

Konfigurieren von AnyConnect für den Zugriffsserver über den IPSec-Tunnel

Inhalt

[Einführung:](#)

[Voraussetzungen:](#)

[Grundlegende Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfigurationen auf FMC](#)

[RAVPN-Konfiguration auf dem von FMC verwalteten FTD.](#)

[IKEv2 VPN auf FTD, von FMC verwaltet:](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einführung:

In diesem Dokument werden die Verfahren für die Bereitstellung einer RAVPN-Konfiguration auf dem vom FMC verwalteten FTD sowie ein Site-to-Site-Tunnel zwischen FTDs beschrieben.

Voraussetzungen:

Grundlegende Anforderungen

- Ein grundlegendes Verständnis von Site-to-Site-VPNs und RAVPNs ist von Vorteil.
- Grundlegende Informationen zur Konfiguration eines richtlinienbasierten IKEv2-Tunnels auf der Cisco FirePOWER-Plattform sind wichtig.

Dieses Verfahren dient zur Bereitstellung einer RAVPN-Konfiguration auf dem vom FMC verwalteten FTD sowie eines Site-to-Site-Tunnels zwischen FTDs, über den AnyConnect-Benutzer auf den Server hinter dem anderen FTD-Peer zugreifen können.

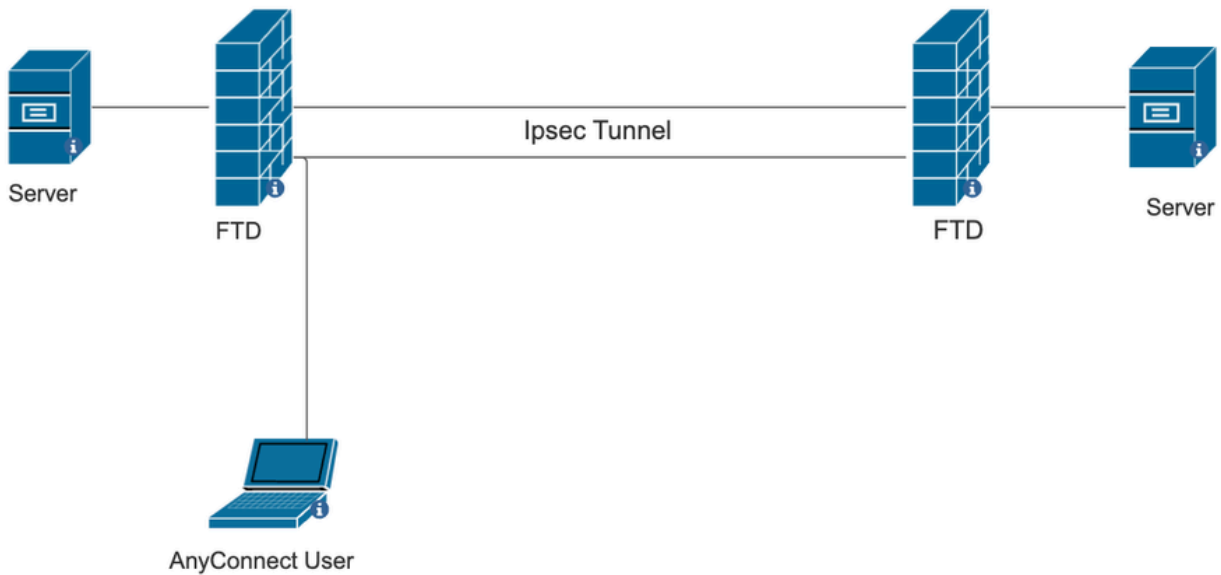
Verwendete Komponenten

- Cisco Firepower Threat Defense für VMware: Version 7.0.0
- FirePOWER Management Center: Version 7.2.4 (Build 169)

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 potenziellen Auswirkungen aller Befehle verstehen..

