Configureer en controleer de SD-WAN IPsec SIG-tunnel met Zscaler

Inhoud

Inleiding

Dit document beschrijft de configuratie stappen en verificatie van SD-WAN IPsec SIG-tunnels met Zscaler.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Security Internet Gateway (SIG).
- Hoe IPsec-tunnels werken, fase1 en fase2 op Cisco IOS®.

Aanvullende vereisten

- NAT moet worden ingeschakeld op de transportinterface die zal worden geconfronteerd met het internet.
- Een DNS-server moet worden gemaakt op VPN 0, en de Zscaler basis URL moet worden opgelost met deze DNS server. Dit is belangrijk, want als dit niet oplost, zullen API-oproepen falen. Layer 7 health checks gaat ook falen, omdat de URL standaard is:

http://gateway.<zscalercloud>.net/vpntest.

- NTP (Network Time Protocol) moet ervoor zorgen dat de Cisco Edge-routertijd nauwkeurig is en dat API-oproepen niet zullen falen.
- Een serviceroute die naar SIG wijst, moet worden geconfigureerd in de Service-VPN-functiesjabloon of CLI:
  IP Sdwan route vrf 1 0.0.0.0/0 service sig

Gebruikte componenten

Dit document is gebaseerd op deze software- en hardwareversies:

- Cisco Edge-router versie 17.6.6a
- vManager versie 20.9.4

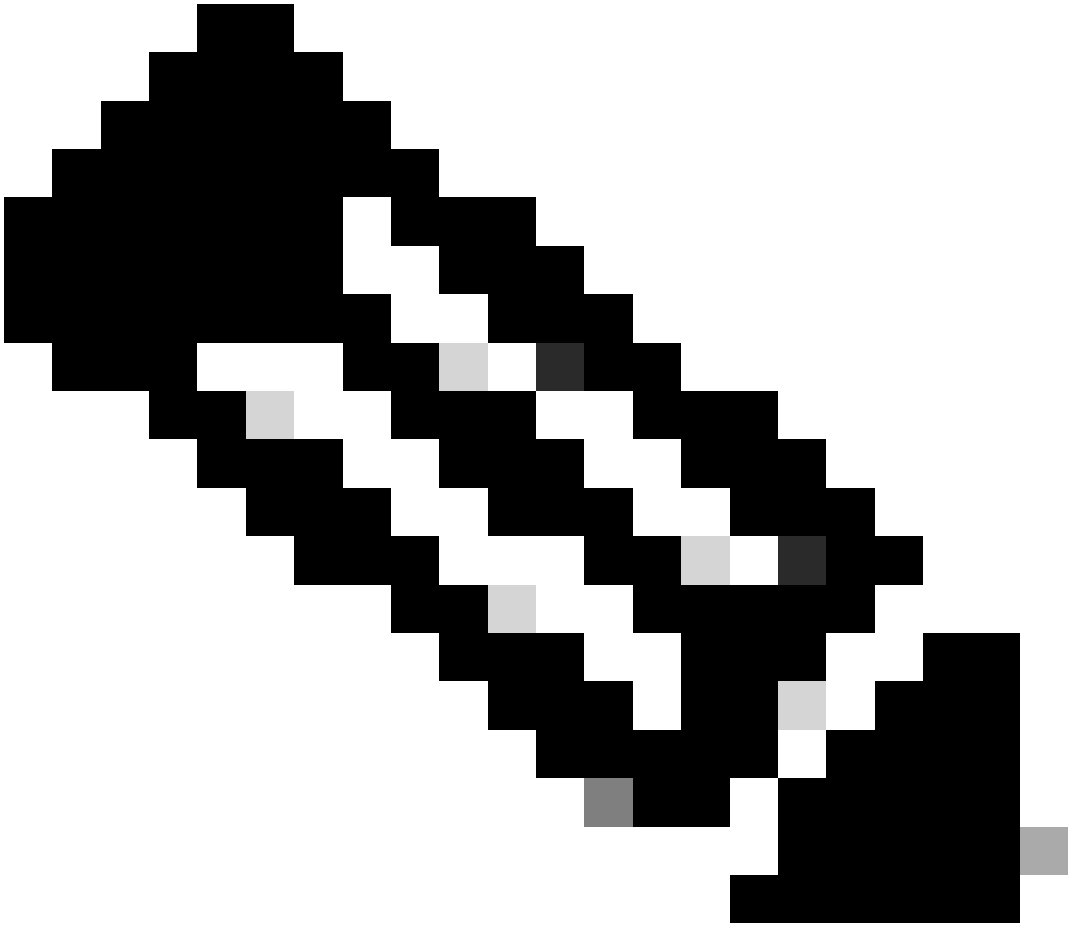
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Opties voor netwerkontwerp

Hier zijn de verschillende soorten implementaties in een active/stand-by combinatie-installatie. Tunnelinsluiting kan worden geïmplementeerd op GRE of IPsec.

