

Konfiguration des IKEv2-IPv6-Site-to-Site-Tunnels zwischen ASA und FTD

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[ASA-Konfiguration](#)

[FTD-Konfiguration](#)

[Zugriffskontrolle umgehen](#)

[Konfigurieren der NAT-Ausnahme](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Referenzen](#)

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel für die Einrichtung eines IPv6-Site-to-Site-Tunnels zwischen einer ASA (Adaptive Security Appliance) und FTD (Firepower Threat Defense) unter Verwendung des IKEv2-Protokolls (Internet Key Exchange Version 2). Die Konfiguration umfasst End-to-End-IPv6-Netzwerkverbindungen mit ASA und FTD als VPN-Terminierungsgeräte.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende Kenntnisse der ASA CLI-Konfiguration
- Grundlegende Kenntnisse der IKEv2- und IPSEC-Protokolle
- Verständnis von IPv6-Adressierung und -Routing
- Grundlegende Kenntnisse der FTD-Konfiguration über FMC

Verwendete Komponenten

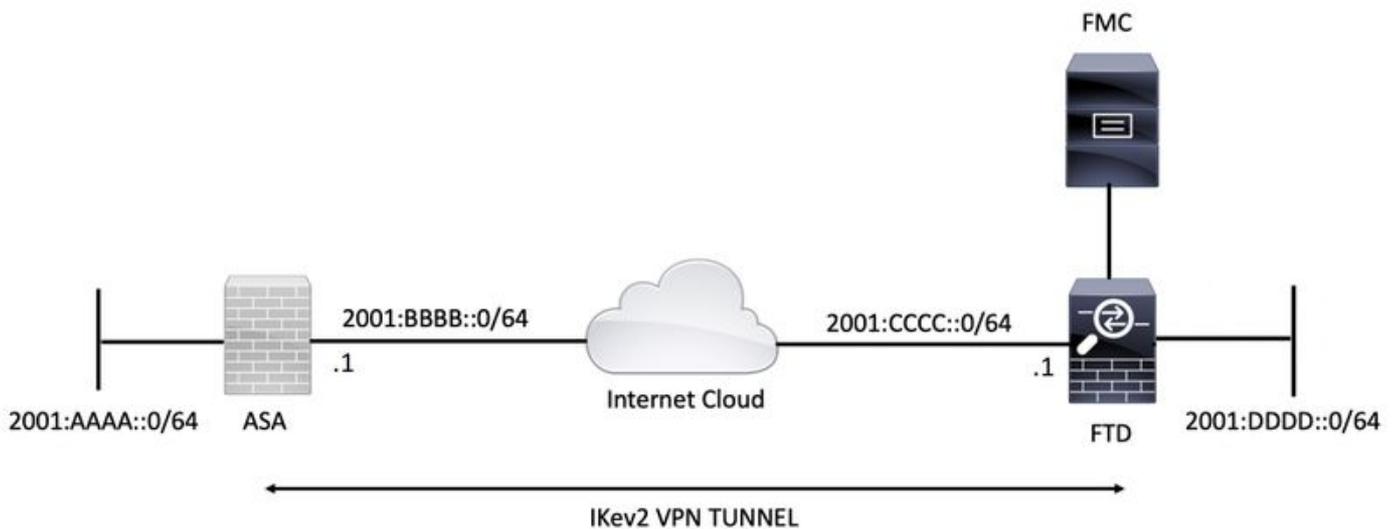
Die Informationen in diesem Dokument basieren auf einer virtuellen Umgebung, die aus Geräten in einer bestimmten Laboreinrichtung erstellt wurde. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Produktion ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA mit 9.6.(4)12
- Cisco FTD mit 6.5.0
- Cisco FMC mit 6.6.0

Konfigurieren

Netzwerkdiagramm



ASA-Konfiguration

In diesem Abschnitt wird die erforderliche Konfiguration für die ASA beschrieben.

