

Konfigurieren eines VRF-kompatiblen, routenbasierten Site-to-Site-VPN auf einem von FDM verwalteten FTD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[FTD konfigurieren](#)

[Konfigurieren der ASA](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Referenz](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein VRF-fähiges, routenbasiertes Site-to-Site-VPN auf einem durch FDM verwalteten FTD konfigurieren.

Voraussetzungen

Anforderungen

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

- Grundlegendes Verständnis von VPN
- Grundlegendes Verständnis von Virtual Routing and Forwarding (VRF)
- 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

- Cisco ASA Version 9.20.3

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.

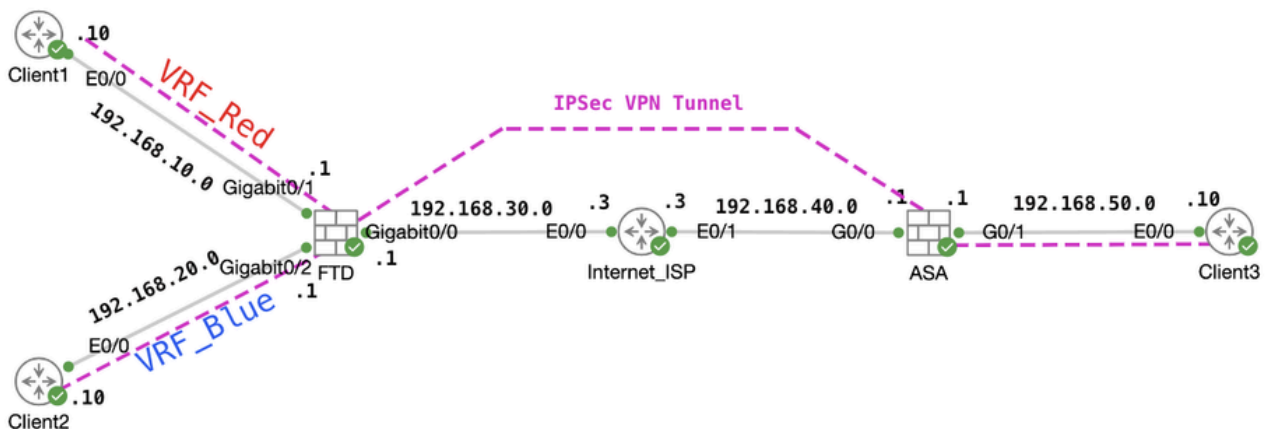
Hintergrundinformationen

Virtual Routing and Forwarding (VRF) im FirePOWER Device Manager (FDM) ermöglicht Ihnen die Erstellung mehrerer isolierter Routing-Instanzen auf einem einzelnen FirePOWER Threat Defense (FTD)-Gerät. Jede VRF-Instanz fungiert als separater virtueller Router mit eigener Routing-Tabelle, die eine logische Trennung des Netzwerkverkehrs ermöglicht und erweiterte Sicherheits- und Datenverkehrsmanagementfunktionen bietet.

In diesem Dokument wird erläutert, wie VRF-kompatibles IPSec VPN mit VTI konfiguriert wird. VRF Red-Netzwerk und VRF Blue-Netzwerk liegen hinter FTD. Client1 im VRF-Rot-Netzwerk und Client2 in VRF-Blau kommunizieren über den IPSec-VPN-Tunnel mit Client 3 hinter der ASA.

