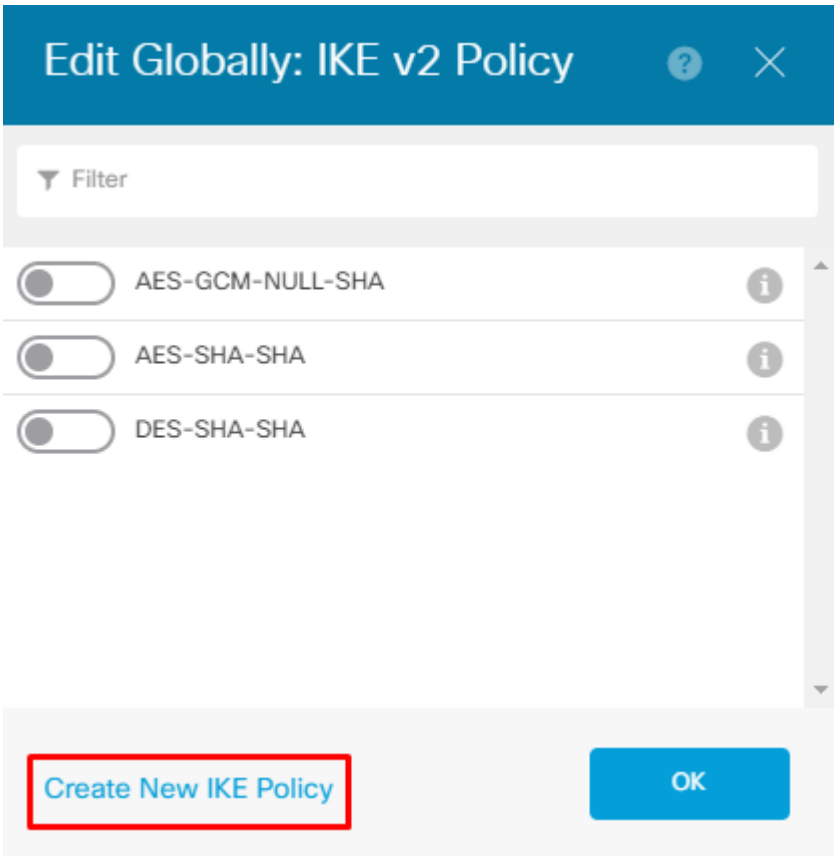
Legen Sie die öffentliche Schnittstelle des Remote-Peers fest. Wählen Sie dann das Netzwerk der Remote-Peers aus, das über das Site-to-Site-VPN verschlüsselt ist, wie im Bild gezeigt.



Klicken Sie auf der nächsten Seite auf die Schaltfläche **Edit** (**Bearbeiten**), um die IKE-Parameter (Internet Key Exchange) wie im Bild dargestellt festzulegen.

