

Umbrella SIG-tunnels configureren voor actieve/back-up- of actieve/actieve scenario's

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Cisco Umbrella SIG - Overzicht](#)

[Umbrella SIG-tunnelbandbreedtebeperking](#)

[Ontvang informatie over uw Cisco Umbrella Portal](#)

[Ontvang de sleutel en de geheime sleutel](#)

[Uw organisatie-id verkrijgen](#)

[Umbrella SIG-tunnels met actief/back-upscenario maken](#)

[Stap 1. Maak een SIG Credentials functiesjabloon.](#)

[Stap 2. Maak een SIG-functiesjabloon.](#)

[Stap 3. Selecteer Uw SIG-provider voor primaire tunnel.](#)

[Stap 4. Voeg de secundaire tunnel toe.](#)

[Stap 5. Maak één paar met hoge beschikbaarheid.](#)

[Stap 6. Bewerk de servicekant VPN-sjabloon om een serviceroute te injecteren.](#)

[WAN Edge-routerconfiguratie voor actief/back-upscenario](#)

[Umbrella SIG-tunnels met actief/actief scenario maken](#)

[Stap 1. Maak een SIG Credentials functiesjabloon.](#)

[Stap 2. Maak twee Loopback-interfaces om de SIG-tunnels te koppelen.](#)

[Stap 3. Maak een SIG-functiesjabloon.](#)

Inleiding

Dit document beschrijft hoe u twee scenario's van Cisco **Umbrella Secure Internet Gateway (SIG)**-tunnels met IPsec op **WAN Edge-router kunt** configureren:

- Twee IPsec-tunnels in een actief/back-upscenario.
- Twee IPsec-tunnels in een actief/actief scenario.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Cisco-paraplu
- IPsec-onderhandeling
- Cisco softwaregedefinieerde Wide Area Network (SD-WAN)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco vManager versie 20.4.2
- Cisco WAN Edge-router C117-4PW* versie 17.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Umbrella SIG - Overzicht

Cisco **Umbrella** is een door de cloud geleverde security service die essentiële functies bij elkaar brengt.

Umbrella verenigt beveiligde webgateway, DNS-beveiliging, cloud-geleverde firewall, cloud access security broker functionaliteit en bedreigingsinformatie.

Diepgaande inspectie en controle zorgen voor naleving van acceptabel gebruik webbeleid en beschermen tegen internetbedreigingen.

SD-WAN routers kunnen integreren met Secure Internet Gateways (SIG) die het merendeel van de verwerking doen om bedrijfsverkeer te beveiligen.

Wanneer SIG is ingesteld, wordt al het clientverkeer, gebaseerd op routes of beleid, doorgestuurd naar SIG.

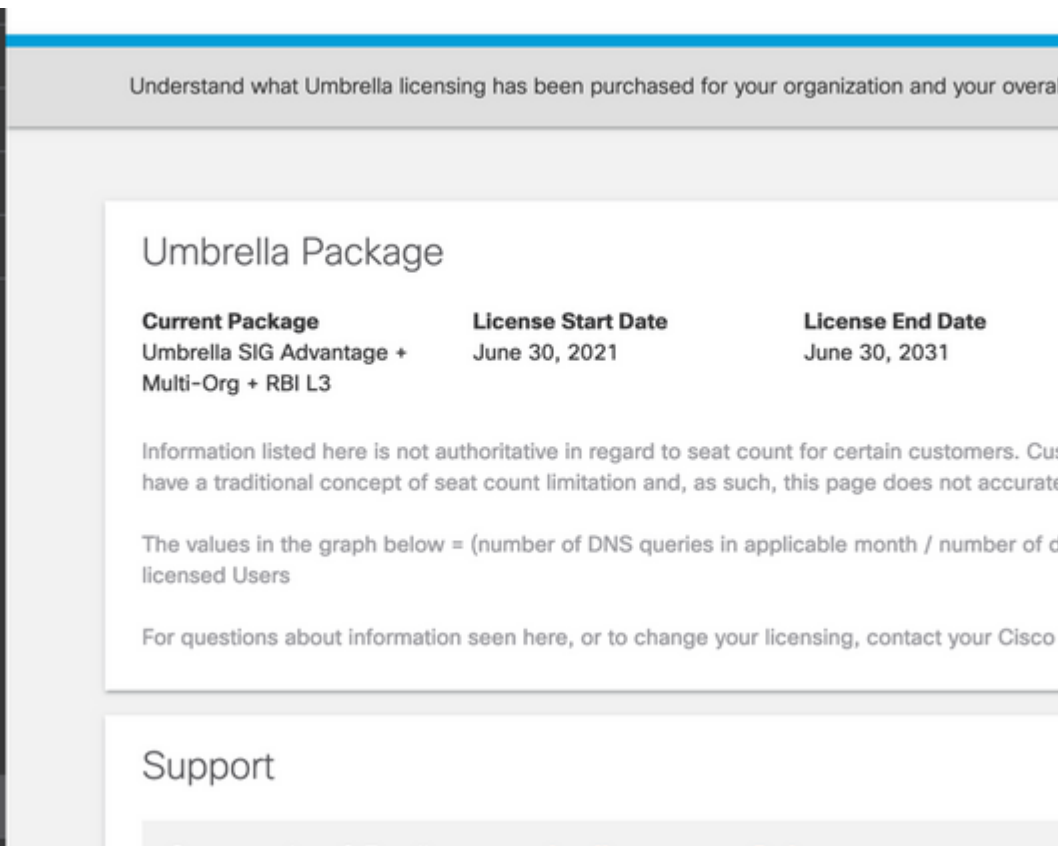
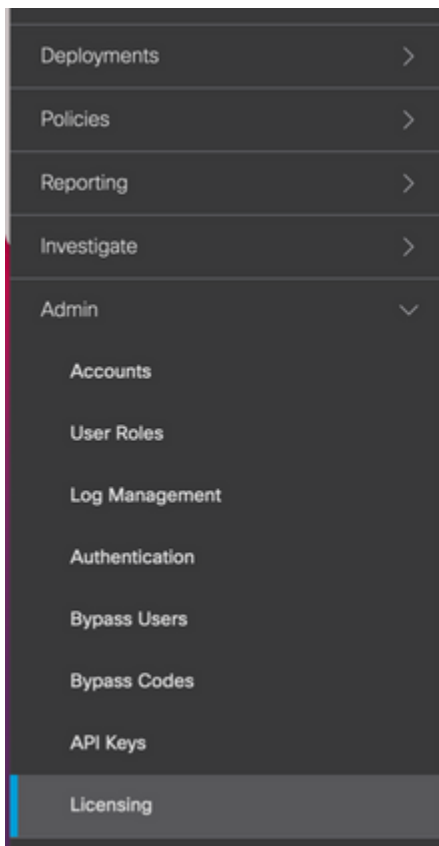
Umbrella SIG-tunnelbandbreedtebeperking

Elke IPsec IKEv2-tunnel naar de **Umbrella**-head-end is beperkt tot ongeveer 250 Mbps. Als er dus meerdere tunnels worden gemaakt en de werklastverdeling in het verkeer wordt verdeeld, overwinnen deze beperkingen als er een hogere bandbreedte nodig is.

Tot vier High Availability tunnelparen kunnen worden gemaakt.

Ontvang informatie over uw Cisco Umbrella Portal

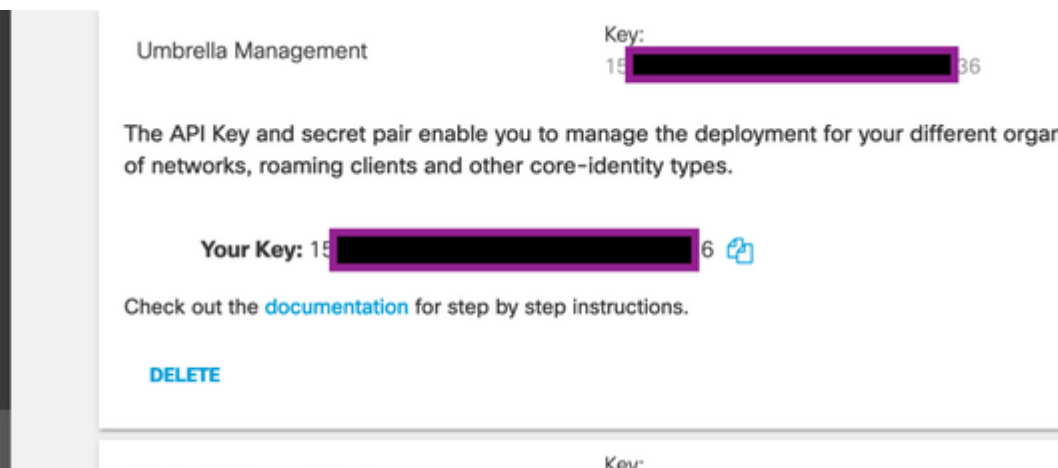
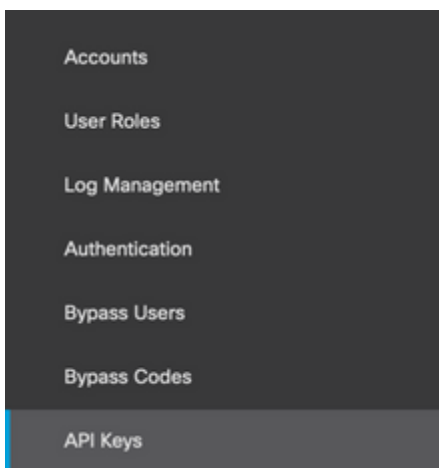
Om de SIG-integratie te kunnen voortzetten, is een **Umbrella**-account met basispakket SIG nodig.



