为活动/备份或活动/活动方案配置Umbrella SIG隧道

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- Cisco Umbrella SIG概述
- Umbrella SIG隧道带宽限制

获取您的Cisco Umbrella门户信息

- 获取密钥和密钥
- 获取您的组织ID

使用主用/备用方案创建Umbrella SIG隧道

- 步骤1:创建SIG凭证功能模板。
- 第二步：创建SIG功能模板。
- 第三步：选择主隧道的SIG提供商。
- 第四步：添加辅助隧道。
- 第五步：创建一个高可用性对。
- 第六步：编辑服务端VPN模板以注入服务路由。
- 主用/备用方案的WAN边缘路由器配置

使用主用/主用方案创建Umbrella SIG隧道

- 步骤1:创建SIG凭证功能模板。
- 第二步：创建两个环回接口以链接SIG隧道。
- 第三步：创建SIG功能模板。

简介

本文档介绍如何配置 **Cisco Umbrella Secure Internet Gateway (SIG)** 两个中均具有IPsec的隧道 **Active/Active** 和 **Active/Standby**.

先决条件

要求

建议掌握下列主题的相关知识：

- 思科 **Umbrella**
- IPsec协商

- 思科软件定义的广域网(SD-WAN)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科vManage版本20.4.2
- 思科广域网边缘路由器C1117-4PW*版本17.4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco Umbrella SIG概述

思科 **Umbrella** 是一项云交付的安全服务，将基本功能集于一身。

Umbrella 统一安全Web网关、DNS安全、云交付防火墙、云访问安全代理功能和威胁情报。

深度检测和控制确保符合可接受使用网络策略并防御互联网威胁。

SD-WAN路由器可以与安全互联网网关(SIG)集成，后者执行大部分处理以保护企业流量。

设置SIG后，所有基于路由或策略的客户端流量都会转发到SIG。

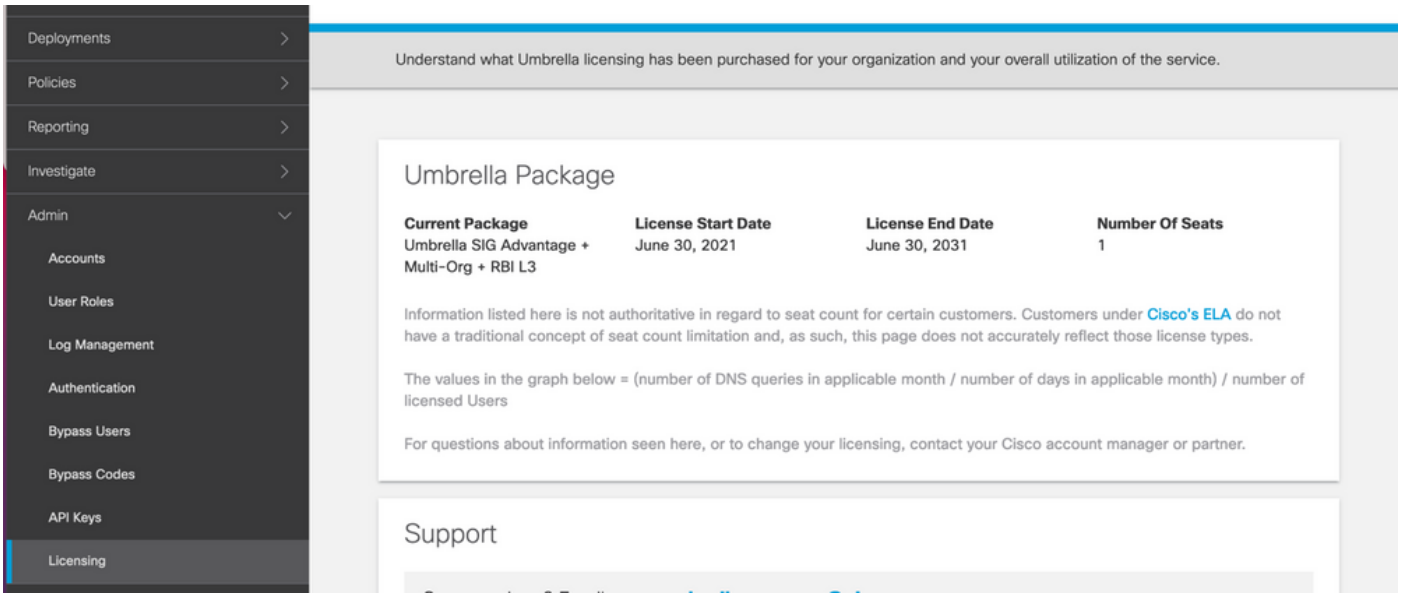
Umbrella SIG隧道带宽限制

到每个IPsec IKEv2隧道 **Umbrella** 头端限制为大约250 Mbps，因此如果创建了多个隧道并对流量进行负载均衡，它们可以克服此类限制，以防需要更高带宽。

