IPsec-tunnel aan servicekant configureren met een C800V op SD-WAN

Inhoud

Inleiding

Dit document beschrijft hoe u een IPSec-tunnel kunt configureren tussen een SD-WAN Cisco Edge-router en een VPN-endpoint met service-VRF.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Componenten

Dit document is gebaseerd op deze software- en hardwareversies:

- Cisco Edge-router versie 17.6.1
- SD-WAN vManager 20.9.3.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten in dit document zijn gestart met een uitgeschakelde (standaard) configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke

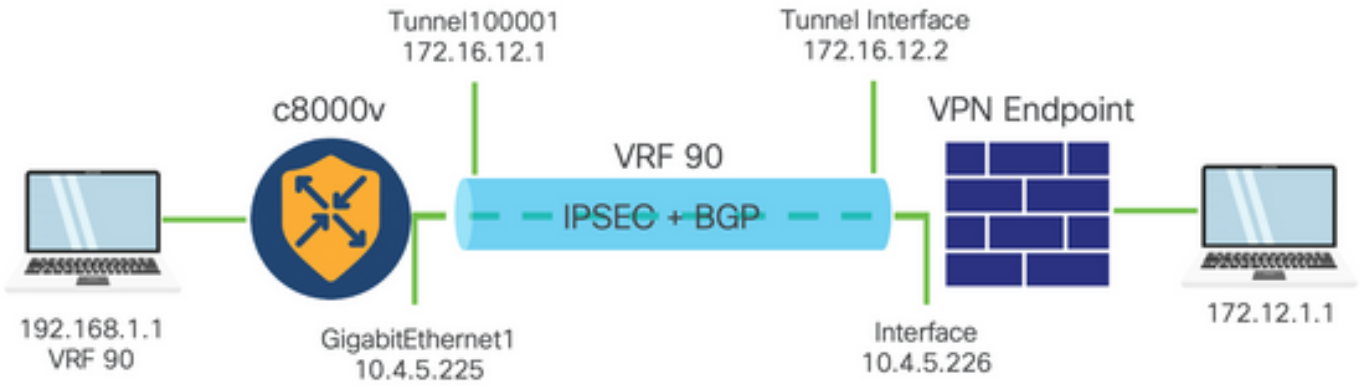
opdracht begrijpt.

Achtergrondinformatie

Achtergrondinformatie omvat het toepassingsgebied van dit document, de bruikbaarheid en de voordelen van het bouwen van een IPSec-tunnelbuis aan servicekant met een C800v op SD-WAN.

- Om een IPSec-tunnel te bouwen in een service Virtual Routing and Forwarding (VRF) tussen een Cisco IOS® XE-router op controller-management-modus en een Virtual Private Network (VPN)-endpoint garandeert gegevensvertrouwelijkheid en -integriteit via het publieke Wide Area Network (WAN). Het vergemakkelijkt ook de veilige uitbreiding van de particuliere netwerken van bedrijven en maakt externe verbindingen via het internet mogelijk terwijl een hoog beveiligingsniveau wordt gehandhaafd.
- De service VRF isoleert verkeer, wat bijzonder waardevol is in multi-client omgevingen of voor het onderhouden van segmentatie tussen verschillende delen van het netwerk. Samengevat, deze configuratie verbetert veiligheid en connectiviteit.
- Dit document is van mening dat BGP (border Gateway Protocol) het routingprotocol is dat wordt gebruikt om de netwerken van de SD-WAN service VRF te communiceren naar het netwerk achter het VPN-endpoint en vice versa.
- De BGP-configuratie valt buiten het bereik van dit document.
- Dit VPN Endpoint kan een firewall, een router of elk type netwerkapparaat zijn dat IPSec-functies heeft. De configuratie van het VPN-Endpoint valt buiten het bereik van dit document.
- Dit document veronderstelt dat de router reeds aan boord is met actieve controleverbindingen en de dienst VRF.

Componenten van IPSEC-configuratie



Fase 1 Internet Key Exchange (IKE)

Fase 1 van het IPSec-configuratieproces omvat onderhandeling van de veiligheidsparameters en verificatie tussen tunneleindpunten. Deze stappen omvatten:

IKE-configuratie

- Definieer een coderingsvoorstel (algoritme en sleutellengte).
- Configureer een IKE-beleid dat coderingsvoorstel, tijd voor bewegend beeld en verificatie bevat.

Externe eindpeers configureren

- Bepaal het IP-adres van het externe einde.
- Configureer gedeelde sleutel (vooraf gedeelde sleutel) voor verificatie.

Configuratie fase 2 (IPSec)

Fase 2 omvat onderhandelingen over de veiligheidstransformaties en toegangsregels voor de verkeersstroom door de tunnel. Deze stappen omvatten:

IPsec-transformatiesets configureren

- Bepaal een voorgestelde transformatie-reeks die het encryptie algoritme en de authentificatie omvat.

Een IPSec-beleid configureren

- Associeer de transformatie-set met een IPSec-beleid.

Tunnelinterfaces configureren

Configureer tunnelinterfaces op beide uiteinden van de IPSec-tunnel.

- Associeer de tunnelinterfaces met het IPSec-beleid.

Configureren

Configuratie op CLI

Stap 1. Definieer een coderingsvoorstel.

<#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
```

Stap 2. Configureer een IKE-beleid dat informatie over voorstellen bevat.

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

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

Stap 3. Bepaal het IP-adres van het externe einde.

```
<#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
```

Stap 4. Configureer gedeelde sleutel (vooraf gedeelde sleutel) voor verificatie.