- Eén actief/stand-by tunnelpaar.
- Eén actief/actief tunnelpaar.
- Meervoudige actieve/stand-by tunnelpaar.
- Meervoudige actieve/actieve tunnelpaar.



Opmerking: op SD-WAN Cisco Edge-routers kunt u een of meer transportinterfaces met internet gebruiken, zodat deze instellingen effectief functioneren.

Configuraties

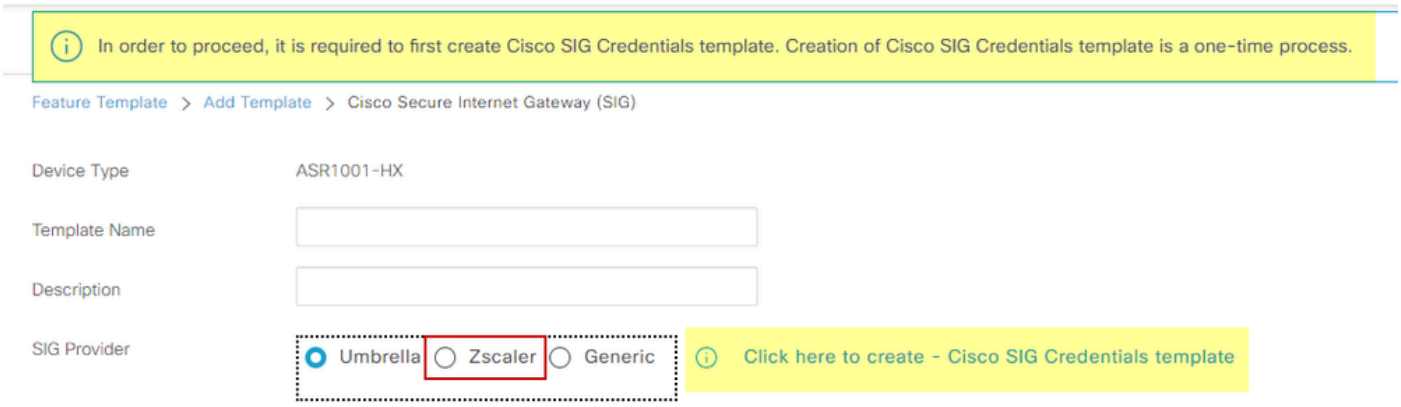
Ga verder met het configureren van deze sjablonen:

- Security Internet Gateway (SIG) Credentials functiesjabloon:
  - U hebt er één nodig voor alle Cisco Edge-routers. Op het Zscaler-portaal moet informatie worden gecreëerd om de nodige velden van de template in te vullen.
- Security Internet Gateway (SIG) functiesjabloon:
  - Onder deze functiesjabloon configureert u IPsec-tunnels, zorgt u voor implementatie met hoge beschikbaarheid (HA) in actieve/actieve of actieve/stand-by modus en selecteert u automatisch of handmatig Zscaler Datacenter.

Als u een Zscaler Credentials-sjabloon wilt maken, navigeer dan naar Configuratie > Sjabloon >

Functiesjabloon > Sjabloon toevoegen.

Selecteer het apparaatmodel dat u hiervoor gaat gebruiken en zoek naar SIG. Wanneer u het voor het eerst maakt, toont het systeem aan dat Zscaler Credentials eerst moet worden gemaakt, zoals in dit voorbeeld:
U moet Zscaler selecteren als SIG provider en klik op de Klik hier om te maken - Cisco SIG Credentials sjabloon.



Sjabloon voor beloning

"

U wordt doorgestuurd naar de Credentials sjabloon. In deze sjabloon moet u de waarden voor alle velden invoeren:

- Naam van template
- Beschrijving
- SIG-provider (automatisch geselecteerd uit de vorige stap)
- Organisatie
- URI met partnerbasis
- Username
- Wachtwoord
- API-sleutel voor partners

Klik op Save (Opslaan).

U wordt doorgestuurd naar de sjabloon Secure Internet Gateway (SIG). Met deze sjabloon kunt u alles configureren wat nodig is voor SD-WAN IPsec SIG met Zscaler.