最多四个 **High Availability** 可以创建隧道对。

获取您的Cisco Umbrella门户信息

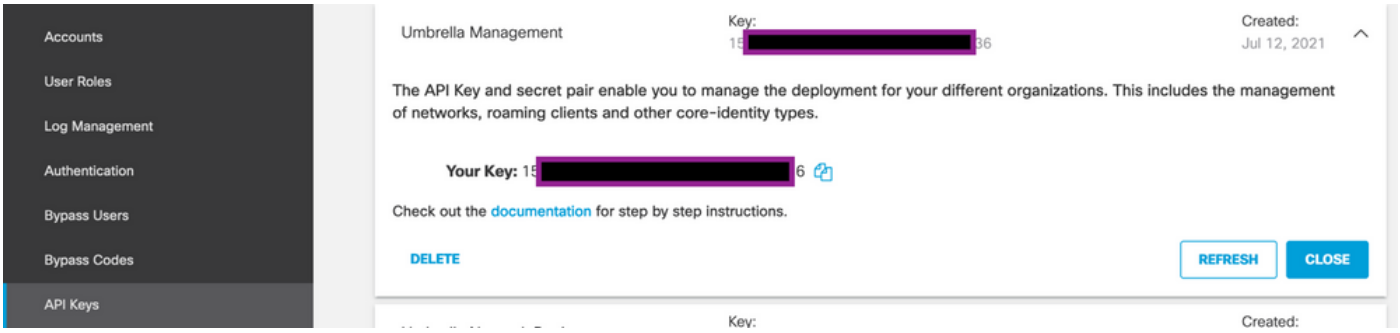
要继续进行SIG集成，请发出 **Umbrella** 需要具有SIG基础软件包的帐户。



获取密钥和密钥

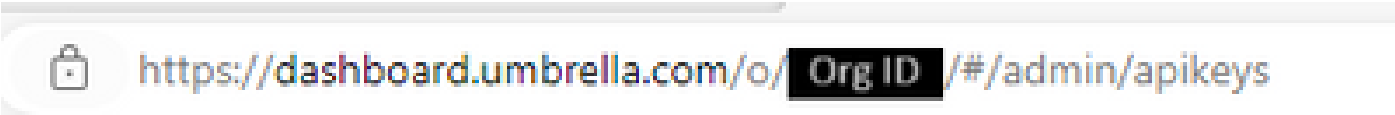
密钥和密钥可以在您获得 Umbrella Management API KEY （此密钥位于“Legacy Keys”下）。如果您不记得或未保存密钥，请单击refresh。

⚠ 注意：如果单击刷新按钮，则需要对所有设备上的这些密钥进行更新；如果存在正在使用的设备，则不建议进行更新。



获取您的组织ID

当您登录时，可以轻松获取组织ID Umbrella 从浏览器地址栏。



使用主用/备用方案创建Umbrella SIG隧道

✎ 注意：使用ECMP的IPsec/GRE隧道路由和负载均衡：此功能在vManage 20.4.1及更高版本中可用，它允许您使用SIG模板将应用流量引导至思科 Umbrella 或第三方SIG提供商

注意：支持Zscaler自动调配：此功能在vManage 20.5.1及更高版本上可用，它使用Zscaler合作伙伴API凭证自动调配从Cisco SD-WAN路由器到Zscaler的隧道。

要配置SIG自动隧道，需要创建/更新几个模板：

- 创建SIG凭证功能模板。
- 创建两个环回接口以链接SIG隧道（仅适用于多个隧道） **Active** 同时使用隧道 — **Active/Active** 场景)。
- 创建SIG功能模板。
- 编辑服务端VPN模板以插入一个 **Service Route.**

