Konfigurieren des serviceseitigen IPSec-Tunnels mit einem C8000V auf dem SD-WAN

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration eines IPSec-Tunnels zwischen einem Cisco Edge-Router mit SD-WAN und einem VPN-Endpunkt mit Service-VRF beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Software-defined Wide Area Network (SD-WAN)
- Internet-Protokollsicherheit (IPSec)

Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- Cisco Edge Router Version 17.6.1
- SD-WAN vManage 20.9.3.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte in diesem Dokument haben mit einer gelöschten (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die

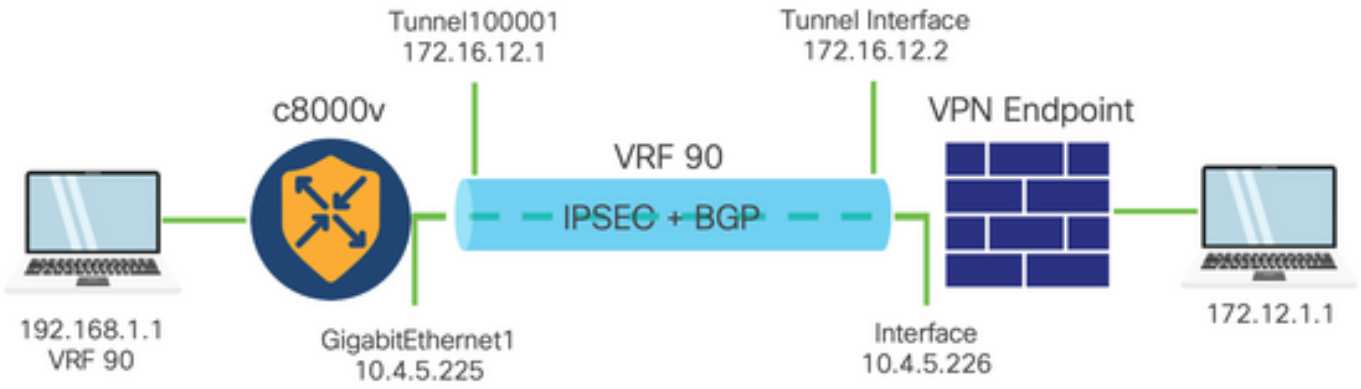
möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Zu den Hintergrundinformationen gehören der Umfang dieses Dokuments, die Benutzerfreundlichkeit und die Vorteile des Aufbaus eines serviceseitigen IPSec-Tunnels mit einem C8000v auf SD-WAN.

- Die Einrichtung eines IPSec-Tunnels in einem VRF (Virtual Routing and Forwarding) zwischen einem Cisco IOS® XE-Router im Controller-Managed-Modus und einem VPN-Endpunkt (Virtual Private Network) gewährleistet Datensicherheit und -integrität über das öffentliche WAN (Wide Area Network). Es erleichtert auch die sichere Erweiterung der privaten Netzwerke der Unternehmen und ermöglichen Remote-Verbindungen über das Internet bei gleichzeitiger Wahrung eines hohen Sicherheitsniveaus.
- Das Service-VRF isoliert den Datenverkehr, was besonders in Umgebungen mit mehreren Clients oder zur Aufrechterhaltung der Segmentierung zwischen verschiedenen Teilen des Netzwerks nützlich ist. Zusammenfassend lässt sich sagen, dass diese Konfiguration die Sicherheit und die Anbindung verbessert.
- In diesem Dokument wird das Border Gateway Protocol (BGP) als Routing-Protokoll für die Kommunikation zwischen den Netzwerken vom SD-WAN-Service-VRF und dem Netzwerk hinter dem VPN-Endpunkt verwendet.
- Die BGP-Konfiguration wird in diesem Dokument nicht behandelt.
- Bei diesem VPN-Endpunkt kann es sich um eine Firewall, einen Router oder ein beliebiges Netzwerkgerät mit IPSec-Funktionen handeln. Die Konfiguration des VPN-Endpunkts wird in diesem Dokument nicht behandelt.
- In diesem Dokument wird davon ausgegangen, dass der Router bereits mit aktiven Steuerverbindungen und Service-VRF verbunden ist.

Komponenten der IPSEC-Konfiguration



Phase 1 Internet Key Exchange (IKE)

Phase 1 des IPSec-Konfigurationsprozesses umfasst die Aushandlung der Sicherheitsparameter und die Authentifizierung zwischen Tunnelendpunkten. Diese Schritte umfassen:

IKE-Konfiguration

- Definieren Sie einen Verschlüsselungsangebot (Algorithmus und Schlüssellänge).
- Konfigurieren Sie eine IKE-Richtlinie, die ein Angebot für die Verschlüsselung, die Time-to-Live und die Authentifizierung enthält.

Konfigurieren von Remote-End-Peers

- Definieren Sie die IP-Adresse des Remote-Endgeräts.
- Konfigurieren Sie den gemeinsamen Schlüssel (vorinstallierter Schlüssel) für die Authentifizierung.

Konfiguration von Phase 2 (IPSec)

Phase 2 umfasst die Aushandlung der Sicherheitstransformationen und Zugriffsregeln für den Datenfluss durch den Tunnel. Diese Schritte umfassen:

Konfigurieren von IPSec-Transformationssätzen

- Definieren Sie einen vorgeschlagenen Transformationssatz, der den Verschlüsselungsalgorithmus und die Authentifizierung umfasst.

Konfigurieren einer IPSec-Richtlinie

- Ordnen Sie den Transformationssatz einer IPSec-Richtlinie zu.

Konfigurieren von Tunnelschnittstellen

Konfigurieren Sie Tunnelschnittstellen an beiden Enden des IPSec-Tunnels.

- Ordnen Sie die Tunnelschnittstellen den IPSec-Richtlinien zu.

Konfigurieren

Konfiguration in CLI

Schritt 1: Definieren Sie einen Vorschlag für die Verschlüsselung.