Ontvang de sleutel en de geheime sleutel

De sleutel en geheime sleutel kan worden gegenereerd op het moment dat u de **Umbrella Management API KEY** krijgt. Als u de geheime sleutel niet meer weet of niet hebt opgeslagen, klikt u op **Vernieuwen**.

Waarschuwing: als op de knop Vernieuwen wordt gedrukt, is een update voor deze toetsen op alle apparaten nodig. De update wordt niet aanbevolen als er apparaten in gebruik zijn.



Uw organisatie-id verkrijgen

De organisatie-ID is gemakkelijk te verkrijgen wanneer u inlogt bij **Umbrella**.

<https://dashboard.umbrella.com/o///#/admin/apikeys>

Umbrella SIG-tunnels met actief/back-upscenario maken

Opmerking: IPsec/GRE-tunnelrouting en taakverdeling met behulp van ECMP: deze functie is beschikbaar in vManager 20.4.1 en verder kunt u de SIG-sjabloon gebruiken om toepassingsverkeer naar Cisco **Umbrella** of een externe SIG-provider te sturen

Opmerking: ondersteuning voor Zscaler Automatische Provisioning: deze functie is beschikbaar op vManager 20.5.1 en verder, dit automatiseert de levering van tunnels van Cisco SD-WAN routers naar Zscaler, met het gebruik van Zscaler partner API-referenties.

Om de SIG automatische tunnels te configureren, moet u een paar sjablonen maken/bijwerken:

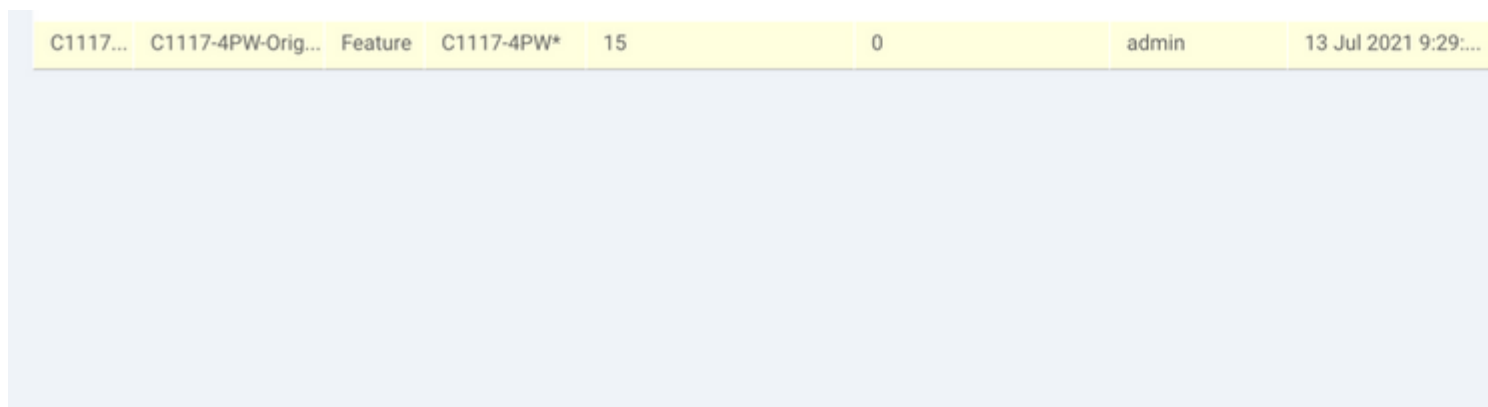
- Maak een SIG Credentials functiesjabloon.
 - Maak twee loopback interfaces om de SIG-tunnels te koppelen (alleen van toepassing met meer dan één actieve tunnel tegelijkertijd - actief/actief scenario).
 - Maak een SIG-functiesjabloon.
 - Bewerk **de servicekant VPN**-sjabloon om een serviceroute te injecteren.
-

Opmerking: Zorg ervoor dat de UDP 4500- en 500-poorten vanaf elk upstream-apparaat zijn toegestaan.

De sjabloonconfiguraties veranderen met de Active/Backup en de Active/Active scenario's waarvoor beide scenario's afzonderlijk worden uitgelegd en weergegeven.

Stap 1. Maak een SIG Credentials functiesjabloon.

Ga naar de functiesjabloon en klik op **Bewerken**.



C1117...	C1117-4PW-Orig...	Feature	C1117-4PW*	15	0	admin	13 Jul 2021 9:29:...
----------	-------------------	---------	------------	----	---	-------	----------------------

Klik in het gedeelte **Aanvullende sjablonen** op **Cisco SIG Credentials**. De optie wordt in de afbeelding weergegeven.

Additional Templates

Global Template *	Factory_Default_Global_CISCO_Template ?
Cisco Banner	Choose...
Cisco SNMP	Choose...
CLI Add-On Template	Choose...
Policy	app-flow-visibility
Probes	Choose...
Security Policy	Choose...
Cisco SIG Credentials *	SIG-Credentials

Geef een naam en beschrijving aan de sjabloon.

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco SIG Credentials > SIG-Credentials

Device Type	C1117-4PW*
Template Name	SIG-Credentials
Description	SIG-Credentials

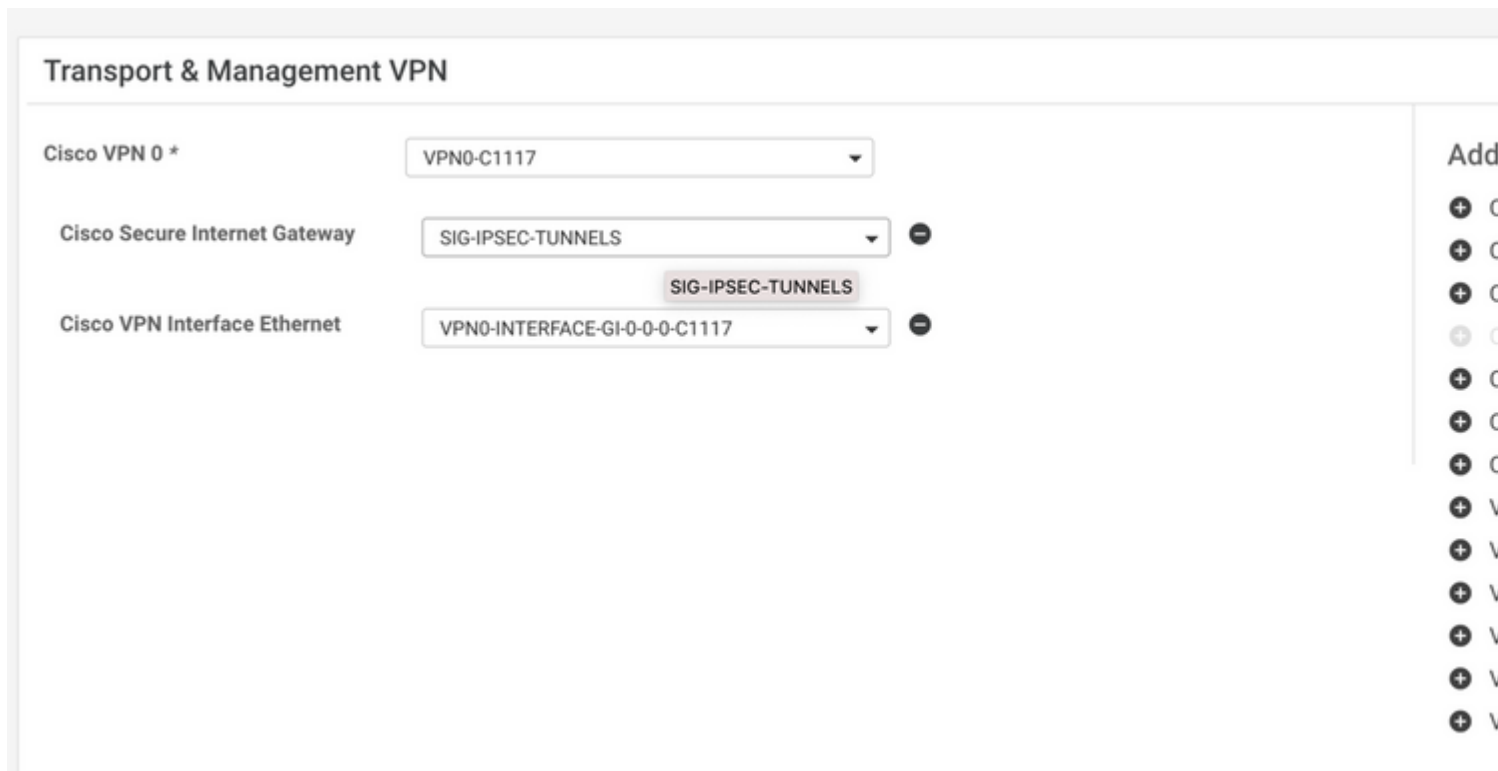
Basic Details

SIG Provider	<input checked="" type="radio"/> Umbrella
Organization ID	<input type="text" value="5"/> [REDACTED]
Registration Key	<input type="text" value="1"/> [REDACTED]
Secret	<input type="text" value="....."/>

[Get Keys](#)

Stap 2. Maak een SIG-functiesjabloon.