Schritt 1: Konfigurieren Sie die ASA-Schnittstellen.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable
```

```
interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

Schritt 2: Legen Sie eine IPv6-Standardroute fest.

```
ipv6 route outside ::/0 2001:bbbb::2
```

Schritt 3: Konfigurieren Sie die IKEv2-Richtlinie, und aktivieren Sie IKEv2 auf der externen

Schnittstelle.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

Schritt 4: Konfigurieren Sie die Tunnelgruppe.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

Schritt 5: Erstellen Sie die Objekte und die Zugriffskontrollliste (ACL), um den interessanten Datenverkehr zu übernehmen.

```
object-group network local-network
network-object 2001:aaaa::/64
```

```
object-group network remote-network
network-object 2001:dddd::/64
```

```
access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

Schritt 6: Konfigurieren Sie die Identity Network Address Translation (NAT)-Regeln für den interessanten Datenverkehr.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

Schritt 7: Konfigurieren Sie das IKEv2 IPsec-Angebot.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

Schritt 8: Legen Sie die Crypto Map fest, und wenden Sie sie auf die externe Schnittstelle an.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route
```

```
crypto map VPN interface outside
```

FTD-Konfiguration

Dieser Abschnitt enthält Anweisungen zur Konfiguration eines FTD mithilfe von FMC.

Definieren der VPN-Topologie

Schritt 1: Navigieren Sie zu **Geräte > VPN > Site-to-Site**.

Auswählen "Add VPN" (VPN hinzufügen) und "FirePOWER Threat Defense Device" (FirePOWER Threat Defense-Gerät) auswählen, wie in diesem Bild gezeigt.