<#root>

```
cEdge(config)#
crypto ikev2 proposal p1-global

cEdge(config-ikev2-proposal)#
encryption aes-cbc-128 aes-cbc-256

cEdge(config-ikev2-proposal)#
integrity sha1 sha256 sha384 sha512
```

```
cEdge(config-ikev2-proposal)#
group 14 15 16
```

Schritt 2: Konfigurieren Sie eine IKE-Richtlinie, die Angebotsinformationen enthält.

```
<#root>
cEdge(config)#
crypto ikev2 policy policy1-global

cEdge(config-ikev2-policy)#
proposal p1-global
```

Schritt 3: Definieren Sie die IP-Adresse des Remote-Endgeräts.

```
<#root>
cEdge(config)#
crypto ikev2 keyring if-ipsec1-ikev2-keyring

cEdge(config-ikev2-keyring)#
peer if-ipsec1-ikev2-keyring-peer

cEdge(config-ikev2-keyring-peer)#
address 10.4.5.226

cEdge(config-ikev2-keyring-peer)#
pre-shared-key Cisco
```

Schritt 4: Konfigurieren Sie den gemeinsamen Schlüssel (vorinstallierter Schlüssel) für die Authentifizierung.

```
<#root>
cEdge(config)#
```

```
crypto ikev2 profile if-ipsec1-ikev2-profile

cEdge(config-ikev2-profile)#
match identity remote address
10.4.5.226 255.255.255.0

cEdge(config-ikev2-profile)#
authentication remote

cEdge(config-ikev2-profile)#
authentication remote pre-share

cEdge(config-ikev2-profile)#
authentication local pre-share

cEdge(config-ikev2-profile)#
keyring local if-ipsec1-ikev2-keyring

cEdge(config-ikev2-profile)#
dpd 10 3 on-demand

cEdge(config-ikev2-profile)#
no config-exchange request

cEdge(config-ikev2-profile)#
```

Schritt 5: Definieren Sie einen vorgeschlagenen Transformationssatz, der den Verschlüsselungsalgorithmus und die Authentifizierung umfasst.

```
<#root>

cEdge(config)#
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256

cEdge(cfg-crypto-trans)#
mode tunnel
```

Schritt 6: Ordnen Sie den Transformationssatz einer IPSec-Richtlinie zu.

<#root>

```
cEdge(config)#
crypto ipsec profile if-ipsec1-ipsec-profile

cEdge(ipsec-profile)#
set security-association lifetime kilobytes disable

cEdge(ipsec-profile)#
set security-association replay window-size 512

cEdge(ipsec-profile)#
set transform-set if-ipsec1-ikev2-transform

cEdge(ipsec-profile)#
set ikev2-profile if-ipsec1-ikev2-profile
```

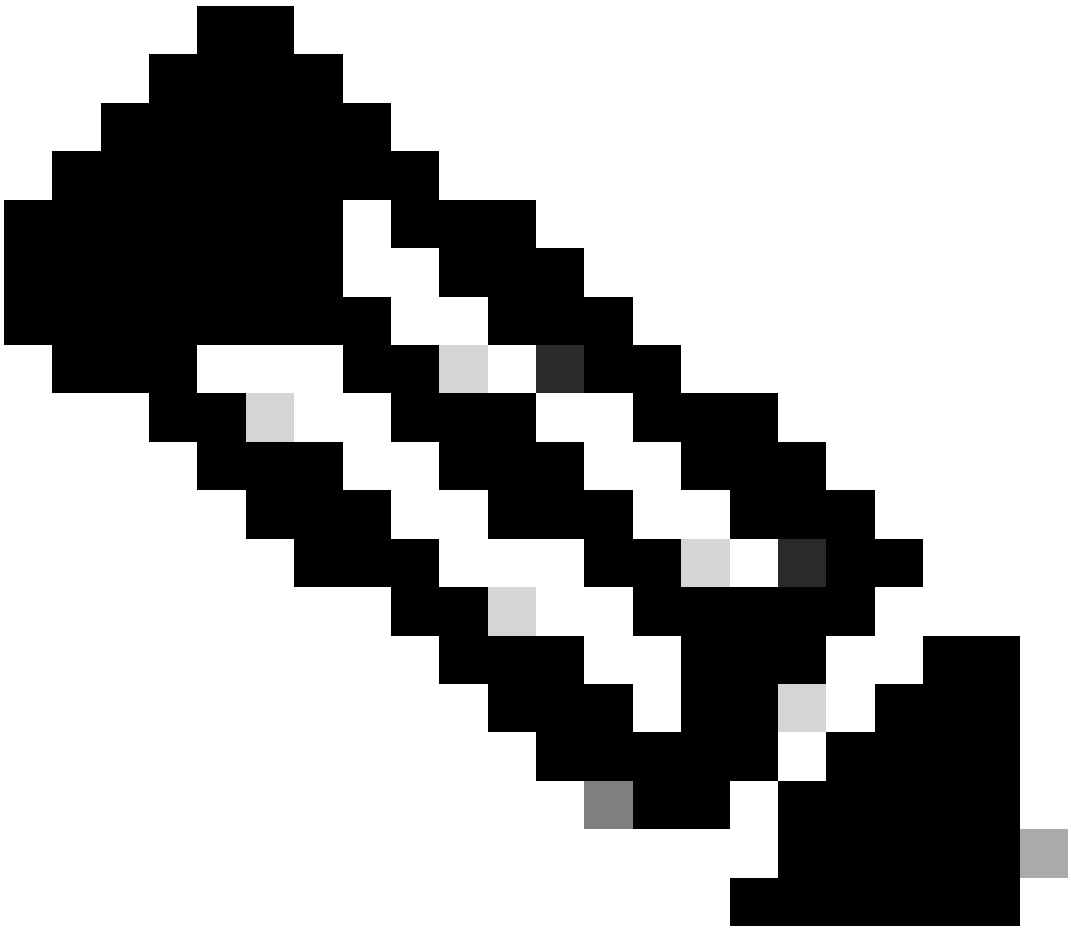
Schritt 7. Erstellen Sie den Schnittstellentunnel, und ordnen Sie ihn den IPSec-Richtlinien zu.