```
<#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)#
```

Stap 5. Definieer een voorgestelde transformatie-set die het encryptie-algoritme en de authenticatie bevat.

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

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

Stap 6. Associeer de transformatie-set met een IPSec-beleid.

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

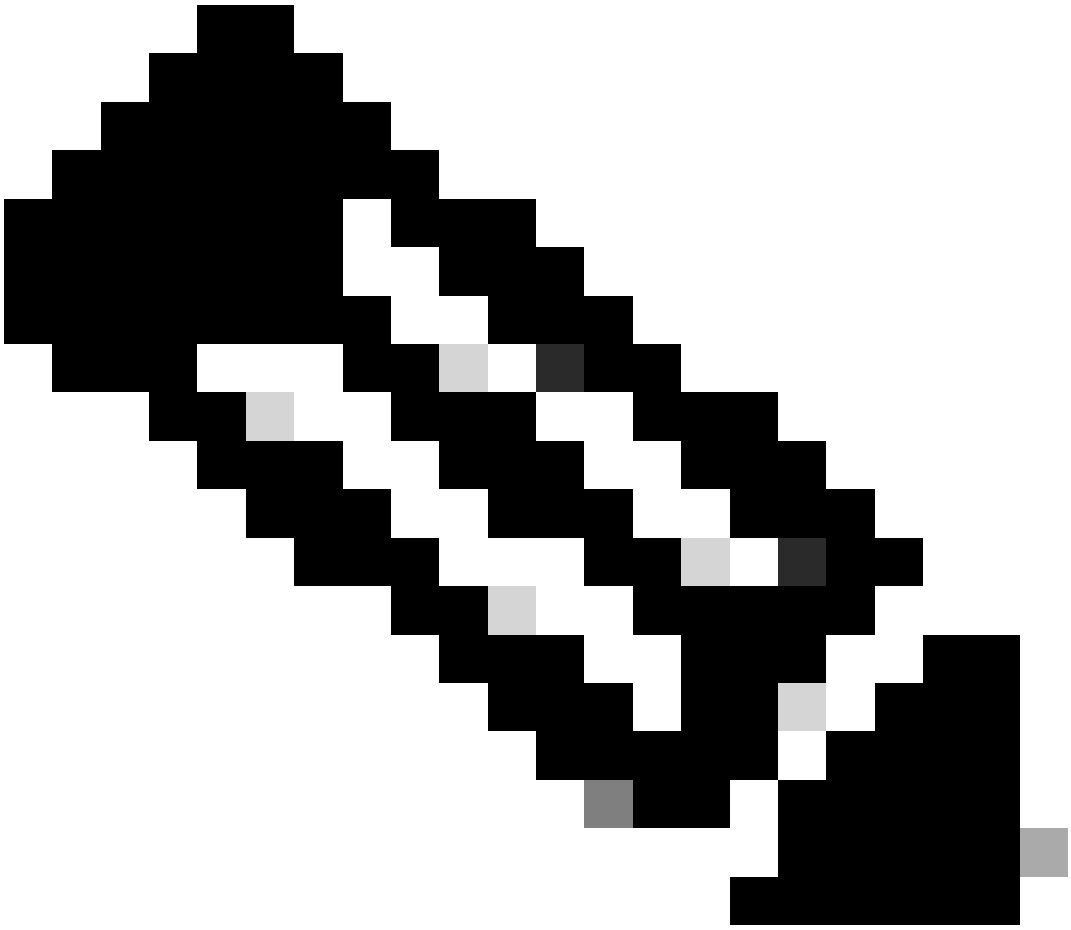
```
crypto ipsec profile if-ipsec1-ipsec-profile

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
```

Stap 7. Maak de interfacetunnel en koppel deze aan het IPSec-beleid.