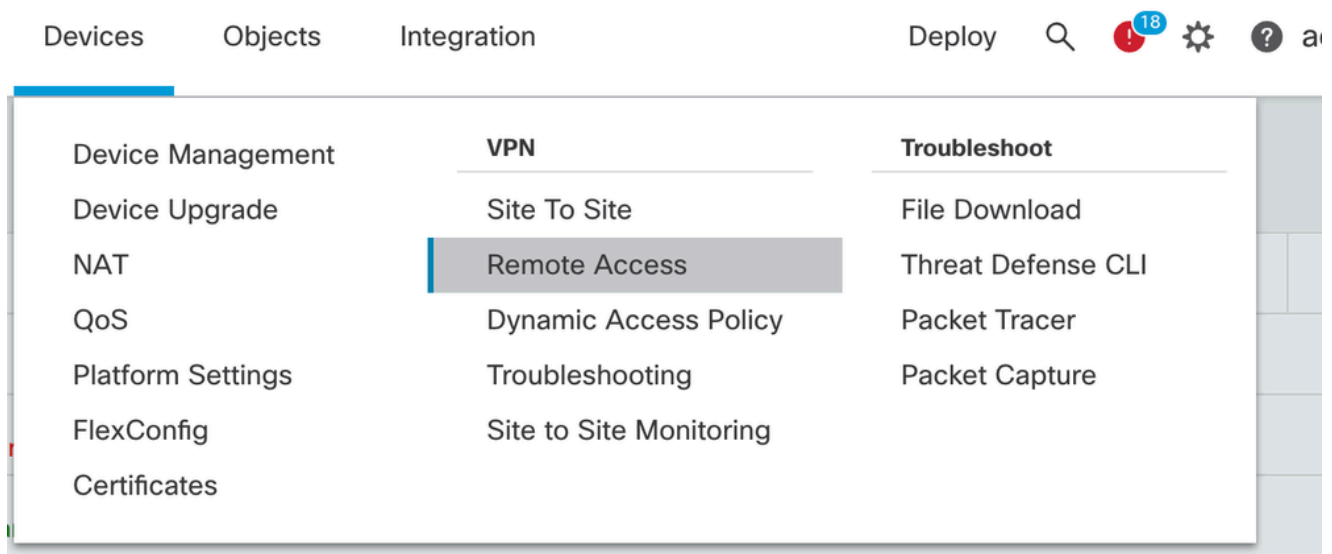
Netzwerkdiagramm



Konfigurationen auf FMC

RAVPN-Konfiguration auf dem von FMC verwalteten FTD.

1. Navigieren Sie zu Geräte > Remotezugriff.



2. Klicken Sie auf Hinzufügen.
3. Konfigurieren Sie einen Namen, und wählen Sie die FTD aus den verfügbaren Geräten aus,

und klicken Sie auf Weiter.

The screenshot shows the 'Remote Access VPN Policy Wizard' at the 'Policy Assignment' step. The progress bar indicates five steps: 1. Policy Assignment (active), 2. Connection Profile, 3. AnyConnect, 4. Access & Certificate, and 5. Summary.

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*
RAVPN

Description:
[Empty field]

VPN Protocols:

- SSL
- IPsec-IKEv2

Targeted Devices:

Available Devices: [Search] 10.106.50.55, 10.88.146.35, New_FTD

Selected Devices: 10.106.50.55

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

- Authentication Server**
Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.
- AnyConnect Client Package**
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.
- Device Interface**
Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

4. Konfigurieren Sie einen Verbindungsprofilnamen, und wählen Sie die Authentifizierungsmethode aus.

HINWEIS: Für dieses Konfigurationsbeispiel werden nur AAA und die lokale Authentifizierung verwendet. Konfigurieren Sie sie jedoch entsprechend Ihren Anforderungen.

The screenshot shows the 'Remote Access VPN Policy Wizard' at the 'Connection Profile' step. The progress bar indicates five steps: 1. Policy Assignment, 2. Connection Profile (active), 3. AnyConnect, 4. Access & Certificate, and 5. Summary.

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RAVPN

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server:* LOCAL (LOCAL or Realm or RADIUS)

Local Realm:* sid_tes_local

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

5. Konfigurieren Sie den VPN-Pool, der für die Zuweisung von IP-Adressen für AnyConnect verwendet wird.

(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

- Use AAA Server (Realm or RADIUS only) ●
- Use DHCP Servers
- Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

6. Gruppenrichtlinie erstellen. Klicken Sie auf +, um eine Gruppenrichtlinie zu erstellen. Fügen Sie den Namen der Gruppenrichtlinie hinzu.

Edit Group Policy ?