Konfigurieren

Netzwerkdiagramm

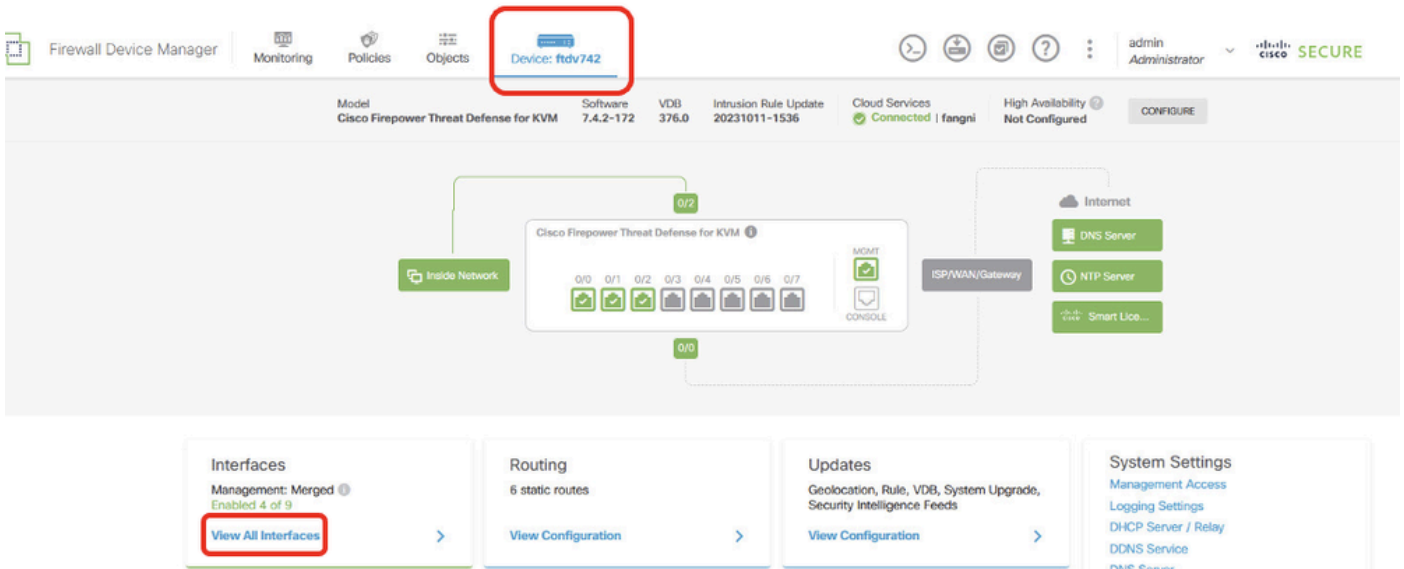


Topologie

FTD konfigurieren

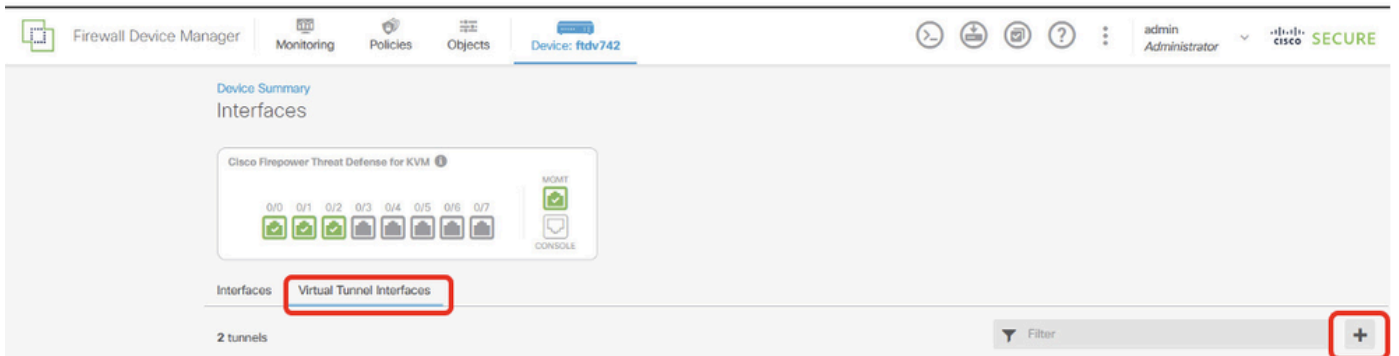
Schritt 1: Es muss sichergestellt werden, dass die vorläufige Konfiguration der IP-Interkonnektivität zwischen den Knoten ordnungsgemäß abgeschlossen wurde. Client1 und Client2 haben die FTD Inside IP-Adresse als Gateway. Der Client3 hat die ASA-interne IP-Adresse als Gateway.

Schritt 2: Erstellen Sie eine virtuelle Tunnelschnittstelle. Melden Sie sich bei der FDM-GUI von FTD an. Navigieren Sie zu Gerät > Schnittstellen . Klicken Sie auf Alle Schnittstellen anzeigen .



FTD_View_Interfaces

Schritt 2.1. Klicken Sie auf die Registerkarte "Virtuelle Tunnelschnittstellen". Klicken Sie auf +.



FTD_Erstellen_VTI

Schritt 2.2. Geben Sie die erforderlichen Informationen ein. 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.

Name
demovti

Status

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

Description

Tunnel ID
1
0 - 10413

Tunnel Source
outside (GigabitEthernet0/0)

IP Address and Subnet Mask
169.254.10.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL **OK**

FTD_Create_VTI_Details

Schritt 3: Navigieren Sie zu Gerät > Site-to-Site-VPN . Klicken Sie auf Konfiguration anzeigen.

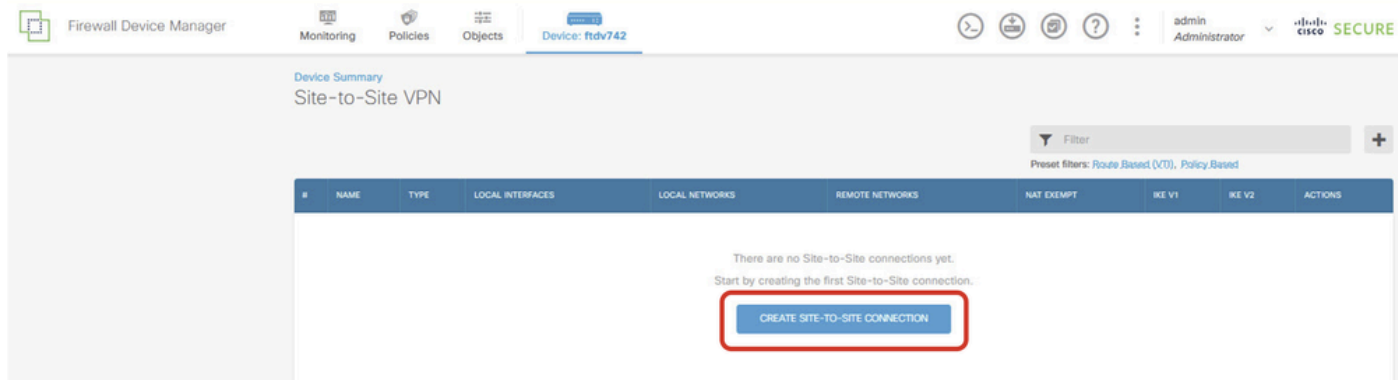
Firewall Device Manager | Monitoring | Policies | Objects | **Device: ftdv742** | admin Administrator | Cisco FIREPOWER SECURE

Model: Cisco Firepower Threat Defense for KVM | Software: 7.4.2-172 | VDB: 376.0 | Intrusion Rule Update: 20231011-1536 | Cloud Services: Issues | Unknown | High Availability: Not Configured | **CONFIGURE**

Inside Network | Cisco Firepower Threat Defense for KVM | Internet | DNS Server | NTP Server | Smart Lic...

