

Configurar túneis Umbrella SIG para cenários ativo/backup ou ativo/ativo

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Visão geral do Cisco Umbrella SIG](#)

[Limitação de largura de banda do túnel Umbrella SIG](#)

[Obtenha as informações do portal Cisco Umbrella](#)

[Obtenha a chave e a chave secreta](#)

[Obtenha a ID da sua organização](#)

[Criar túneis Umbrella SIG com cenário ativo/de backup](#)

[Etapa 1. Crie um Modelo de Recurso de Credenciais SIG.](#)

[Etapa 2. Crie um Modelo de Recurso SIG.](#)

[Etapa 3. Selecione seu provedor SIG para o túnel principal.](#)

[Etapa 4. Adicione o túnel secundário.](#)

[Etapa 5. Crie um par de alta disponibilidade.](#)

[Etapa 6. Edite o Modelo de VPN do lado do serviço para Injetar uma Rota de Serviço.](#)

[Configuração do roteador de borda WAN para cenário ativo/de backup](#)

[Criar túneis Umbrella SIG com cenário ativo/ativo](#)

[Etapa 1. Crie um Modelo de Recurso de Credenciais SIG.](#)

[Etapa 2. Crie duas interfaces de loopback para conectar os túneis SIG.](#)

[Etapa 3. Crie um Modelo de Recurso SIG.](#)

Introdução

Este documento descreve como configurar Cisco Umbrella Secure Internet Gateway (SIG) túneis com IPsec em ambos *Active/Active* e *Active/Standby*.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Cisco Umbrella
- negociação de IPsec

- Rede de longa distância definida por software da Cisco (SD-WAN)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco vManage versão 20.4.2
- Roteador Cisco WAN Edge C1117-4PW* versão 17.4.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Visão geral do Cisco Umbrella SIG

Cisco **Umbrella** é um serviço de segurança fornecido em nuvem que reúne funções essenciais.

Umbrella unifica o gateway seguro da Web, a segurança de DNS, o firewall fornecido na nuvem, a funcionalidade do agente de segurança de acesso à nuvem e a inteligência contra ameaças.

A inspeção e o controle profundos garantem a conformidade com políticas da Web de uso aceitável e protegem contra ameaças da Internet.

Os roteadores SD-WAN podem se integrar com os Secure Internet Gateways (SIG), que fazem a maior parte do processamento para proteger o tráfego empresarial.

Quando o SIG é configurado, todo o tráfego do cliente, com base em rotas ou políticas, é encaminhado ao SIG.

Limitação de largura de banda do túnel Umbrella SIG

Cada túnel IPsec IKEv2 para o **Umbrella** o headend é limitado a aproximadamente 250 Mbps, portanto, se vários túneis forem criados e a carga balancear o tráfego, eles superarão essas limitações caso seja necessária uma largura de banda maior.

Até quatro **High Availability** pares de túneis podem ser criados.

Obtenha as informações do portal Cisco Umbrella

Para prosseguir com a integração do SIG, um **Umbrella** É necessária uma conta com o pacote SIG Essentials.

Current Package	License Start Date	License End Date	Number Of Seats
Umbrella SIG Advantage + Multi-Org + RBI L3	June 30, 2021	June 30, 2031	1


Information listed here is not authoritative in regard to seat count for certain customers. Customers under [Cisco's ELA](#) do not have a traditional concept of seat count limitation and, as such, this page does not accurately reflect those license types.

The values in the graph below = (number of DNS queries in applicable month / number of days in applicable month) / number of licensed Users

For questions about information seen here, or to change your licensing, contact your Cisco account manager or partner.


Obtenha a chave e a chave secreta

A chave e a chave secreta podem ser geradas no momento em que você recebe a **Umbrella Management API KEY** (esta chave está em 'Legacy Keys'). Se você não se lembra ou não salvou a chave secreta, clique em atualizar.

 Cuidado: se o botão Atualizar for clicado, uma atualização dessas chaves será necessária em todos os dispositivos; a atualização não será recomendada se houver dispositivos em uso.

Key	Created
15 [REDACTED] 36	Jul 12, 2021

The API Key and secret pair enable you to manage the deployment for your different organizations. This includes the management of networks, roaming clients and other core-identity types.

Your Key: 15 [REDACTED] 6 

Check out the [documentation](#) for step by step instructions.


[DELETE](#) [REFRESH](#) [CLOSE](#)


Obtenha a ID da sua organização

A ID da organização pode ser facilmente obtida ao fazer login no **Umbrella** na barra de endereços do navegador.

[https://dashboard.umbrella.com/o/\[REDACTED\]/#/admin/apikeys](https://dashboard.umbrella.com/o/[REDACTED]/#/admin/apikeys)


Criar túneis Umbrella SIG com cenário ativo/de backup

 Observação: Roteamento de túnel IPsec/GRE e balanceamento de carga usando ECMP: esse recurso está disponível no vManage 20.4.1 e posteriores, ele permite que você use o modelo SIG para orientar o tráfego de aplicativos para a Cisco Umbrella ou um provedor de SIG de terceiros

 Observação: suporte para Zscaler Automatic Provisioning: esse recurso está disponível no vManage 20.5.1 e posteriores, isso automatiza o provisionamento de túneis de roteadores Cisco SD-WAN para Zscaler, com o uso de credenciais de API de parceiro Zscaler.

Para configurar os túneis automáticos SIG, é necessário criar/atualizar alguns modelos:

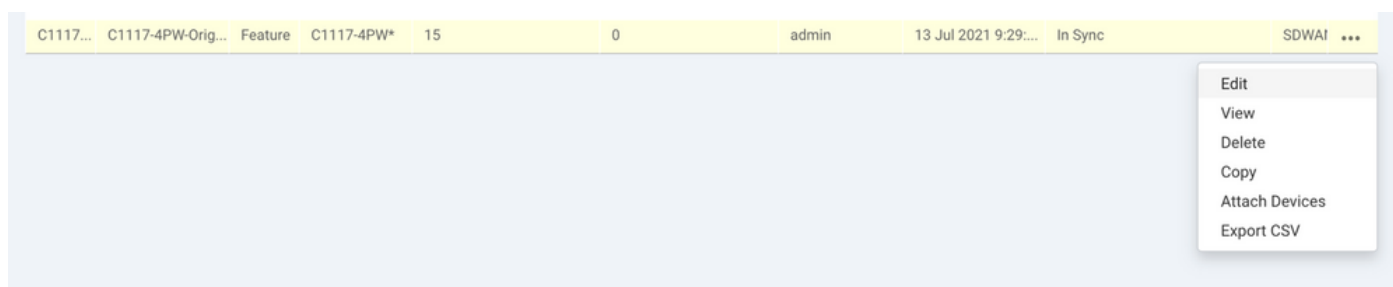
- Crie um modelo de recurso de Credenciais SIG.
 - Crie duas interfaces de loopback para ligar os túneis SIG (aplicável apenas com mais de uma) **Active** túnel ao mesmo tempo - **Active/Active** cenário).
 - Crie um modelo de recurso SIG.
 - Edite o Modelo de VPN do lado do serviço para injetar um **Service Route**.
-

 Observação: certifique-se de que as portas UDP 4500 e 500 sejam permitidas em qualquer dispositivo upstream.