Name:*

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

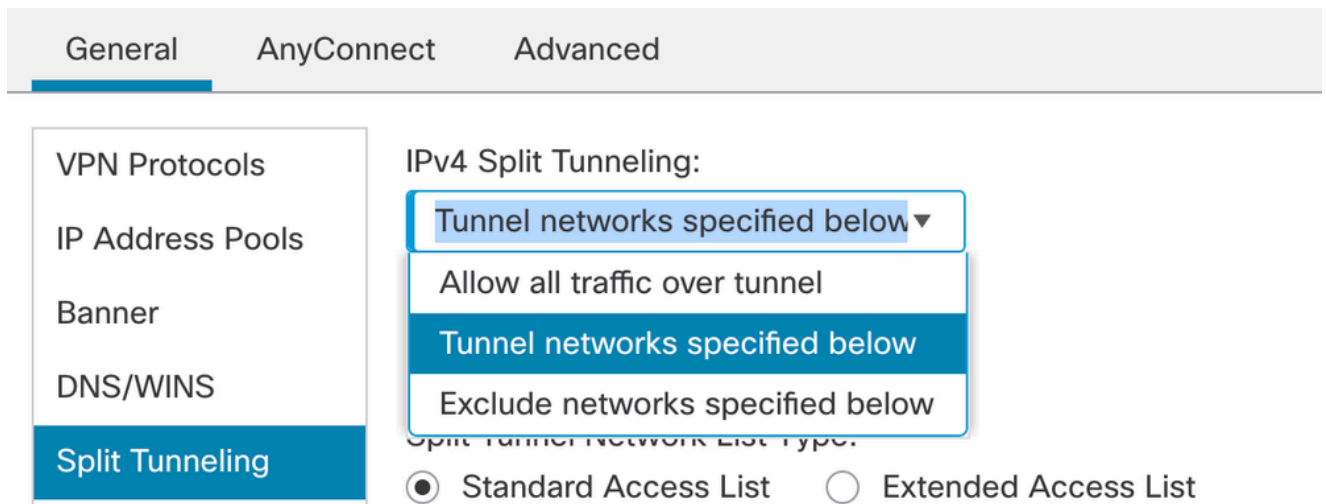
DNS/WINS

Split Tunneling

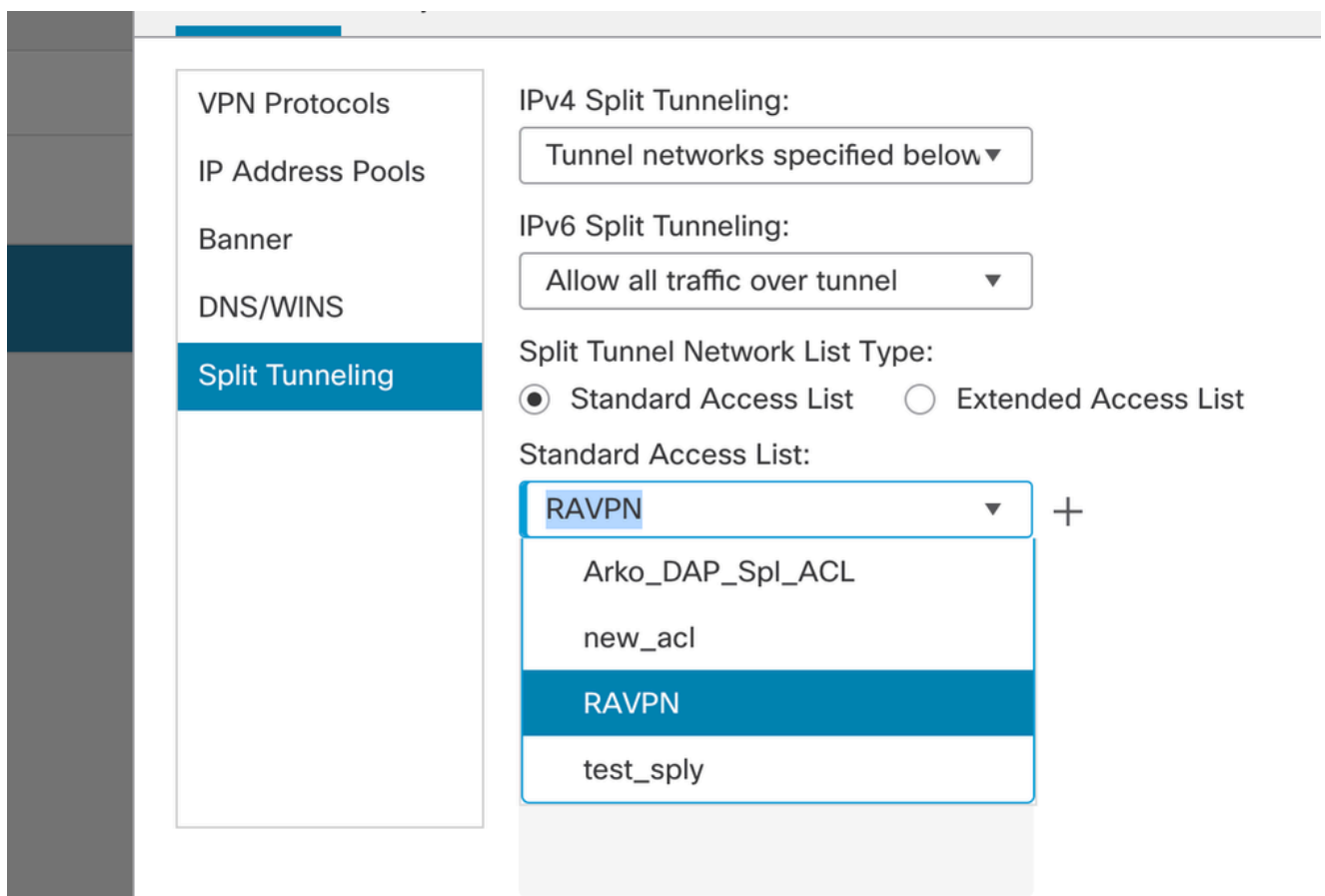
VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