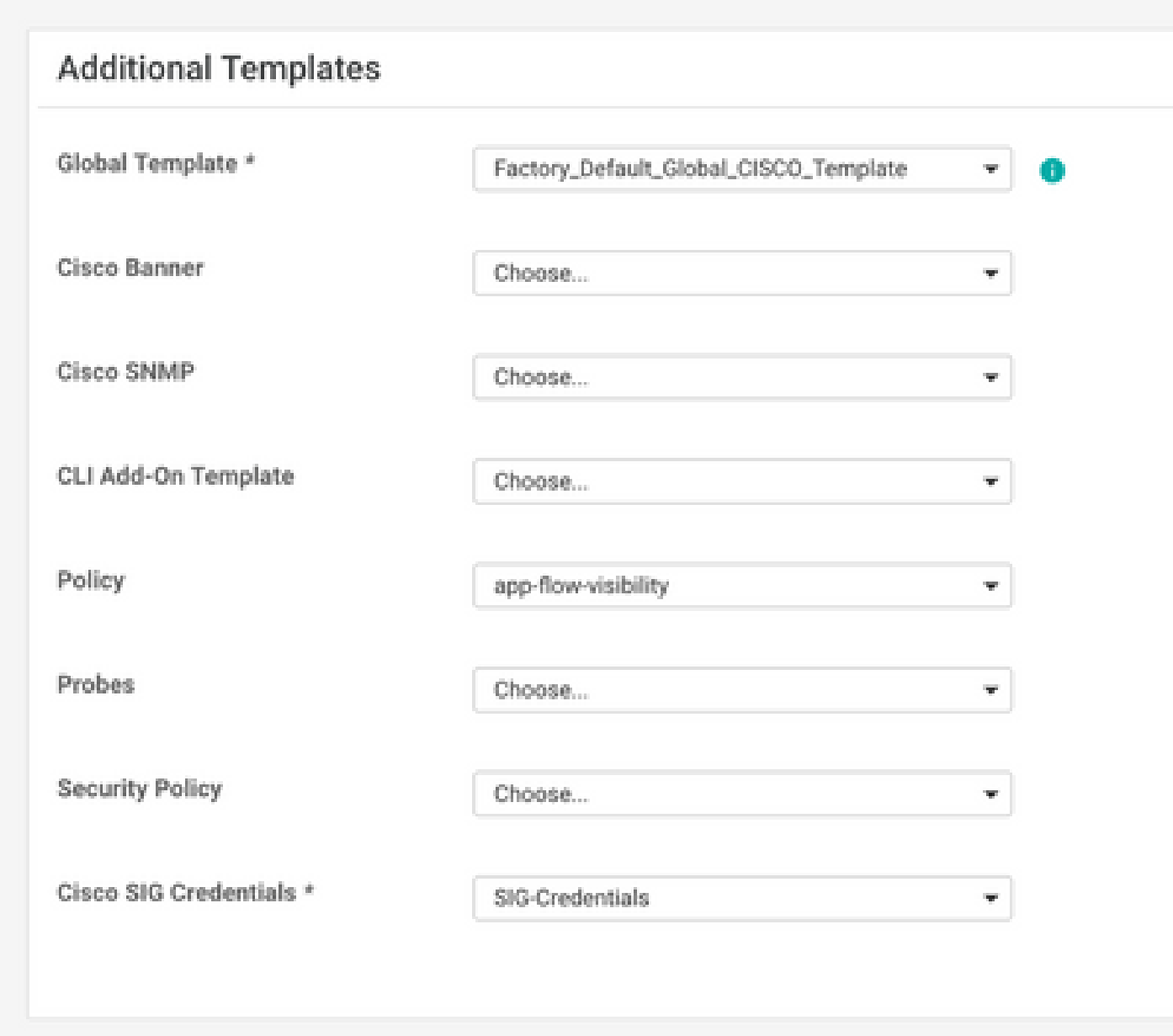
注意：确保允许来自任何上游设备的UDP 4500和500端口。

模板配置会随着更改而更改 **Active/Backup** 和 **Active/Active** 两种情景分别进行解释和展示的场景。

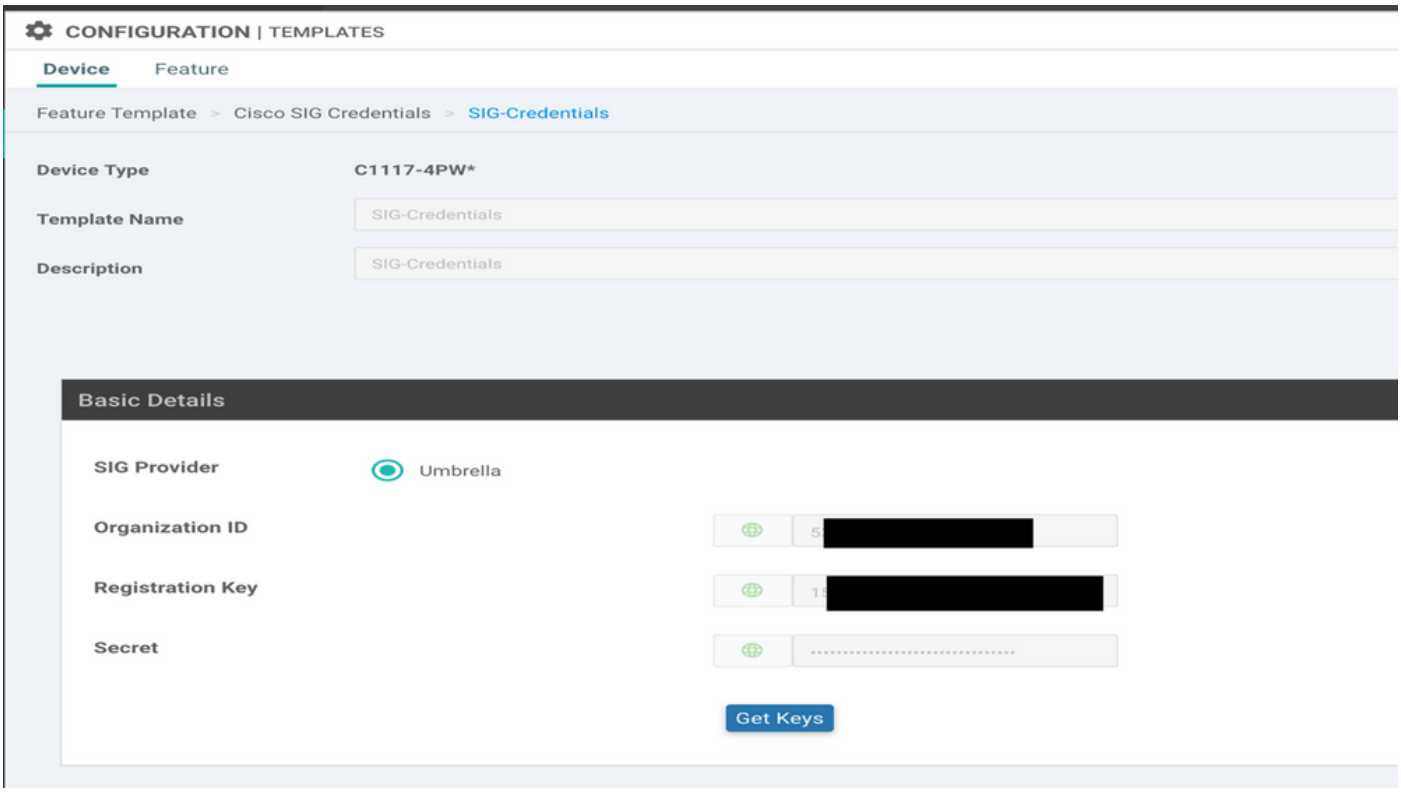
步骤1:创建SIG凭证功能模板。

转到功能模板并单击 **Edit.**

在 **Additional templates,**点击 **Cisco SIG Credentials.**该选项如图所示。

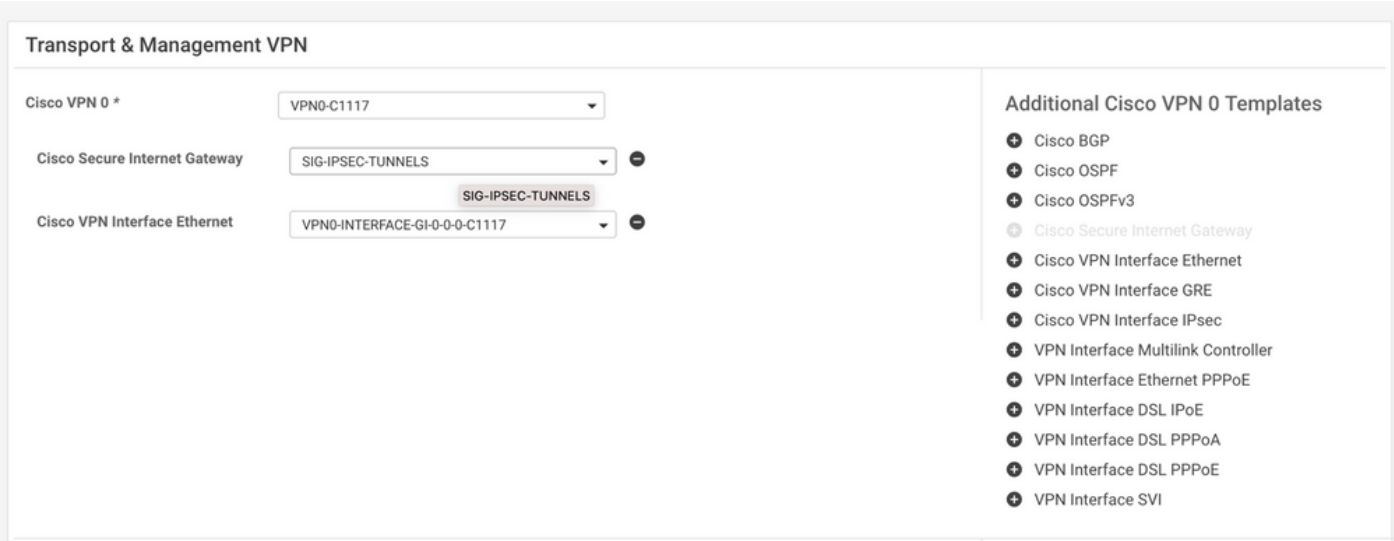

Additional Templates
Global Template *