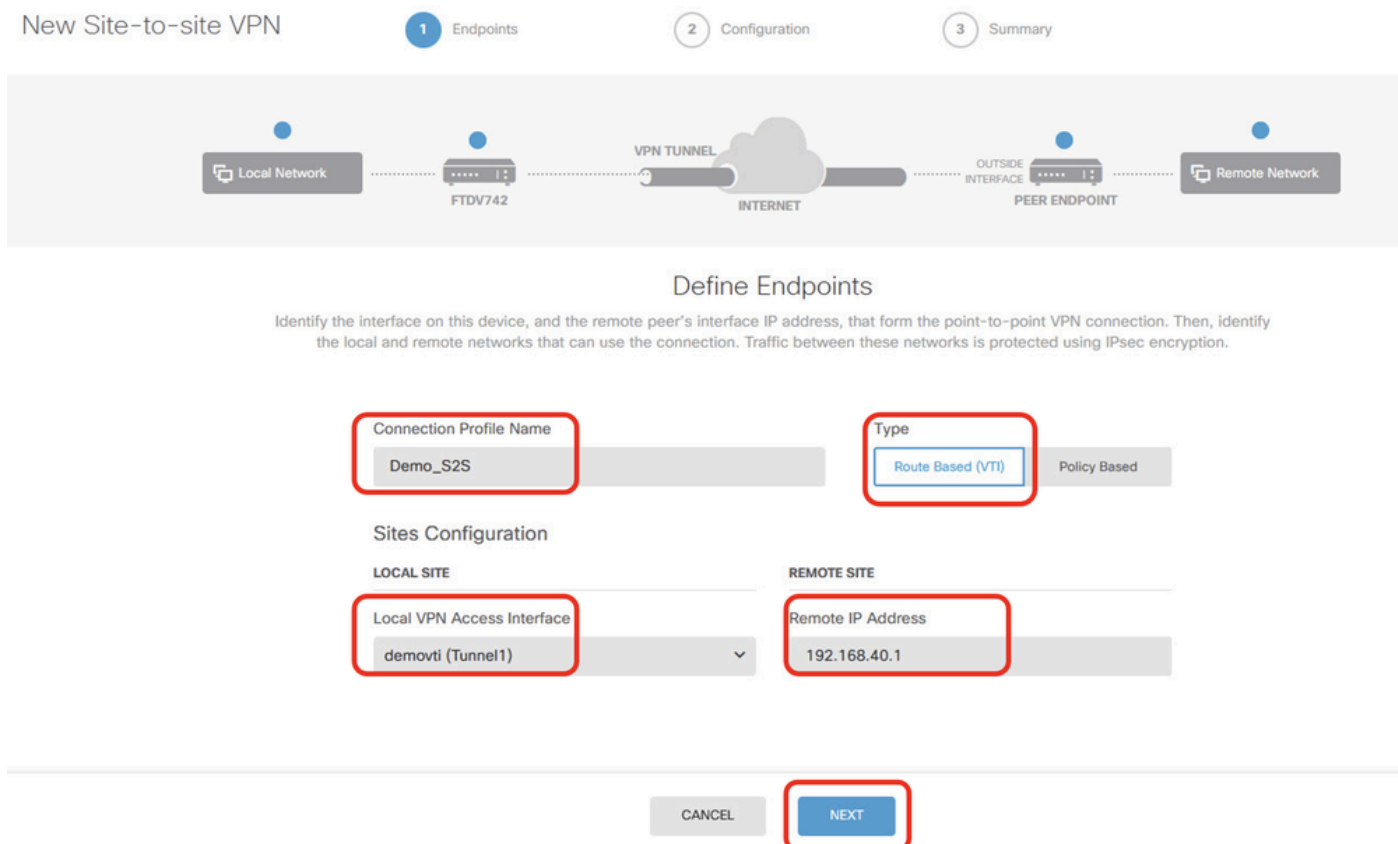
| | | | |
|--|--|---|---|
| Interfaces Management: Merged Enabled 4 of 9 View All Interfaces | Routing 1 static route View Configuration | Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration | System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server Hostname Time Services SSL Settings See more |
| Smart License Registered Tier: FTDv50 - 10 Gbps View Configuration | Backup and Restore View Configuration | Troubleshoot No files created yet REQUEST FILE TO BE CREATED | |
| Site-to-Site VPN There are no connections yet View Configuration | Remote Access VPN Requires Secure Client License No connections 1 Group Policy Configure | Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration | Device Administration Audit Events, Deployment History, Download Configuration View Configuration |

Schritt 3.1. Erstellen Sie ein neues Site-to-Site-VPN. Klicken Sie auf DIE Schaltfläche SITE-TO-SITE-VERBINDUNG ERSTELLEN. Oder klicken Sie auf die Schaltfläche +.

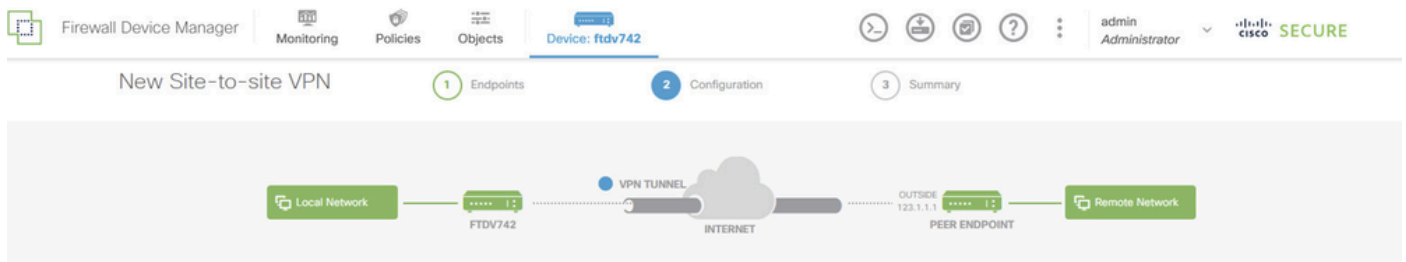


Schritt 3.2: Bereitstellen notwendige Informationen. Klicken Sie auf die Schaltfläche WEITER.

- Verbindungsprofilname: Demo S2S
- Typ: Routenbasiert (VTI)
- Lokale VPN-Zugangsoberfläche: demovti (erstellt in Schritt 2)
- Remote-IP-Adresse: 192.168.40.1 (dies ist die Peer-ASA außerhalb der IP-Adresse)



Schritt 3.3: Navigieren Sie zur IKE-Richtlinie. Klicken Sie auf die Schaltfläche BEARBEITEN.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

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

IKE VERSION 2

IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

None selected 

FTD_Bearbeiten_IKE_Richtlinie

Schritt 3.4: Für die IKE-Richtlinie können Sie eine vordefinierte Richtlinie verwenden oder eine neue erstellen, indem Sie auf **Neue IKE-Richtlinie erstellen** klicken.

In diesem Beispiel wird ein vorhandener IKE-Richtlinienname AES-SHA-SHA umgeschaltet. Klicken Sie auf **OK**, um zu speichern.

Filter

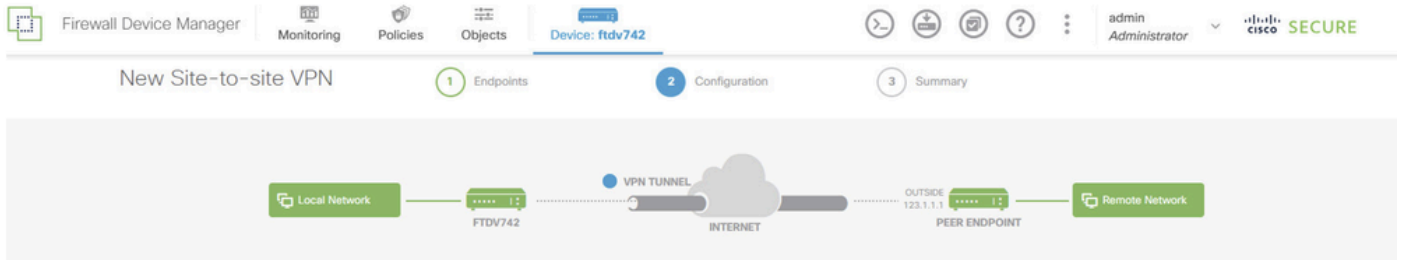
| | | |
|-------------------------------------|------------------|---|
| <input type="checkbox"/> | AES-GCM-NULL-SHA | i |
| <input checked="" type="checkbox"/> | AES-SHA-SHA | i |
| <input type="checkbox"/> | DES-SHA-SHA | i |

Create New IKE Policy

OK

FTD_Aktivieren_IKE_Richtlinie

Schritt 3.5. Navigieren Sie zu IPSec-Angebot. Klicken Sie auf die Schaltfläche BEARBEITEN.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

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

IKE VERSION 2

IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

None selected 1

FTD_Bearbeiten_IPSec_Angebot

Schritt 3.6. Für ein IPSec-Angebot können Sie das vordefinierte verwenden oder ein neues erstellen, indem Sie auf Neues IPSec-Angebot erstellen klicken.