As configurações do modelo mudam com o **Active/Backup** e o **Active/Active** cenários para os quais ambos os cenários são explicados e expostos separadamente.

Etapa 1. Crie um Modelo de Recurso de Credenciais SIG.

Vá para o modelo de recurso e clique em **Edit**.



Na seção de **Additional templates**, clique em **Cisco SIG Credentials**. A opção é mostrada na imagem.

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 ▼	

Dê um nome e uma descrição para o modelo.

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  [REDACTED]

Registration Key  [REDACTED]

Secret  [REDACTED]

[Get Keys](#)

Etapa 2. Crie um Modelo de Recurso SIG.

Navegue até o modelo de recurso e, na seção **Transport & Management VPN** selecione o modelo de recurso Cisco Secure Internet Gateway.

Transport & Management VPN

Cisco VPN 0 * VPN0-C1117

Cisco Secure Internet Gateway SIG-IPSEC-TUNNELS

Cisco VPN Interface Ethernet VPN0-INTERFACE-GI-0-0-0-C1117

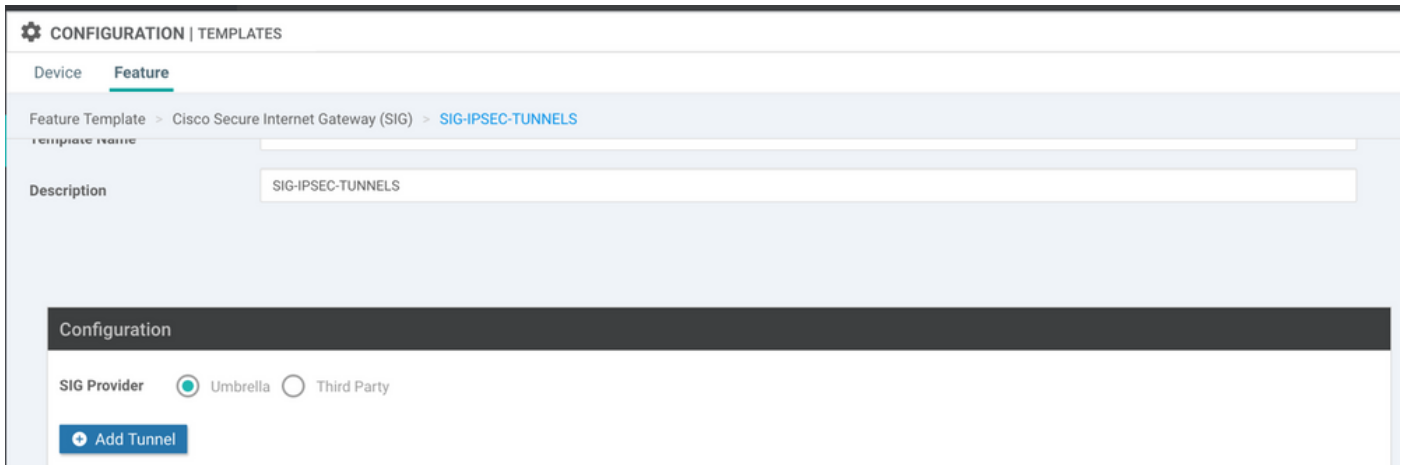
Additional Cisco VPN 0 Templates

- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- ⦿ Cisco Secure Internet Gateway
- Cisco VPN Interface Ethernet
- Cisco VPN Interface GRE
- Cisco VPN Interface IPsec
- VPN Interface Multilink Controller
- VPN Interface Ethernet PPPoE
- VPN Interface DSL IPoE
- VPN Interface DSL PPPoA
- VPN Interface DSL PPPoE
- VPN Interface SVI

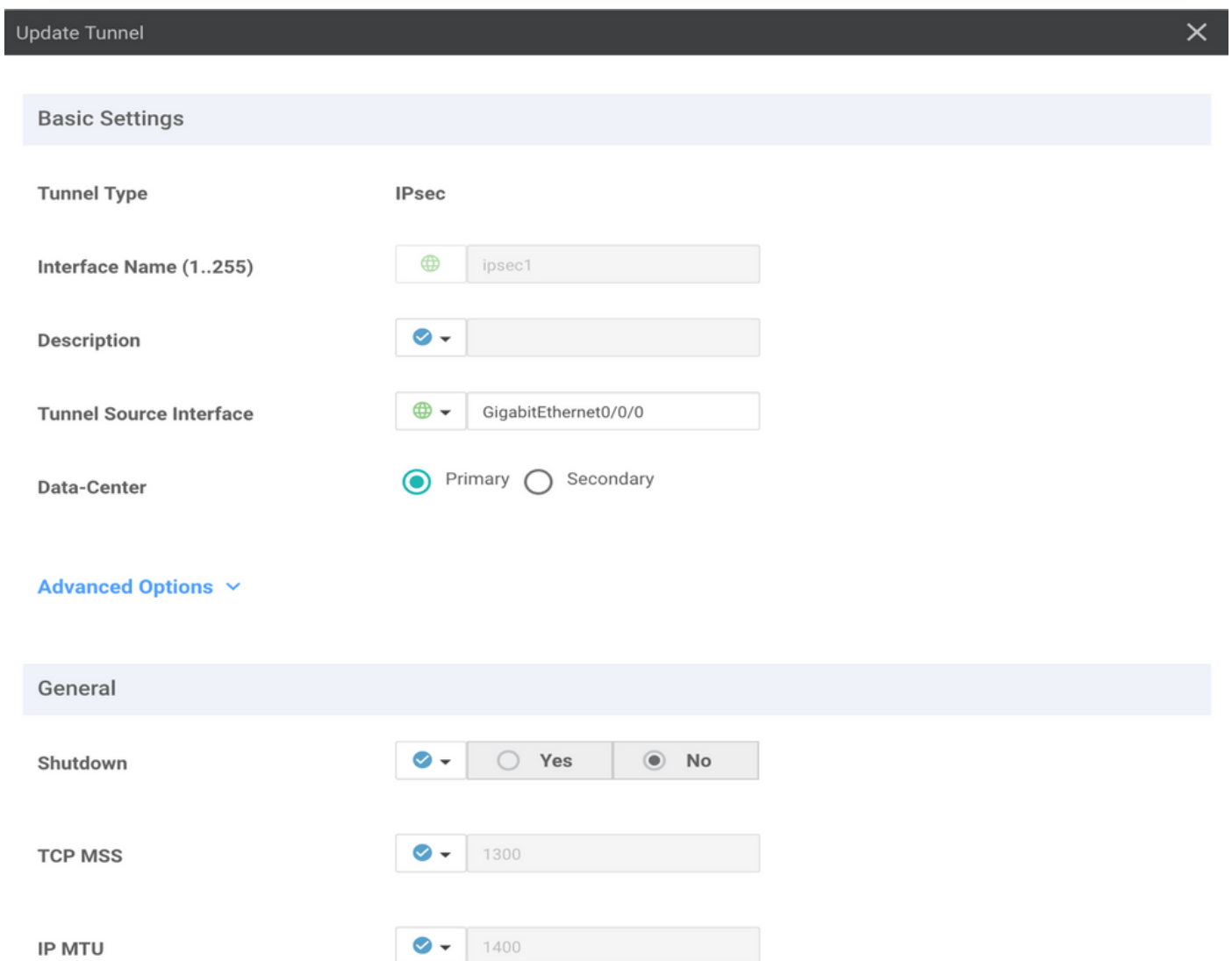
Dê um nome e uma descrição para o modelo.