Factory_Default_Global_CISCO_Template
Cisco Banner
Choose...
Cisco SNMP
Choose...
CLI Add-On Template
Choose...
Policy
app-flow-visibility
Probes
Choose...
Security Policy
Choose...
Cisco SIG Credentials *
SIG-Credentials

为模板提供名称和说明。



第二步：创建SIG功能模板。

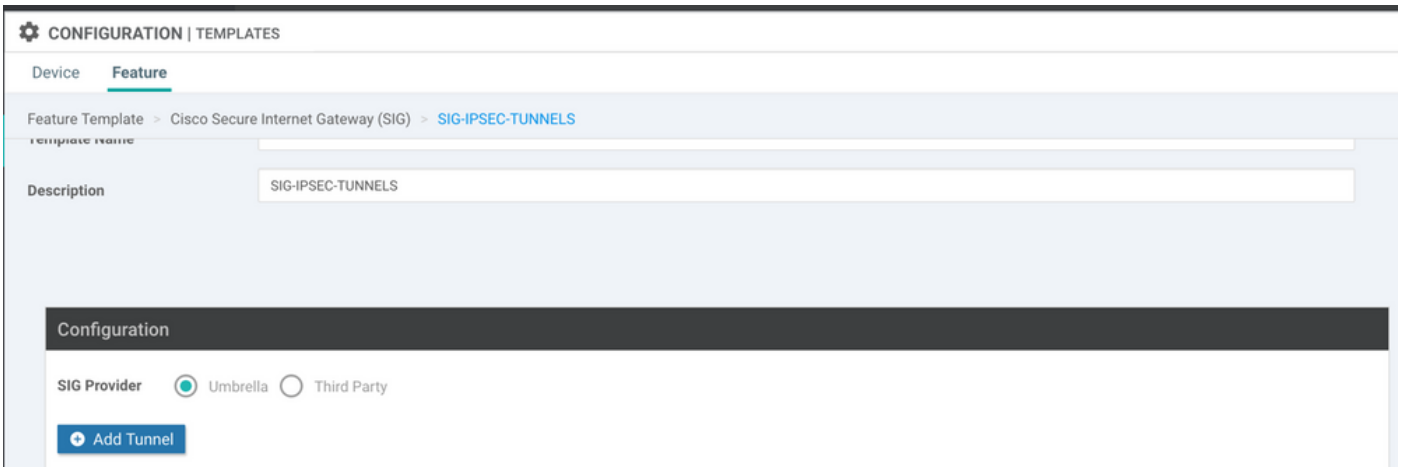
导航至功能模板，并在部分下方 **Transport & Management VPN** 选择Cisco Secure Internet Gateway功能模板。