In diesem Beispiel ein- und ausschalten eines vorhandenen IPSec-Angebotsnamens AES-SHA. Klicken Sie auf OK zu speichern.

Select IPsec Proposals



The screenshot shows a dialog box titled "Select IPsec Proposals". At the top left is a plus sign icon. Below it is a "Filter" input field and a "SET DEFAULT" button. The main area contains a list of proposals: "AES-GCM *In Default Set*", "AES-SHA" (which is selected and highlighted in blue), and "DES-SHA-1". Each proposal has an information icon (i) to its right. At the bottom, there are three buttons: "Create new IPsec Proposal" (in blue), "CANCEL", and "OK" (which is highlighted with a red box).

FTD_Enable_IPsec_Proposal

Schritt 3.7: Blättern Sie auf der Seite nach unten, und konfigurieren Sie den vorinstallierten Schlüssel. Klicken Sie auf die Schaltfläche WEITER.

Notieren Sie sich diesen vorinstallierten Schlüssel, und konfigurieren Sie ihn später auf der ASA.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURI

FTDV742 | INTERNET | PEER ENDPOINT

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

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

IKE VERSION 2 | IKE VERSION 1

IKE Policy
Globally applied

IPSec Proposal
Custom set selected

Authentication Type
 Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

FTD_Konfiguration_Pre_Shared_Key

Schritt 3.8: 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.

Demo_S2S Connection Profile

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

VPN Access Interface demovti (169.254.10.1) ↔ **Peer IP Address** 192.168.40.1

IKE V2

IKE Policy aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14

IPSec Proposal aes,aes-192,aes-256-sha-512,sha-384,sha-256,sha-1

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

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

Diffie-Hellman: Null (not selected)
Group:

BACK **FINISH**

FTD_Überprüfung_VPN_Konfiguration

Schritt 3.9: 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.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURE

Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → **Access Control** → Intrusion

1 rule

| # | NAME | ACTION | SOURCE | | | DESTINATION | | | APPLICATIONS | URLS | USERS | ACTIONS |
|---|------------|--------|--------|----------|-------|-------------|----------|-------|--------------|------|-------|---------|
| | | | ZONES | NETWORKS | PORTS | ZONES | NETWORKS | PORTS | | | | |
| 1 | Demo_allow | Allow | ANY | ANY | ANY | ANY | ANY | ANY | ANY | ANY | | |

Default Action: Access Control **Block**

FTD_ACP_Beispiel

Schritt 3.10: (Optional) Konfigurieren Sie die NAT-Ausschlussregel für den Client-Datenverkehr

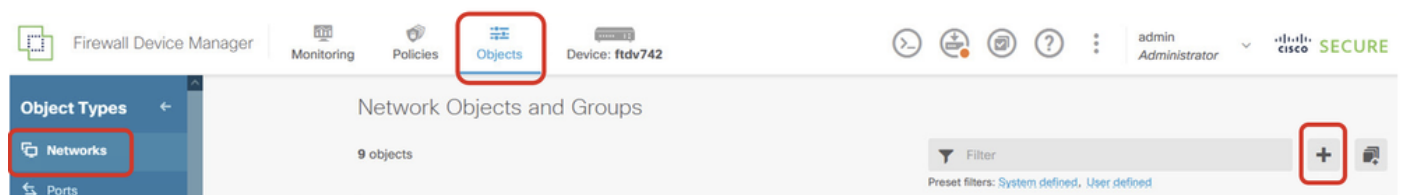
auf FTD, wenn eine dynamische NAT für den Client für den Zugriff auf das Internet konfiguriert ist. In diesem Beispiel muss keine NAT-Ausschlussregel konfiguriert werden, da für FTD keine dynamische NAT konfiguriert ist.

Schritt 3.11: Bereitstellen der Konfigurationsänderungen



Schritt 4: Konfigurieren virtueller Router

Schritt 4.1. Erstellen Sie Netzwerkobjekte für die statische Route. Navigieren Sie zu Objekte > Netzwerke, und klicken Sie auf +.



FTD_NetObjects erstellen

Schritt 4.2: Bereitstellen der erforderlichen Informationen zu jedem Netzwerkobjekt Klicken Sie auf OK.