- SSL
- IPsec-IKEv2

7. Gehen Sie zu Split Tunneling. Wählen Sie die hier angegebenen Tunnelnetzwerke aus:



8. Wählen Sie im Dropdown-Menü die gewünschte Zugriffsliste aus. Wenn noch keine ACL konfiguriert ist: Klicken Sie auf das +-Symbol, um die Standard-Zugriffsliste hinzuzufügen und eine neue zu erstellen. Klicken Sie auf Speichern.



9. Wählen Sie die hinzugefügte Gruppenrichtlinie aus, und klicken Sie auf Weiter.

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

10. Wählen Sie das AnyConnect-Image aus.

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect	anyconnect410.pkg	<input type="text" value="Windows"/>
<input checked="" type="checkbox"/>	anyconnect-win-4.10.07073-we...	anyconnect-win-4.10.07073-webdeploy-k9...	<input type="text" value="Windows"/>
<input type="checkbox"/>	secure_client_5-1-2	cisco-secure-client-win-5_1_2_42-webde...	<input type="text" value="Windows"/>

11. Wählen Sie die Schnittstelle aus, die für die AnyConnect-Verbindung aktiviert werden muss, fügen Sie das Zertifikat hinzu, wählen Sie die Richtlinie "Zugriffskontrolle umgehen" für

Network Interface for Incoming VPN Access AAA
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.
Interface group/Security Zone:* +
 Enable DTLS on member interfaces

All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates
Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.
Certificate Enrollment:* +

Access Control for VPN Traffic
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.
 Bypass Access Control policy for decrypted traffic (bypass permitt-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

entschlüsselten Datenverkehr aus, und klicken Sie auf "Weiter".

12. Überprüfen Sie die Konfiguration, und klicken Sie auf Fertig stellen.

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: RAVPN
 Device Targets: 10.106.50.55
 Connection Profile: RAVPN
 Connection Alias: RAVPN
 AAA:
 Authentication Method: AAA Only
 Authentication Server: sid_tes_local (Local)
 Authorization Server: -
 Accounting Server: -
 Address Assignment:
 Address from AAA: -
 DHCP Servers: -
 Address Pools (IPv4): vpn_pool
 Address Pools (IPv6): -
 Group Policy: DfltGrpPolicy
 AnyConnect Images: anyconnect-win-4.10.07073-webdeploy-k9.pkg
 Interface Objects: sid_outside
 Device Certificates: cert1_1

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.
- Port Configuration
SSL will be enabled on port 443. IPsec-IKEV2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

Cancel Back Finish

13. Klicken Sie auf Speichern und Bereitstellen.

RAVPN

Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

Local Realm: New_Realm Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN

IKEv2 VPN auf FTD, von FMC verwaltet:

1. Navigieren Sie zu Geräte > Site-to-Site.

Devices Objects Integration Deploy Search 19 Settings Help ad

Device Management VPN Troubleshoot

Device Upgrade Site To Site File Download

NAT Remote Access Threat Defense CLI

QoS Dynamic Access Policy Packet Tracer

Platform Settings Troubleshooting Packet Capture

FlexConfig Site to Site Monitoring

Certificates

2. Klicken Sie auf Hinzufügen.
3. Klicken Sie für Knoten A auf +:

Center

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	

Node B: +

Device Name	VPN Interface	Protected Networks	

4. Wählen Sie die FTD vom Gerät aus, wählen Sie die Schnittstelle aus, fügen Sie das lokale Subnetz hinzu, das über den IPSec-Tunnel verschlüsselt werden muss (und in diesem Fall auch die VPN-Pooladressen enthält), und klicken Sie auf OK.

Edit Endpoint



Device:*

Interface:*

IP Address:*

This IP is Private

Connection Type:

Certificate Map:

 +

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)

FTD-Lan	
VPN_Pool_Subnet	

+

5. Klicken Sie auf + für Knoten B:

> Wählen Sie das Extranet vom Gerät aus, und geben Sie den Namen des Peer-Geräts an.

> Konfigurieren Sie die Peer-Details, und fügen Sie das Remote-Subnetz hinzu, auf das über den VPN-Tunnel zugegriffen werden muss, und klicken Sie auf OK.

Edit Endpoint ?

Device:*

Device Name:*

IP Address:*
 Static Dynamic

Certificate Map:
 +

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended)

Remote-Lan2 +

Remote-Lan +

6. Klicken Sie auf die Registerkarte IKE: Konfigurieren Sie die IKEv2-Einstellungen gemäß Ihren Anforderungen.

Edit VPN Topology



Topology Name:*

FTD-S2S-FTD

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

IKEv1

IKEv2

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:*

FTD-ASA

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

Enforce hex-based pre-shared key only

Cancel

Save

7. Klicken Sie auf die Registerkarte IPsec: Konfigurieren Sie die IPsec-Einstellungen gemäß Ihren Anforderungen.

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

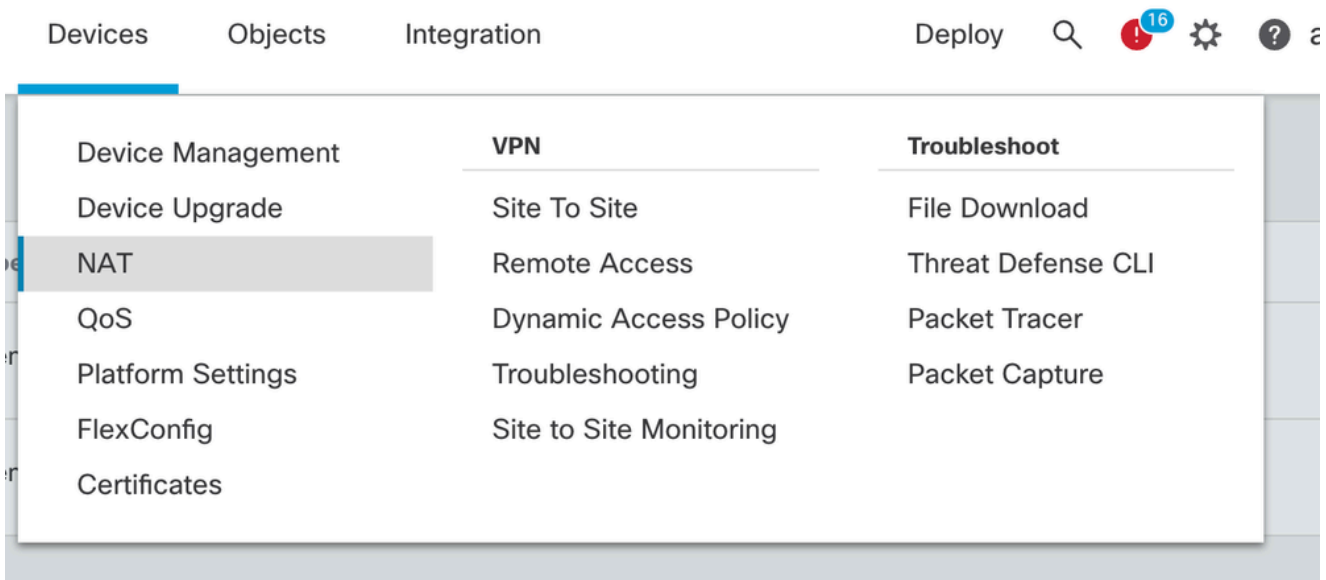
Enable Security Association (SA) Strength Enforcement
 Enable Reverse Route Injection
 Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