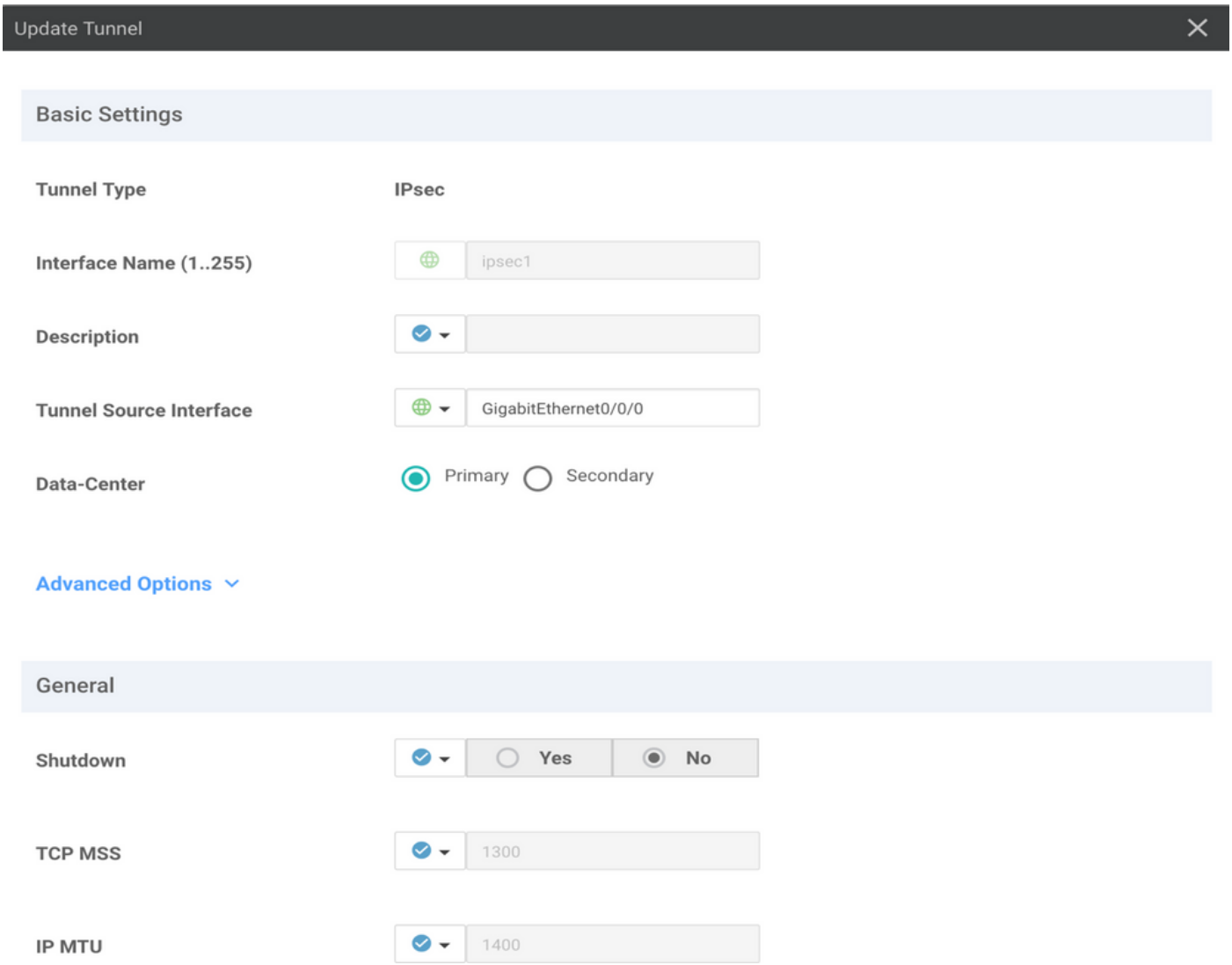
为模板提供名称和说明。

第三步：选择主隧道的SIG提供商。

点击 **Add Tunnel.**



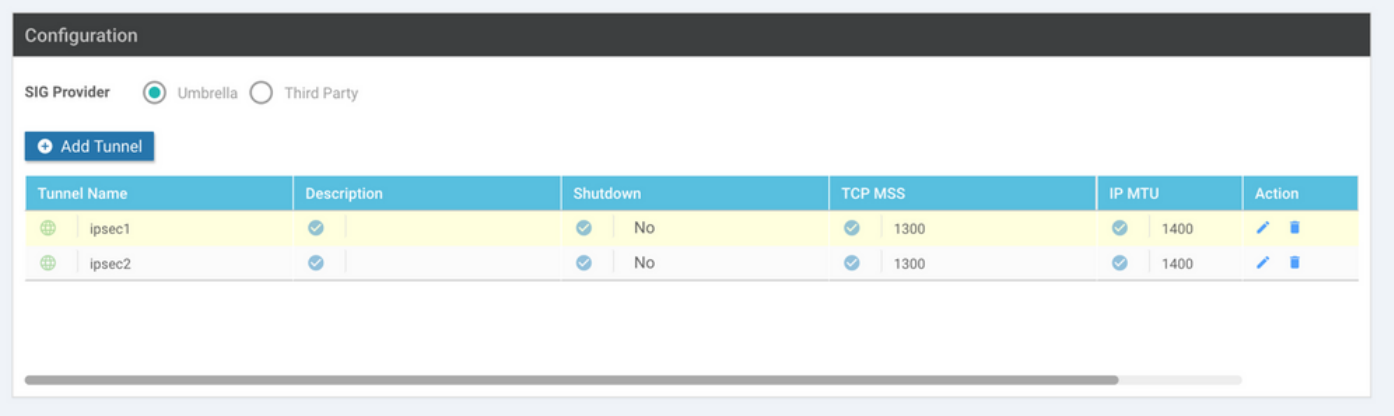
配置基本详细信息并保留 **Data-Center** 作为 **Primary**，然后单击 **Add.**