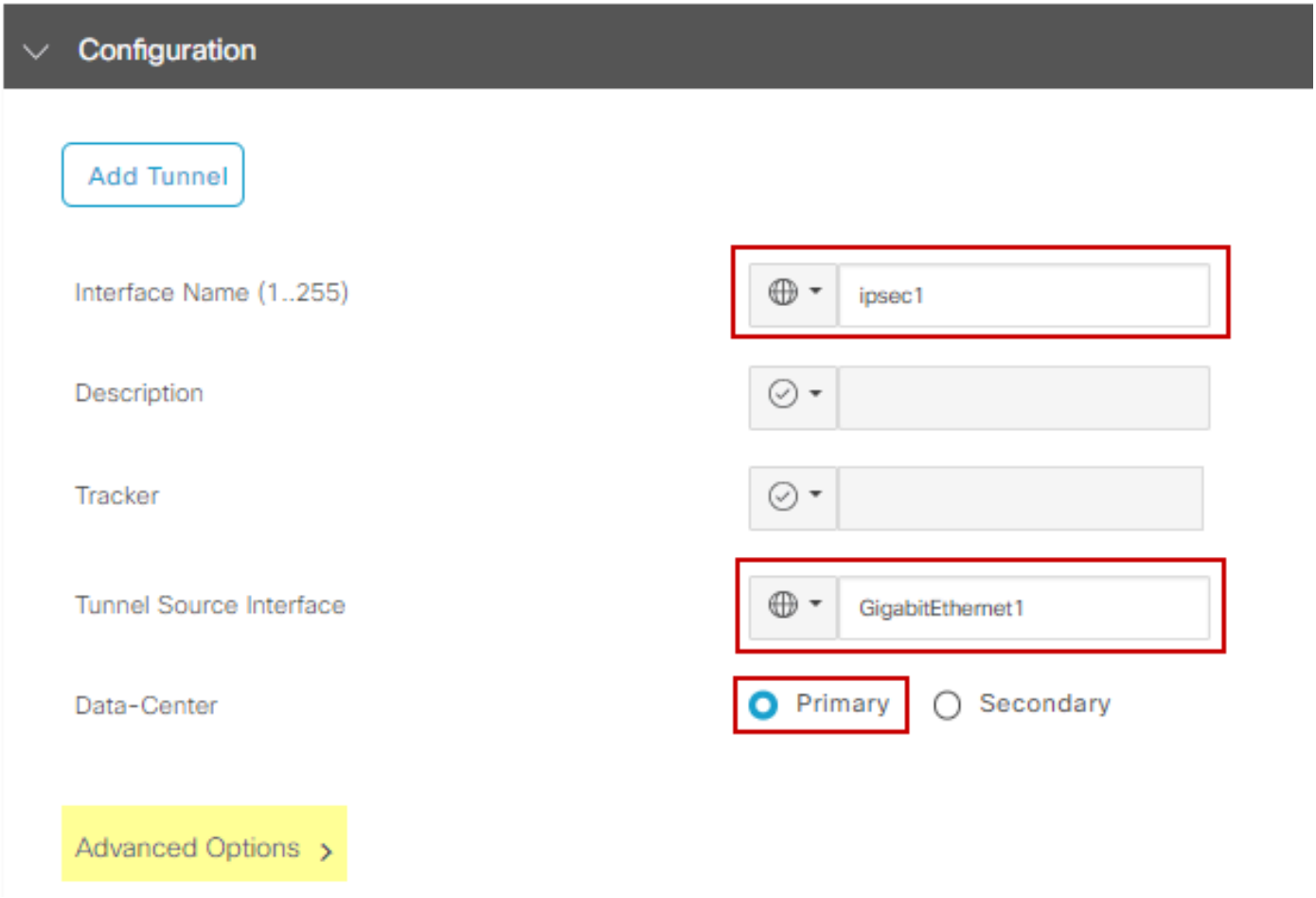
Geef in het eerste deel van de template een naam en een beschrijving. De standaard tracker wordt automatisch ingeschakeld. De API URL die gebruikt wordt voor de Zscaler Layer 7 health check is: zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest.

In Cisco IOS XE moet u een IP-adres voor de tracker instellen. Elke privé IP binnen het /32 bereik is acceptabel. Het IP-adres dat u instelt, kan worden gebruikt door de Loopback 65530 interface, die automatisch wordt gemaakt voor het uitvoeren van Zscaler-gezondheidsinspecties.

Onder Configuration kunt u de IPsec-tunnels maken door op Tunnel toevoegen te klikken. Maak in

het nieuwe pop-upvenster selecties op basis van uw vereisten.

In dit voorbeeld is IPsec1 gemaakt met behulp van WAN-interface Gigabit Ethernet1 als tunnelbron. Dan kan het verbinding maken met het Primary Zcaler Data-Center. Aanbevolen wordt de waarden van de geavanceerde opties als standaard te houden.