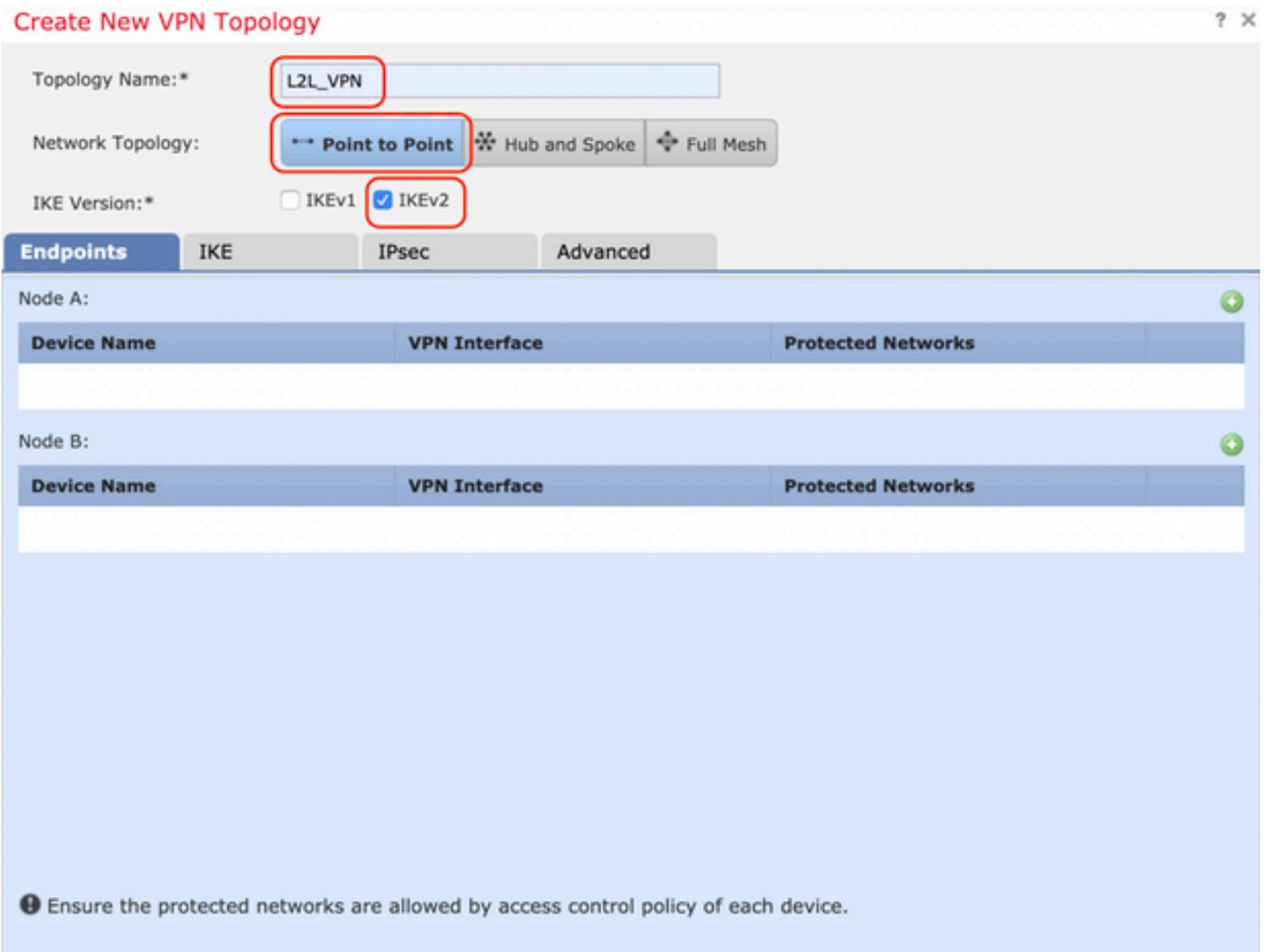


Schritt 2: Das Feld "Neue VPN-Topologie erstellen" wird angezeigt. dem VPN einen leicht identifizierbaren Namen geben.

Netzwerktopologie: Point-to-Point

IKE-Version: IKEv2

In diesem Beispiel ist bei der Auswahl von Endpunkten Knoten A FTD. Knoten B ist die ASA. Klicken Sie auf die grüne Plus-Schaltfläche, um Geräte zur Topologie hinzuzufügen.



Schritt 3: Fügen Sie das FTD als ersten Endpunkt hinzu.

Wählen Sie die Schnittstelle aus, auf die die Crypto Map angewendet wird. Die IP-Adresse sollte automatisch aus der Gerätekonfiguration übernommen werden.

Klicken Sie unter Protected Networks auf das grüne Pluszeichen, um Subnetze auszuwählen, die über diesen VPN-Tunnel verschlüsselt sind. In diesem Beispiel besteht das Netzwerkobjekt 'Local Proxy' auf dem FMC aus dem IPv6-Subnetz '2001:DDDD::/64'.

Edit Endpoint



Device:*

FTDv

Interface:*

OUTSIDE

IP Address:*

2001:CCCC::1

This IP is Private

Connection Type:

Bidirectional

Certificate Map:



Protected Networks:*

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

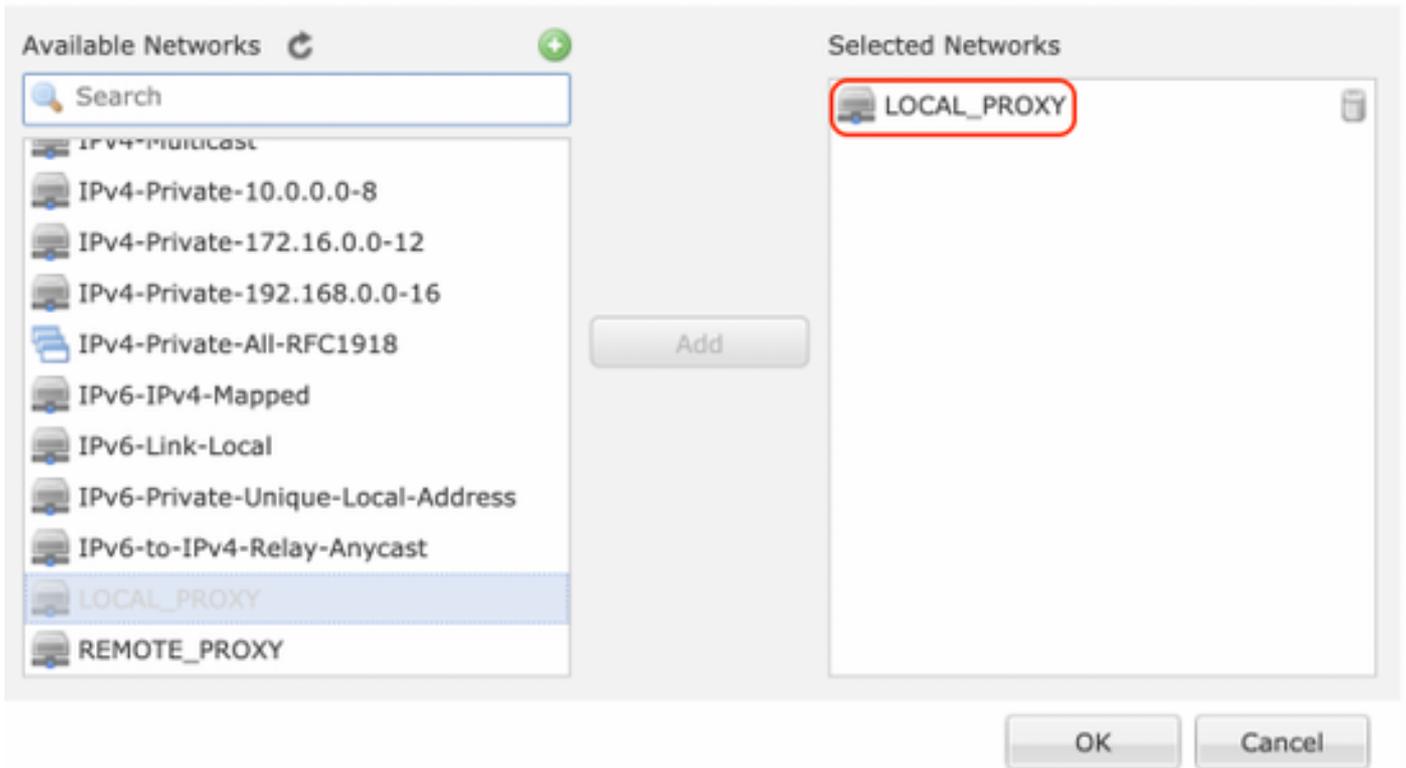


 LOCAL_PROXY 

OK

Cancel

Network Objects



Mit dem obigen Schritt ist die FTD-Endpunktconfiguration abgeschlossen.

Schritt 4: Klicken Sie auf das grüne Pluszeichen für Knoten B, der eine ASA im Konfigurationsbeispiel darstellt. Geräte, die nicht vom FMC verwaltet werden, gelten als Extranet. Fügen Sie einen Gerätenamen und eine IP-Adresse hinzu.

Schritt 5: Wählen Sie das grüne Pluszeichen, um geschützte Netzwerke hinzuzufügen.