步骤4.添加辅助隧道。

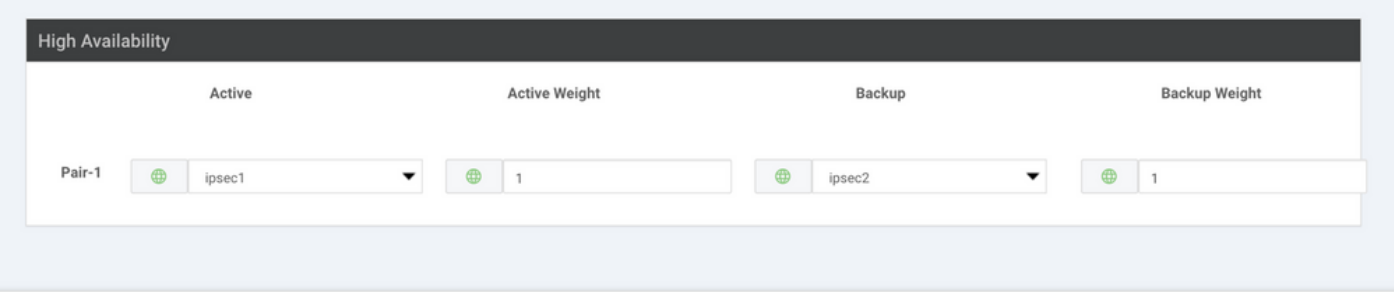
添加第二个隧道配置，使用 **Data-Center** 作为 **Secondary** 这次的接口名称为ipsec2。

vManage配置如下所示：



第五步：创建一个高可用性对。

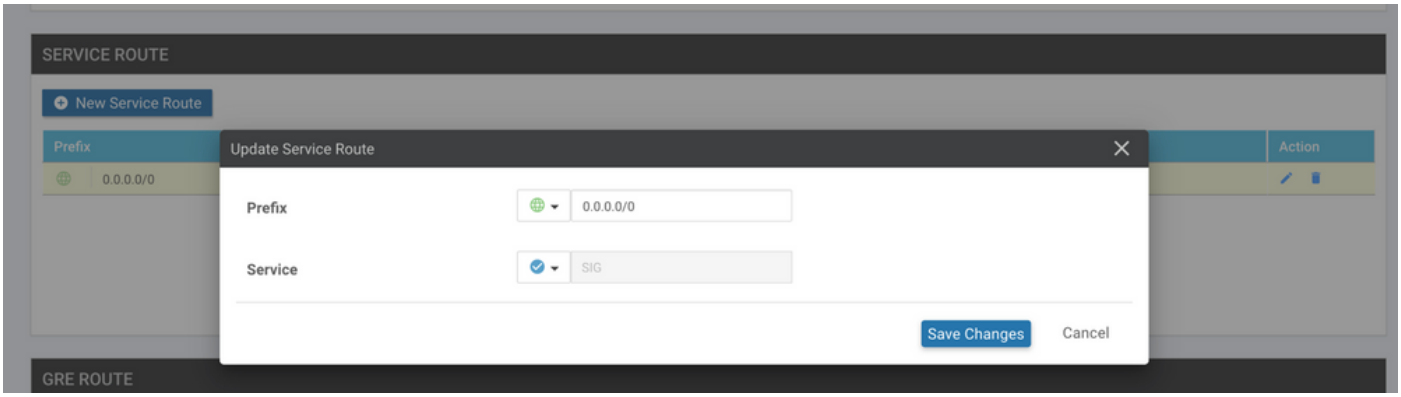
在 **High Availability** 部分，选择ipsec1作为Active，选择ipsec2隧道作为Backup。



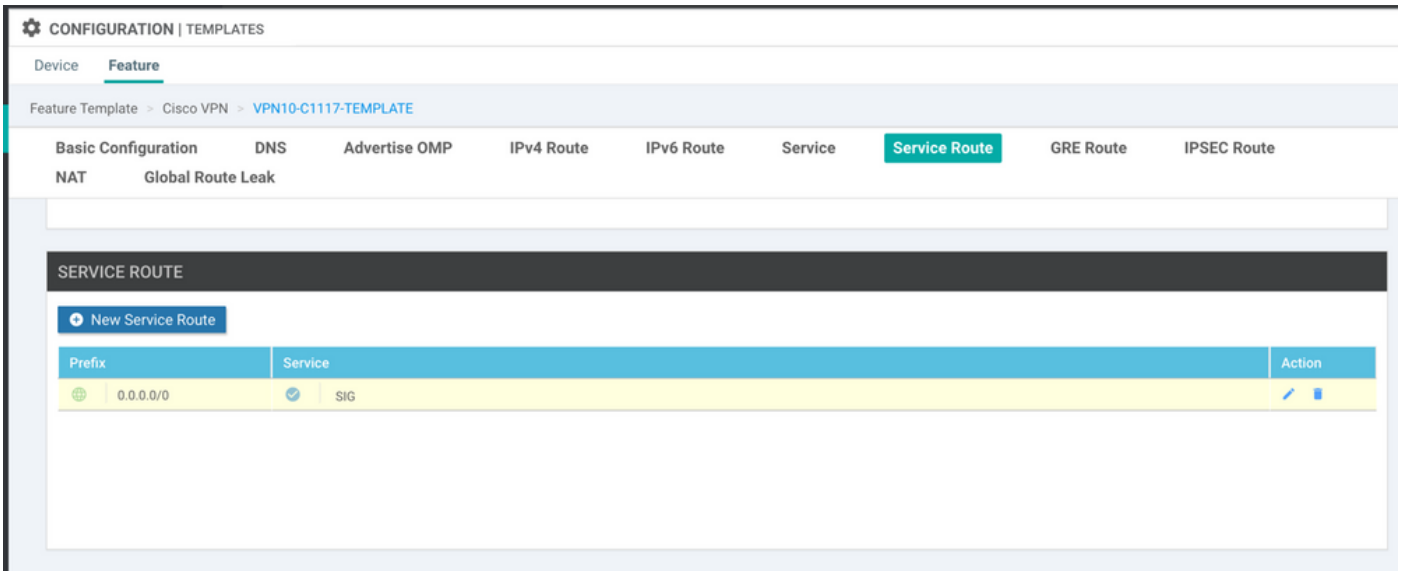
注：最多4个 **High Availability** 可以同时创建隧道对和最多4个活动隧道。