Navigeer naar de functiesjabloon en selecteer onder de sectie **Transport & Management VPN** de functiesjabloon **Cisco Secure Internet Gateway**.



Geef een naam en beschrijving aan de sjabloon.

Stap 3. Selecteer Uw SIG-provider voor primaire tunnel.

Klik op **Tunnel toevoegen**.



Configureer de basisgegevens en houd het **datacenter** als **primair**, klik vervolgens op **Toevoegen**.

Basic Settings

Tunnel Type

IPsec

Interface Name (1..255)

Description

Tunnel Source Interface

Data-Center

 Primary SecondaryAdvanced Options ▼

General

Shutdown

 Yes No

TCP MSS

IP MTU

Stap 4. Voeg de secundaire tunnel toe.

Voeg een tweede tunnelconfiguratie toe, gebruik dit keer **Data-Center** als **Secundair** en de interfacenaam als *ipsec2*.

vManager-configuratie wordt weergegeven zoals hier wordt getoond:

Configuration

SIG Provider Umbrella Third Party

[+ Add Tunnel](#)

Tunnel Name	Description	Shutdown	TCP MSS
ipsec1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300
ipsec2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300

Stap 5. Maak één paar met hoge beschikbaarheid.

Selecteer in het gedeelte Hoge beschikbaarheid de **ipsec1** als **actief** en de **ipsec2**-tunnel als **back-up**.

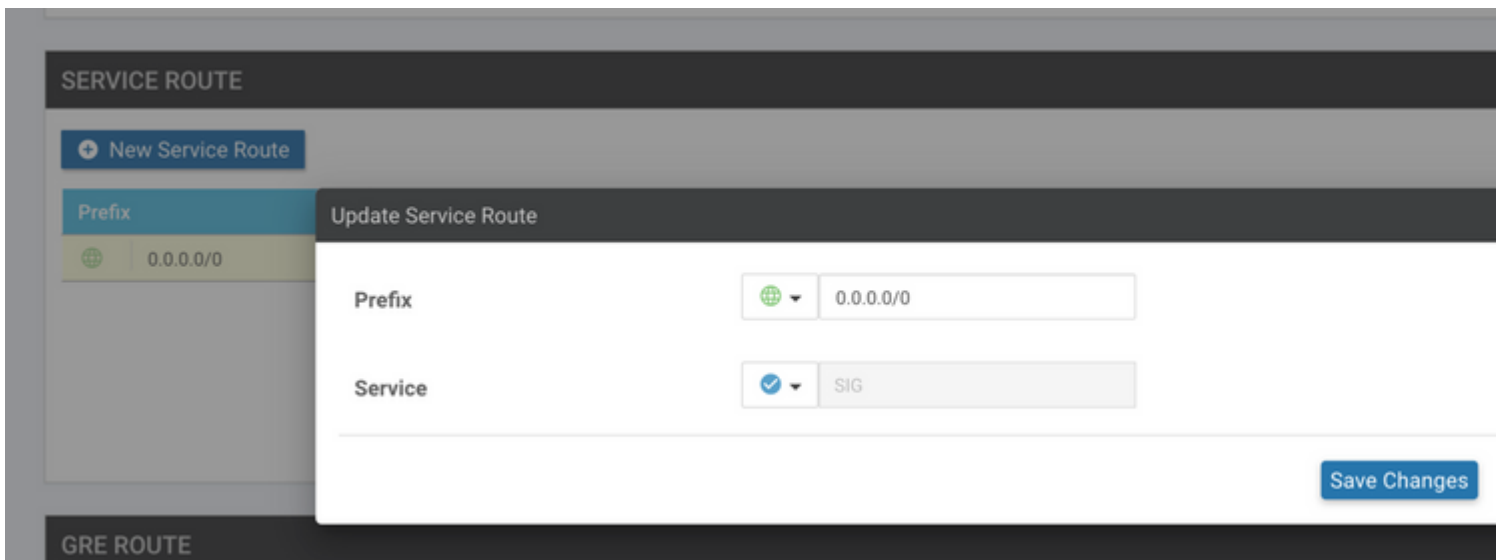
High Availability

	Active	Active Weight	Backup
Pair-1	ipsec1	1	ipsec2

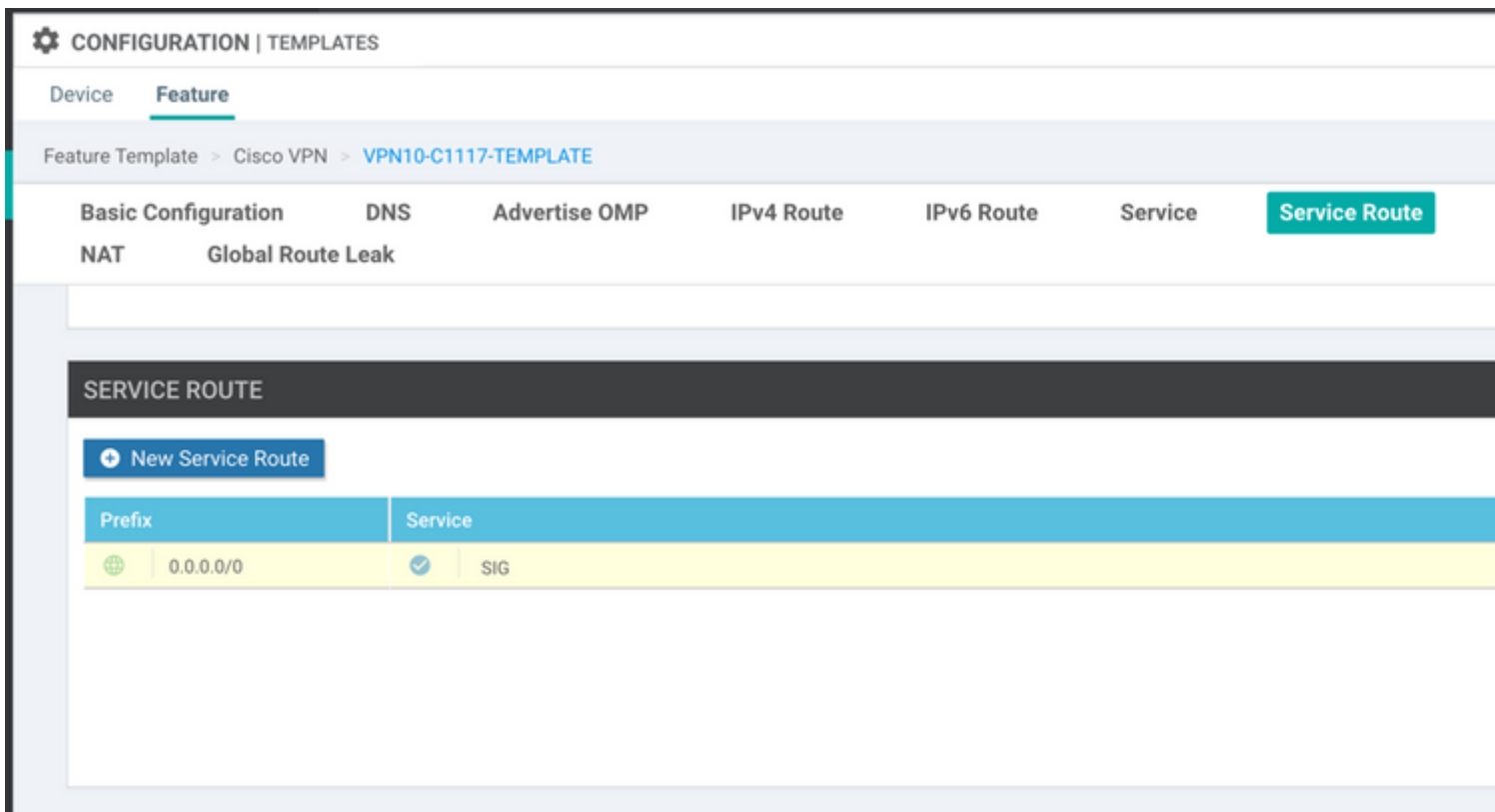
Opmerking: Tot 4 hoge beschikbaarheid tunnelparen en een maximum van 4 actieve tunnels kunnen tegelijkertijd gecreëerd worden.

Stap 6. Bewerk de servicekant VPN-sjabloon om een servicroute te injecteren.

Navigeer naar het gedeelte **Service VPN** en navigeer binnen de servicesjabloon naar het gedeelte **Service Route** en voeg een **0.0.0.0** met **SIG**-serviceroute toe. Voor dit document wordt VRF/VPN 10 gebruikt.



De route **0.0.0.0 SIG** wordt weergegeven zoals hier wordt weergegeven.



Opmerking: om ervoor te zorgen dat het serviceverkeer daadwerkelijk uitgaat, moet NAT worden geconfigureerd in de WAN-interface.