Etapa 3. Selecione seu provedor SIG para o túnel principal.

Clique em **Add Tunnel**.



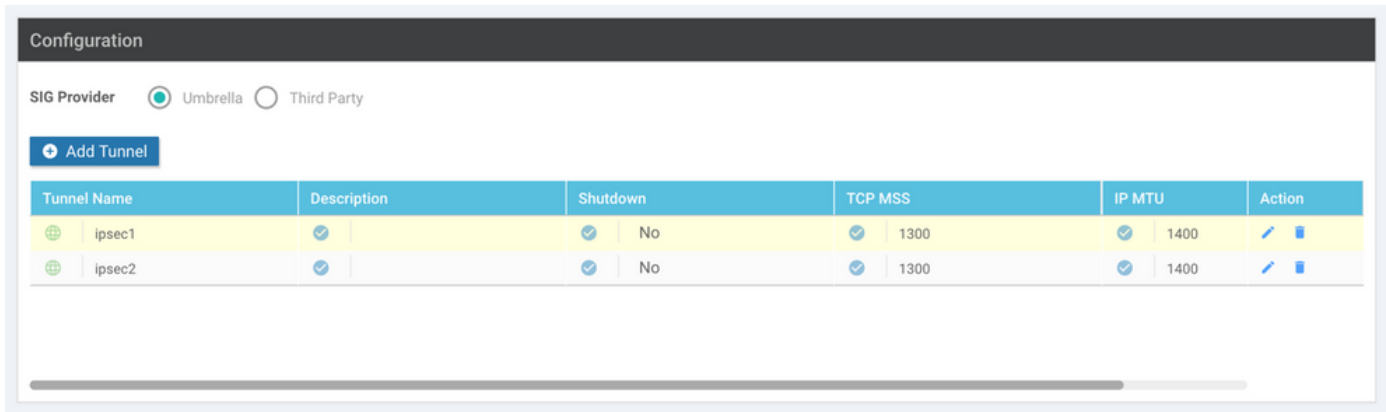
Configure os detalhes básicos e mantenha **Data-Center** como **Primary** e clique em **Add**.



Etapa 4. Adicione o túnel secundário.

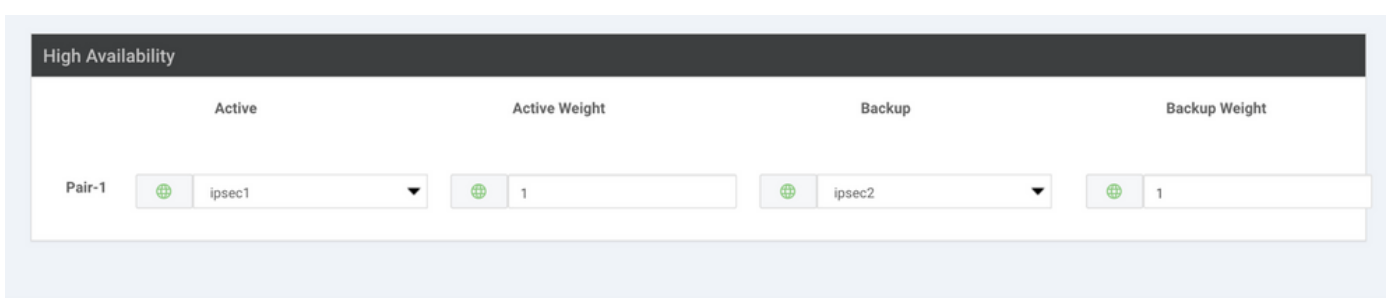
Adicione uma segunda configuração de túnel, use **Data-Center** como **Secondary** desta vez e o nome da interface como **ipsec2**.


A configuração do vManage aparece como mostrado aqui:



Etapa 5. Crie um par de alta disponibilidade.