- Name: local_blue_192.168.20.0
- Typ: Netzwerk
- Netzwerk: 192.168.20.0/24

Add Network Object



Name

local_blue_192.168.20.0

Description

Type



Network



Host

Network

192.168.20.0/24

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

CANCEL

OK

FTD_VRF_Blau_Netzwerk

- Name: local_red_192,168.10,0
- Typ: Netzwerk
- Netzwerk: 192.168.10.0/24

Add Network Object



Name

local_red_192.168.10.0

Description

Type



Network



Host

Network

192.168.10.0/24

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

CANCEL

OK

FTD_VRF_Rot_Netzwerk

- Name: remote_192,168,50,0
- Typ: Netzwerk
- Netzwerk: 192.168.50.0/24

Add Network Object



Name

remote_192.168.50.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.50.0/24

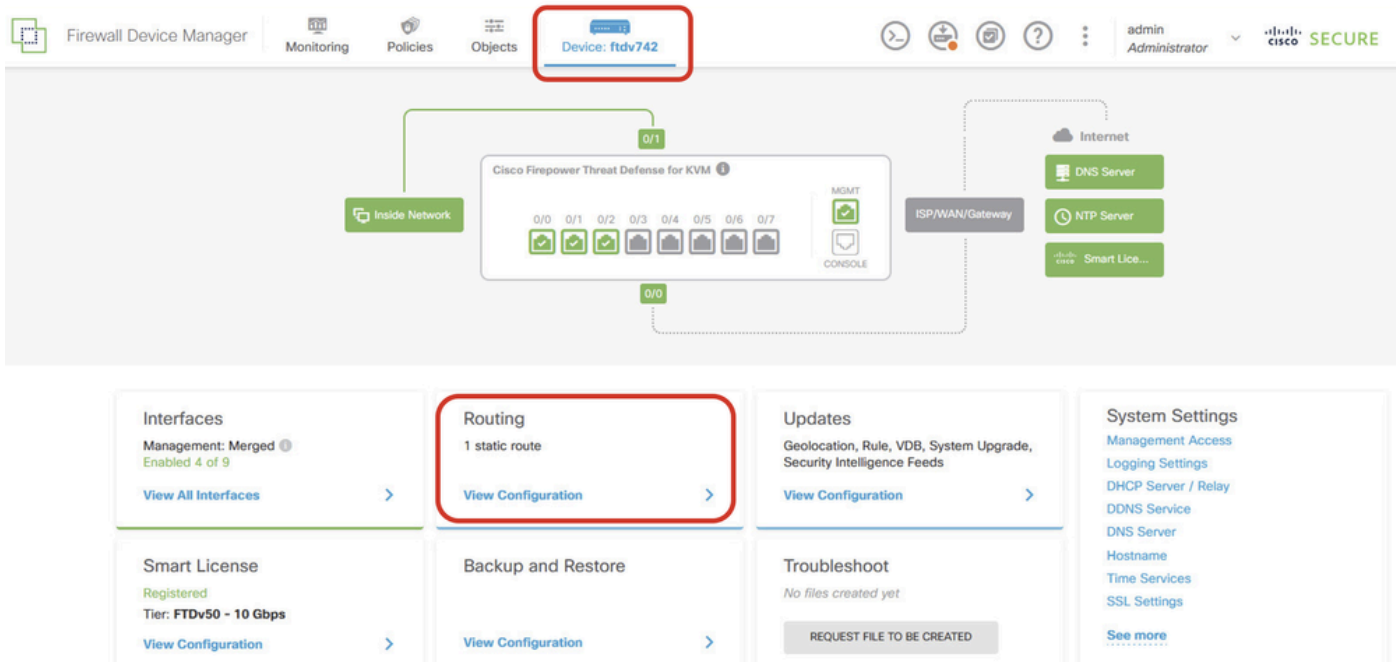
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

FTD_Remote_Netzwerk

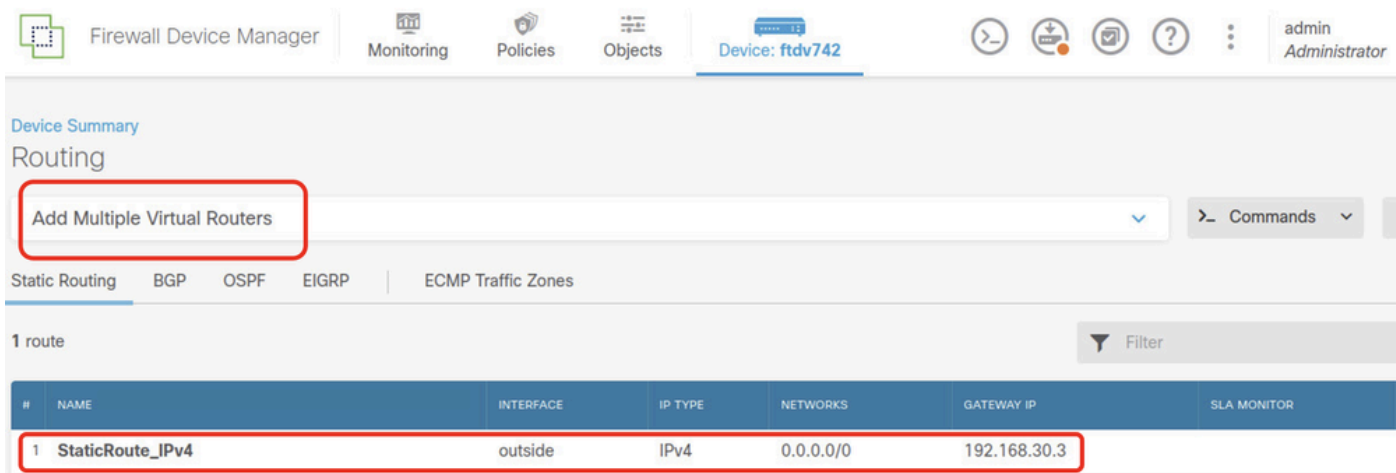
Schritt 4.3: Erstellen des ersten virtuellen Routers Navigieren Sie zu Gerät > Routing . Klicken Sie auf Konfiguration anzeigen .



FTD_Ansicht_Routing_Konfiguration

Schritt 4.4: Klicken Sie auf Mehrere virtuelle Router hinzufügen .

Anmerkung: Eine statische Route über eine externe Schnittstelle wurde bereits während der FDM-Initialisierung konfiguriert. Falls Sie es nicht haben, konfigurieren Sie es bitte manuell.



FTD_Hinzufügen_Erster_Virtueller_Router1

Schritt 4.5. Klicken Sie auf ERSTEN BENUTZERDEFINIERTEN VIRTUELLEN ROUTER ERSTELLEN .

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator

Device Summary

Routing

Virtual Route Forwarding (Virtual Routing) Description

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device.

Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

CREATE FIRST CUSTOM VIRTUAL ROUTER

FTD_Hinzufügen_Erster_Virtueller_Router2

Schritt 4.6: Bereitstellen der erforderlichen Informationen für den ersten virtuellen Router. Klicken Sie auf OK. Nach der Erstellung des ersten virtuellen Routers wird automatisch ein VRF-Name Global angezeigt.

- Name: VRF_Rot
- Schnittstellen: inside_red (GigabitEthernet0/1)

Firewall Device Manager | admin Administrator

Device Summary

Routing

Virtual Route Forwarding (Virtual Routing) Description

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device.

Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

Add Virtual Router

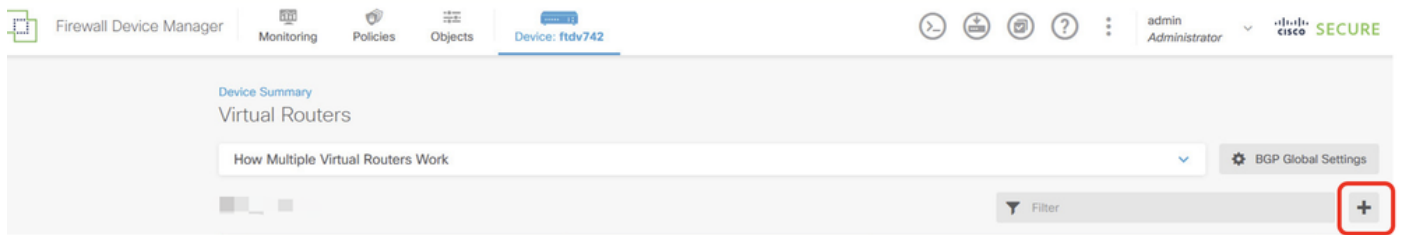
Name:

Description:

Interfaces:

FTD_Hinzufügen_Erster_Virtueller_Router3

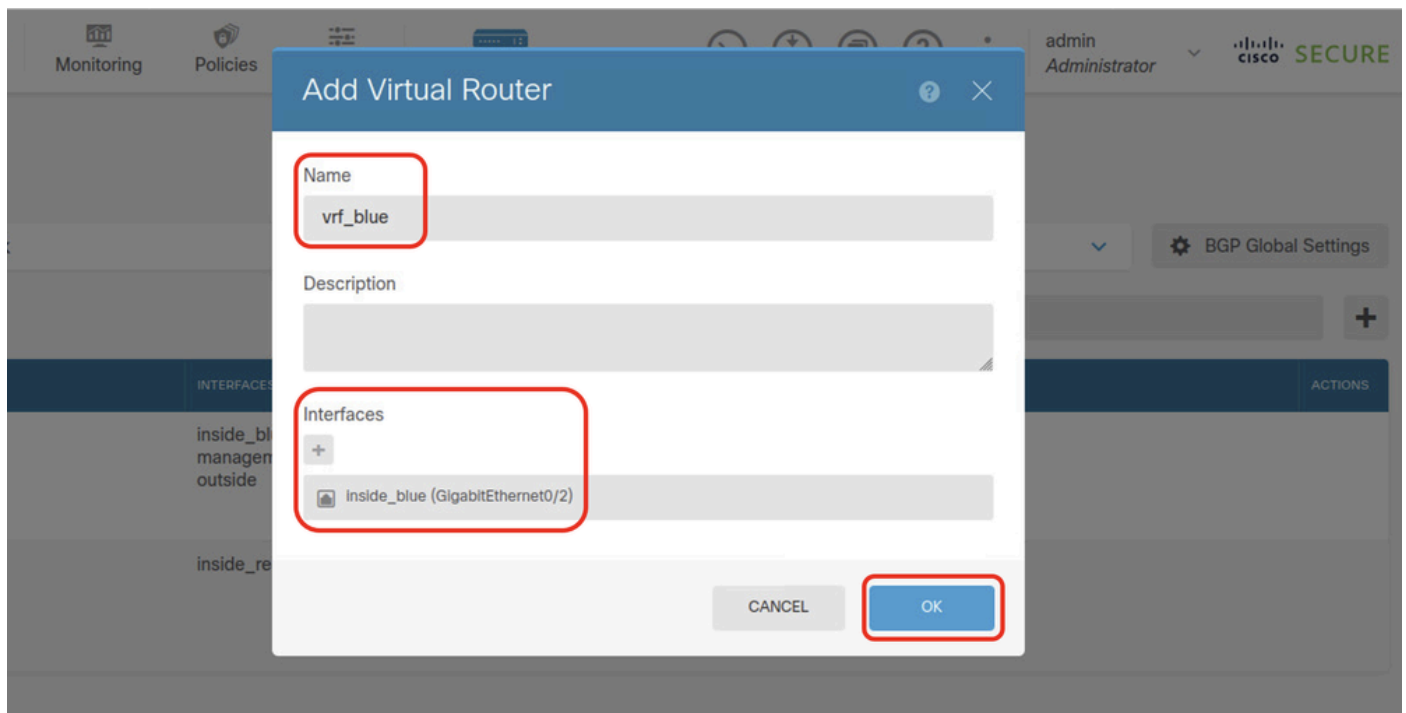
Schritt 4.7: Erstellen Sie einen zweiten virtuellen Router. Navigieren Sie zu Gerät > Routing . Klicken Sie auf Konfiguration anzeigen . Klicken Sie auf +.



FTD_Add_Second_Virtueller_Router

Schritt 4.8: Bereitstellen der erforderlichen Informationen für den zweiten virtuellen Router. Klicken Sie auf die Schaltfläche OK.

- Name: VRF_Blau
- Schnittstellen: inside_blue (GigabitEthernet0/2)



FTD_Add_Second_Virtueller_Router2

Schritt 5: Erstellen Sie einen Route Leak von vrf_blue zu Global. Diese Route ermöglicht Endpunkten im Netzwerk 192.168.20.0/24, Verbindungen zu initiieren, die den Site-to-Site-VPN-Tunnel passieren würden. In diesem Beispiel schützt der Remote-Endpunkt das Netzwerk 192.168.50.0/24.

Navigieren Sie zu Gerät > Routing . Klicken Sie auf Konfiguration anzeigen. klicken Sie auf das Symbol Anzeigen. in der Zelle Action für den virtuellen Router vrf_blue ein.

Device Summary
Virtual Routers

How Multiple Virtual Routers Work

3 virtual routers

| # | NAME | INTERFACES | SHOW/TROUBLESHOOT | ACTIONS |
|---|----------|-----------------------|--|----------------------|
| 1 | Global | management outside | Routes IPv6 routes BGP OSPF | |
| 2 | vrf_blue | inside_blue | Routes IPv6 routes BGP OSPF | View |
| 3 | vrf_red | inside_red | Routes IPv6 routes BGP OSPF | |

FTD_Ansicht_VRF_Blau

Schritt 5.1. Klicken Sie auf die Registerkarte "Static Routing". Klicken Sie auf +.

Device Summary / Virtual Routers
vrf_blue

How Multiple Virtual Routers Work

Virtual Router Properties | **Static Routing** | BGP | OSPF | ECMP Traffic Zones

Commands

Filter +

FTD_Create_Static_Route_VRF_Blau

Schritt 5.2: Geben Sie die erforderlichen Informationen ein. Klicken Sie auf OK.

- Name: Blau_zu_ASA
- Schnittstelle: demovti (Tunnel1)
- Netzwerke: remote_192,168,50,0
- Gateway: Lassen Sie dieses Feld leer.