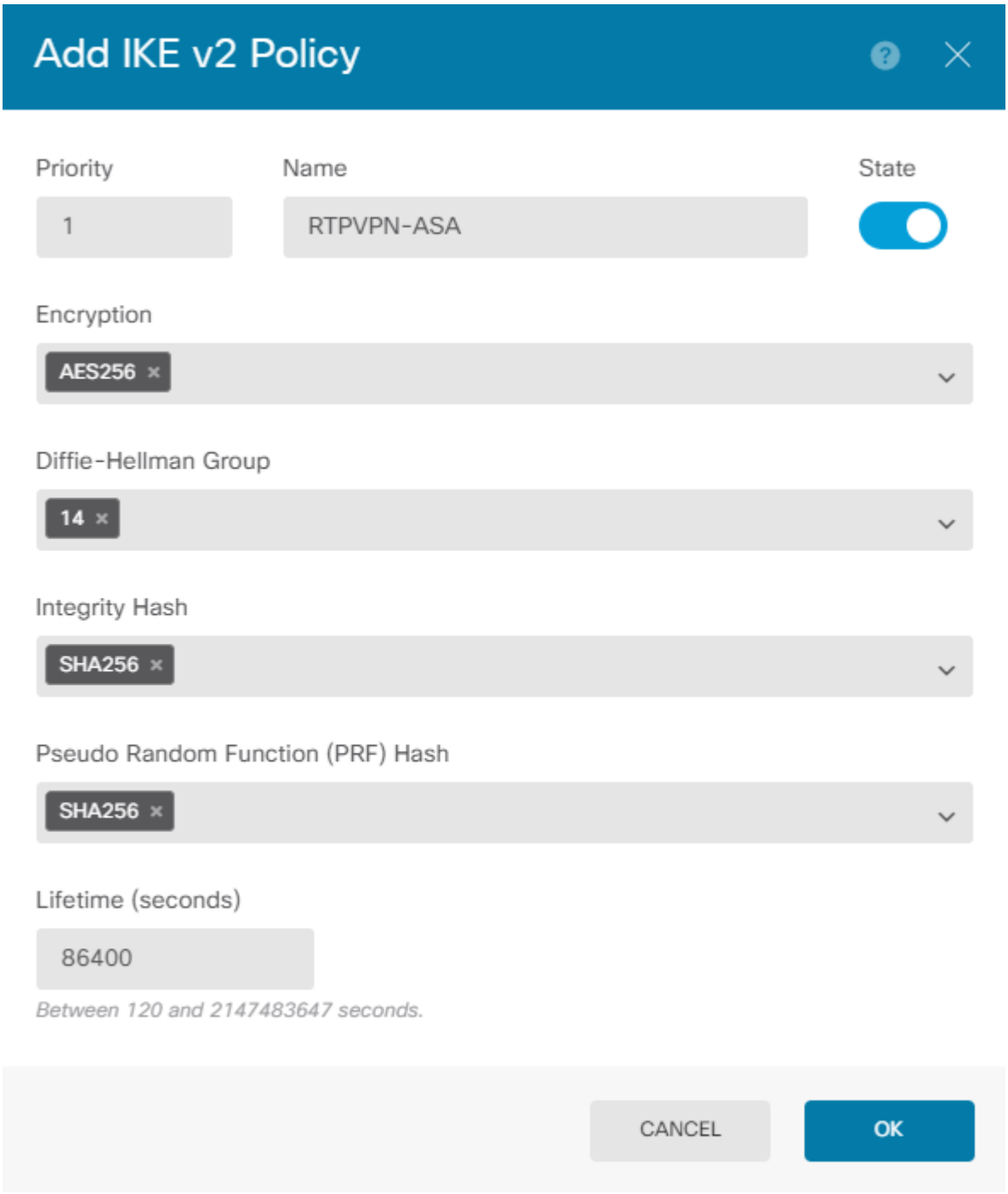


Wählen Sie die Schaltfläche **Create New IKE Policy** (Neue IKE-Richtlinie erstellen), wie im Bild dargestellt.

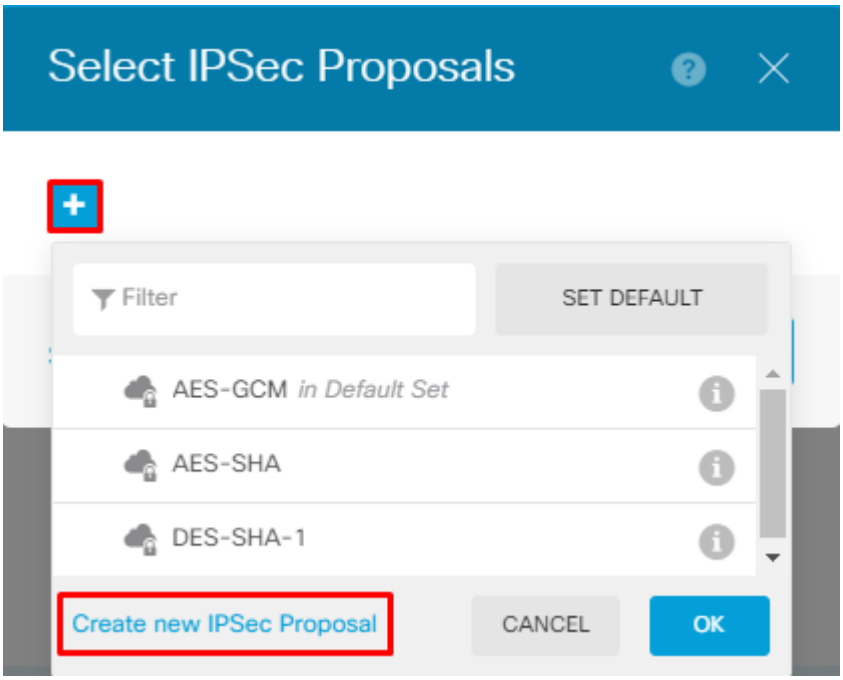


In diesem Leitfaden werden folgende Parameter für den IKEv2-Erstaustausch verwendet:

Verschlüsselung AES-256
Integrität SHA256
DH-Gruppe 14
PRF SHA256



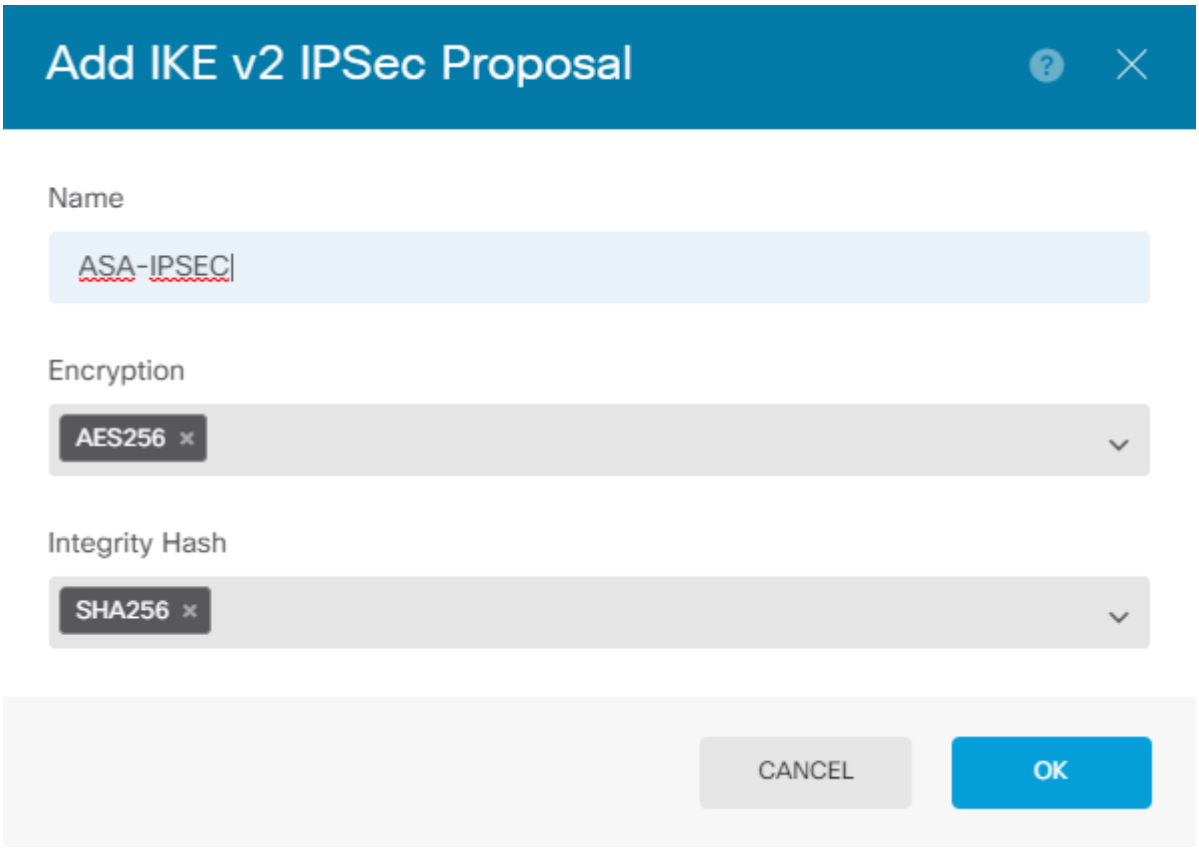
Wenn Sie wieder auf der Hauptseite sind, wählen Sie die Schaltfläche **Bearbeiten** für das IPSec-Angebot aus. Erstellen Sie einen neuen IPSec-Vorschlag, wie im Bild dargestellt.



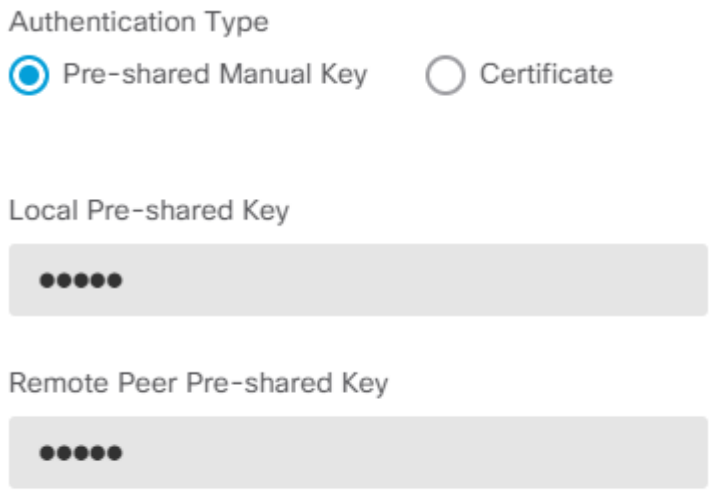
In diesem Leitfaden werden folgende Parameter für IPSec verwendet:

Verschlüsselung AES-256

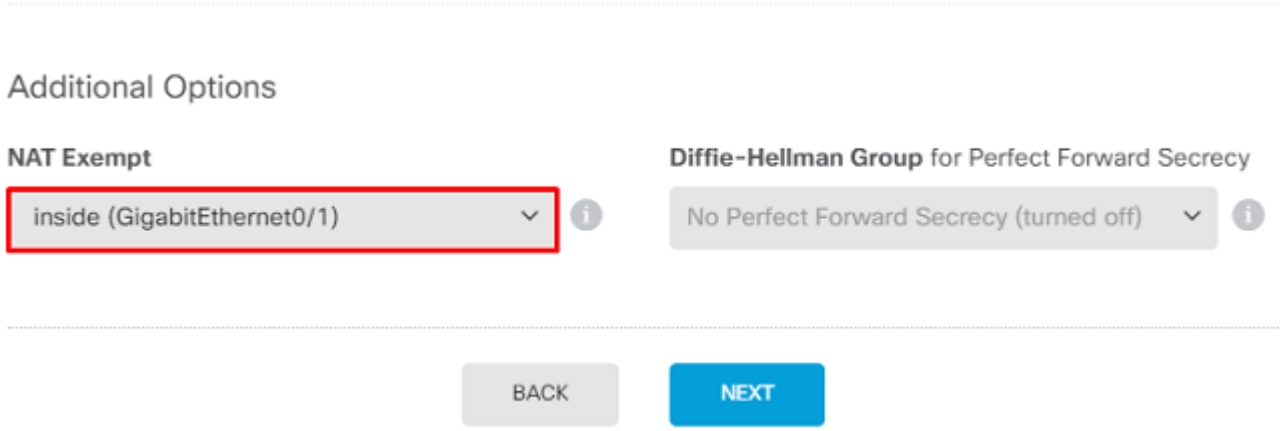
Integrität SHA256



Legen Sie für die Authentifizierung den vorinstallierten Schlüssel fest, und geben Sie den vorinstallierten Schlüssel (Pre-Shared Key, PSK) ein, der auf beiden Seiten verwendet wird. In diesem Leitfaden wird der PSK von Cisco verwendet, wie in der Abbildung dargestellt.



Legen Sie die interne Schnittstelle für NAT Exempt fest. Wenn mehrere interne Schnittstellen verwendet werden, muss unter **Policies (Richtlinien) > NAT (NAT)** eine manuelle Regel für NAT-Ausnahmen erstellt werden.



Auf der letzten Seite wird eine Zusammenfassung der Site-to-Site-Verbindung angezeigt. Stellen Sie sicher, dass die richtigen IP-Adressen ausgewählt und die richtigen Verschlüsselungsparameter verwendet werden, und drücken Sie die Schaltfläche "Beenden". Bereitstellung des neuen standortübergreifenden VPN.

Die ASA-Konfiguration wird mithilfe der CLI abgeschlossen.

ASA-Konfiguration

1. Aktivieren Sie IKEv2 auf der externen Schnittstelle der ASA:

```
Crypto ikev2 enable outside
```

2. Erstellen Sie die IKEv2-Richtlinie, die dieselben Parameter definiert, die auch für das FTD konfiguriert wurden:

```
Crypto ikev2 policy 1
 Encryption aes-256
 Integrity sha256
 Group 14
 Prf sha256
 Lifetime seconds 86400
```

3. Erstellen Sie eine Gruppenrichtlinie, die das IKEv2-Protokoll zulässt:

```
Group-policy FDM_GP internal
Group-policy FDM_GP attributes
Vpn-tunnel-protocol ikev2
```

4. Erstellen Sie eine Tunnelgruppe für die öffentliche FTD-IP-Adresse des Peers. Verweisen Sie auf die Gruppenrichtlinie, und geben Sie den Pre-Shared Key an:

```
Tunnel-group 172.16.100.10 type ipsec-l2l
Tunnel-group 172.16.100.10 general-attributes
 Default-group-policy FDM_GP
Tunnel-group 172.16.100.10 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco
 ikev2 remote-authentication pre-shared-key cisco
```