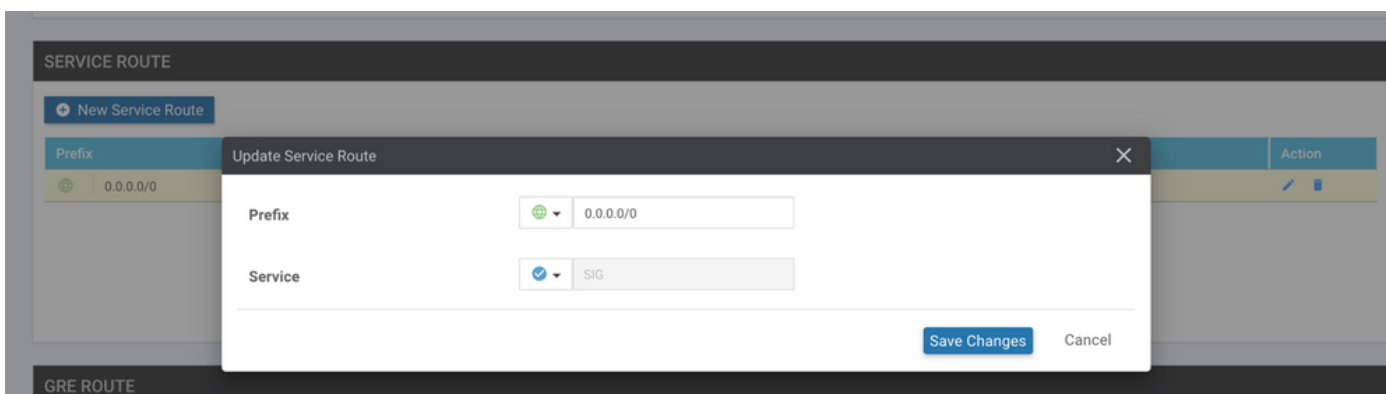
No âmbito do **High Availability** selecione o túnel ipsec1 como Ativo e o túnel ipsec2 como Backup.



 Observação: até 4 **High Availability** pares de túneis e um máximo de 4 túneis ativos podem ser criados ao mesmo tempo.

Etapa 6. Edite o Modelo de VPN do lado do serviço para Injetar uma Rota de Serviço.

Navegue até a página **Service VPN** seção e, dentro do **Service VPN** modelo, navegue até a seção **Service Route** e adicionar um 0.0.0.0 com **SIG Service Route**. Para este documento, o VRF/VPN 10 é usado.



A rota 0.0.0.0 SIG é exibida como mostrado aqui.

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Cisco VPN > VPN10-C1117-TEMPLATE

Basic Configuration DNS Advertise OMP IPv4 Route IPv6 Route Service **Service Route** GRE Route IPSEC Route

NAT Global Route Leak

SERVICE ROUTE

+ New Service Route

Prefix	Service	Action
0.0.0.0/0	<input checked="" type="checkbox"/> SIG	

Observação: para que o tráfego do serviço realmente saia, o NAT precisa ser configurado na interface da WAN.

Anexe este modelo ao dispositivo e envie a configuração por push:

TASK VIEW

Push Feature Template Configuration | Validation Success | Initiated By: admin From: 128.107.241.174

Total Task: 1 | In Progress : 1

Search Options

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
In progress	Pushing configuration t...	C1117-4PWE-FGL2149...	C1117-4PW*	C1117-4PWE-FGL2149...	10.10.10.10	10	1.1.1.2

[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.

Configuração do roteador de borda WAN para cenário ativo/de backup

```

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-i
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
```

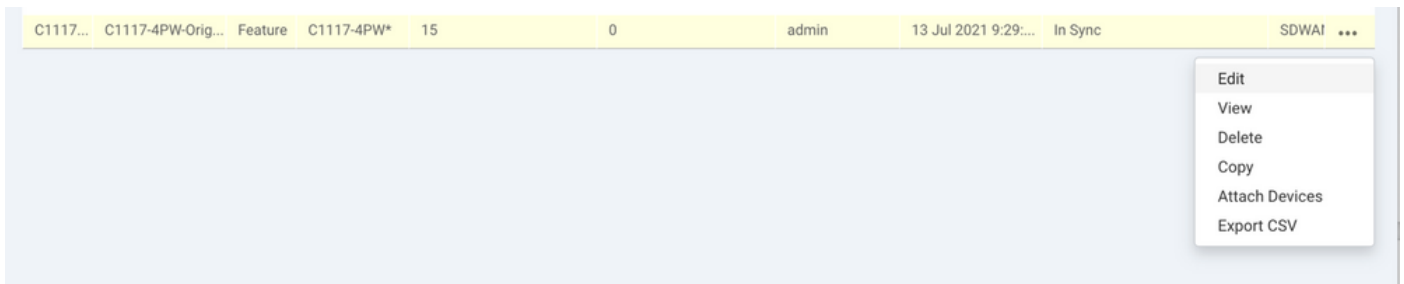
```
tunnel mode sdwan
exit
interface Tunnel100001
no shutdown
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
tunnel source GigabitEthernet0/0/0
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec1-ipsec-profile
tunnel vrf multiplexing
exit
interface Tunnel100002
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
```

Criar túneis Umbrella SIG com cenário ativo/ativo

Etapa 1. Crie um Modelo de Recurso de Credenciais SIG.

Navegue até o modelo de recurso e clique em **Edit**



Na seção de **Additional templates**, selecione **Cisco SIG Credentials**. A opção é mostrada na imagem.

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 ▼	

Dê um nome e uma descrição para o modelo.