8. Konfigurieren Sie Nat-Exempt für Ihren interessanten Datenverkehr (optional)
 Klicken Sie auf Geräte > NAT.



9. Die hier konfigurierte NAT ermöglicht es RAVPN und internen Benutzern, über den S2S IPsec-Tunnel auf Server zuzugreifen.

☐	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options	
						Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
<input type="checkbox"/>	3	↔	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	4	↔	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan2		FTD-Lan	Remote-Lan2		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	5	↔	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan		FTD-Lan	Remote-Lan		Dns: false route-lookup no-proxy-arp	

10. Führen Sie auf die gleiche Weise die Konfiguration am anderen Peer-End für den S2S-Tunnel aus.

HINWEIS: Die Krypto-ACL oder die Subnetze für den interessanten Datenverkehr müssen auf beiden Peers Spiegelkopien der jeweils anderen sein.

Überprüfung

1. RAVPN-Verbindung überprüfen:

```
<#root>
```

```
firepower# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username : test
```

```
Index : 5869
```

```
Assigned IP : 2.2.2.1 Public IP : 10.106.50.179
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
```

```
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx : 15470 Bytes Rx : 2147
```

```
Group Policy : RAVPN Tunnel Group : RAVPN
```

```
Login Time : 03:04:27 UTC Fri Jun 28 2024
```

```
Duration : 0h:14m:08s
```

```
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
```

```
Audt Sess ID : 0a6a3468016ed000667e283b
```

```
Security Grp : none Tunnel Zone : 0
```

2. Überprüfen der IKEv2-Verbindung:

<#root>

```
firepower# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:2443, Status:UP-ACTIVE

, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote Status Role  
3363898555
```

```
10.106.52.104/500 10.106.52.127/500 READY INITIATOR
```

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/259 sec

Child sa: local selector 2.2.2.0/0 - 2.2.2.255/65535

remote selector 10.106.54.0/0 - 10.106.54.255/65535

ESP spi in/out: 0x4588dc5b/0x284a685

3. Überprüfen der IPsec-Verbindung:

<#root>

```
firepower# show crypto ipsec sa peer 10.106.52.127  
peer address: 10.106.52.127
```

Crypto map tag: CSM_outsidel_map

,

seq num: 2, local addr: 10.106.52.104

```
access-list CSM_IPSEC_ACL_1 extended permit ip 2.2.2.0 255.255.255.0 10.106.54.0 255.255.255.0
```

```
local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.106.54.0/255.255.255.0/0/0)
```

current_peer: 10.106.52.127

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 3, #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.: 10.106.52.104/500, remote crypto endpt.: 10.106.52.127/500
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: 0284A685
current inbound spi : 4588DC5B

i

nbound esp sas:

spi: 0x4588DC5B (1166597211)

SA State: active

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

in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map
sa timing: remaining key lifetime (kB/sec): (3962879/28734)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000000F

outbound esp sas:

spi: 0x0284A685 (42247813)

SA State: active

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

```
in use settings ={L2L, Tunnel, IKEv2, }  
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map  
sa timing: remaining key lifetime (kB/sec): (4285439/28734)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001
```

Fehlerbehebung

1. Sammeln Sie das dart-Paket, oder aktivieren Sie die AnyConnect-Fehlerbehebung, um das AnyConnect-Verbindungsproblem zu beheben.
2. Verwenden Sie zur Fehlerbehebung für den IKEv2-Tunnel die folgenden Debugging-Methoden:

```
debug crypto condition peer <peer IP address>  
debug crypto ikev2 platform 255  
debug crypto ikev2 protocol 255  
debug crypto ipsec 255
```

3. Um das Datenverkehrsproblem auf dem FTD zu beheben, nehmen Sie die Paketerfassung und überprüfen Sie die Konfiguration.

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.