```
<#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
```

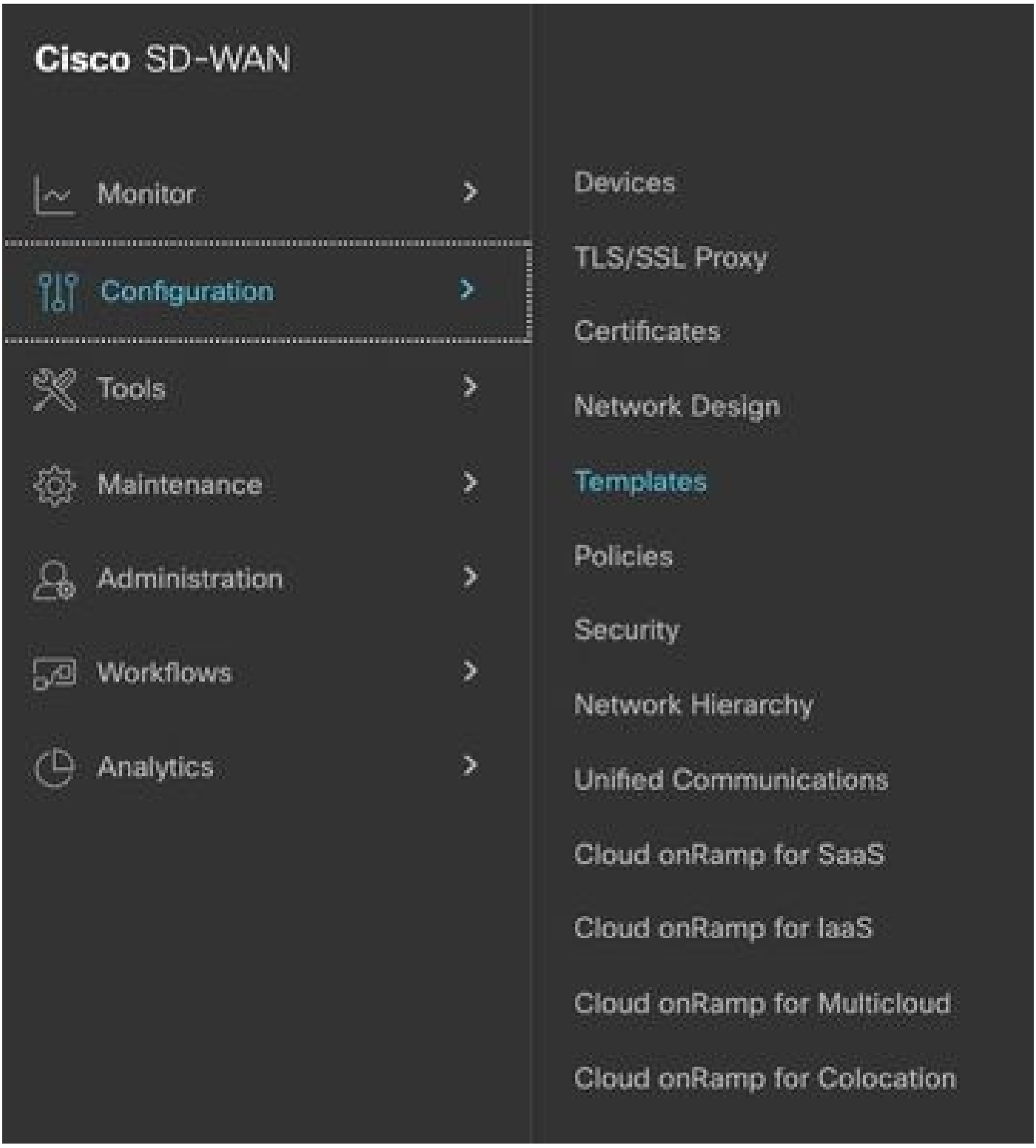
Configuratie op een CLI-invoegsjabloon op de vManager



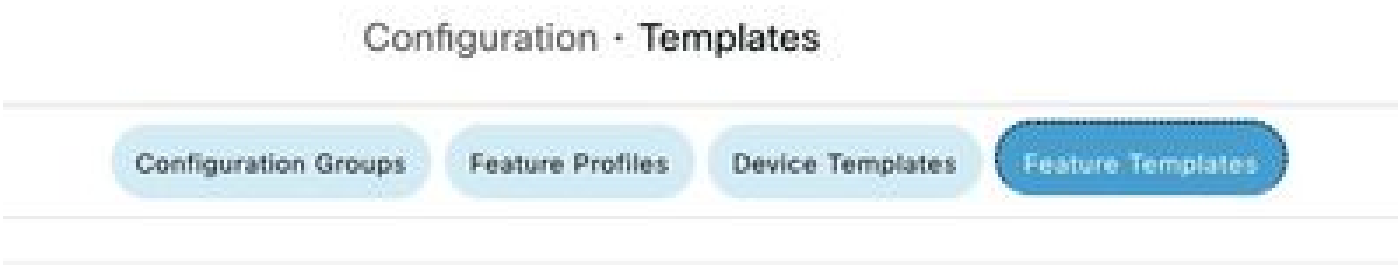
Opmerking: dit type configuratie kan alleen worden toegevoegd via CLI Add-on sjabloon.

Stap 1. Navigeer naar Cisco vManager en log in.

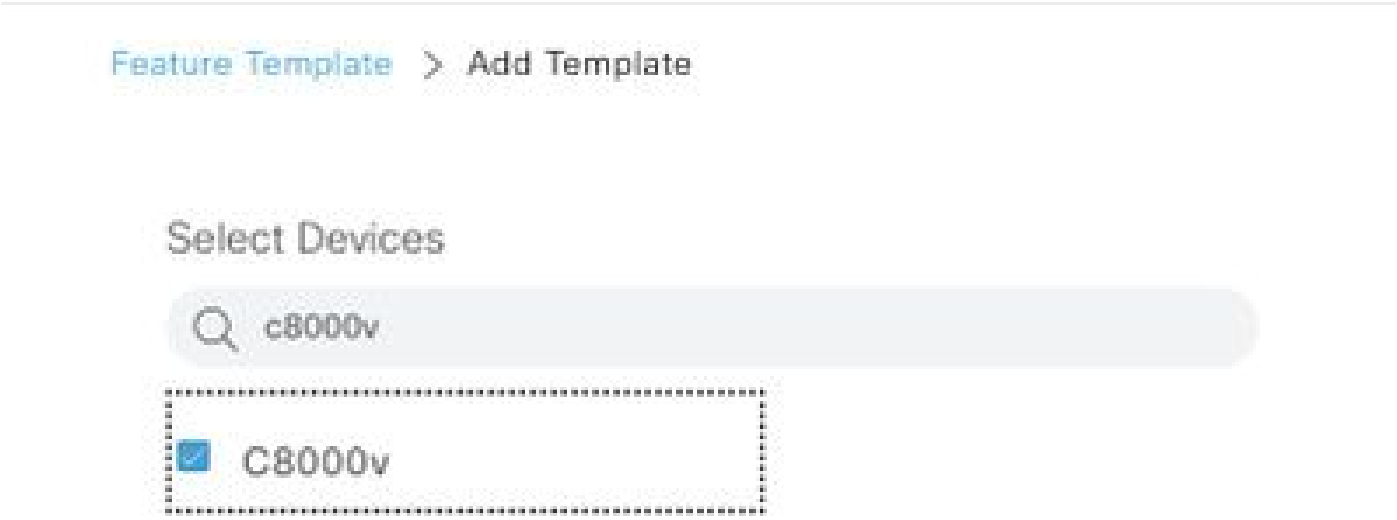