Hang deze sjabloon aan het apparaat en druk op de configuratie:

TASK VIEW

Push Feature Template Configuration | ✔ Validation Success ▾

Total Task: 1 | In Progress : 1

Search Options ▾

Status	Message	Chassis Number	Device Model	Hostname	System IP
In progress	Pushing configuration t...	C1117-4PWE-FGL2149...	C1117-4PW*	C1117-4PWE-FGL2149...	10.10.10.10

```

[19-Jul-2021 14:05:03 UTC] Configuring device with feature template: C1117-4PW-Original-Template
[19-Jul-2021 14:05:03 UTC] Generating configuration from template
[19-Jul-2021 14:05:03 UTC] Checking and creating device in vManage
[19-Jul-2021 14:05:04 UTC] Device is online
[19-Jul-2021 14:05:04 UTC] Updating device configuration in vManage
[19-Jul-2021 14:05:10 UTC] Pushing configuration to device.

```

WAN Edge-routerconfiguratie voor actief/back-upscenario

```

system
  host-name <HOSTNAME>
  system-ip <SYSTEM-IP>
  overlay-id 1
  site-id <SITE-ID>
  sp-organization-name <ORG-NAME>
  organization-name <SP-ORG-NAME>
  vbond <VBOND-IP> port 12346
!
secure-internet-gateway
  umbrella org-id <UMBRELLA-ORG-ID>
  umbrella api-key <UMBRELLA-API-KEY-INFO>
  umbrella api-secret <UMBRELLA-SECRET-INFO>
!
sdwan
  service sig vrf global
  ha-pairs
    interface-pair Tunnel100001 active-interface-weight 1 Tunnel100002 backup-interface-weight 1
  !
!
interface GigabitEthernet0/0/0
  tunnel-interface
  encapsulation ipsec weight 1
  no border
  color biz-internet
  no last-resort-circuit
  no low-bandwidth-link
  no vbond-as-stun-server
  vmanage-connection-preference 5
  port-hop
  carrier default
  nat-refresh-interval 5
  hello-interval 1000

```

```
hello-tolerance          12
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
interface Tunnel100001
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-in
exit
interface Tunnel100002
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference secondary-dc source-
exit
appqoe
 no tcpopt enable
!
security
 ipsec
  rekey          86400
  replay-window  512
  authentication-type sha1-hmac ah-sha1-hmac
!
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname <DEVICE-HOSTNAME>
username admin privilege 15 secret 9 <SECRET-PASSWORD>
vrf definition 10
 rd 1:10
  address-family ipv4
   route-target export 1:10
   route-target import 1:10
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
!
vrf definition Mgmt-intf
 description Transport VPN
 rd      1:512
  address-family ipv4
   route-target export 1:512
   route-target import 1:512
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
!
ip sdwan route vrf 10 0.0.0.0/0 service sig
```

```
no ip http server
no ip http secure-server
no ip http ctc authentication
ip nat settings central-policy
vlan 10
exit
interface GigabitEthernet0/0/0
  no shutdown
  arp timeout 1200
  ip address dhcp client-id GigabitEthernet0/0/0
  no ip redirects
  ip dhcp client default-router distance 1
  ip mtu 1500
  load-interval 30
  mtu 1500
exit
interface GigabitEthernet0/1/0
  switchport access vlan 10
  switchport mode access
  no shutdown
exit
interface GigabitEthernet0/1/1
  switchport mode access
  no shutdown
exit
interface Vlan10
  no shutdown
  arp timeout 1200
  vrf forwarding 10
  ip address <VLAN-IP-ADDRESS> <MASK>
  ip mtu 1500
  ip nbar protocol-discovery
exit
interface Tunnel0
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  no ip redirects
  ipv6 unnumbered GigabitEthernet0/0/0
  no ipv6 redirects
  tunnel source GigabitEthernet0/0/0
  tunnel mode sdwan
exit
interface Tunnel100001
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  ip mtu 1400
  tunnel source GigabitEthernet0/0/0
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec1-ipsec-profile
  tunnel vrf multiplexing
exit
interface Tunnel100002
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  ip mtu 1400
  tunnel source GigabitEthernet0/0/0
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec2-ipsec-profile
  tunnel vrf multiplexing
exit
```

```

clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
logging console
no logging rate-limit
aaa authentication log in default local
aaa authorization exec default local
aaa session-id common
mac address-table aging-time 300
no crypto ikev2 diagnose error
crypto ikev2 policy policy1-global
  proposal p1-global
!
crypto ikev2 profile if-ipsec1-ikev2-profile
  no config-exchange request
  dpd 10 3 on-demand
  dynamic
  lifetime 86400
!
crypto ikev2 profile if-ipsec2-ikev2-profile
  no config-exchange request
  dpd 10 3 on-demand
  dynamic
  lifetime 86400
!
crypto ikev2 proposal p1-global
  encryption aes-cbc-128 aes-cbc-256
  group 14 15 16
  integrity sha1 sha256 sha384 sha512
!
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
  mode tunnel
!
crypto ipsec transform-set if-ipsec2-ikev2-transform esp-gcm 256
  mode tunnel
!
crypto ipsec profile if-ipsec1-ipsec-profile
  set ikev2-profile if-ipsec1-ikev2-profile
  set transform-set if-ipsec1-ikev2-transform
  set security-association lifetime kilobytes disable
  set security-association lifetime seconds 3600
  set security-association replay window-size 512
!
crypto ipsec profile if-ipsec2-ipsec-profile
  set ikev2-profile if-ipsec2-ikev2-profile
  set transform-set if-ipsec2-ikev2-transform
  set security-association lifetime kilobytes disable
  set security-association lifetime seconds 3600
  set security-association replay window-size 512
!
no crypto isakmp diagnose error
no network-clock revertive

```

Umbrella SIG-tunnels met actief/actief scenario maken

Stap 1. Maak een SIG Credentials functiesjabloon.

Navigeer naar de functiesjabloon en klik op **Bewerken**.

C1117...	C1117-4PW-Orig...	Feature	C1117-4PW*	15	0	admin	13 Jul 2021 9:29...
----------	-------------------	---------	------------	----	---	-------	---------------------

Selecteer in het gedeelte **Aanvullende sjablonen Cisco SIG Credentials**. De optie wordt in de afbeelding weergegeven.

Additional Templates

Global Template *	Factory_Default_Global_CISCO_Template	1
Cisco Banner	Choose...	
Cisco SNMP	Choose...	
CLI Add-On Template	Choose...	
Policy	app-flow-visibility	
Probes	Choose...	
Security Policy	Choose...	
Cisco SIG Credentials *	SIG-Credentials	

Geef een naam en beschrijving aan de sjabloon.

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco SIG Credentials > **SIG-Credentials**

Device Type C1117-4PW*

Template Name SIG-Credentials

Description SIG-Credentials

Basic Details

SIG Provider Umbrella

Organization ID

Registration Key

Secret

Get Keys

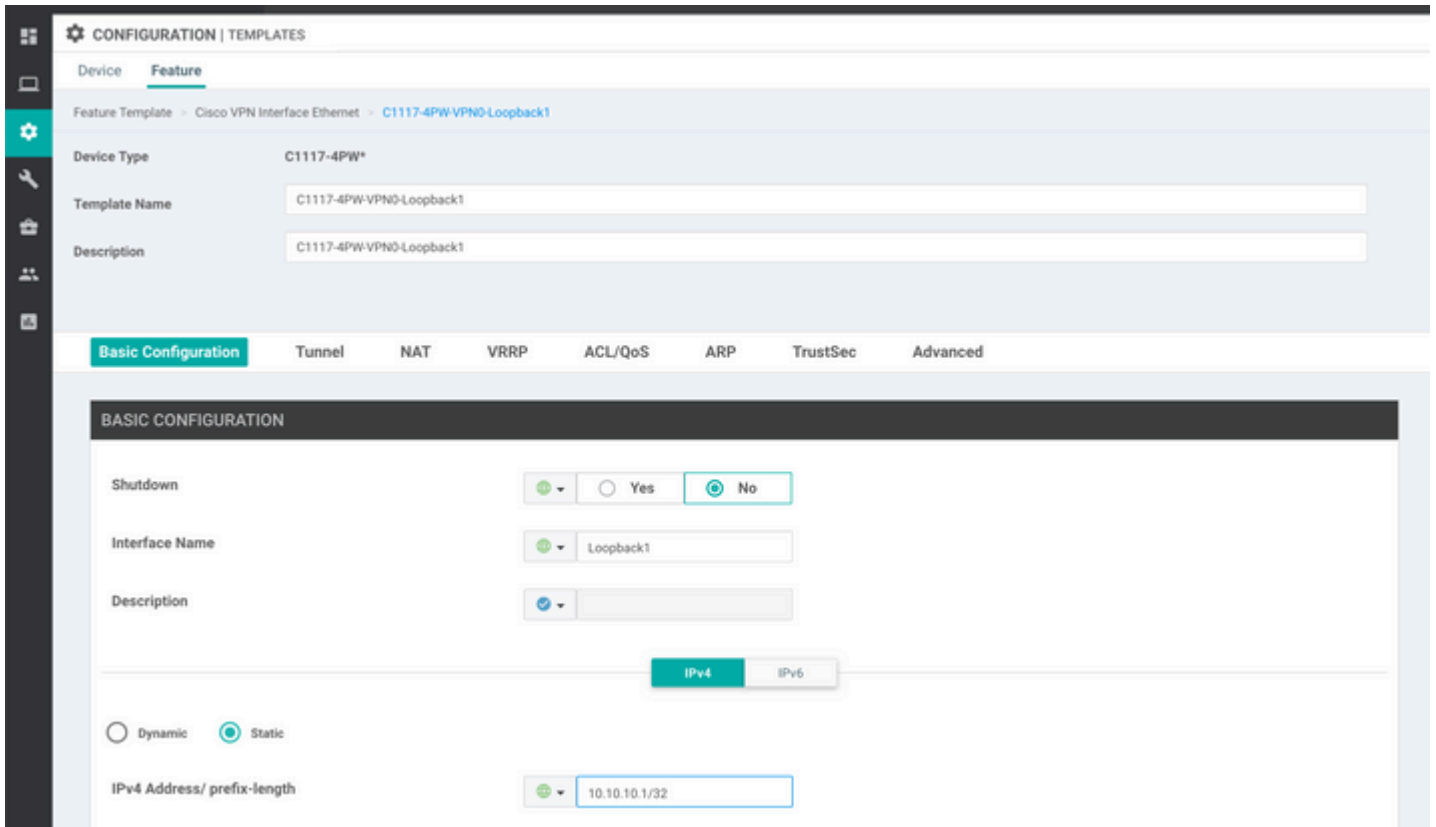
Stap 2. Maak twee Loopback-interfaces om de SIG-tunnels te koppelen.