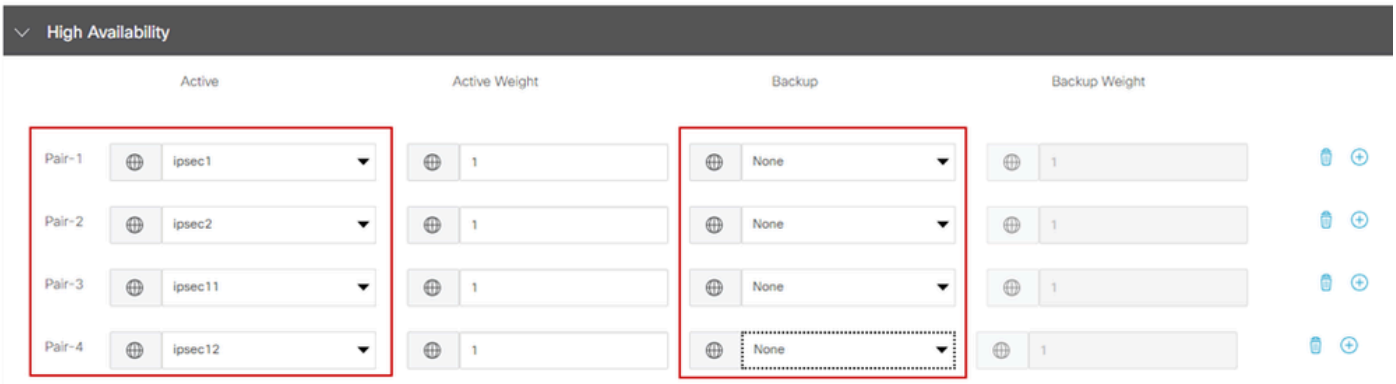


IPsec-interfaceconfiguratie

Hoge beschikbaarheid

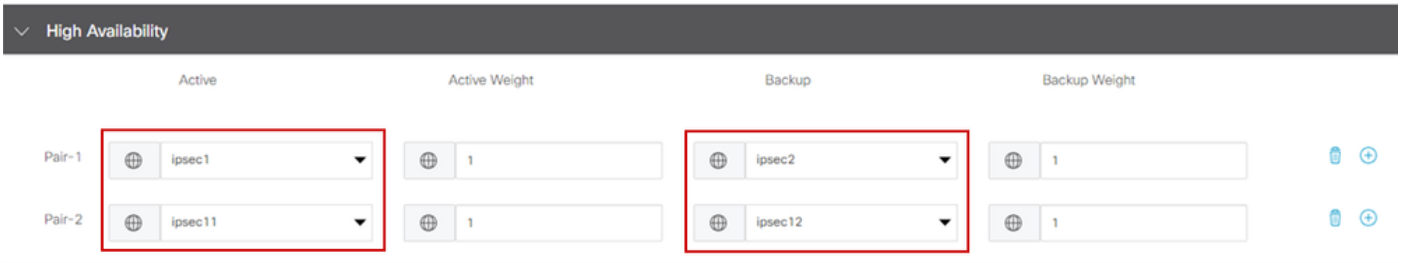
In deze sectie kiest u of het ontwerp actief/actief of actief/stand-by zal zijn en bepaalt u welke IPsec-interface actief zal zijn.

Dit is een voorbeeld van een Active/Active-ontwerp. Alle interfaces worden geselecteerd onder Actief, waarbij back-up zonder blijft.



Actief/actief ontwerp

In dit voorbeeld wordt een Active/Standby-ontwerp getoond. IPsec1 en IPsec1 worden als actieve interfaces geselecteerd, terwijl IPsec2 en IPsec12 worden aangewezen als standby interfaces.