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

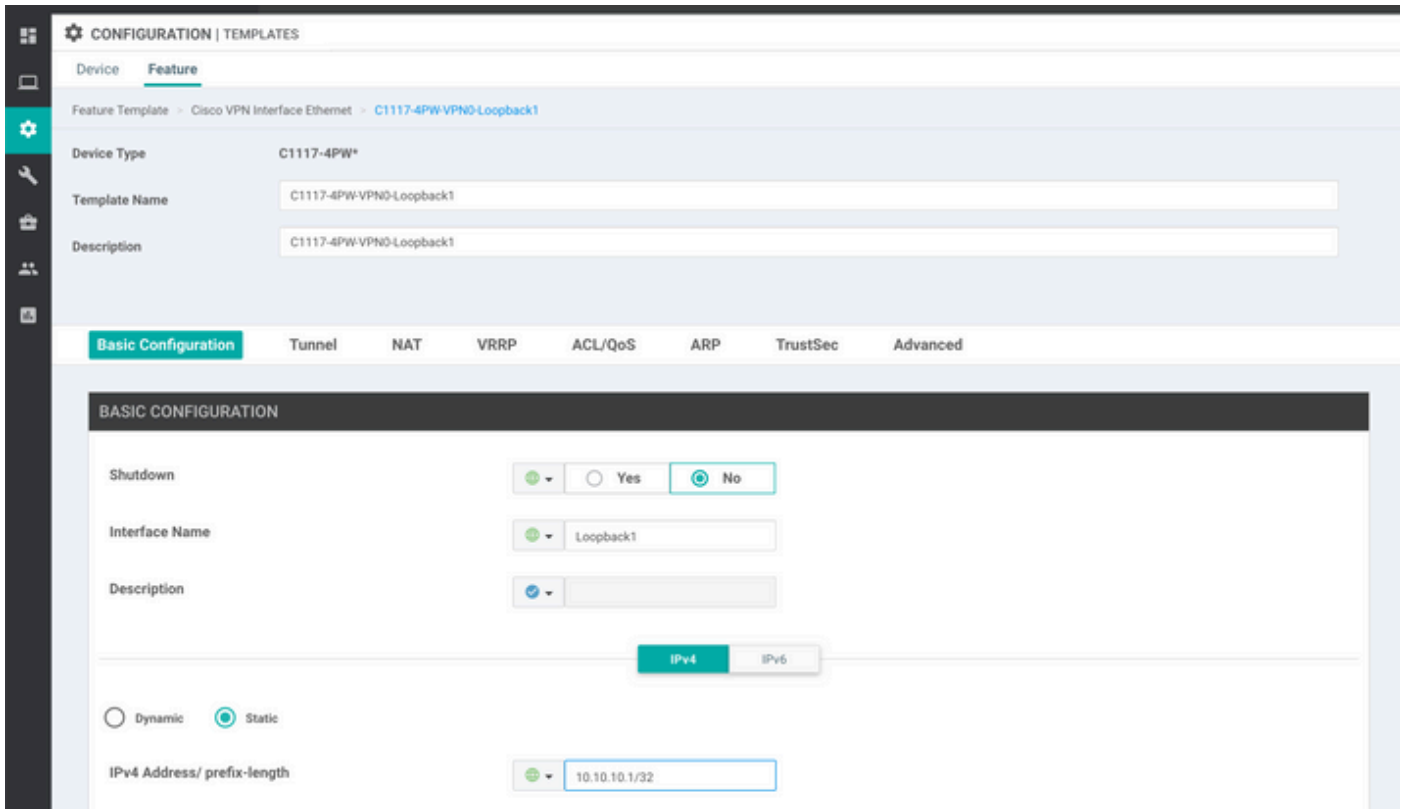
Etapa 2. Crie duas interfaces de loopback para conectar os túneis SIG.

 Observação: crie uma interface de loopback para cada túnel SIG configurado no modo ativo, isso é necessário porque cada túnel precisa de um ID IKE exclusivo.

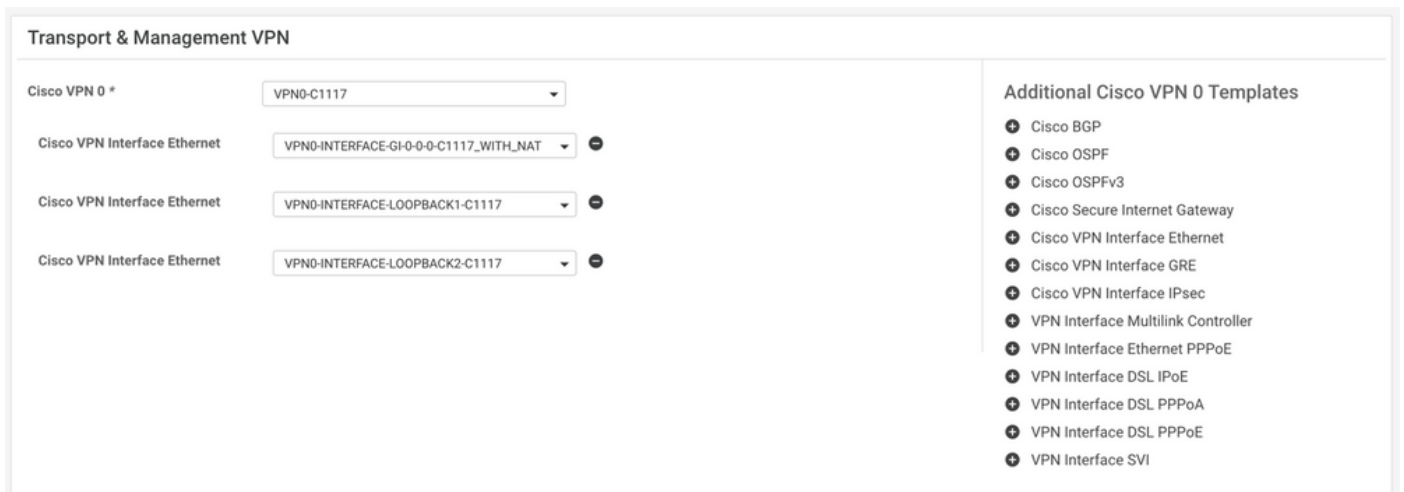
 Observação: este cenário é Ativo/Ativo, portanto, dois Loopbacks são criados.

Configure o nome da interface e o endereço IPv4 para o Loopback.

 Observação: o endereço IP configurado para o loopback é um endereço fictício.



Crie o segundo modelo de Loopback e anexe-o ao modelo do dispositivo. O modelo do dispositivo deve ter dois modelos de loopback anexados:



Etapa 3. Crie um Modelo de Recurso SIG.

Navegue até o modelo de recurso SIG e, na seção **Transport & Management VPN** selecionar **Cisco Secure Internet Gateway** modelo de recurso.

Etapa 4. Selecione o provedor SIG para o túnel principal.

Clique em **Add Tunnel**.

CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Cisco Secure Internet Gateway (SIG) > SIG-IPSEC-TUNNELS

Template name


Description SIG-IPSEC-TUNNELS

Configuration

SIG Provider Umbrella Third Party

[Add Tunnel](#)

Configure os detalhes básicos e mantenha **Data-Center** COMO **Primary**.

 Observação: o parâmetro Tunnel Source Interface é o Loopback (para este documento Loopback1) e como Tunnel Route-via Interface a interface física (para este documento GigabitEthernet0/0/0)