Edit Endpoint ? X

Device:* Extranet

Device Name:* ASA

IP Address:* Static Dynamic
2001:BBBB::1

Certificate Map: +

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

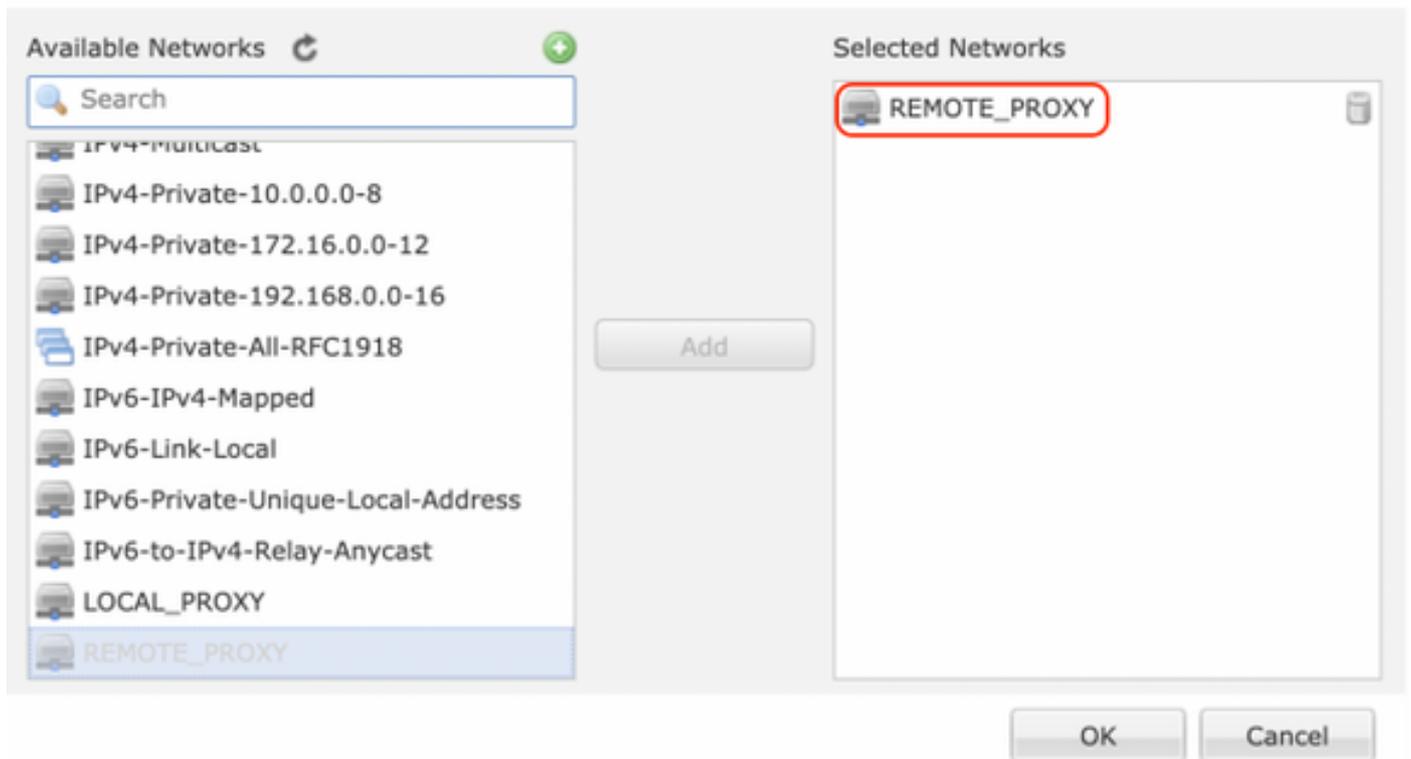
 REMOTE_PROXY 

OK Cancel

Schritt 6: Wählen Sie die zu verschlüsselnden ASA-Subnetze aus, und fügen Sie sie den ausgewählten Netzwerken hinzu.

'Remote Proxy' ist das ASA-Subnetz '2001:AAAA:/64' in diesem Beispiel.