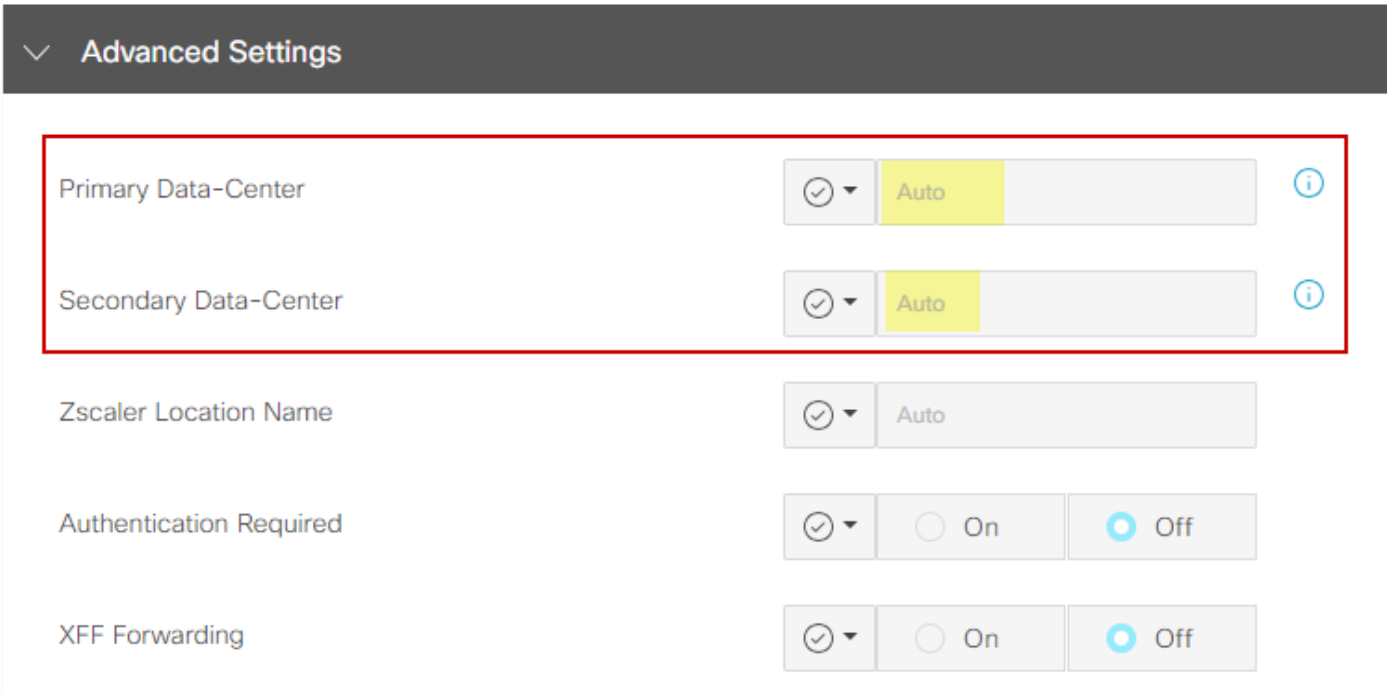
Active/Standby Design

Geavanceerde instellingen

In dit gedeelte zijn de belangrijkste configuraties het Primaire datacenter en het Secundaire datacenter.

Aanbevolen wordt om zowel automatisch als handmatig te configureren, maar het wordt niet aangeraden om ze als gemengd te configureren.

Als u ervoor kiest deze handmatig te configureren, selecteert u de juiste URL in het Zscaler-portal, gebaseerd op uw Partner Base URI



Automatisch of handmatig datacenter

Klik op Opslaan als u klaar bent.

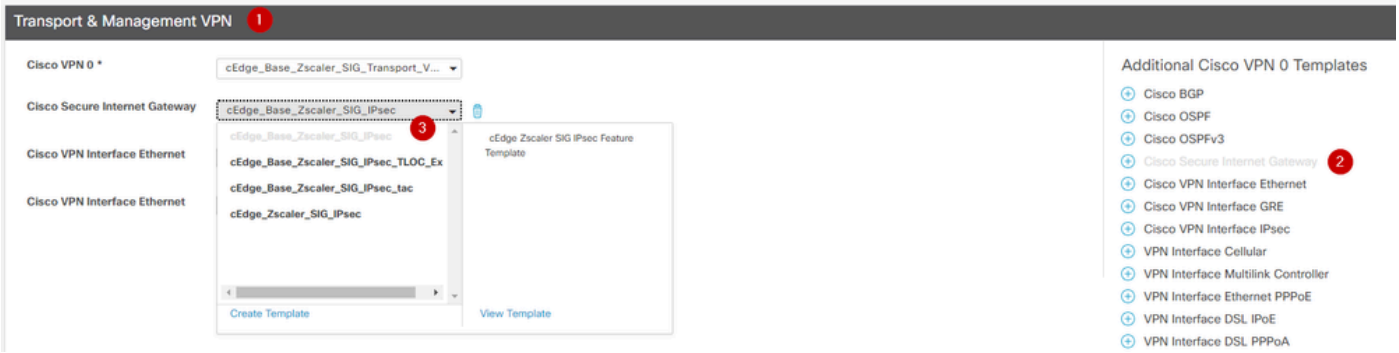
Zodra u klaar bent met de SIG-sjablonen configuratie moet u deze toepassen onder de apparaatsjabloon. Op deze manier wordt de configuratie naar de Cisco Edge-routers gedrukt.

Om deze stappen te voltooien navigeer naar Configuratie > Templates > Apparaatsjabloon, op drie punten klik Bewerken.