Opmerking: Maak een Loopback-interface voor elke SIG-tunnel in actieve modus, dit is nodig omdat elke tunnel een unieke IKE-id nodig heeft.

Opmerking: dit scenario is actief/actief, daarom worden twee Loopbacks gemaakt.

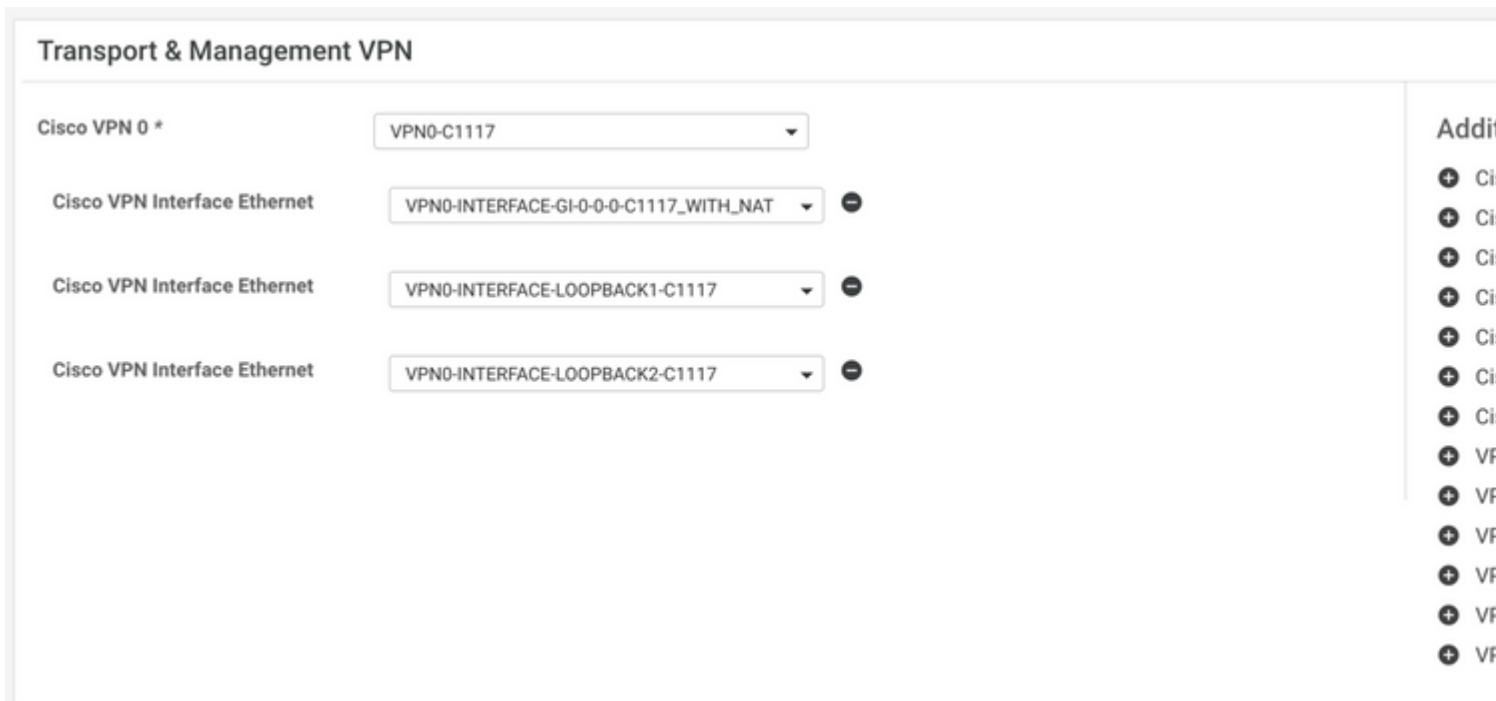
Configureer de interfacenaam en IPv4-adres voor de terugkoppeling.

Opmerking: het IP-adres dat voor de loopback is ingesteld, is een dummy-adres.



â€f

Maak de tweede Loopback-sjabloon en voeg deze aan de apparaatsjabloon toe. De apparaatsjabloon moet twee Loopback-sjablonen hebben toegevoegd:



Stap 3. Maak een SIG-functiesjabloon.

Navigeer naar de SIG-functiesjabloon en selecteer onder de sectie **Transport & Management VPN** de functiesjabloon voor **Cisco Secure Internet Gateway**.

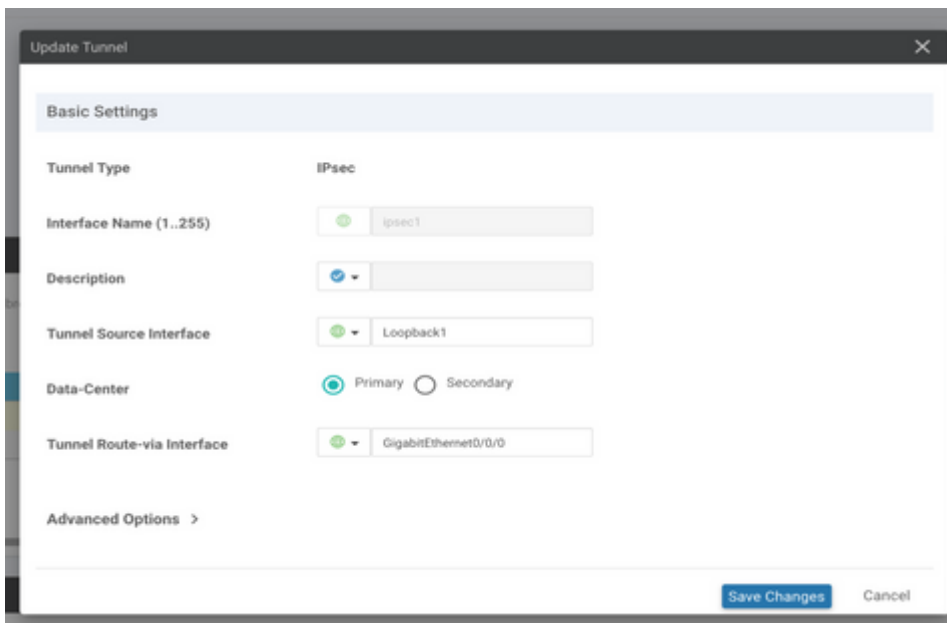
Stap 4. Selecteer de SIG-provider voor de primaire tunnel.

Klik op **Tunnel toevoegen**.



Configureer de basisgegevens en houd het **datacenter** als **primair**.