Stap 2. Navigeer naar Configuration > Templates.



Stap 3. Navigeer naar functiesjablonen > Sjabloon toevoegen.

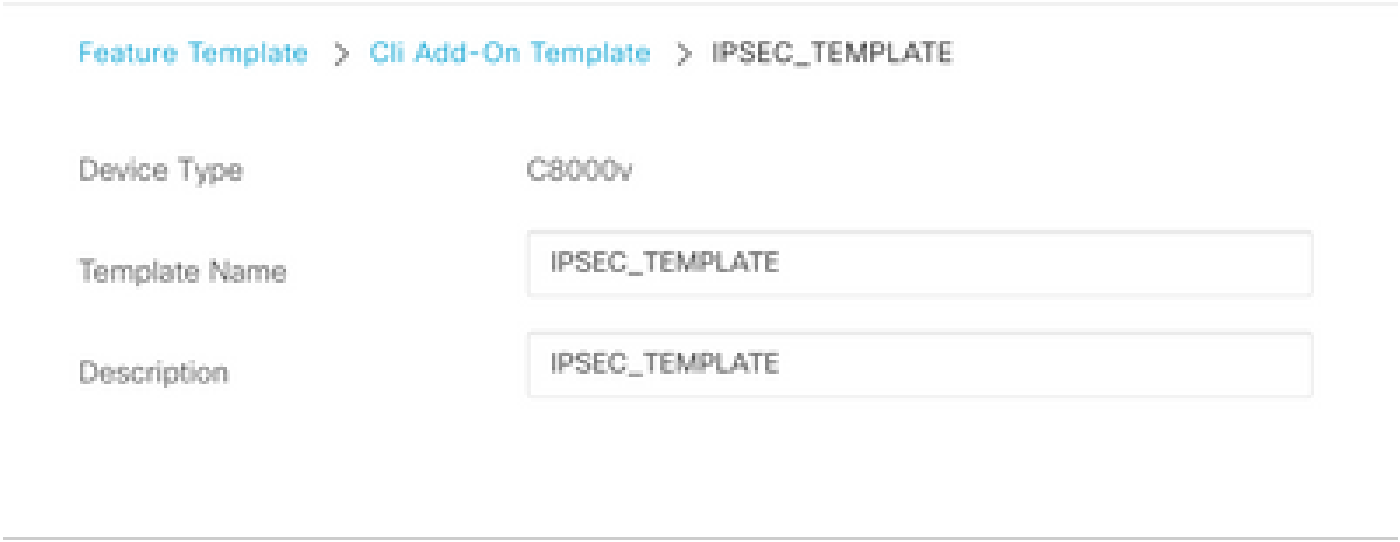


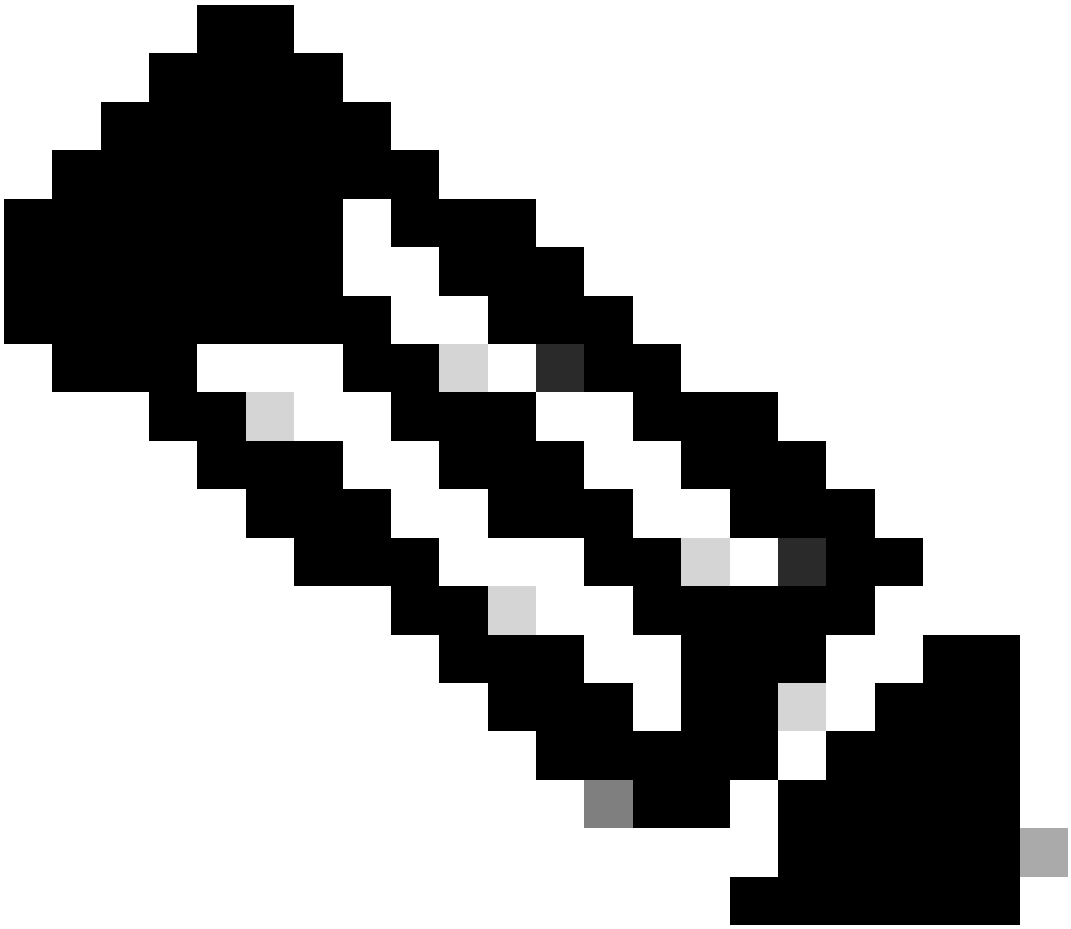
Stap 4. Filter het model en kies de c8000v router.



Stap 5. Navigeer naar andere sjablonen en klik op CLI Add-On Template.

Stap 6. Voeg een Sjabloonnaam en een beschrijving toe.