Update Tunnel

Basic Settings

Tunnel Type IPsec

Interface Name (1..255) ipsec1

Description

Tunnel Source Interface Loopback1

Data-Center Primary Secondary

Tunnel Route-via Interface GigabitEthernet0/0/0

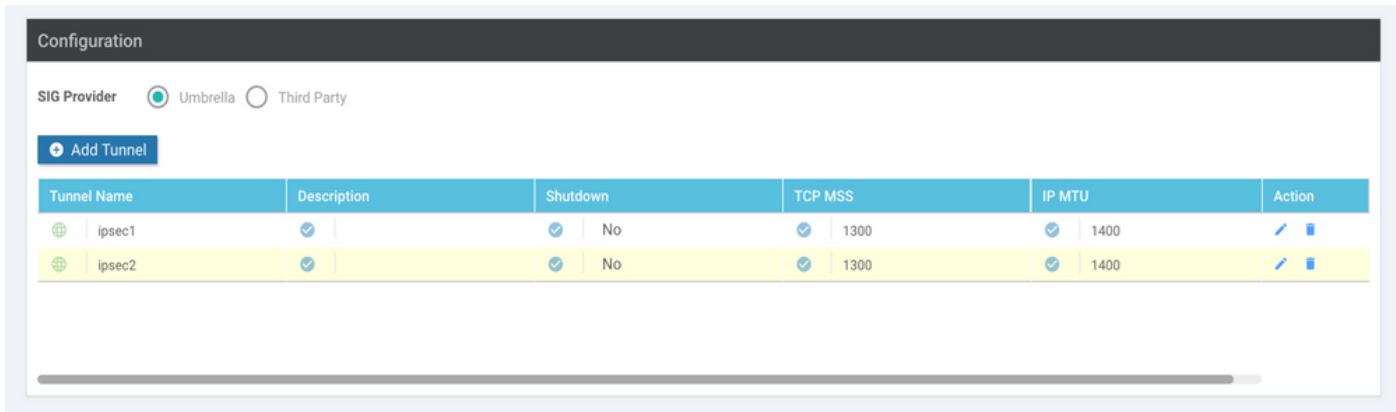
Advanced Options >

[Save Changes](#) [Cancel](#)

Etapa 5. Adicione o túnel secundário.

Adicione uma segunda configuração de túnel, use **Data-Center** como **Primary** e o nome da interface como ipsec2.

A configuração do vManage aparece como mostrado aqui:

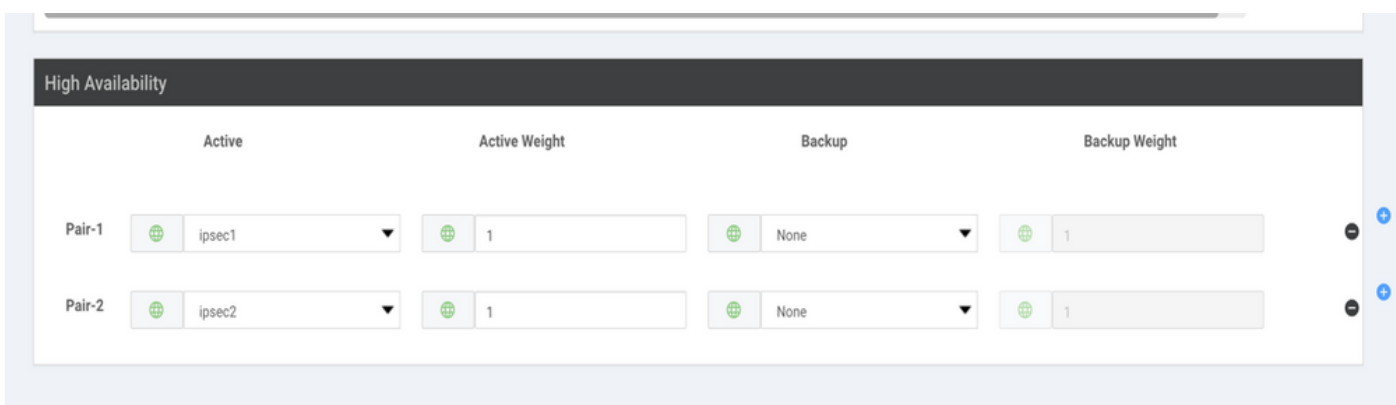


Etapa 6. Crie Dois Pares De Alta Disponibilidade.

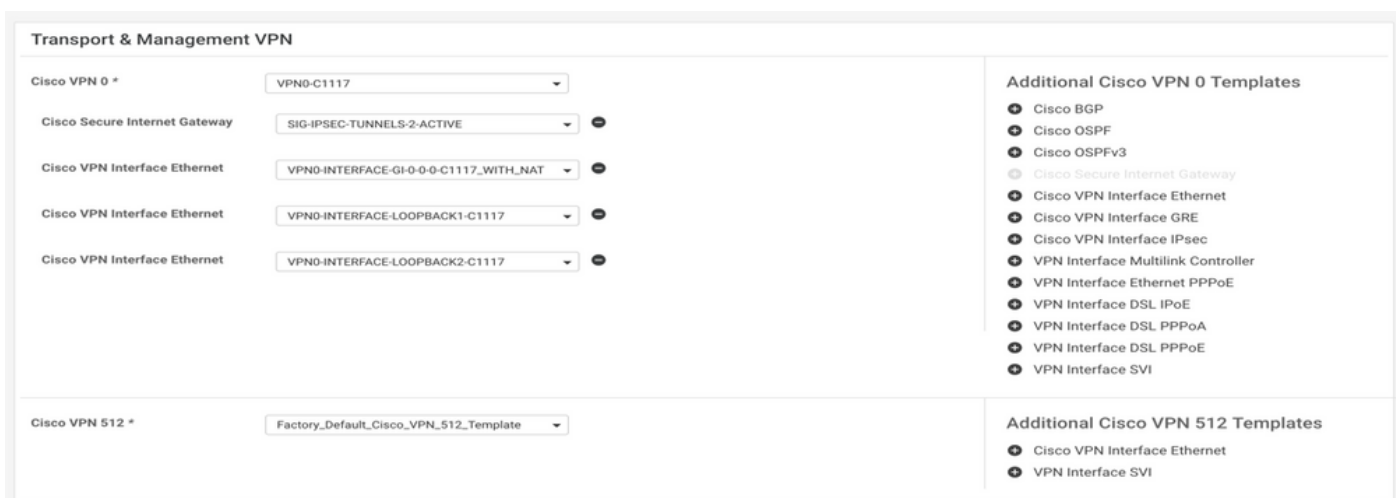
No âmbito do **High Availability**, crie duas **High Availability** pares.

- No primeiro par HA, selecione o ipsec1 como Ativo e selecione **None** para backup.
- No segundo par HA, selecione ipsec2 como Ativo (Ativo) e selecione **None** e para backup.