第六步：编辑服务端VPN模板以注入服务路由。

导航至 **Service VPN** 部分和，在 **Service VPN** 模板，导航到相应部分 **Service Route** 并添加带SIG的0.0.0.0 **Service Route**.本文档使用VRF/VPN 10。

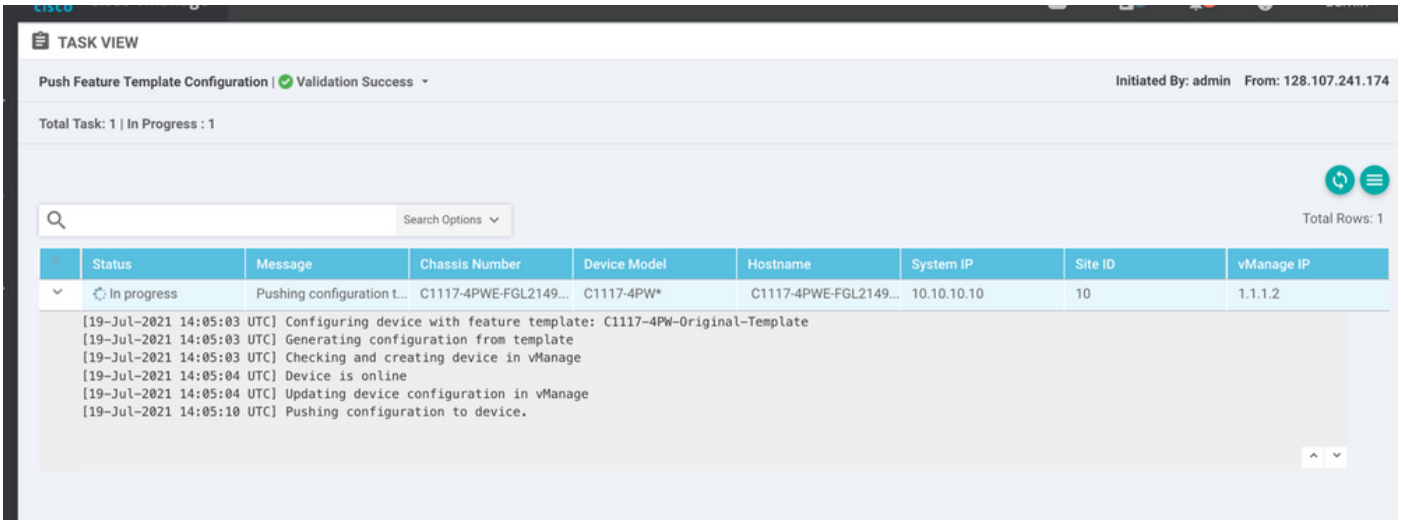


0.0.0.0 SIG路由如下图所示。



注：要使服务流量实际传出，必须在WAN接口中配置NAT。

将此模板附加到设备并推送配置：



主用/备用方案的WAN边缘路由器配置

```
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
```

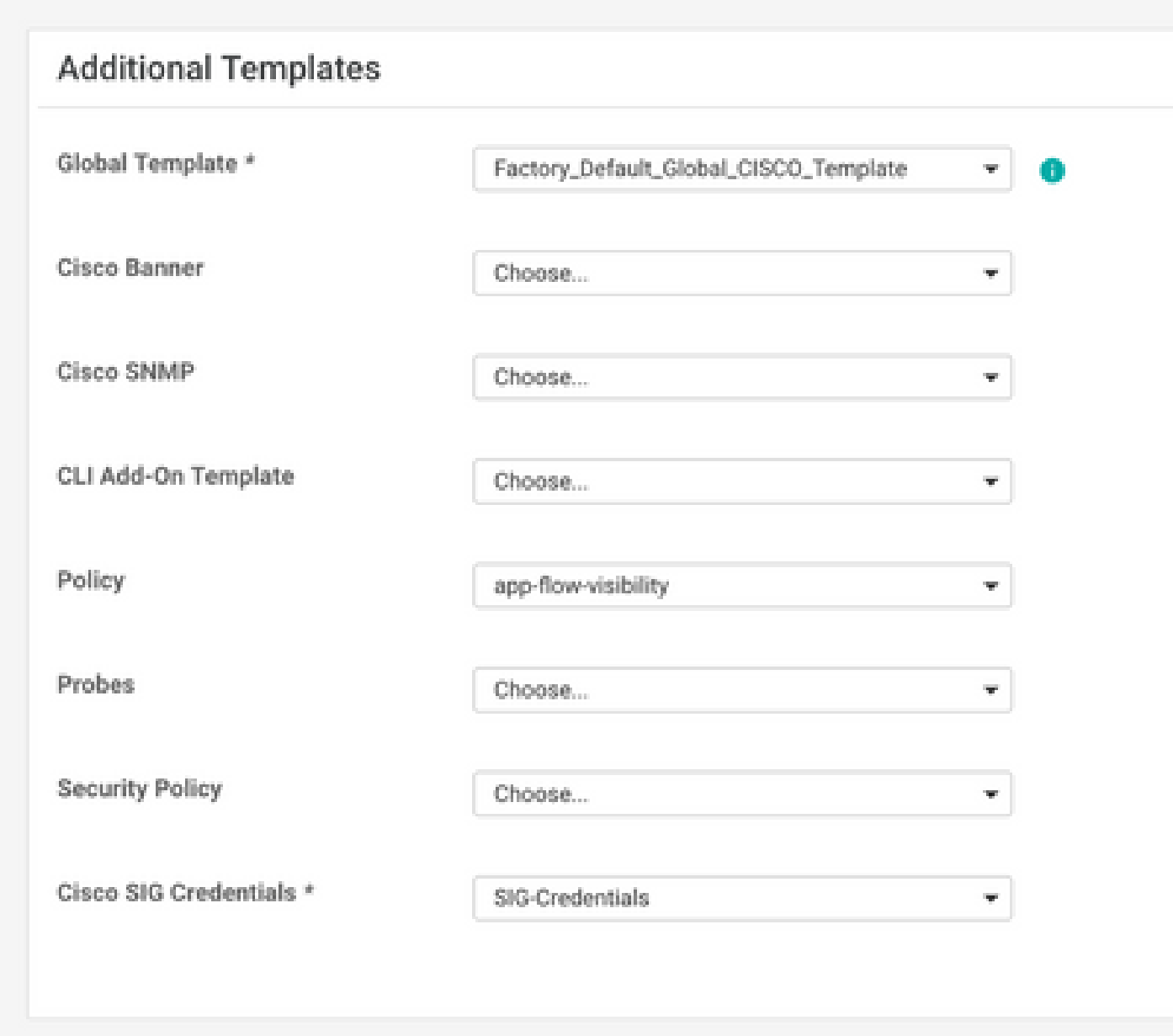
```
 set security-association replay window-size 512
!
crypto ipsec profile if-ipsec2-ipsec-profile
 set ikev2-profile if-ipsec2-ikev2-profile
 set transform-set if-ipsec2-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
no crypto isakmp diagnose error
no network-clock revertive
```