Name
Blue_to_ASA

Description

Interface
demovti (Tunnel1) Belongs to current Router
N/A

Protocol
 IPv4 IPv6

Networks
+
remote_192.168.50.0

Gateway
Please select a gateway Metric
1

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

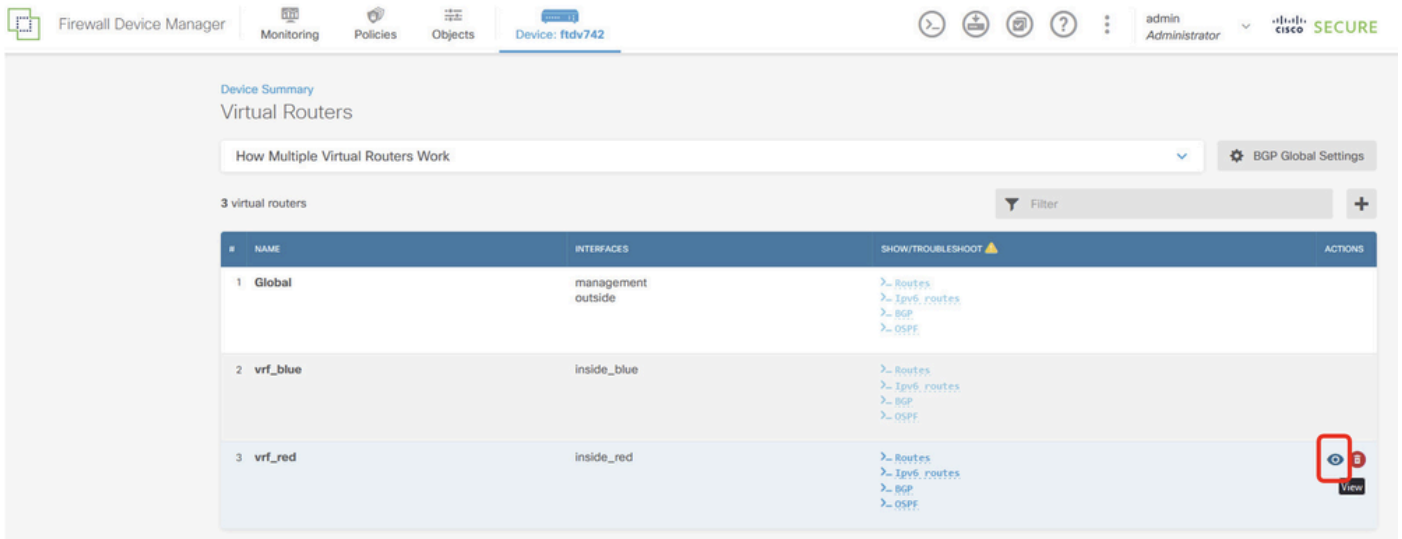
CANCEL OK

FTD_Create_Static_Route_VRF_Blue_Details

Schritt 6: Erstellen Sie einen Route Leak von vrf_red zu Global. Diese Route ermöglicht Endpunkten im Netzwerk 192.168.10.0/24, Verbindungen zu initiieren, die den Site-to-Site-VPN-

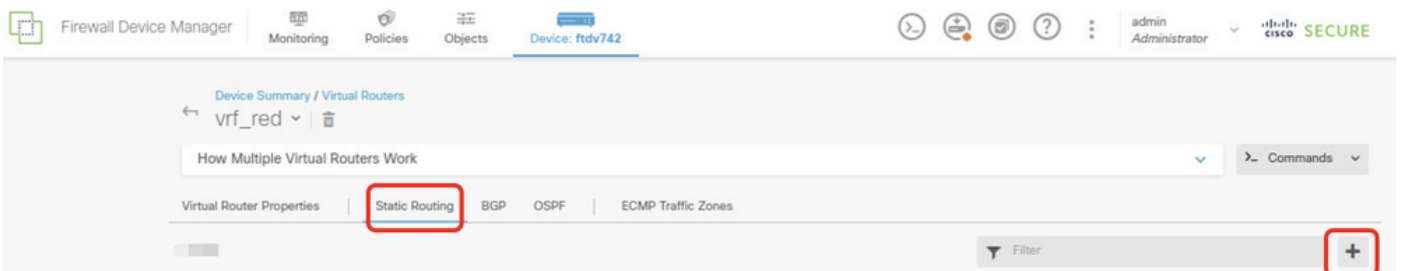
Tunnel passieren würden. In diesem Beispiel schützt der Remote-Endpunkt das Netzwerk 192.168.50.0/24.

Navigieren Sie zu Gerät > Routing . Klicken Sie auf Konfiguration anzeigen. klicken Sie auf das Symbol Anzeigen. in der Zelle Action für den virtuellen Router vrf_red ein.



FTD_Ansicht_VRF_Rot

Schritt 6.1. Klicken Sie auf die Registerkarte "Static Routing". Klicken Sie auf +.



FTD_Erstellen_Statische_Route_VRF_Rot

Schritt 6.2: Geben Sie die erforderlichen Informationen ein. Klicken Sie auf OK.

- Name: Rot_zu_ASA
- Schnittstelle: demovti (Tunnel1)
- Netzwerke: remote_192,168,50,0
- Gateway: Lassen Sie dieses Feld leer.

vrf_red

Add Static Route



Name

Red_to_ASA

Description

Interface

demovti (Tunnel1)

Belongs to current Router

N/A

Protocol



IPv4



IPv6

Networks



remote_192.168.50.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

FTD_Create_Static_Route_VRF_Red_Details

Schritt 7: Route Leak von Global- zu virtuellen Routern erstellen. Die Routen ermöglichen Endpunkten, die durch das Remote-Ende des Site-to-Site-VPN geschützt sind, den Zugriff auf das


Netzwerk 192.168.10.0/24 im virtuellen Router vrf_red und auf das Netzwerk 192.168.20.0/24 im virtuellen Router vrf_blue.

Navigieren Sie zu Gerät > Routing . Klicken Sie auf Konfiguration anzeigen . Klicken Sie auf das Symbol Anzeigen in der Zelle Aktion für den globalen virtuellen Router.

Device Summary
Virtual Routers

How Multiple Virtual Routers Work

3 virtual routers

| # | NAME | INTERFACES | SHOW/TROUBLESHOOT | ACTIONS |
|---|----------|-----------------------|--|---|
| 1 | Global | management outside | > Routes > IPv6 routes > BGP > OSPF |  |
| 2 | vrf_blue | inside_blue | > Routes > IPv6 routes > BGP > OSPF | |
| 3 | vrf_red | inside_red | > Routes > IPv6 routes > BGP > OSPF | |

FTD_Ansicht_VRF_Global

Schritt 7.1. Klicken Sie auf die Registerkarte "Static Routing". Klicken Sie auf +.

Device Summary / Virtual Routers
Global

How Multiple Virtual Routers Work

Virtual Router Properties | **Static Routing** | BGP | OSPF | EIGRP | ECMP Traffic Zones

3 routes

| # | NAME | INTERFACE | IP TYPE | NETWORKS | GATEWAY IP | SLA MONITOR | METRIC | ACTIONS |
|---|------------------|-----------|---------|-----------|--------------|-------------|--------|---|
| 1 | StaticRoute_IPv4 | outside | IPv4 | 0.0.0.0/0 | 192.168.30.3 | | 1 |  |

FTD_Create_Static_Route_VRF_Global

Schritt 7.2: Geben Sie die erforderlichen Informationen ein. Klicken Sie auf OK.

- Name: S2S_undicht_blau
- Schnittstelle: inside_blue (GigabitEthernet0/2)
- Netzwerke: local_blue_192.168.20.0
- Gateway: Lassen Sie dieses Feld leer.