Network Objects



Konfigurieren der IKE-Parameter

Schritt 1: Geben Sie auf der Registerkarte IKE die Parameter für den anfänglichen IKEv2-Austausch an. Klicken Sie auf das grüne Pluszeichen, um eine neue IKE-Richtlinie zu erstellen.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:*

Authentication Type:

Pre-shared Key Length:* Characters (Range 1-127)

IKEv2 Settings

Policy:*

Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Schritt 2: Geben Sie in der neuen IKE-Richtlinie eine Prioritätsnummer sowie die Lebensdauer von Phase 1 der Verbindung an. In diesem Leitfaden werden folgende Parameter für den ersten Austausch verwendet:
Integrität (SHA256),
Verschlüsselung (AES-256),
PRF (SHA256) und
Diffie-Hellman Group (Gruppe 14).

Alle IKE-Richtlinien auf dem Gerät werden an den Remote-Peer gesendet, unabhängig davon, was im ausgewählten Richtlinienabschnitt angegeben ist. Die erste Übereinstimmung des Remote-Peers wird für die VPN-Verbindung ausgewählt.

[Optional] Wählen Sie aus, welche Richtlinie zuerst mit dem Prioritätsfeld gesendet wird. Priorität 1 wird zuerst gesendet.

Edit IKEv2 Policy

Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384
- NULL

Add

Selected Algorithms

SHA256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

Save

Cancel

Edit IKEv2 Policy



Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

Available Algorithms

- MDS
- SHA
- SHA512
- SHA256
- SHA384

Add

Selected Algorithms

- SHA256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority:

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

Available Groups

- 1
- 2
- 5
- 14
- 15
- 16
- 19
- 20
- 21

Add

Selected Groups

- 14

Save Cancel

Schritt 3: Wenn die Parameter hinzugefügt wurden, wählen Sie die oben konfigurierte Richtlinie aus, und wählen Sie den Authentifizierungstyp aus.

Wählen Sie die Option Pre-shared Manual Key (Vorinstallierter manueller Schlüssel) aus. Für diesen Leitfadens wird der vorinstallierte Schlüssel "**cisco123**" verwendet.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:*

Authentication Type:

Pre-shared Key Length:* Characters (Range 1-127)

IKEv2 Settings

Policy:*

Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Konfigurieren von IPSEC-Parametern

Schritt 1: Wechseln Sie zur Registerkarte IPsec, und erstellen Sie ein neues IPsec-Angebot, indem Sie auf das Bleistiftsymbol klicken, um den Transformationsatz zu bearbeiten.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

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)

— **ESPv3 Settings**

Schritt 2: Erstellen Sie einen neuen IKEv2 IPsec-Vorschlag, indem Sie das grüne Pluszeichen auswählen und die Parameter für Phase 2 wie folgt eingeben:

ESP-Hash: SHA-1

ESP-Verschlüsselung: AES-256

Edit IKEv2 IPsec Proposal



Name:*

Ikev2__IPSec_Proposal

Description:

ESP Hash

ESP Encryption

Available Algorithms

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5
- NULL

Selected Algorithms

SHA-1

Add

Save

Cancel

Edit IKEv2 IPsec Proposal



Name:*

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-256

Add

Selected Algorithms

- AES-256**

Save **Cancel**

Schritt 3: Nachdem das neue IPsec-Angebot erstellt wurde, fügen Sie es den ausgewählten Transformationssätzen hinzu.

IKEv2 IPsec Proposal



Available Transform Sets

- AES-GCM
- AES-SHA
- DES_SHA-1
- Ikev2__IPSec_Proposal**

Add

Selected Transform Sets

- Ikev2__IPSec_Proposal**

OK **Cancel**

Schritt 4: Das neu ausgewählte IPsec-Angebot ist jetzt unter den IKEv2 IPsec-Angeboten aufgeführt.

Bei Bedarf können die Phase-2-Lebensdauer und PFS hier bearbeitet werden. In diesem Beispiel ist die Lebensdauer als Standard festgelegt und PFS deaktiviert.

Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals tunnel_aes256_sha IKEv2 IPsec Proposals* Ikev2_IPSec_Proposal

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

Sie müssen entweder die folgenden Schritte konfigurieren, um die Zugriffskontrolle zu umgehen, oder Zugriffskontrollrichtlinien erstellen, um VPN-Subnetze über FTD zuzulassen.