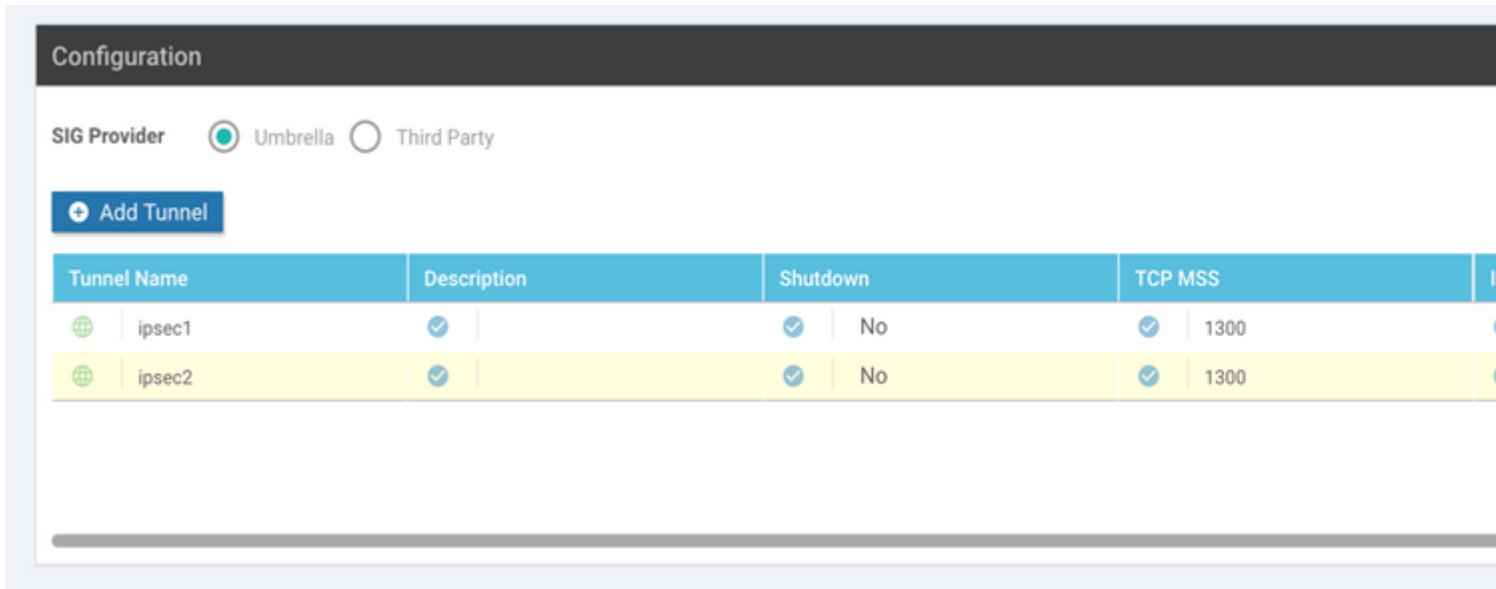
Opmerking: de bron-interfaceparameter voor tunnels is de Loopback (voor dit document Loopback1) en als router-via-interface voor tunnels de fysieke interface (voor dit document Gigabit Ethernet0/0/0)



Stap 5. Voeg de secundaire tunnel toe.

Voeg een tweede tunnelconfiguratie toe, gebruik ook **Data-Center** als **Primair**, en de interfacenaam als *ipsec2*.

vManager-configuratie wordt weergegeven zoals hier wordt getoond:

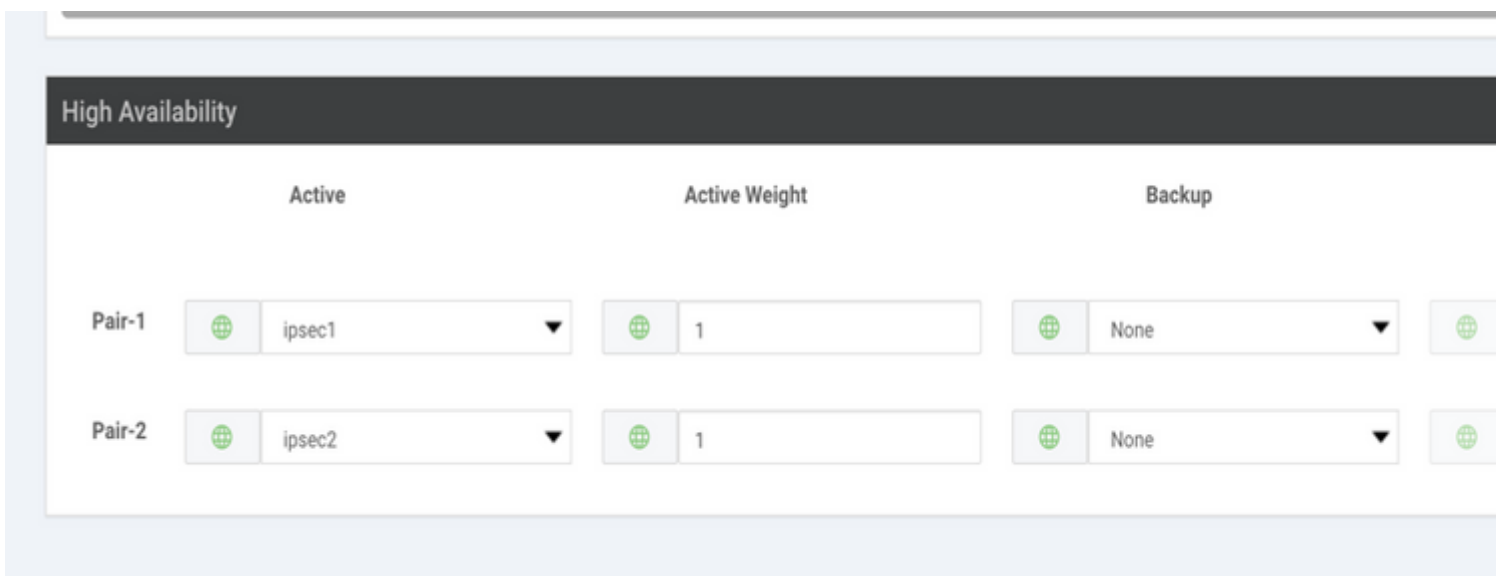


Stap 6. Maak twee paren met hoge beschikbaarheid.

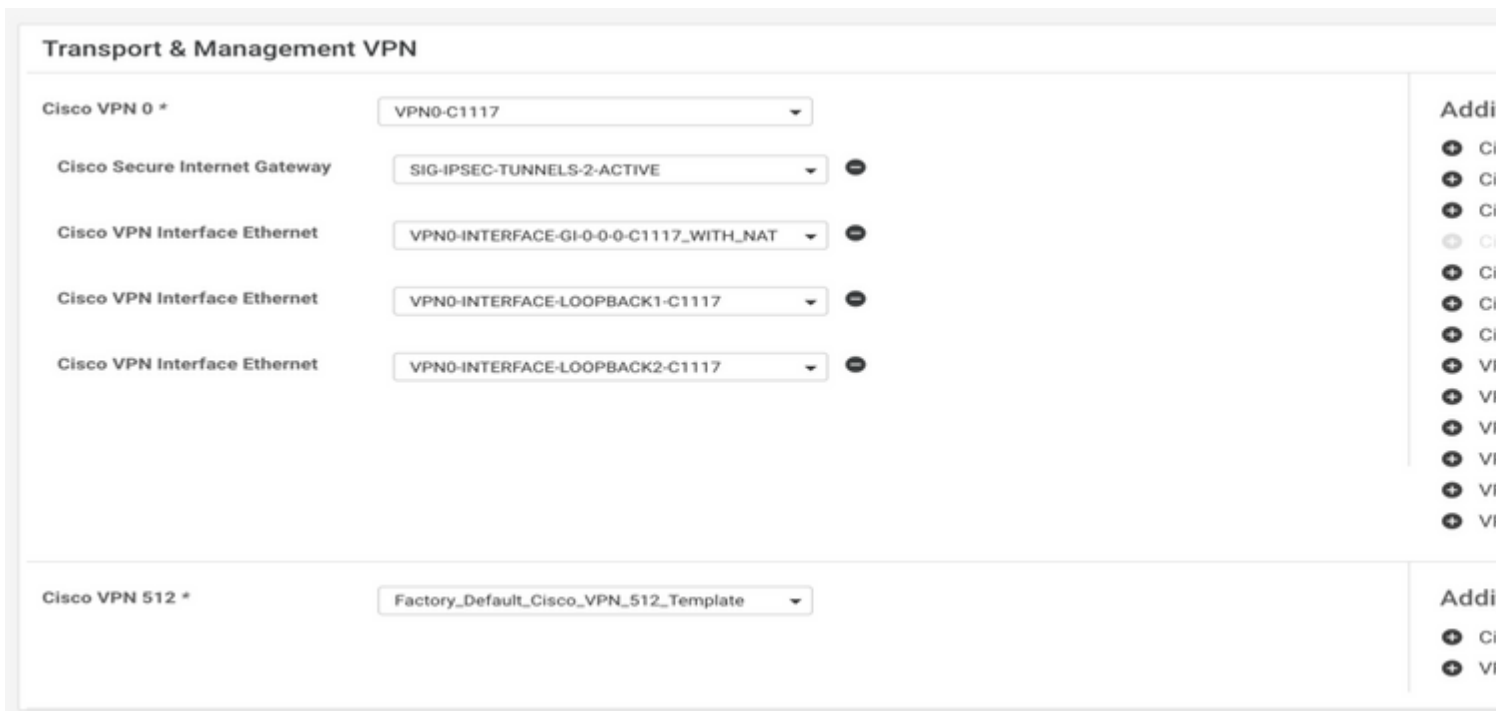
Voer in het gedeelte **Hoge beschikbaarheid** twee paren hoge beschikbaarheid in.

- Selecteer in het eerste HA-paar de ipsec1 als actief en selecteer **Geen** voor back-up.
- Selecteer in het tweede HA-paar de ipsec2 als actief **Geen** en voor back-up.