Global Add Static Route



Name

S25_leak_blue

Description

 The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.

Interface

inside_blue (GigabitEthernet0/2)

Belongs to different Router

vt_blue

Protocol

IPv4

IPv6

Networks

+

local_blue_192.168.20.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

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

```
crypto ikev2 policy 20
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 21 20 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

Schritt 10: Erstellen Sie einen IKEv2 ipsec-Vorschlag, der die gleichen Parameter definiert, die auch für den FTD konfiguriert wurden.

<#root>

```
crypto ipsec ikev2 ipsec-proposal
```

AES-SHA

```
protocol esp encryption aes-256 aes-192 aes
protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

Schritt 11: Erstellen eines IPSec-Profil, referenzieren ipsec-Proposal wurde in Schritt 10 erstellt.

<#root>

```
crypto ipsec profile
```

```
demo_ipsec_profile
```

```
set ikev2 ipsec-proposal
```

AES-SHA

```
set security-association lifetime kilobytes 4608000
set security-association lifetime seconds 28800
```

Schritt 12: Erstellen einer Gruppenrichtlinie, die das IKEv2-Protokoll zulässt

<#root>

```
group-policy
```

```
demo_gp_192.168.30.1
```

```
internal
```

```
group-policy demo_gp_192.168.30.1 attributes
vpn-tunnel-protocol ikev2
```

Schritt 13: Erstellen Sie eine Tunnelgruppe für den Peer-FTD außerhalb der IP-Adresse. Verwenden Sie dabei die in Schritt 12 erstellte Gruppenrichtlinie, und Konfigurieren desselben Pre-Shared Keys mit FTD(erstellt in Schritt 3.7).

```
<#root>
```

```
tunnel-group 192.168.30.1 type ipsec-l2l
tunnel-group 192.168.30.1 general-attributes
default-group-policy
```

```
demo_gp_192.168.30.1
```

```
tunnel-group 192.168.30.1 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

Schritt 14: Aktivieren Sie IKEv2 auf der externen Schnittstelle.

```
crypto ikev2 enable outside
```

Schritt 15: Erstellen eines virtuellen Tunnels

```
<#root>
```

```
interface Tunnel1
nameif demovti_asa
ip address 169.254.10.2 255.255.255.0
tunnel source interface outside
tunnel destination 192.168.30.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile
```

```
demo_ipsec_profile
```

Schritt 16: Erstellen Sie eine statische Route.

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

Überprüfung

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

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

FTD:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftdv742#
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
32157565 192.168.30.1/500 192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/67986 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: 0x4cf55637/0xa493cc83
```

```
ftdv742# show crypto ipsec sa
interface: 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 (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.40.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: A493CC83
current inbound spi : 4CF55637
```

```

inbound esp sas:
  spi: 0x4CF55637 (1291146807)
  SA State: active
  transform: esp-aes-256 esp-sha-512-hmac no compression
  in use settings ={L2L, Tunnel, IKEv2, VTI, }
  slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
  sa timing: remaining key lifetime (kB/sec): (4055040/16867)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
outbound esp sas:
  spi: 0xA493CC83 (2761149571)
  SA State: active
  transform: esp-aes-256 esp-sha-512-hmac no compression
  in use settings ={L2L, Tunnel, IKEv2, VTI, }
  slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
  sa timing: remaining key lifetime (kB/sec): (4285440/16867)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

```

ASA:

```
ASA9203# show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```

Tunnel-id Local                               Remote
26025779 192.168.40.1/500                       192.168.30.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/68112 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: 0xa493cc83/0x4cf55637

```

```
ASA9203#
```

```
ASA9203# show cry
```

```
ASA9203# show crypto ipsec sa
```

```
interface: demovti_asa
```

```
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1
```

```

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.30.1

```

```

#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0

```

```
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 4CF55637
current inbound spi : A493CC83
```

```
inbound esp sas:
```

```
spi: 0xA493CC83 (2761149571)
```

```
SA State: active
```

```
transform: esp-aes-256 esp-sha-512-hmac no compression
```

```
in use settings ={L2L, Tunnel, IKEv2, VTI, }
```

```
slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
```

```
sa timing: remaining key lifetime (kB/sec): (4101120/16804)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Anti replay bitmap:
```

```
0x00000000 0x00000001
```

```
outbound esp sas:
```

```
spi: 0x4CF55637 (1291146807)
```

```
SA State: active
```

```
transform: esp-aes-256 esp-sha-512-hmac no compression
```

```
in use settings ={L2L, Tunnel, IKEv2, VTI, }
```

```
slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
```

```
sa timing: remaining key lifetime (kB/sec): (4055040/16804)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Anti replay bitmap:
```

```
0x00000000 0x00000001
```

Schritt 2: Überprüfen der Route von VRF und Global auf 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
SI    192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI    192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
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
```

```
ftdv742# show route vrf vrf_blue
```

Routing Table: vrf_blue

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 not set

```
C      192.168.20.0 255.255.255.0 is directly connected, inside_blue
L      192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

ftdv742# show route vrf vrf_red

Routing Table: vrf_red

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 not set

```
C      192.168.10.0 255.255.255.0 is directly connected, inside_red
L      192.168.10.1 255.255.255.255 is directly connected, inside_red
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

Schritt 3: Überprüfen des Ping-Tests

Vor dem Ping überprüfen Sie die Zähler von show crypto ipsec sa | inc interface:|encap|decap on FTD.

In diesem Beispiel zeigt Tunnel1 30 Pakete für Kapselung und Entkapselung.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

Client1 hat Client3 erfolgreich gepingt.

```
Client1#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 = 5/299/620 ms
```

Client2 hat Client3 erfolgreich gepingt.

```
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 = 11/297/576 ms
```

Überprüfen Sie die Zähler von `show crypto ipsec sa | inc interface:|encap|decap` auf FTD, nachdem ein Ping erfolgreich durchgeführt wurde.

In diesem Beispiel zeigt Tunnel1 40 Pakete für Kapselung und Entkapselung nach einem erfolgreichen Ping. Außerdem erhöhten sich beide Zähler um 10 Pakete, die den 10 Ping-Echo-Anforderungen entsprechen. Dies zeigt an, dass der Ping-Verkehr erfolgreich durch den IPSec-Tunnel geleitet wurde.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap  
interface: demovti  
    #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40  
    #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40  
    #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 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 Debug-Befehle verwenden, um Fehler im Routenabschnitt zu beheben.

debug ip routing

Referenz

[Konfigurationsleitfaden für Cisco Secure Firewall Device Manager, Version 7.4](#)

[Konfigurationsleitfaden für die Cisco Secure Firewall ASA VPN CLI, 9.20](#)

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.