Opmerking: voor meer informatie over het maken van variabelen op een CLI Add-On Template raadpleegt u CLI Add-On Feature Templates.

Stap 7. Voeg de opdrachten toe.

CLI CONFIGURATION

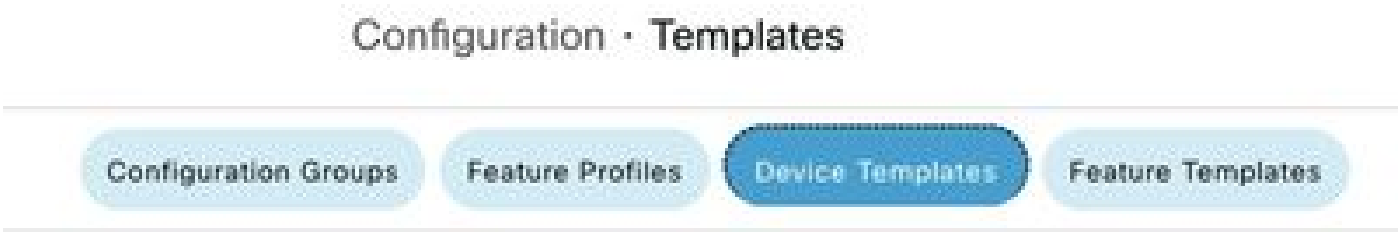
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key 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

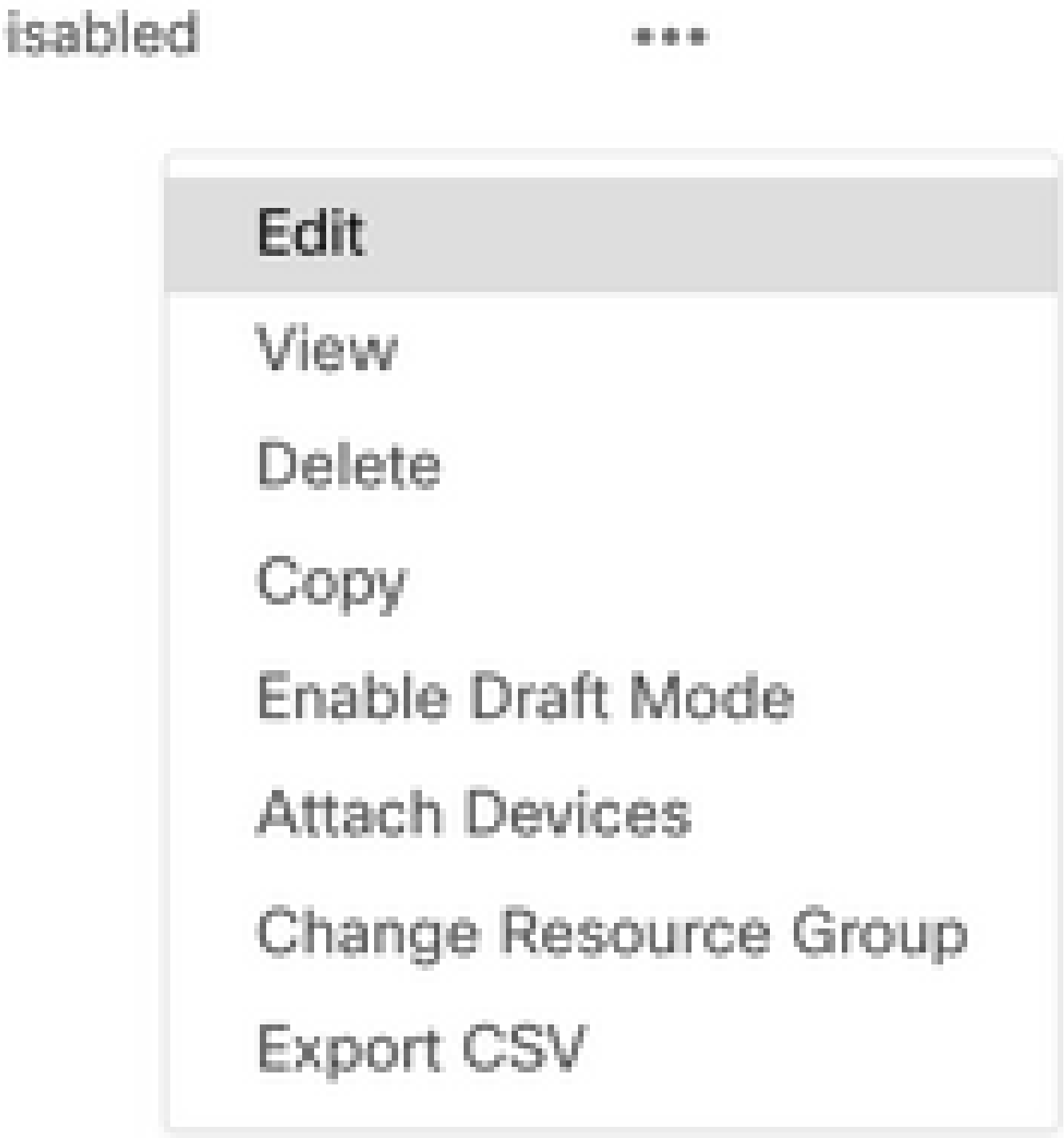