<#root>

```
cEdge(config)#
interface Tunnel100001

cEdge(config-if)#
vrf forwarding 90

cEdge(config-if)#
ip address 172.16.12.1 255.255.255.252

cEdge(config-if)#
ip mtu 1500

cEdge(config-if)#
tunnel source GigabitEthernet1

cEdge(config-if)#
tunnel mode ipsec ipv4

cEdge(config-if)#
```

```
tunnel destination 10.4.5.226

cEdge(config-if)#
tunnel path-mtu-discovery

cEdge(config-if)#
tunnel protection ipsec profile if-ipsec1-ipsec-profile
```

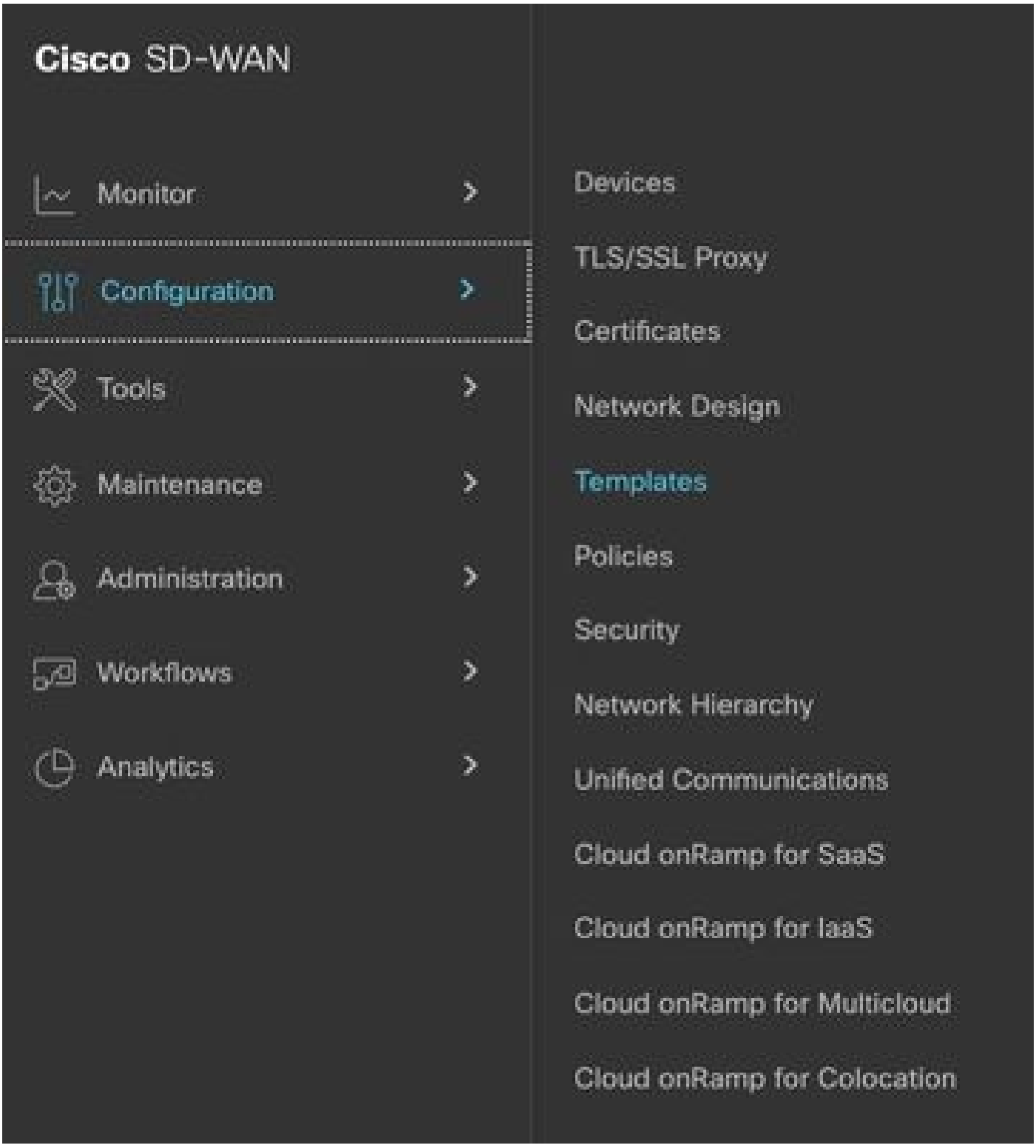
Konfiguration auf einer CLI-Add-On-Vorlage auf vManage



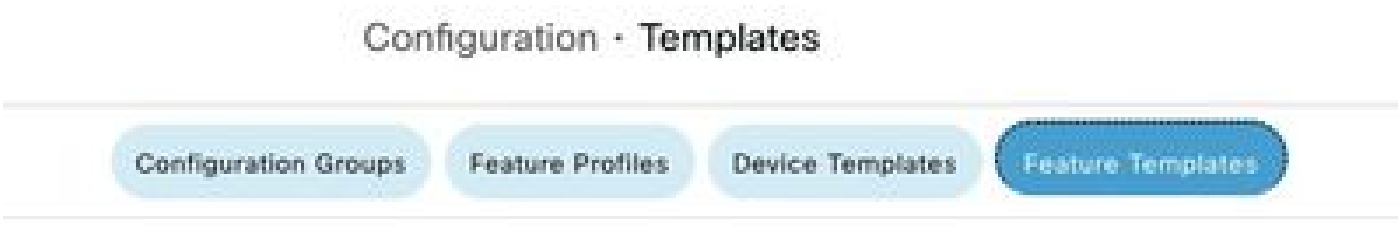
> Hinweis: Dieser Konfigurationstyp kann nur über eine CLI-Add-On-Vorlage hinzugefügt werden.

Schritt 1: Navigieren Sie zum Cisco vManage, und melden Sie sich an.