1. Onder Transport & Management VPN

2. Voeg Secure Internet Gateway-sjabloon toe.

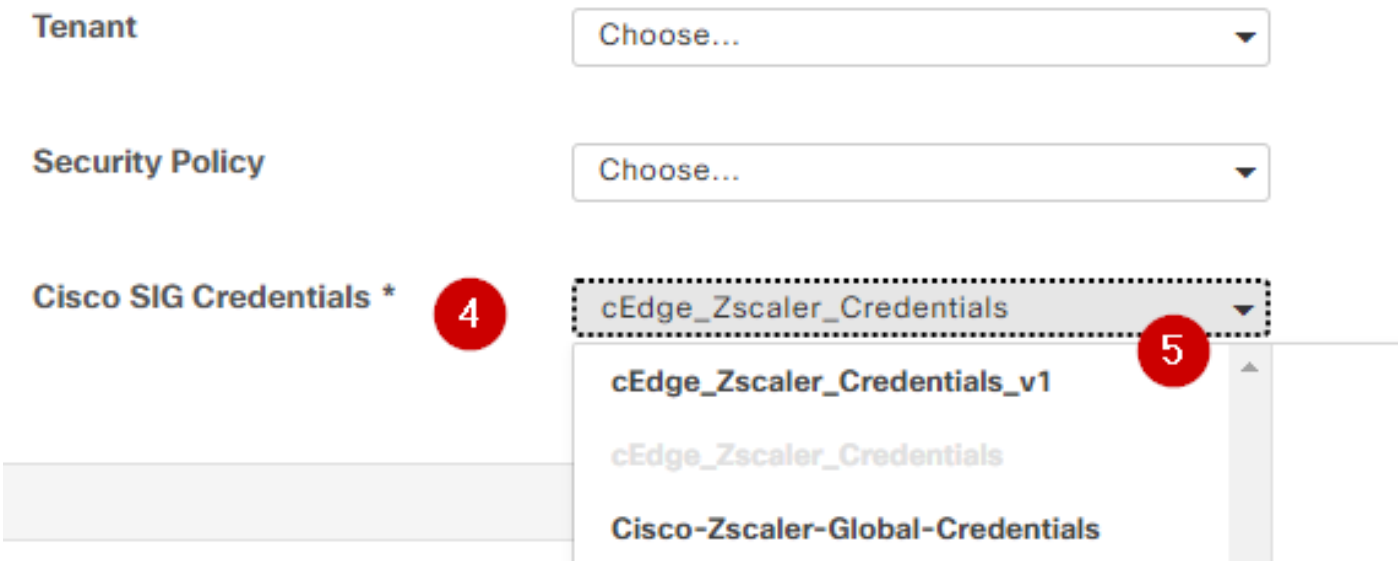
3. Selecteer op Cisco Secure Internet Gateway de juiste SIG-functiesjabloon in het keuzemenu.



SIG-sjabloon toevoegen op apparaatsjabloon

Onder Aanvullende sjablonen

4. In Cisco SIG-referenties
5. Selecteer de juiste Cisco SIG Credentials sjabloon in het vervolgkeuzemenu:



Credentials SIG-sjabloon

Klik op Update, let op als uw apparaatsjabloon een actieve sjabloon is. Gebruik de standaardstappen om configuraties op een actieve sjabloon te drukken.

Verifiëren

Verificatie kan worden uitgevoerd tijdens het configuratievoorbeeld terwijl u de wijzigingen drukt, wat u moet opmerken zijn:

```
secure-internet-gateway
     zscaler organization <removed>
     zscaler partner-base-uri <removed>
     zscaler partner-key <removed>
     zscaler username <removed>
     zscaler password <removed>
    !
```

Uit dit voorbeeld kunt u zien dat het ontwerp actief/stand-by is

<#root>

```
ha-pairs
  interface-pair

Tunnel100001 active

-interface-weight 1

Tunnel100002 backup

-interface-weight 1
  interface-pair
```

```
Tunnel100011 active

-interface-weight 1

Tunnel100012 backup

-interface-weight 1
```

U gaat merken meer configuraties worden toegevoegd zoals crypto ikev2 profielen en beleid, meerdere interface beginnend met Tunnel1xxxxx, vrf definitie 65530, ip sdwan route vrf 1 0.0.0.0/0 service sig.

Al deze wijzigingen maken deel uit van de IPsec SIG-tunnels met Zscaler.

Dit voorbeeld toont aan hoe de configuratie voor de tunnelinterface eruit ziet:

```
interface Tunnel100001
     no shutdown
     ip unnumbered       GigabitEthernet1
     no ip clear-dont-fragment
     ip mtu              1400
     tunnel source GigabitEthernet1
     tunnel destination dynamic
     tunnel mode ipsec ipv4
     tunnel protection ipsec profile if-ipsec1-ipsec-profile
     tunnel vrf multiplexing
```

Nadat configuraties met succes op de Cisco Edge-routers zijn gedrukt, kunt u opdrachten gebruiken om te controleren of de tunnels al dan niet worden gestart.