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

Stap 8. Klik op Opslaan.

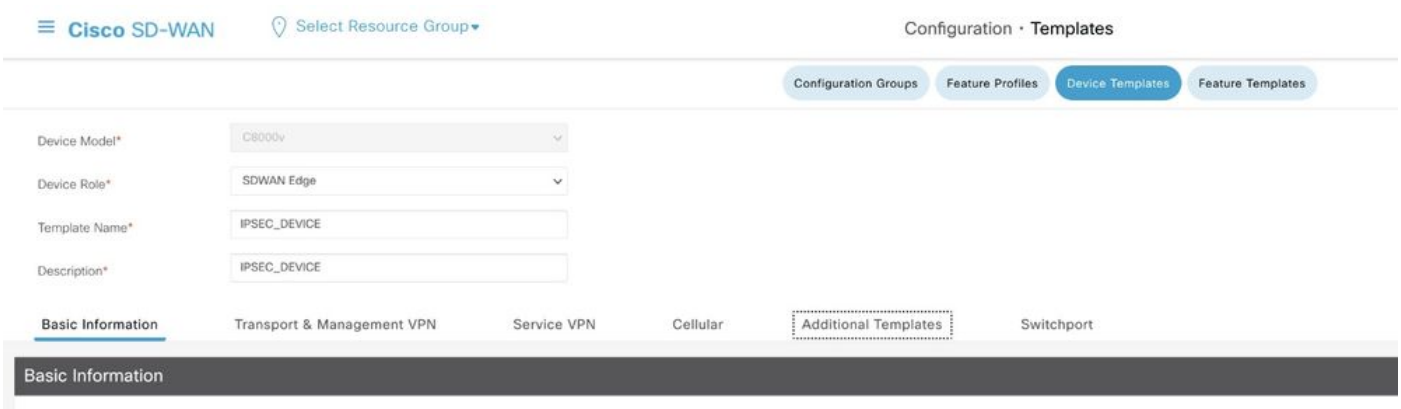
Stap 9. Navigeren naar apparaatsjablonen.



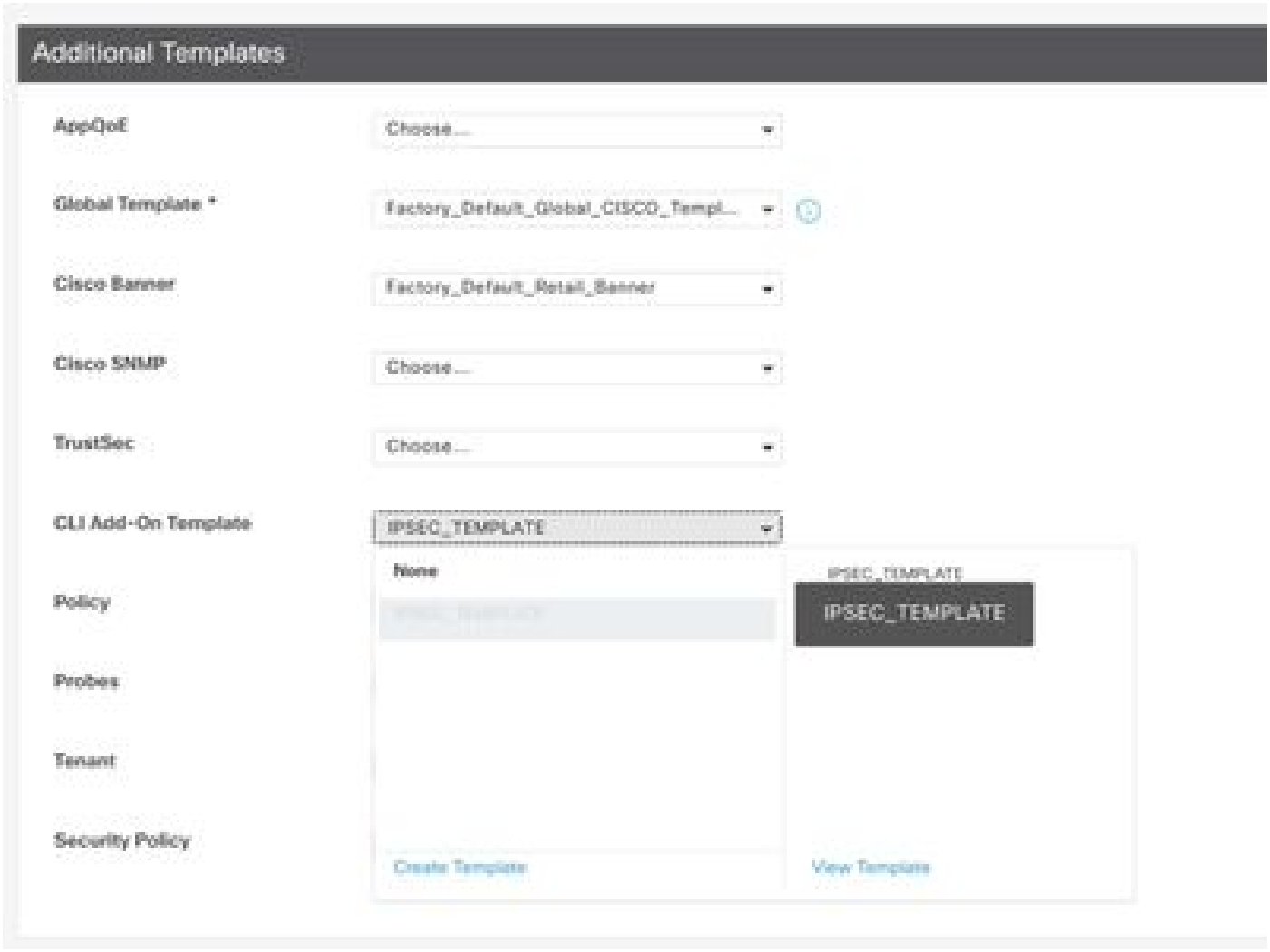
Stap 10. Kies de juiste apparaatsjabloon en bewerk deze op de 3 punten.



Stap 11. Ga naar extra sjablonen.

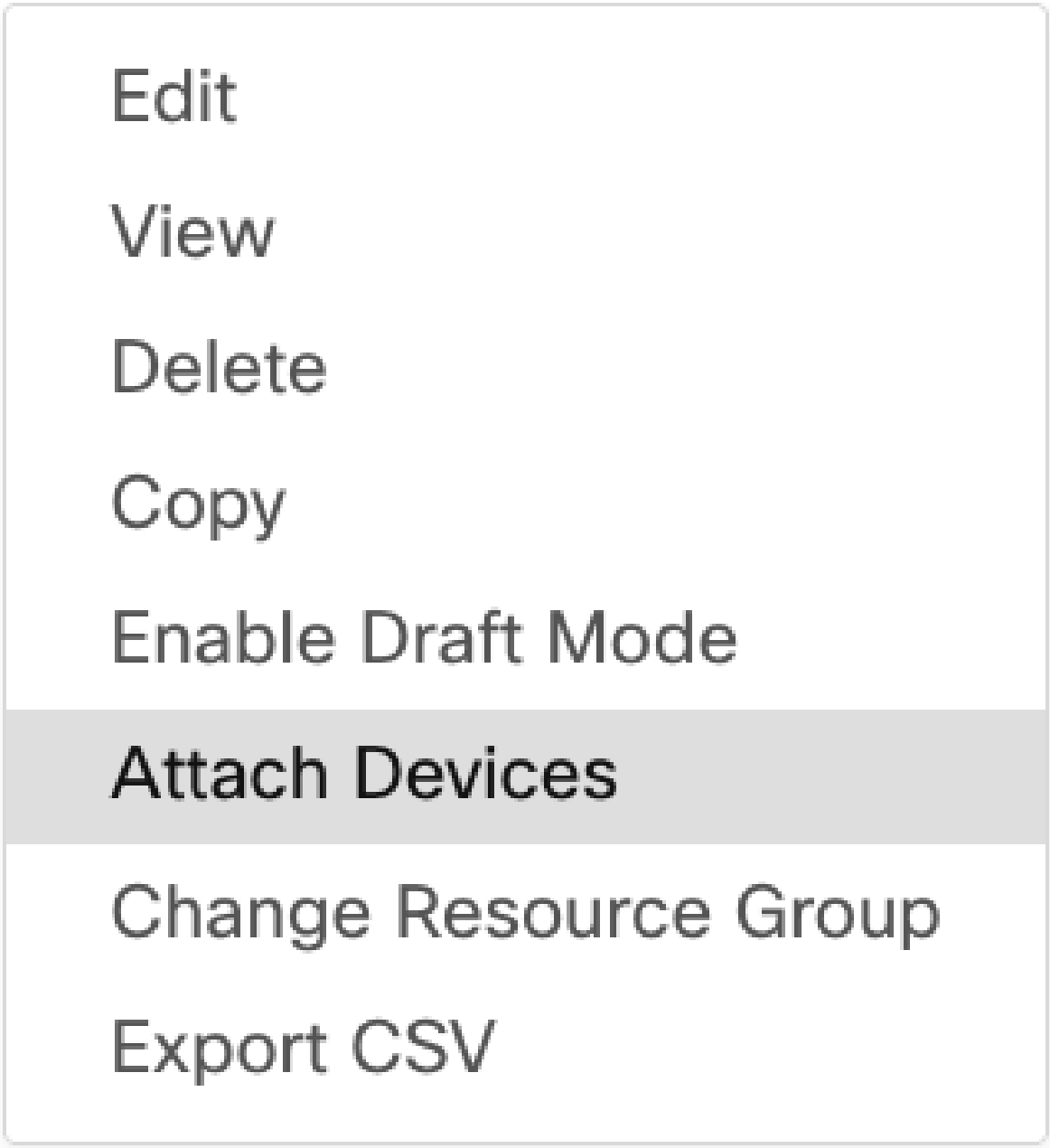


Stap 12. Kies op CLI Add-On Template de eerder gemaakte functiesjabloon.



Stap 13. Klik op Bijwerken.

Stap 14. Klik op Attachapparaten vanaf 3 punten en selecteer de juiste router om de sjabloon naar te duwen.



Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Voer de korte opdracht van de IP-interface in om de status van de IPSec-tunnel te verifiëren.

<#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#
```