Zugriffskontrolle umgehen

Wenn `sysopt permit-vpn` nicht aktiviert ist, muss eine Zugriffskontrollrichtlinie erstellt werden, um den VPN-Datenverkehr über das FTD-Gerät zuzulassen. Wenn `sysopt permit-vpn` aktiviert ist, überspringen Sie die Erstellung einer Zugriffskontrollrichtlinie. In diesem Konfigurationsbeispiel wird die Option "Zugriffskontrolle umgehen" verwendet.

Der Parameter `sysopt permit-vpn` kann unter `Advanced > Tunnel` aktiviert werden.

Vorsicht: Mit dieser Option können Sie die Zugriffskontrollrichtlinie nicht mehr verwenden, um den von den Benutzern stammenden Datenverkehr zu überprüfen. VPN-Filter oder herunterladbare ACLs können weiterhin zum Filtern des Benutzerdatenverkehrs verwendet werden. Dies ist ein globaler Befehl und gilt für alle VPNs, wenn dieses Kontrollkästchen aktiviert ist.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | **Advanced**

IKE
IPsec
Tunnel

NAT Settings

- Keepalive Messages Traversal
- Interval: Seconds (Range 10 - 3600)

Access Control for VPN Traffic

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Certificate Map Settings

- Use the certificate map configured in the Endpoints to determine the tunnel
- Use the certificate OU field to determine the tunnel
- Use the IKE identity to determine the tunnel
- Use the peer IP address to determine the tunnel

Save Cancel

Konfigurieren der NAT-Ausnahme

Konfigurieren Sie eine NAT-Freischaltungsanweisung für den VPN-Datenverkehr. Es muss eine NAT-Ausnahme vorhanden sein, um zu verhindern, dass der VPN-Datenverkehr einer anderen NAT-Anweisung entspricht und den VPN-Datenverkehr nicht korrekt übersetzt.

Schritt 1: Navigieren Sie zu **Geräte > NAT** und erstellen Sie eine neue Richtlinie, indem Sie auf **New Policy > Threat Defence NAT** klicken.



New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTDv

Selected Devices

FTDv

Schritt 2: Klicken Sie auf **Regel hinzufügen**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

NAT_Exempt Show Warnings Show Save Cancel

Policy Assignments (1)

Rules

Filter by Device

#	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	
▼ NAT Rules Before											
▼ Auto NAT Rules											
▼ NAT Rules After											

Schritt 3: Erstellen Sie eine neue statische manuelle NAT-Regel.

Verweisen Sie auf die internen und externen Schnittstellen für die NAT-Regel. Durch die Angabe der Schnittstellen auf der Registerkarte Schnittstellenobjekte wird verhindert, dass diese Regeln den Datenverkehr von anderen Schnittstellen beeinflussen.

Navigieren Sie zur Registerkarte Übersetzung, und wählen Sie das Quell- und Zielsubnetz aus. Da es sich um eine NAT-Freistellungsregel handelt, stellen Sie sicher, dass die ursprüngliche Quelle/das ursprüngliche Ziel und die übersetzte Quelle/Ziel identisch sind.

Add NAT Rule

? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

Original Packet

Original Source:* +

Original Destination: +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: +

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

Klicken Sie auf die Registerkarte Erweitert, und aktivieren Sie **no-proxy-arp** und **route-lookup**.