<#root>

```
Router#show sdwan secure-internet-gateway zscaler tunnels

HTTP

TUNNEL IF                                                TUNNEL

RESP

NAME          TUNNEL NAME                                ID        FQDN           TUNNEL FSM STATE

CODE

-------------------------------------------------------------------------------------------------------
Tunnel100001  site<removed>Tunnel100001             <removed>   <removed>     add-vpn-credential-info

200

Tunnel100002  site<removed>Tunnel100002              <removed>  <removed>     add-vpn-credential-info
```

200

Als u geen httpresp code 200 ziet, betekent dit dat u te maken hebt met een probleem met het wachtwoord of de partnersleutel.

Om de interfacestatus te verifiëren gebruik het bevel.

<#root>

Router#

show ip interface brief

```
Interface              IP-Address      OK? Method Status    Protocol
GigabitEthernet1       10.2.234.146    YES DHCP   up            up
GigabitEthernet2       10.2.58.221     YES other  up            up
GigabitEthernet3       10.2.20.77      YES other  up            up
GigabitEthernet4       10.2.248.43     YES other  up            up
Sdwan-system-intf      10.10.10.221    YES unset  up            up
Loopback65528          192.168.1.1     YES other  up            up
Loopback65530          192.168.0.2     YES other  up            up   <<< This is the IP that you used or
NVI0                   unassigned      YES unset  up            up
Tunnel2                10.2.58.221     YES TFTP   up            up
Tunnel3                10.2.20.77      YES TFTP   up            up
Tunnel100001           10.2.58.221     YES TFTP   up            up
Tunnel100002           10.2.58.221     YES TFTP   up            up
```

Om de status van de tracker te verifiëren, voert u de opdrachten tonen endpoint-tracker en toont u endpoint-tracker records. Dit helpt u de URL te bevestigen die de tracker gebruikt

```
Router#show endpoint-tracker
Interface              Record Name            Status          RTT in msecs    Probe ID        Next Hop
Tunnel100001           #SIGL7#AUTO#TRACKER    Up              194             44              None
Tunnel100002           #SIGL7#AUTO#TRACKER    Up              80              48              None
```

```
Router#show endpoint-tracker records
Record Name            Endpoint                              EndPoint Type   Threshold(ms)    Multiplier
#SIGL7#AUTO#TRACKER    http://gateway.<removed>.net/vpnt API_URL         1000            2
```

Andere validaties die u kunt doen zijn:
Om er zeker van te zijn dat de routes op VRF naar IPsec-tunnels wijzen, voert u deze opdracht uit:

toon ip route vrf 1

Gateway of last resort is 0.0.0.0 naar netwerk 0.0.0.0

S* 0.0.0.0/0 [2/65535], Tunnel100002
[2/65535], Tunnel100001
10.0.0.0/8 is variabel subnetted, 4 subnetten, 2 maskers

Om nog verder te valideren, kunt u pingen naar het internet en een traceroute doen om de hop die het verkeer neemt te controleren:

<#root>

```
Router#
```

ping vrf 1 cisco.com

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to <removed>, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 406/411/417 ms
```

<#root>

```
Router1#
```

traceroute vrf 1 cisco.com

```
Type escape sequence to abort.
Tracing the route to redirect-ns.cisco.com (<removed>)
VRF info: (vrf in name/id, vrf out name/id)
1 * * *
2
```

<The IP here need to be Zcaler IP>

```
 195 msec 193 msec 199 msec
3
```

<The IP here need to be Zcaler IP>

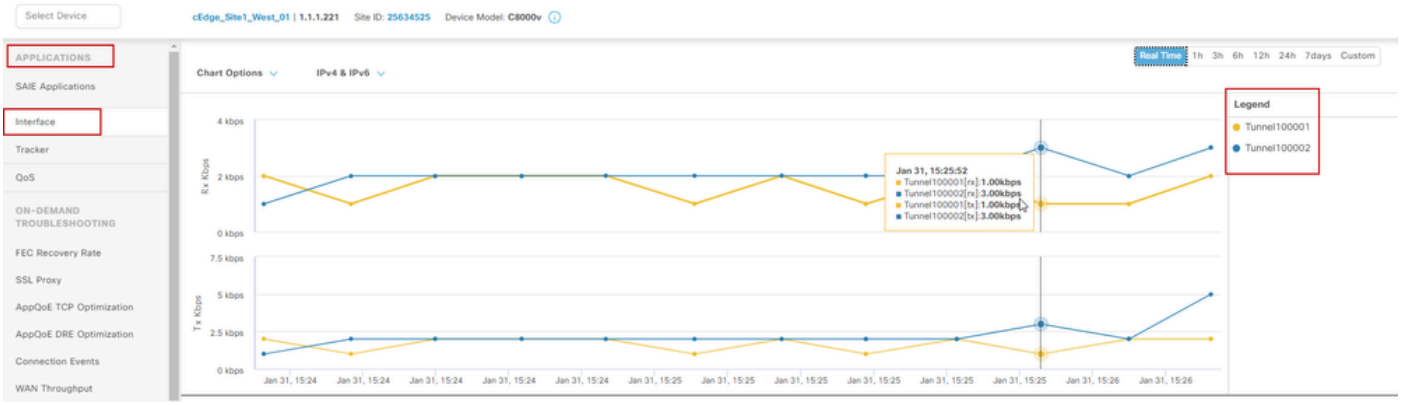
```
 200 msec
```

<The IP here need to be Zcaler IP>