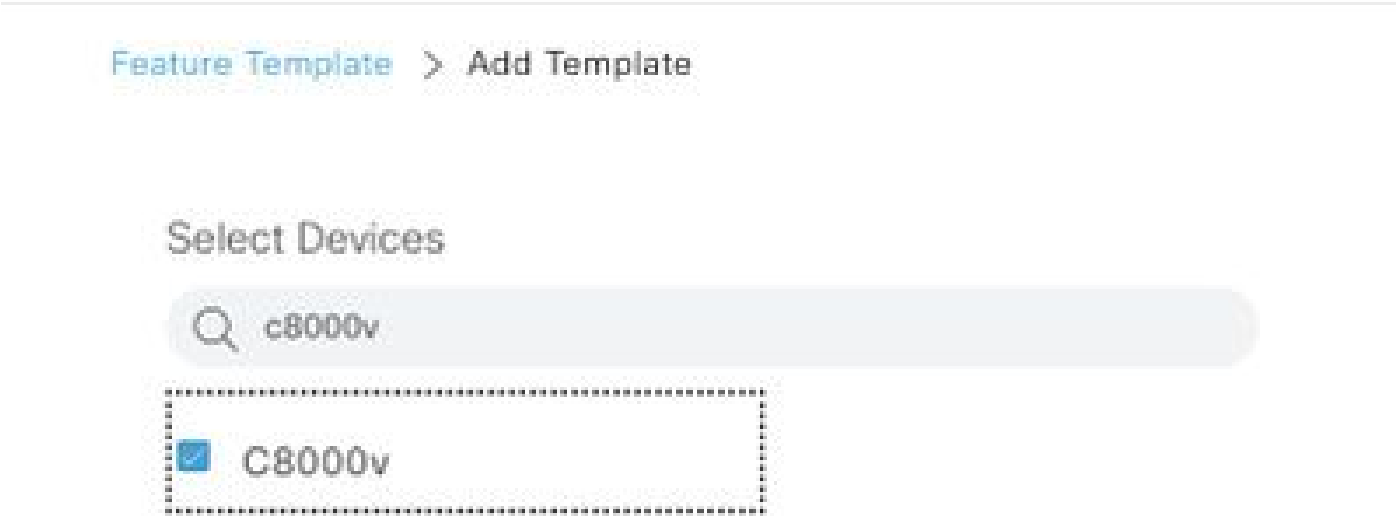
Schritt 2: Navigieren Sie zu Konfiguration > Vorlagen.



Schritt 3: Navigieren Sie zu Funktionsvorlagen > Vorlage hinzufügen.

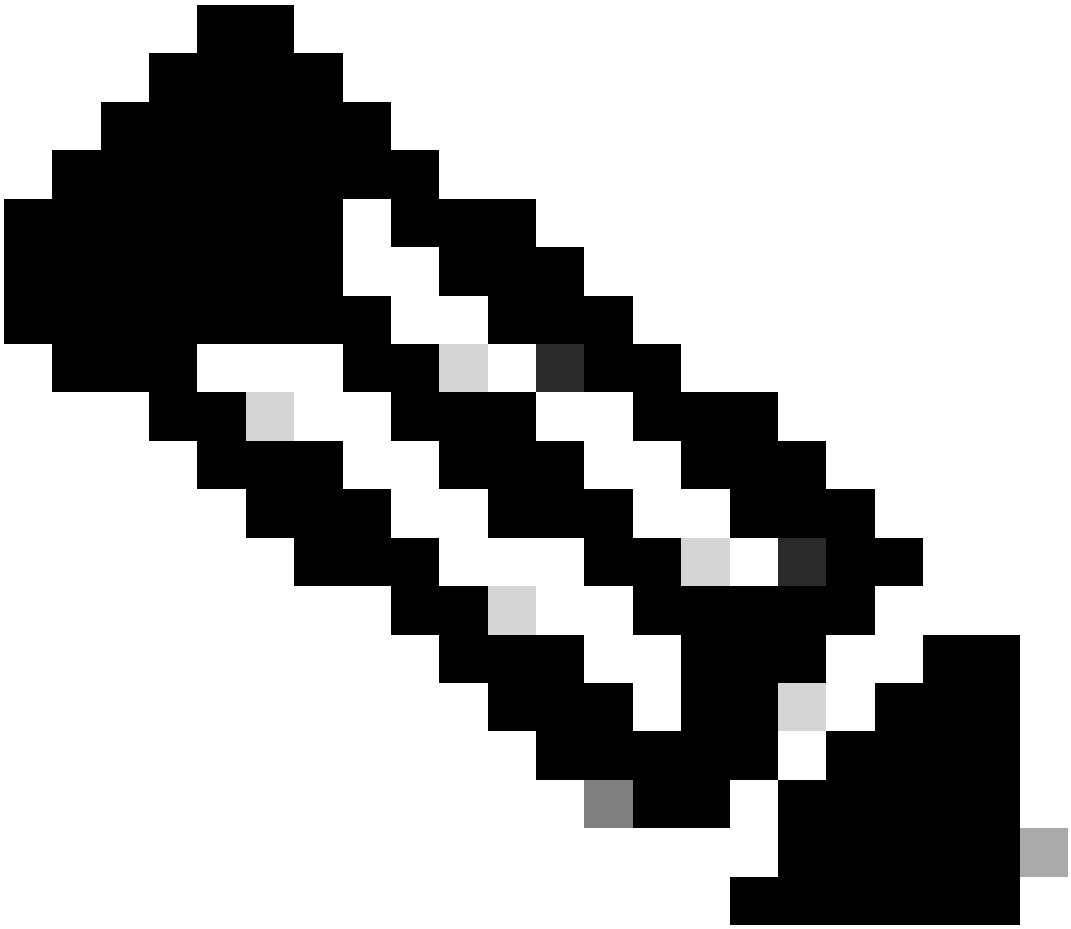


Schritt 4: Filtern Sie das Modell, und wählen Sie den c8000v-Router.



Schritt 5: Navigieren Sie zu Andere Vorlagen, und klicken Sie auf CLI-Add-On-Vorlage.

Schritt 6: Fügen Sie einen Vorlagennamen und eine Beschreibung hinzu.



Hinweis: Weitere Informationen zum Erstellen von Variablen in einer CLI-Add-On-Vorlage finden Sie unter CLI-Add-On-Funktionsvorlagen.

Schritt 7. Fügen Sie die Befehle hinzu.