Add NAT Rule

? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: Translation **Advanced** PAT Pool

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

Speichern Sie diese Regel, und bestätigen Sie die letzte NAT-Anweisung in der NAT-Liste.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

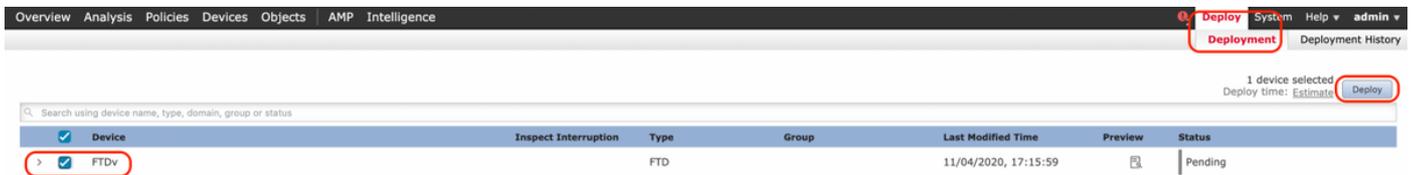
Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

NAT_Exempt
Enter Description Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	
1		Static	LAN	WAN	LOCAL_PROXY	REMOTE_PROXY	LOCAL_PROXY	REMOTE_PROXY	Dns: false route-lookup no-proxy-arp

Schritt 4: Speichern Sie die Konfiguration nach Abschluss der Konfiguration und stellen Sie sie im FTD bereit.



Überprüfen

Initiieren Sie interessanten Datenverkehr vom LAN-Computer, oder Sie können den folgenden Befehl zur Paketverfolgung auf der ASA ausführen.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

Hinweis: Hier steht Type = 128 und Code=0 für ICMPv6 "Echo Request".

Im folgenden Abschnitt werden die Befehle beschrieben, die Sie auf ASA- oder FTD-LINA-CLI ausführen können, um den Status des IKEv2-Tunnels zu überprüfen.

Dies ist ein Beispiel für eine Ausgabe von ASA:

```
ciscoasa# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local                               Remote
          Status                               Role
6638313 2001:bbbb::1/500                       2001:cccc::1/500
          READY    INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/224 sec
Child sa: local selector 2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
          remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
          ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8
```

```
ciscoasa# show crypto ipsec sa detail
```

```
interface: outside
```

```
  Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1
```

```
access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
current_peer: 2001:cccc::1
```

```
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #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
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

#pkts invalid pad (rcv): 0,
#pkts invalid ip version (rcv): 0,
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
path mtu 1500, ipsec overhead 94(64), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: D95ECDB8
current inbound spi : A0FD3FE6

inbound esp sas:

spi: 0xA0FD3FE6 (2700951526)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VP
sa timing: remaining key lifetime (kB/sec): (4055040/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

outbound esp sas:

spi: 0xD95ECDB8 (3646868920)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VPN
sa timing: remaining key lifetime (kB/sec): (4193280/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa# **show vpn-sessiondb detail l2l filter name 2001:cccc::1**

Session Type: LAN-to-LAN Detailed

Connection : 2001:cccc::1
Index : 473 IP Addr : 2001:cccc::1
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA1
Bytes Tx : 352 Bytes Rx : 352
Login Time : 12:27:36 UTC Sun Apr 12 2020
Duration : 0h:06m:40s

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:

Tunnel ID : 473.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 86000 Seconds
PRF : SHA256 D/H Group : 14
Filter Name :

IPsec:

Tunnel ID : 473.2

```
Local Addr   : 2001:aaaa::/64/0/0
Remote Addr  : 2001:dddd::/64/0/0
Encryption   : AES256                Hashing      : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds          Rekey Left(T): 28400 Seconds
Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes             Idle TO Left : 23 Minutes
Bytes Tx     : 352                    Bytes Rx     : 352
Pkts Tx     : 11                      Pkts Rx     : 11
```

Fehlerbehebung

Führen Sie zur Fehlerbehebung bei Problemen mit der IKEv2-Tunneleinrichtung in ASA und FTD die folgenden Debugbefehle aus:

```
debuggen crypto condition peer <Peer IP>
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255
```

Im Folgenden finden Sie ein Beispiel für die Arbeit von IKEv2-Debuggen als Referenz:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debug.html>

Referenzen

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html>