```
 199 msec *
.....
```

U kunt IPsec-interfaces vanuit vManager GUI valideren door op Monitor > Apparaat of Monitor > Netwerk te navigeren (voor codes 20.6 en vroege versie).

- Selecteer uw router en navigeer Toepassingen > Interfaces.
- Selecteer Tunnel100001 en Tunnel100002 om het real-time verkeer te zien of pas per vereist tijdkader aan:



IPsec-tunnels voor bewaking

Problemen oplossen

Als de SIG-tunnel niet actief is, zijn hier de enkele stappen om het probleem op te lossen.

Stap 1: Controleer de fouten met behulp van de opdracht tonen sdwan beveiligde-internet-gateway zscaler tunnels. Vanuit de output, als u HTTP RESP Code 401 opmerkt, geeft het aan dat er een probleem is met verificatie.

U kunt de waarden in de SIG Credentials sjabloon controleren om te zien of het wachtwoord, of de Partnersleutel, juist is.

<#root>

Router#

show sdwan secure-internet-gateway zscaler tunnels

HTTP

TUNNEL IF TUNNEL LOCATION

RESP

NAME TUNNEL NAME ID FQDN TUNNEL FSM STATE ID LOCATION F

LAST HTTP REQ

```
CODE

--------------------------------------------------------------------------------------------------------
Tunnel100001   site<removed>Tunnel100001   0                tunnel-st-invalid  <removed>  location-ini
req-auth-session      401

Tunnel100002   site<removed>Tunnel100002   0                tunnel-st-invalid  <removed>  location-ini
req-auth-session      401

Tunnel100011   site<removed>Tunnel100011   0                tunnel-st-invalid  <removed>  location-ini
req-auth-session      401

Tunnel100012   site<removed>Tunnel100012   0                tunnel-st-invalid  <removed>  location-ini
req-auth-session      401
```

Voor verdere debugging dient u deze opdrachten in te schakelen en te zoeken naar logberichten met betrekking tot SIG, HTTP of tracker:

- debug platform software sdwan ftm sig
- debug platform software sdwan sig
- debug platform software sdwan tracker
- debug platform software sdwan ftm rtm-events

Dit is een voorbeeld van uitvoer van debug opdrachten:

<#root>

```
Router#
show logging | inc SIG


Jan 31 19:39:38.666: ENDPOINT TRACKER: endpoint tracker SLA already unconfigured: #SIGL7#AUTO#TRACKER
Jan 31 19:39:38.669: ENDPOINT TRACKER: endpoint tracker SLA already unconfigured: #SIGL7#AUTO#TRACKER
Jan 31 19:59:18.240: SDWAN INFO:
 Tracker entry Tunnel100001/#SIGL7#AUTO#TRACKER state => DOWN


Jan 31 19:59:18.263: SDWAN INFO: Tracker entry Tunnel100002/#SIGL7#AUTO#TRACKER state => DOWN
Jan 31 19:59:18.274: SDWAN INFO: Tracker entry Tunnel100011/#SIGL7#AUTO#TRACKER state => DOWN
Jan 31 19:59:18.291: SDWAN INFO: Tracker entry Tunnel100012/#SIGL7#AUTO#TRACKER state => DOWN
```

Stel het bevel in werking tonen ip interfacememorandum en controleer het Protocol van de

tunnelinterface als er omhoog of omlaag verschijnen.

<#root>

```
Router#
```

show ip interface brief

```
Interface              IP-Address      OK? Method Status    Protocol
GigabitEthernet1       10.2.234.146    YES DHCP   up            up
GigabitEthernet2       10.2.58.221     YES other  up            up
```

Tunnel100001 10.2.58.221 YES TFTP up down

Tunnel100002 10.2.58.221 YES TFTP up down

Na het bevestigen dat er geen problemen zijn met de Zscaler-referenties, kunt u de SIG-interface verwijderen uit de apparaatsjabloon en het naar de router duwen.

Zodra de push is voltooid, pas de SIG-sjabloon toe en duw het terug naar de router. Deze methode dwingt de tunnels van nul te worden herschikt.

Gerelateerde informatie

- Cisco Technical Support en downloads

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.