CLI CONFIGURATION

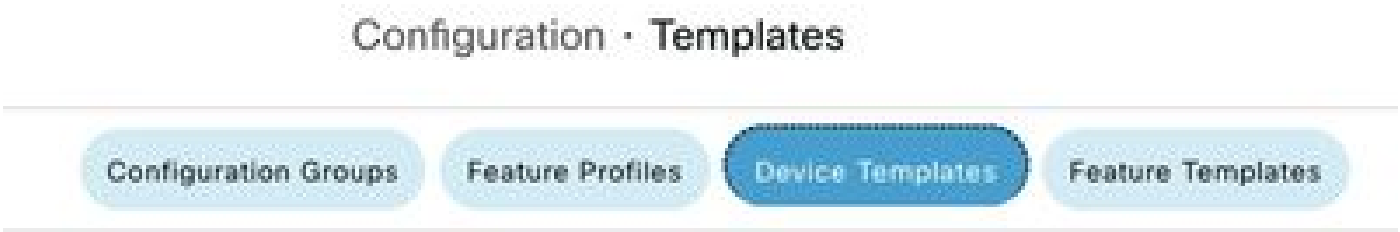
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key Cisco
 !
!
!
crypto ikev2 profile if-ipsec1-ikev2-profile
 match identity remote address 10.4.5.226 255.255.255.0
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
 set transform-set if-ipsec1-ikev2-transform
 set ikev2-profile if-ipsec1-ikev2-profile
!
!
!
```

CLI CONFIGURATION

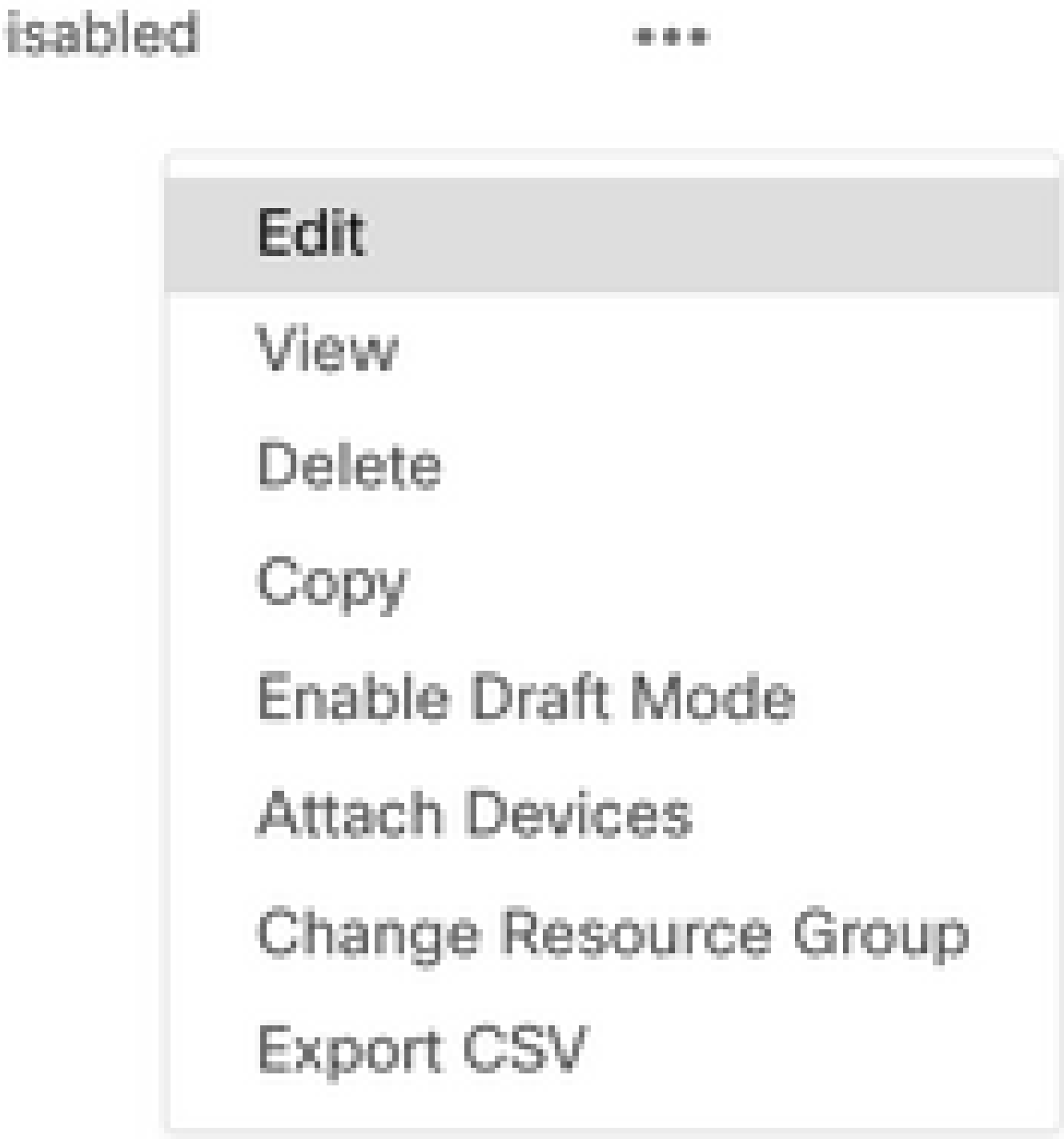
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
 set transform-set if-ipsec1-ikev2-transform
 set ikev2-profile if-ipsec1-ikev2-profile
!
!
!
!
!
!
!
!
interface Tunnel100001
 description Tunnel 1 - Ipsec BGP vWAN Azure
 vrf forwarding 90
 ip address 20.20.20.1 255.255.255.252
 ip mtu 1500
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.4.5.226
 tunnel path-mtu-discovery
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
!
```

Schritt 8: Klicken Sie auf Speichern.

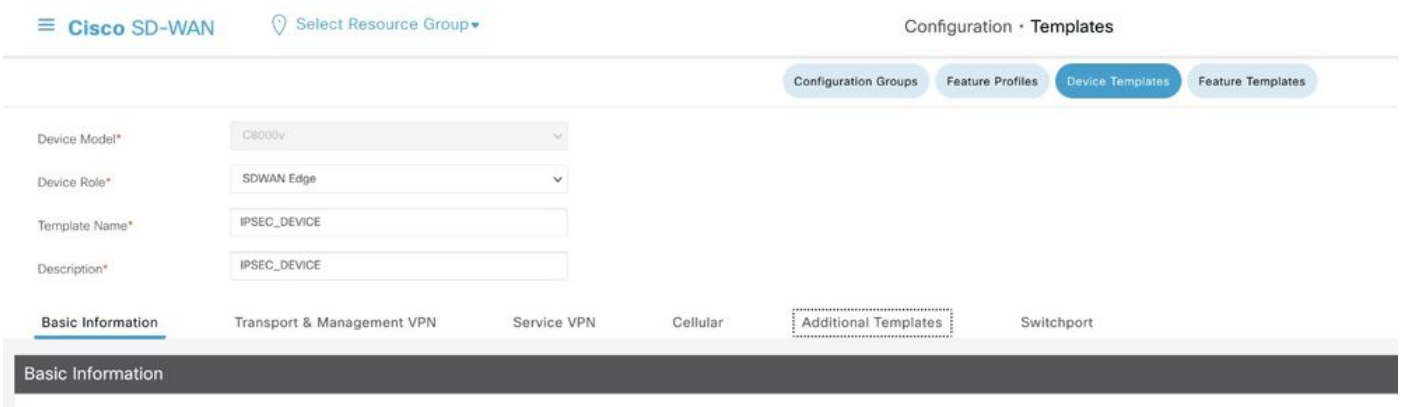
Schritt 9. Navigieren Sie zu Gerätevorlagen.