De vManager-configuratie voor hoge beschikbaarheid wordt weergegeven zoals aangegeven:

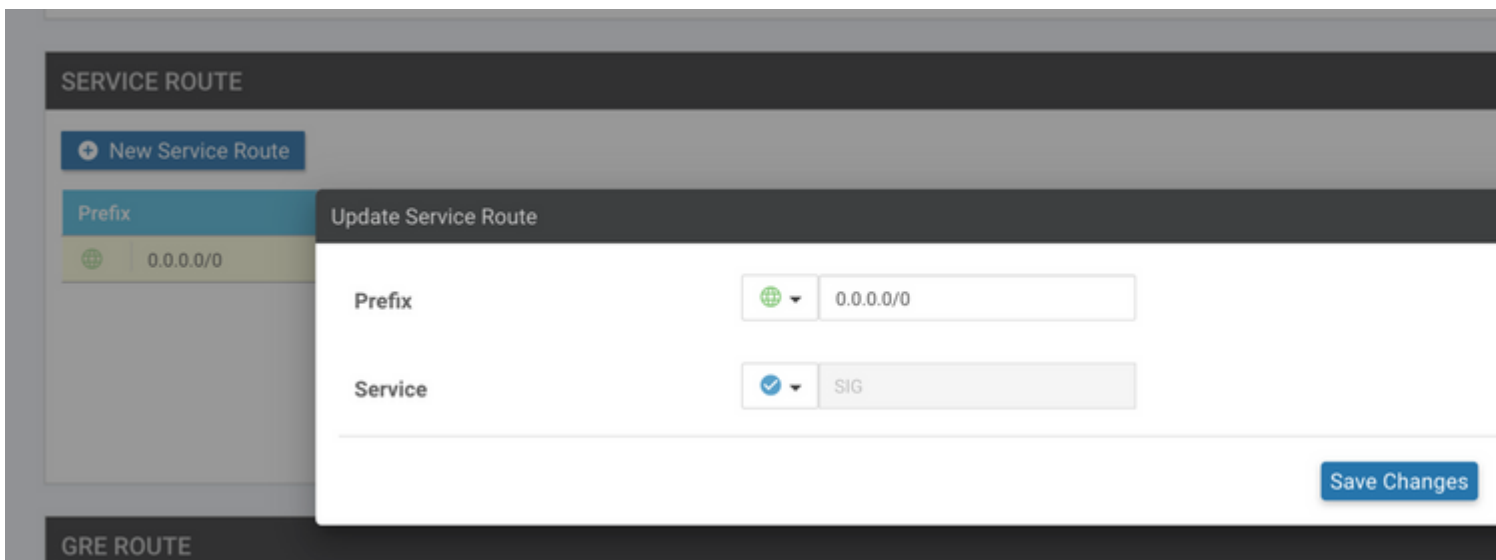


De apparaatsjabloon heeft de twee Loopback-sjablonen en de SIG-functiemaljabloon eveneens toegevoegd.



Stap 7. Bewerk de servicekant VPN-sjabloon om een servicroute te injecteren.

Navigeer naar de sectie **Service VPN** en navigeer binnen de VPN van servicesjabloon naar de sectie **Service Route** en voeg een **0.0.0.0** met **SIG**-servicroute toe.



De route 0.0.0.0 SIG wordt weergegeven zoals hier.

Opmerking: om ervoor te zorgen dat het serviceverkeer daadwerkelijk uitgaat, moet NAT worden geconfigureerd in de WAN-interface.

Hang deze sjabloon aan het apparaat en druk op de configuratie.

WAN Edge-routerconfiguratie voor actief/actief scenario

```
system
 host-name <HOSTNAME>
 system-ip <SYSTEM-IP>
 overlay-id 1
 site-id <SITE-ID>
 sp-organization-name <ORG-NAME>
 organization-name <SP-ORG-NAME>
 vbond <VBOND-IP> port 12346
!
secure-internet-gateway
 umbrella org-id <UMBRELLA-ORG-ID>
 umbrella api-key <UMBRELLA-API-KEY-INFO>
 umbrella api-secret <UMBRELLA-SECRET-INFO>
!
sdwan
 service sig vrf global
  ha-pairs
   interface-pair Tunnel100001 active-interface-weight 1 None backup-interface-weight 1
   interface-pair Tunnel100002 active-interface-weight 1 None backup-interface-weight 1
!
interface GigabitEthernet0/0/0
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color biz-internet
  no last-resort-circuit
  no low-bandwidth-link
  no vbond-as-stun-server
  vmanage-connection-preference 5
  port-hop
  carrier default
  nat-refresh-interval 5
  hello-interval 1000
  hello-tolerance 12
  allow-service all
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  no allow-service snmp
  no allow-service bfd
 exit
exit
interface Tunnel100001
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-inter
 exit
interface Tunnel100002
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-inter
 exit
exit
appqoe
no tcpopt enable
!
security
 ipsec
 rekey 86400
 replay-window 512
```

```
authentication-type sha1-hmac ah-sha1-hmac
!
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname <DEVICE HOSTNAME>
username admin privilege 15 secret 9 <secret-password>
vrf definition 10
  rd 1:10
  address-family ipv4
  route-target export 1:10
  route-target import 1:10
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
!
vrf definition Mgmt-intf
  description Transport VPN
  rd 1:512
  address-family ipv4
  route-target export 1:512
  route-target import 1:512
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
no ip source-route
ip sdwan route vrf 10 0.0.0.0/0 service sig
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
ip nat settings central-policy
vlan 10
exit
interface GigabitEthernet0/0/0
  no shutdown
  arp timeout 1200
  ip address dhcp client-id GigabitEthernet0/0/0
  no ip redirects
  ip dhcp client default-router distance 1
  ip mtu 1500
  ip nat outside
  load-interval 30
  mtu 1500
exit
interface GigabitEthernet0/1/0
  switchport access vlan 10
  switchport mode access
  no shutdown
  exit
interface Loopback1
  no shutdown
  arp timeout 1200
  ip address 10.20.20.1 255.255.255.255
  ip mtu 1500
  exit
interface Loopback2
```

```
no shutdown
arp timeout 1200
ip address 10.10.10.1 255.255.255.255
ip mtu 1500
exit
interface Vlan10
no shutdown
arp timeout 1200
vrf forwarding 10
ip address 10.1.1.1 255.255.255.252
ip mtu 1500
ip nbar protocol-discovery
exit
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0
no ip redirects
ipv6 unnumbered GigabitEthernet0/0/0
no ipv6 redirects
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
interface Tunnel100001
no shutdown
ip unnumbered Loopback1
ip mtu 1400
tunnel source Loopback1
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec1-ipsec-profile
tunnel vrf multiplexing
tunnel route-via GigabitEthernet0/0/0 mandatory
exit
interface Tunnel100002
no shutdown
ip unnumbered Loopback2
ip mtu 1400
tunnel source Loopback2
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec2-ipsec-profile
tunnel vrf multiplexing
tunnel route-via GigabitEthernet0/0/0 mandatory
exit
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
logging console
no logging rate-limit
aaa authentication log in default local
aaa authorization exec default local
aaa session-id common
mac address-table aging-time 300
no crypto ikev2 diagnose error
crypto ikev2 policy policy1-global
proposal p1-global
!
crypto ikev2 profile if-ipsec1-ikev2-profile
no config-exchange request
dpd 10 3 on-demand
dynamic
lifetime 86400
```

```
!  
crypto ikev2 profile if-ipsec2-ikev2-profile  
  no config-exchange request  
  dpd 10 3 on-demand  
  dynamic  
  lifetime 86400  
!  
crypto ikev2 proposal p1-global  
  encryption aes-cbc-128 aes-cbc-256  
  group 14 15 16  
  integrity sha1 sha256 sha384 sha512  
!  
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256  
  mode tunnel  
!  
crypto ipsec transform-set if-ipsec2-ikev2-transform esp-gcm 256  
  mode tunnel  
!  
crypto ipsec profile if-ipsec1-ipsec-profile  
  set ikev2-profile if-ipsec1-ikev2-profile  
  set transform-set if-ipsec1-ikev2-transform  
  set security-association lifetime kilobytes disable  
  set security-association lifetime seconds 3600  
  set security-association replay window-size 512  
!  
crypto ipsec profile if-ipsec2-ipsec-profile  
  set ikev2-profile if-ipsec2-ikev2-profile  
  set transform-set if-ipsec2-ikev2-transform  
  set security-association lifetime kilobytes disable  
  set security-association lifetime seconds 3600  
  set security-association replay window-size 512  
!
```

Opmerking: Hoewel dit document **Umbrella** focus is, zijn dezelfde scenario's van toepassing op Azure en SIG-tunnels van derden.