Problemen oplossen

Voer de opdracht show crypto ikev2 sessie uit om gedetailleerde informatie weer te geven over de IKEv2-sessies die op het apparaat zijn ingesteld.

```
<#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#
```

Voer de opdracht show crypto ipsec als interface Tunnel10001 om informatie over IPSec Security Associations (SA's) weer te geven.

```
<#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#
```

Voer de opdracht tonen crypto ikev2 statistieken om statistieken en tellers met betrekking tot IKEv2 sessies weer te geven.

<#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#
```

Voer de opdracht show crypto sessie om informatie over actieve security sessies op het apparaat weer te geven.

<#root>

```
cEdge#
```

show crypto session

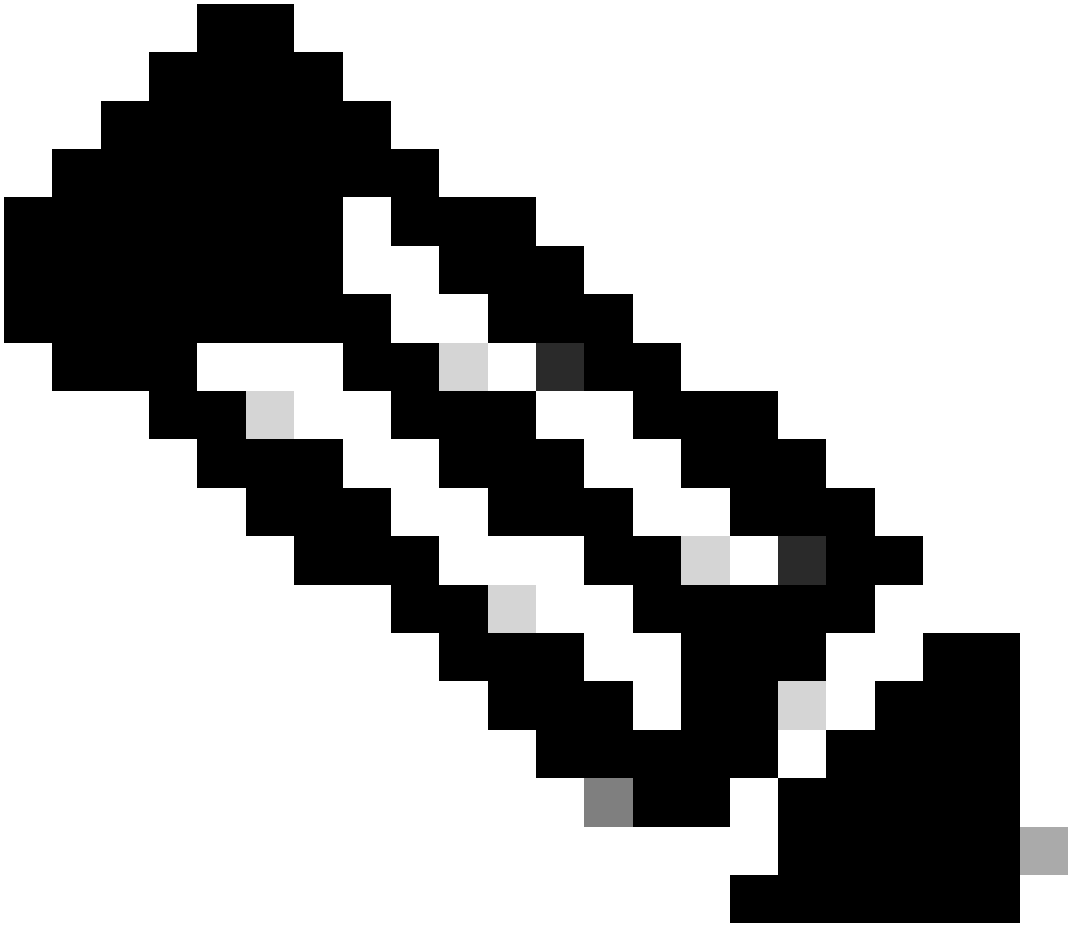
```
Crypto session current status

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
```

Om informatie te verkrijgen over met IPSec verband houdende pakketdalingen in de apparaatpakketprocessor kunt u uitvoeren:

toon platform hardware qfp actieve functie ipsec datapath laat vallen helder

toon platform hardware qfp actieve statistieken drop clear

Deze opdrachten moeten worden voorgedrukt om de Tunnel interface te sluiten en niet te sluiten om de tellers en statistieken te wissen, dit kan helpen om informatie te verkrijgen over IPsec-gerelateerde pakketdalingen in een apparaat pakketprocessor datapath.



Opmerking: deze opdrachten kunnen worden uitgevoerd zonder de optie leeg te maken. Het is belangrijk om te benadrukken dat de druppeltellers historisch zijn.

<#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#

Na gesloten en geen gesloten de Tunnel Interface kunt u deze bevelen in werking stellen om te zien of er een registratie van nieuwe statistieken of tellers was:

toon ip interfacememememorandum | omvat tunnel100001

toon platform hardware qfp actieve statistieken drop

toon platform hardware qfp actieve functie ipsec datapath druppels

<#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#
```

Nuttige opdrachten

<#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

Gerelateerde informatie

IPsec-paarsgewijze toetsen

Cisco Catalyst SD-WAN security configuratiegids, Cisco IOS® XE Catalyst SD-WAN release 17.x

Inleiding tot Cisco IPsec-technologie

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.