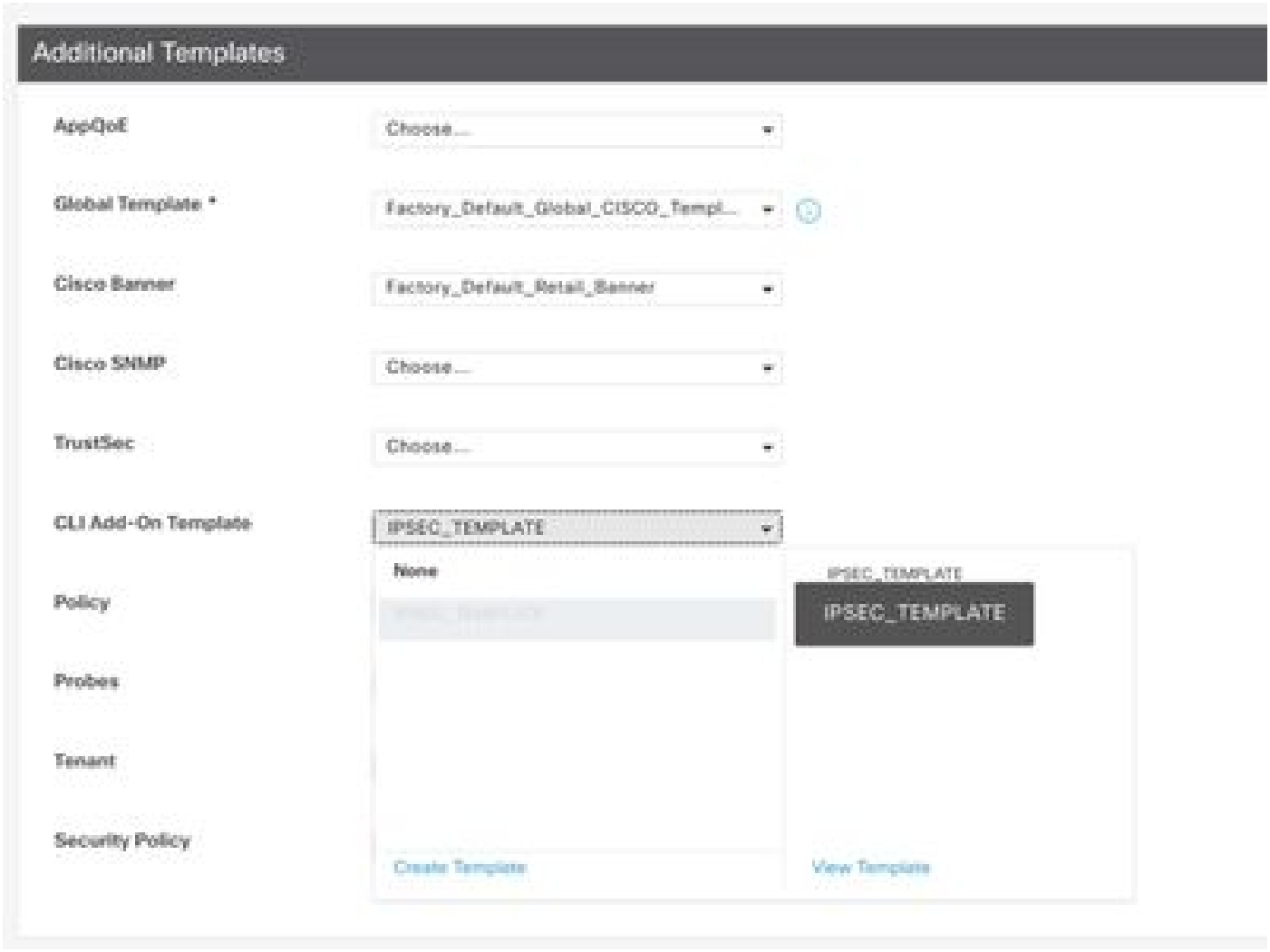
Schritt 10. Wählen Sie die richtige Gerätevorlage aus, und bearbeiten Sie sie für die drei Punkte.



Schritt 11. Navigieren Sie zu Zusätzliche Vorlagen.