5. Erstellen Sie eine Zugriffsliste, die den zu verschlüsselnden Datenverkehr definiert: (FTDSubnet 10.10.116.0/24) (ASASubnet 10.10.110.0/24):

```
Object network FDMSubnet
 Subnet 10.10.116.0 255.255.255.0
Object network ASASubnet
 Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. Erstellen Sie einen IKEv2-IPsec-Vorschlag, der auf die im FTD angegebenen Algorithmen verweist:

```
Crypto ipsec ikev2 ipsec-proposal FDM
```

```
Protocol esp encryption aes-256
Protocol esp integrity sha-256
```

7. Erstellen Sie einen Crypto Map-Eintrag, der die Konfiguration verknüpft:

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

8. Erstellen Sie eine NAT-Ausnahmegenehmigung, die verhindert, dass der VPN-Datenverkehr von der Firewall mit NATTED versehen wird:

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FDMSubnet FDMSubnet
no-proxy-arp route-lookup
```

Überprüfung

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

Versuchen Sie, Datenverkehr über den VPN-Tunnel zu initiieren. Beim Zugriff auf die Befehlszeile der ASA oder FTD kann dies mit dem Befehl "Packet Tracer" erfolgen. Wenn Sie den Befehl "Packet-Tracer" verwenden, um den VPN-Tunnel zu öffnen, muss dieser zweimal ausgeführt werden, um zu überprüfen, ob der Tunnel gestartet wird. Bei der ersten Ausführung des Befehls ist der VPN-Tunnel ausgefallen, sodass der Befehl "packet-tracer" mit VPN encrypt DROP fehlschlägt. Verwenden Sie nicht die interne IP-Adresse der Firewall als Quell-IP-Adresse im Paket-Tracer, da dies immer fehlschlägt.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside
```

```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0

Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Navigieren Sie zur CLI des FTD oder ASA, um den Tunnelstatus zu überwachen.

Überprüfen Sie über die FTD-CLI Phase-1 und Phase-2 mit dem Befehl **show crypto ikev2 sa**.

```
> show crypto ikev2 sa

IKEv2 SAs:

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

```
Tunnel-id Local                                                 Remote
  3821043 172.16.100.10/500                                      192.168.200.10/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1150 sec
Child sa: local selector  10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Anfängliche Verbindungsprobleme

Wenn Sie ein VPN aufbauen, gibt es zwei Seiten, die den Tunnel aushandeln. Daher ist es am besten, beide Seiten des Gesprächs zu erhalten, wenn Sie eine Fehlerbehebung für jede Art von Tunnelausfall durchführen. Eine detaillierte Anleitung zum Debuggen von IKEv2-Tunneln finden Sie hier: So debuggen Sie IKEv2-VPNs

Die häufigste Ursache von Tunnelausfällen ist ein Verbindungsproblem. Die beste Methode, dies zu bestimmen, ist die Paketerfassung auf dem Gerät.

Verwenden Sie diesen Befehl, um die Paketerfassung auf dem Gerät zu übernehmen:

```
Capture capout interface outside match ip host 172.16.100.10 host 192.168.200.10
```

Sobald die Erfassung implementiert ist, versuchen Sie, Datenverkehr über das VPN zu senden, und prüfen Sie, ob bei der Paketerfassung bidirektionaler Datenverkehr vorhanden ist.

Überprüfen Sie die Paketerfassung mit dem Befehl **show cap capout**.

```
firepower# show cap capout

4 packets captured

   1: 01:21:06.763983       172.16.100.10.500 > 192.168.200.10.500:  udp 574
   2: 01:21:06.769415       192.168.200.10.500 > 172.16.100.10.500:  udp 619
   3: 01:21:06.770666       172.16.100.10.500 > 192.168.200.10.500:  udp 288
   4: 01:21:06.773748       192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

Datenverkehrsspezifische Probleme

Häufige Datenverkehrsprobleme bei Benutzern:

- Routing-Probleme hinter dem FTD - internes Netzwerk kann Pakete nicht zu den zugewiesenen IP-Adressen und VPN-Clients zurückleiten.
- Zugriffskontrolllisten blockieren den Datenverkehr.
- Network Address Translation (NAT) wird für VPN-Datenverkehr nicht umgangen.

Zugehörige Informationen

Weitere Informationen zu Site-to-Site-VPNs auf dem von FDM verwalteten FTD finden Sie hier.

- FTD verwaltet durch FDM - Konfigurationsleitfaden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.