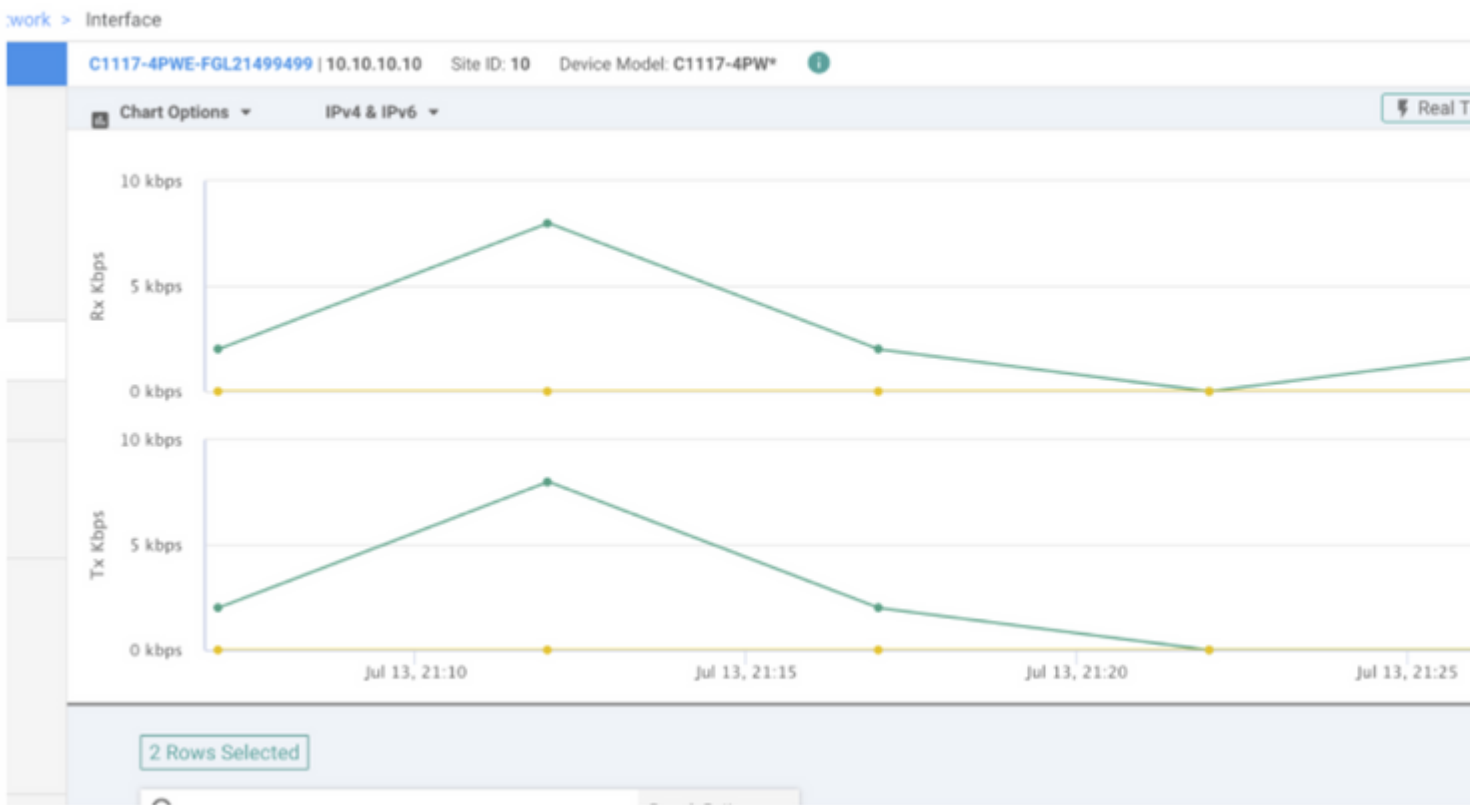
Verifiëren

Controleer het actieve/back-upscenario

In vManager is het mogelijk om de status van de SIG IPSec-tunnels te bewaken. Navigeer naar **Monitor > Network en** selecteer het gewenste WAN-randapparaat.

Klik links op het tabblad **Interfaces**; er wordt een lijst weergegeven van alle interfaces in het apparaat. Dit omvat de interfaces ipsec1 en ipsec2.

Het beeld toont aan dat de ipsec1 tunnel al het verkeer door:sturen en ipsec2 gaat geen verkeer over.



Het is ook mogelijk om de tunnels op het Cisco **Umbrella** portal te verifiëren zoals aangegeven in de afbeelding.

Cisco Umbrella

Overview

Deployments

- Core Identities
- Networks
- Network Devices
- Roaming Computers
- Mobile Devices
- Chromebook Users
- Network Tunnels**
- Users and Groups
- Configuration
 - Domain Management
 - Sites and Active Directory
 - Internal Networks
 - Root Certificate
 - SAML Configuration
 - Service Account Exceptions

Deployments / Core Identities

Network Tunnels

To create a tunnel, you must choose a Tunnel ID and Passphrase. A unique set of credentials must be used for each tunnel. For more information, see the documentation.

Active Tunnels: 2

Inactive Tunnels: 0

Unestablished Tunnels: 0

Data Center Locations: 2

FILTERS Search with a tunnel name

2 Total

Tunnel Name	Device Type	Tunnel Status	Tunnel ID	Data Center Location	Device Public
SIT [REDACTED]	Viptela cEdge	Active	et [REDACTED]		
SIT [REDACTED]	Viptela cEdge	Active	fd [REDACTED]		

Gebruik de opdracht **show sdwan secure-internet-gateway tunnels** op de CLI om de tunnelinformatie weer te geven.

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
```

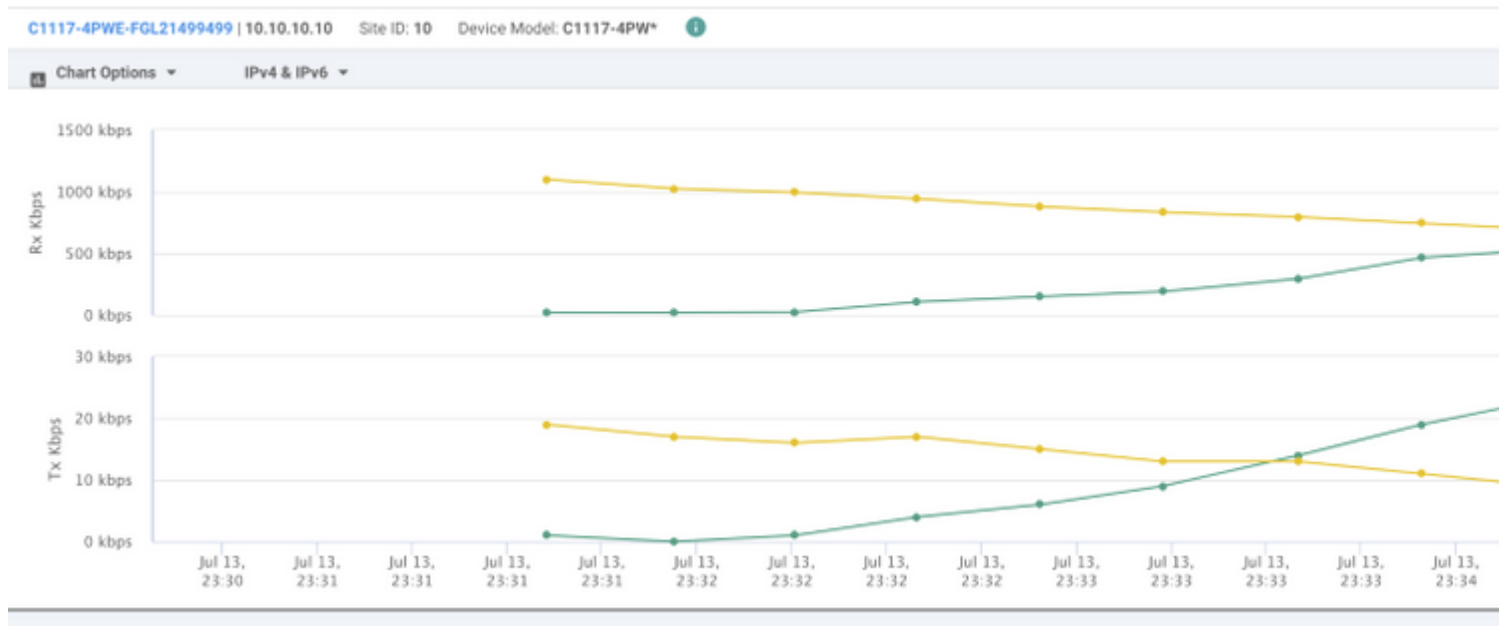
TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	540798313	SITE10SYS10x10x10x10IFTunnel100001	st-tun-create-notif	200	create-tunnel
Tunnel100002	540798314	SITE10SYS10x10x10x10IFTunnel100002	st-tun-create-notif	200	create-tunnel

Controleer actief/actief scenario

In de vManager is het mogelijk om de status van de SIG IPsec-tunnels te bewaken. Navigeer naar **Monitor > Network en** selecteer het gewenste WAN-randapparaat.

Klik op het tabblad **Interfaces** aan de linkerkant - en er wordt een lijst weergegeven van alle interfaces in het apparaat. Dit omvat de interfaces ipsec1 en ipsec2.

Het beeld toont aan dat zowel ipsec1 als ipsec2 voorwaarts verkeer tunnelt.



Gebruik de opdracht **show sdwan secure-internet-gateway tunnels** op de CLI om de tunnelinformatie weer te geven.

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
```

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	540798313	SITE10SYS10x10x10x10IFTunnel100001	st-tun-create-notif	200	create-tunnel
Tunnel100002	540798314	SITE10SYS10x10x10x10IFTunnel100002	st-tun-create-notif	200	create-tunnel

Gerelateerde informatie

- [Uw apparaten integreren met beveiligde internetgateways - Cisco IOS® XE release 17.x](#)
- [http://Network Tunnelconfiguratie - Umbrella SIG](#)
- [Paraplu aan de slag](#)
- [Technische ondersteuning en documentatie â€™ Cisco Systems](#)

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.