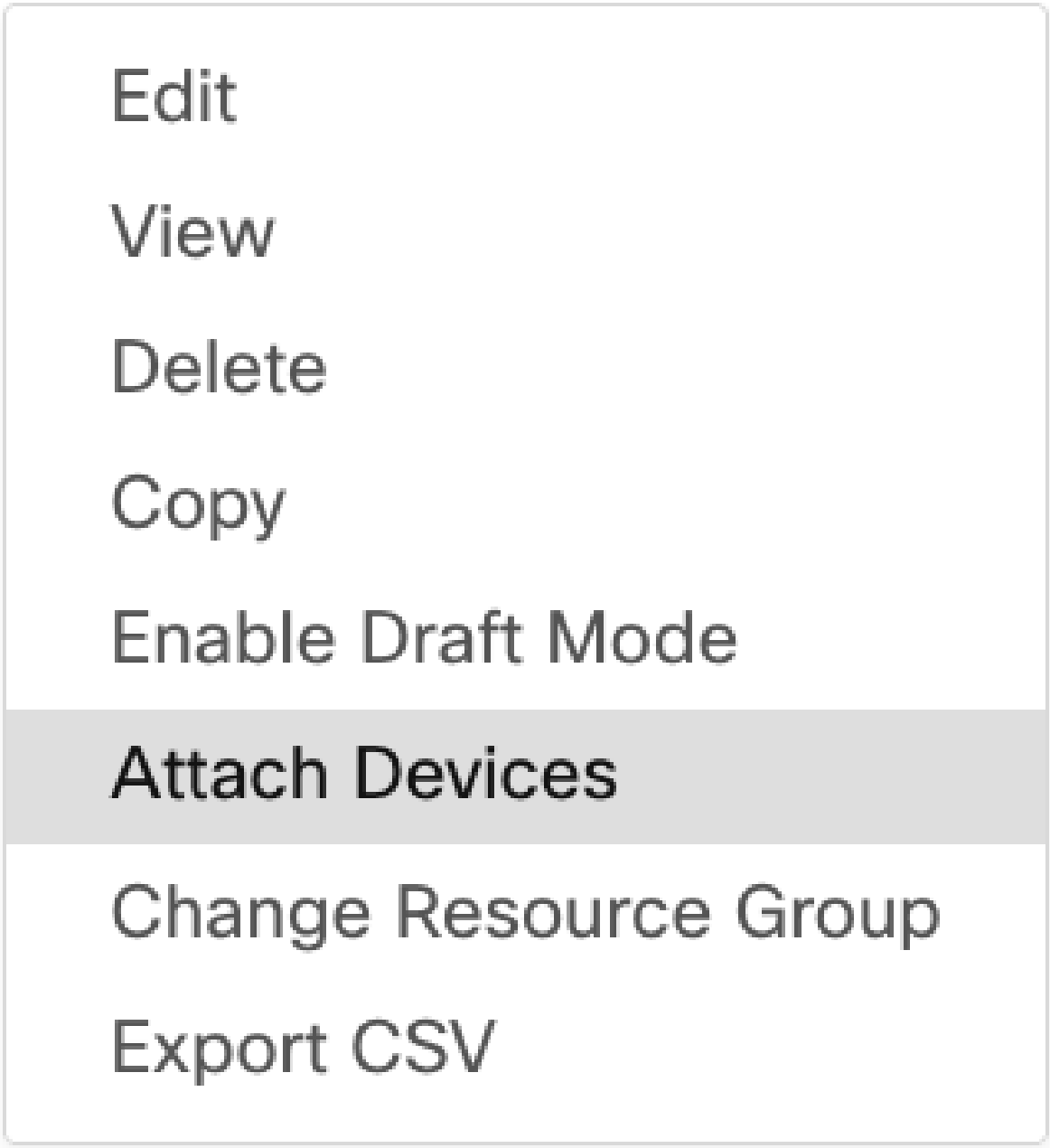


Schritt 12: Wählen Sie in der CLI-Add-On-Vorlage die zuvor erstellte Funktionsvorlage aus.



Schritt 13: Klicken Sie auf Aktualisieren.

Schritt 14: Klicken Sie auf Geräte aus drei Punkten anhängen, und wählen Sie den richtigen Router aus, an den die Vorlage gesendet werden soll.



Überprüfung

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

Führen Sie den Befehl show ip interface brief aus, um den Status des IPSec-Tunnels zu überprüfen.

<#root>

cEdge#

```
show ip interface brief


Interface IP-Address OK? Method Status Protocol
GigabitEthernet1 10.4.5.224 YES other up up

--- output omitted ---


Tunnel100001 172.16.12.1 YES other up up


cEdge#
```

Fehlerbehebung

Führen Sie den Befehl show crypto ikev2 session aus, um detaillierte Informationen zu den IKEv2-Sitzungen anzuzeigen, die auf dem Gerät eingerichtet wurden.

```
<#root>

cEdge#

show crypto ikev2 session


IPv4 Crypto IKEv2 Session

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

Tunnel-id Local Remote fvrf/ivrf Status
1 10.4.5.224/500 10.4.5.225/500 none/90 READY
Encr: AES-CBC, keysize: 128, PRF: SHA1, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/207 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: 0xFC13A6B7/0x1A2AC4A0

IPv6 Crypto IKEv2 Session

cEdge#
```

Führen Sie den Befehl show crypto ipsec sa interface Tunnel100001 aus, um Informationen zu IPSec-Sicherheitszuordnungen (SAs) anzuzeigen.

```
<#root>

cEdge#

show crypto ipsec sa interface Tunnel100001
```

```
interface: Tunnel100001
Crypto map tag: Tunnel100001-head-0, local addr 10.4.5.224

protected vrf: 90
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 10.4.5.225 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 38, #pkts encrypt: 38, #pkts digest: 38
#pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.4.5.224, remote crypto endpt.: 10.4.5.225
plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x1A2AC4A0(439010464)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xFC13A6B7(4229146295)
transform: esp-gcm 256 ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: CSR:1, sibling_flags FFFFFFFF80000048, crypto map: Tunnel100001-head-0
sa timing: remaining key lifetime (sec): 2745
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 512
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x1A2AC4A0(439010464)
transform: esp-gcm 256 ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: CSR:2, sibling_flags FFFFFFFF80000048, crypto map: Tunnel100001-head-0
sa timing: remaining key lifetime (sec): 2745
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 512
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
cEdge#
```

Führen Sie den Befehl show crypto ikev2 statistics aus, um Statistiken und Zähler zu IKEv2-Sitzungen anzuzeigen.

<#root>

cEdge#

show crypto ikev2 statistics

```
------------------------------------------------------------------------------
Crypto IKEv2 SA Statistics
------------------------------------------------------------------------------
System Resource Limit: 0 Max IKEv2 SAs: 0 Max in nego(in/out): 40/400
Total incoming IKEv2 SA Count: 0 active: 0 negotiating: 0
Total outgoing IKEv2 SA Count: 1 active: 1 negotiating: 0
Incoming IKEv2 Requests: 0 accepted: 0 rejected: 0
Outgoing IKEv2 Requests: 1 accepted: 1 rejected: 0
Rejected IKEv2 Requests: 0 rsrc low: 0 SA limit: 0
IKEv2 packets dropped at dispatch: 0
Incoming Requests dropped as LOW Q limit reached : 0
Incoming IKEV2 Cookie Challenged Requests: 0
accepted: 0 rejected: 0 rejected no cookie: 0
Total Deleted sessions of Cert Revoked Peers: 0

cEdge#
```

Führen Sie den Befehl show crypto session aus, um Informationen über aktive Sicherheitssitzungen auf dem Gerät anzuzeigen.