A configuração do vManage para **High Availability** aparece como mostrado:



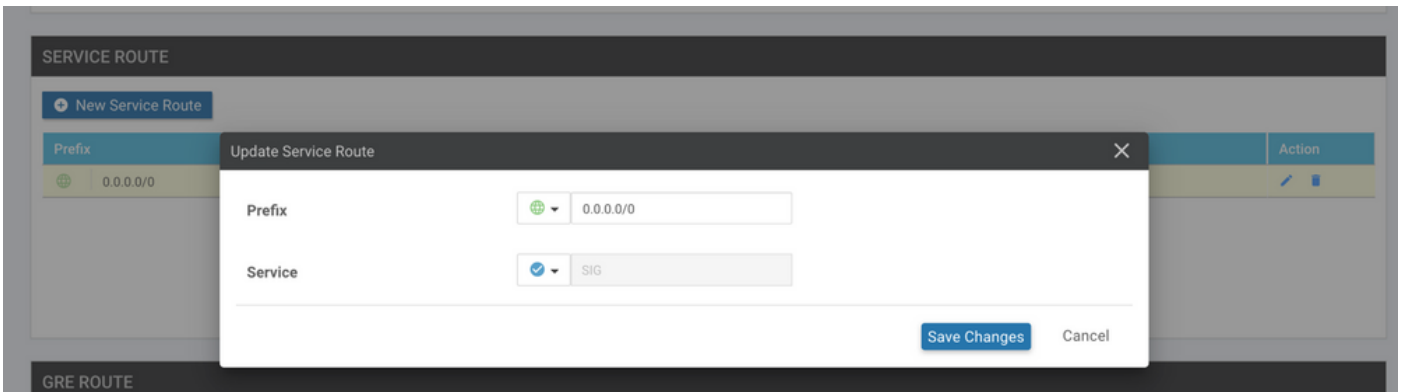
O modelo de dispositivo tem os dois modelos de loopback e o modelo de recurso SIG anexado também.




Passo 7. Edite o Modelo de VPN do lado do serviço para Injetar uma Rota de

Serviço.

Navegue até a página **Service VPN** e no modelo **VPN of service**, navegue até a seção **Service Route** e adicionar um **0.0.0.0** com **SIG** **Service Route**



A rota SIG 0.0.0.0 aparece como mostrado aqui.

 **Observação:** para que o tráfego do serviço realmente saia, o NAT precisa ser configurado na interface da WAN.

Anexe esse modelo ao dispositivo e envie a configuração por push.

Configuração do roteador de borda WAN para cenário ativo/ativo


```
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-inte
exit
interface Tunnel100002
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-inte
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
!
```

 Observação: embora este documento seja focado no Umbrella, os mesmos cenários se aplicam a túneis do Azure e de SIG de terceiros.

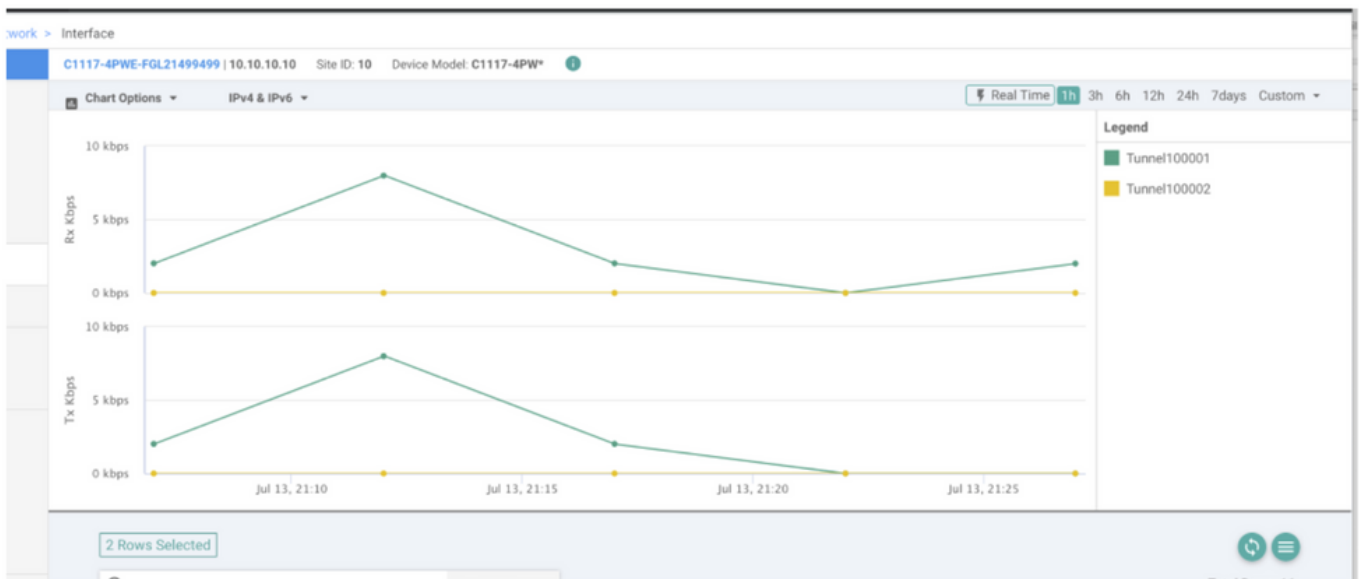
Verificar

Verificar cenário ativo/de backup

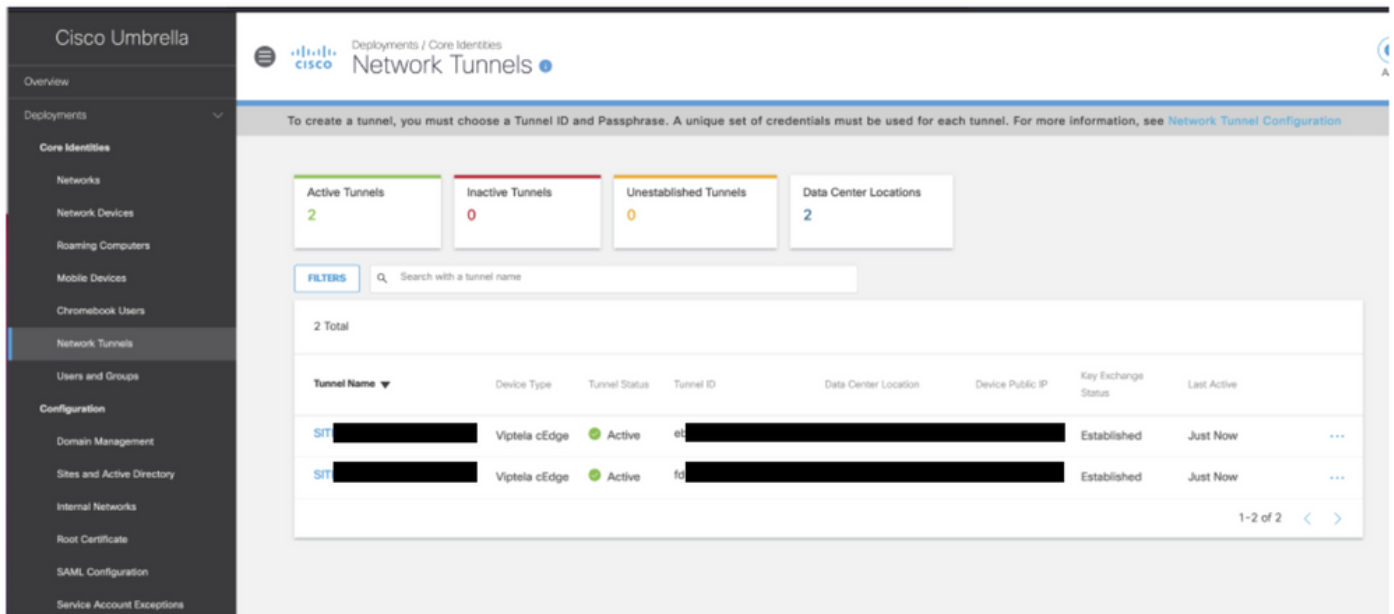
No vManage, é possível monitorar o status dos túneis SIG IPsec. Navegue até **Monitor > Network**, selecione o dispositivo de borda da WAN desejado.