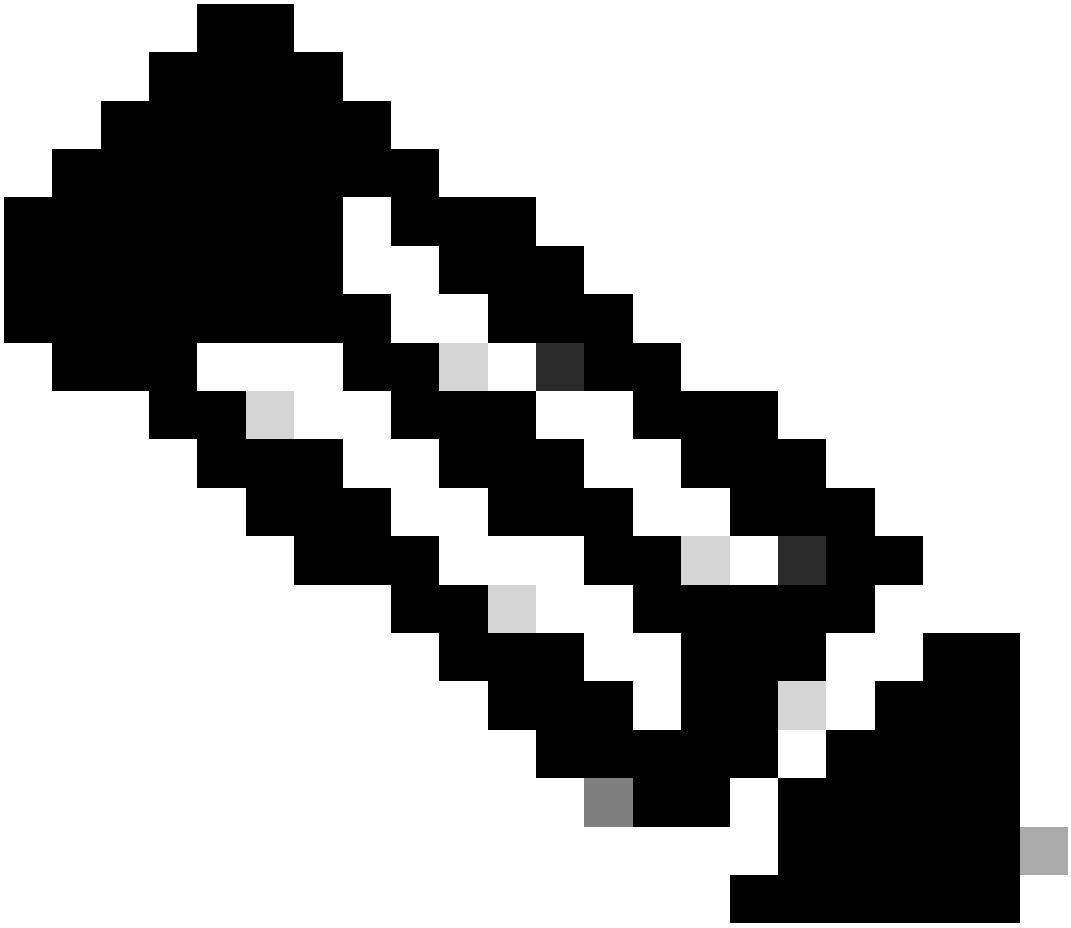
```
<#root>

cEdge#

show crypto session


Crypto session current status

Interface: Tunnel100001
Profile: if-ipsec1-ikev2-profile
Session status: UP-ACTIVE
Peer: 10.4.5.225 port 500
Session ID: 1
IKEv2 SA: local 10.4.5.224/500 remote 10.4.5.225/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

Um Informationen über IPSec-bezogene Paketverluste im Gerätepaketprozessor abzurufen, können Sie Folgendes ausführen:

show plattform hardware qfp active feature ipsec datapath drops clear

show plattform hardware qfp aktive statistik drop clear

Diese Befehle müssen vor dem Beenden gesetzt werden, und wenn die Tunnelschnittstelle nicht geschlossen wird, um die Zähler und Statistiken zu löschen, kann dies dazu beitragen, Informationen über IPsec-bezogene Paketverluste in einem Gerätepaketprozessor-Datenpfad zu erhalten.



Hinweis: Diese Befehle können ausgeführt werden, ohne dass die Option deaktiviert ist. Es ist wichtig zu betonen, dass die Zähler für das Ablegen historisch sind.

<#root>

```
cEdge#
```

```
show platform hardware qfp active feature ipsec datapath drops clear
```

```
----------------------------------------------------------------------
Drop Type Name Packets
----------------------------------------------------------------------


IPSEC detailed dp drop counters cleared after display.
```

```
cEdge#
```

<#root>

cEdge#

show platform hardware qfp active statistics drop clear

Last clearing of QFP drops statistics : Thu Sep 28 01:35:11 2023

Global Drop Stats Packets Octets

Ipv4NoRoute 17 3213
UnconfiguredIpv6Fia 18 2016

cEdge#

Nach dem Beenden und nicht nach dem Beenden der Tunnelschnittstelle können Sie diese Befehle ausführen, um festzustellen, ob neue Statistiken oder Zähler registriert wurden:

show ip interface brief | Tunnel100001 einschließen

show plattform hardware qfp aktive statistik drop

show plattform hardware qfp active feature ipsec datapath drops

<#root>

cEdge#

show ip interface brief | include Tunnel100001

Tunnel100001 169.254.21.1 YES other up up
cEdge#
cEdge#sh pl hard qfp act feature ipsec datapath drops

Drop Type Name Packets

<#root>

cEdge#

show platform hardware qfp active statistics drop

Last clearing of QFP drops statistics : Thu Sep 28 01:35:11 2023
(5m 23s ago)

Global Drop Stats Packets Octets

Ipv4NoRoute 321 60669
UnconfiguredIpv6Fia 390 42552

```
cEdge#
```

<#root>

```
cEdge#
```

show platform hardware qfp active feature ipsec datapath drops

```
----------------------------------------------------------------------
Drop Type Name Packets
----------------------------------------------------------------------


cEdge#
```

Nützliche Befehle

<#root>

show crypto ipsec sa peer <peer_address> detail

show crypto ipsec sa peer <peer_address> platform

show crypto ikev2 session

show crypto ikev2 profile

show crypto isakmp policy

show crypto map

show ip static route vrf NUMBER

show crypto isakmp sa

debug crypto isakmp

debug crypto ipsec

Zugehörige Informationen

IPsec-Schlüssel für paarweise Verbindungen

Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS® XE Catalyst SD-WAN Version 17.x

Einführung in die Cisco IPsec-Technologie

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.