Clique no botão **Interfaces** no lado esquerdo; uma lista de todas as interfaces no dispositivo é exibida. Isso inclui as interfaces ipsec1 e ipsec2.

A imagem mostra que o túnel ipsec1 encaminha todo o tráfego e o ipsec2 não passa tráfego.



Também é possível verificar os túneis no Cisco Umbrella é mostrado na imagem.



Use o `show sdwan secure-internet-gateway tunnels` no CLI para exibir as informações de Túneis.

```
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

Use o `show endpoint-tracker` e `show ip sla summary` na CLI para exibir informações sobre os rastreadores e SLAs gerados automaticamente.

```
cEdge_Site1_East_01#show endpoint-tracker
Interface          Record Name          Status      RTT in msec  Probe ID  Next Hop
Tunnel100001      #SIGL7#AUTO#TRACKER Up           8           14        None
Tunnel100002      #SIGL7#AUTO#TRACKER Up           2           12        None
```

```
cEdge_Site1_East_01#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds
```

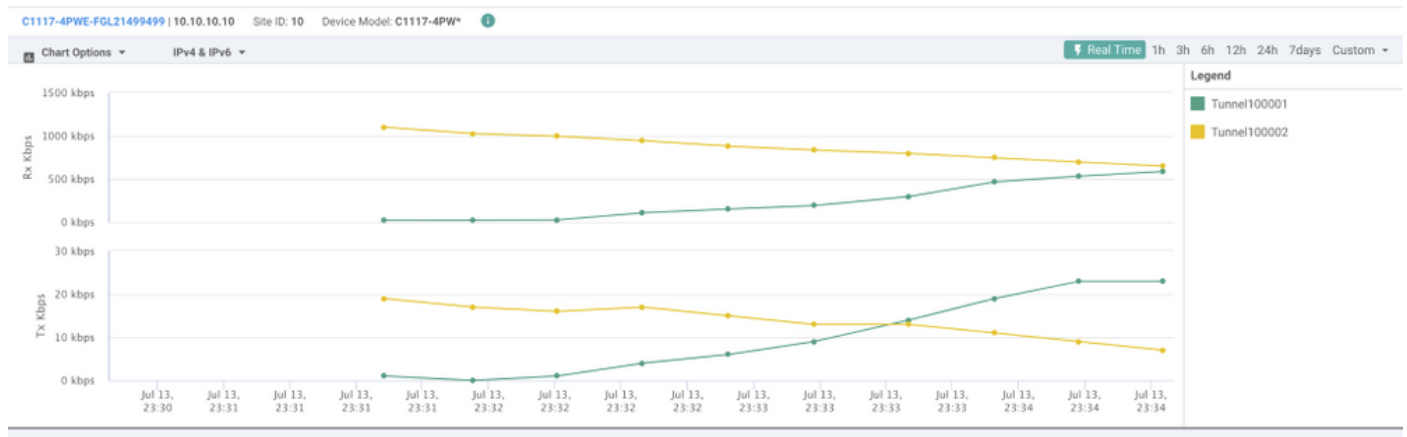
ID	Type	Destination	Stats	Return Code	Last Run
*12	http	10.10.10.10	RTT=6	OK	8 seconds ago
*14	http	10.10.10.10	RTT=17	OK	3 seconds ago

Verificar Cenário Ativo/Ativo

No vManage é possível monitorar o status dos túneis SIG IPsec. Navegue até **Monitor > Network**, selecione o dispositivo de borda da WAN desejado.

Clique no botão **Interfaces** no lado esquerdo - e uma lista de todas as interfaces no dispositivo é exibida. Isso inclui as interfaces ipsec1 e ipsec2.

A imagem mostra que os túneis ipsec1 e ipsec2 encaminham o tráfego.



Use o `show sdwan secure-internet-gateway tunnels` na CLI para exibir as informações de Túneis.

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

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunne1100001	540798313	SITE10SYS10x10x10x10IFTunne1100001	st-tun-create-notif	200	create-tunne1
Tunne1100002	540798314	SITE10SYS10x10x10x10IFTunne1100002	st-tun-create-notif	200	create-tunne1

Use o `show endpoint-tracker` e `show ip sla summary` na CLI para exibir informações sobre os rastreadores e SLAs gerados automaticamente.

```
cEdge_Site1_East_01#show endpoint-tracker
```

Interface	Record Name	Status	RTT in msecs	Probe ID	Next Hop
Tunne1100001	#SIGL7#AUTO#TRACKER	Up	8	14	None
Tunne1100002	#SIGL7#AUTO#TRACKER	Up	2	12	None

```
cEdge_Site1_East_01#show ip sla summary
```

IPSLAs Latest Operation Summary

Codes: * active, ^ inactive, ~ pending

All Stats are in milliseconds. Stats with u are in microseconds

ID	Type	Destination	Stats	Return	Last
----	------	-------------	-------	--------	------

				Code	Run
*12	http	10.10.10.10	RTT=6	OK	8 seconds ago
*14	http	10.10.10.10	RTT=17	OK	3 seconds ago

Informações Relacionadas

- [Integre seus dispositivos com gateways de Internet seguros - Cisco IOS® XE versão 17.x](#)
- [http://Network Configuração do túnel - Umbrella SIG](#)
- [Introdução ao Umbrella](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.