使用主用/主用方案创建Umbrella SIG隧道

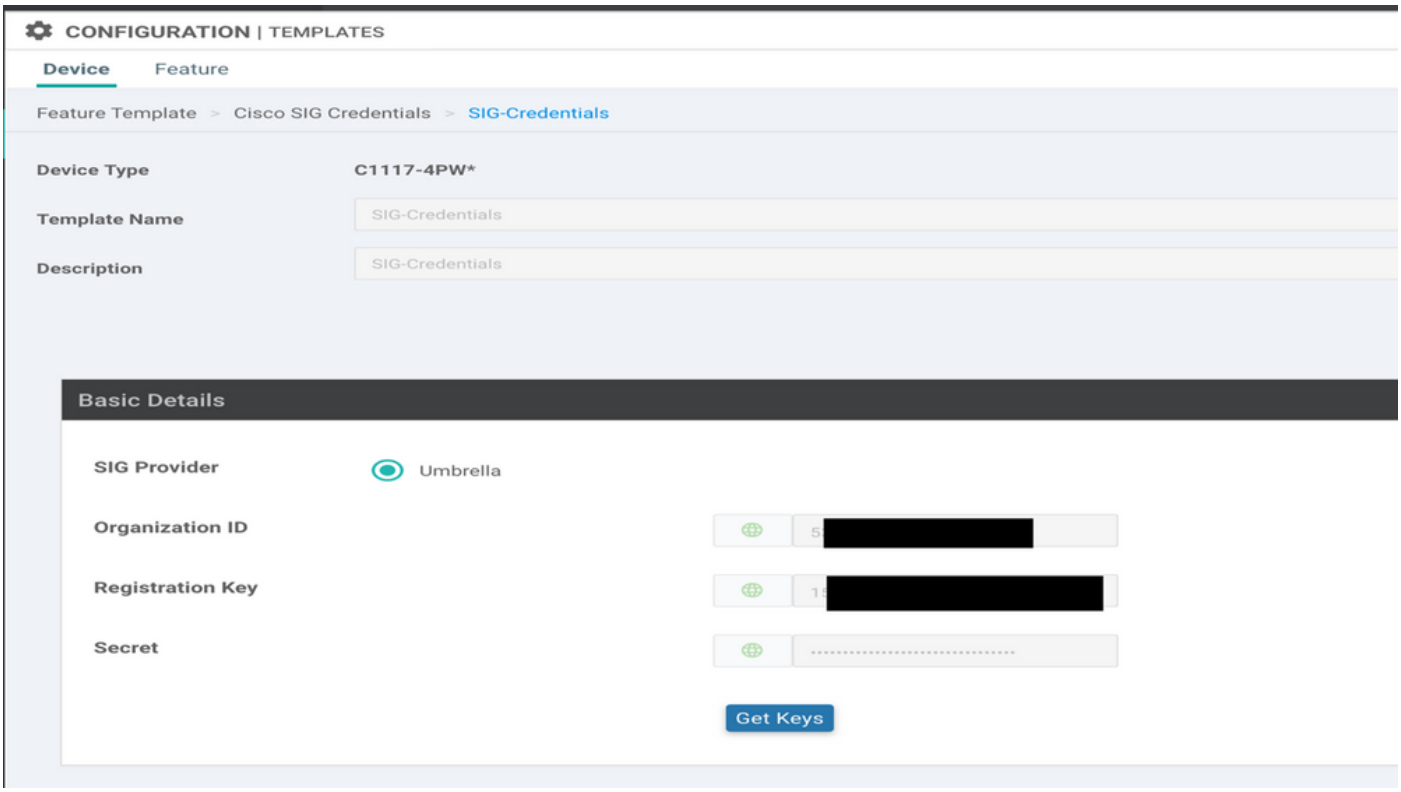
步骤1:创建SIG凭证功能模板。

导航到功能模板并单击 **Edit**

在 **Additional templates**,选择 **Cisco SIG Credentials**.该选项显示在图像上。


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

为模板提供名称和说明。



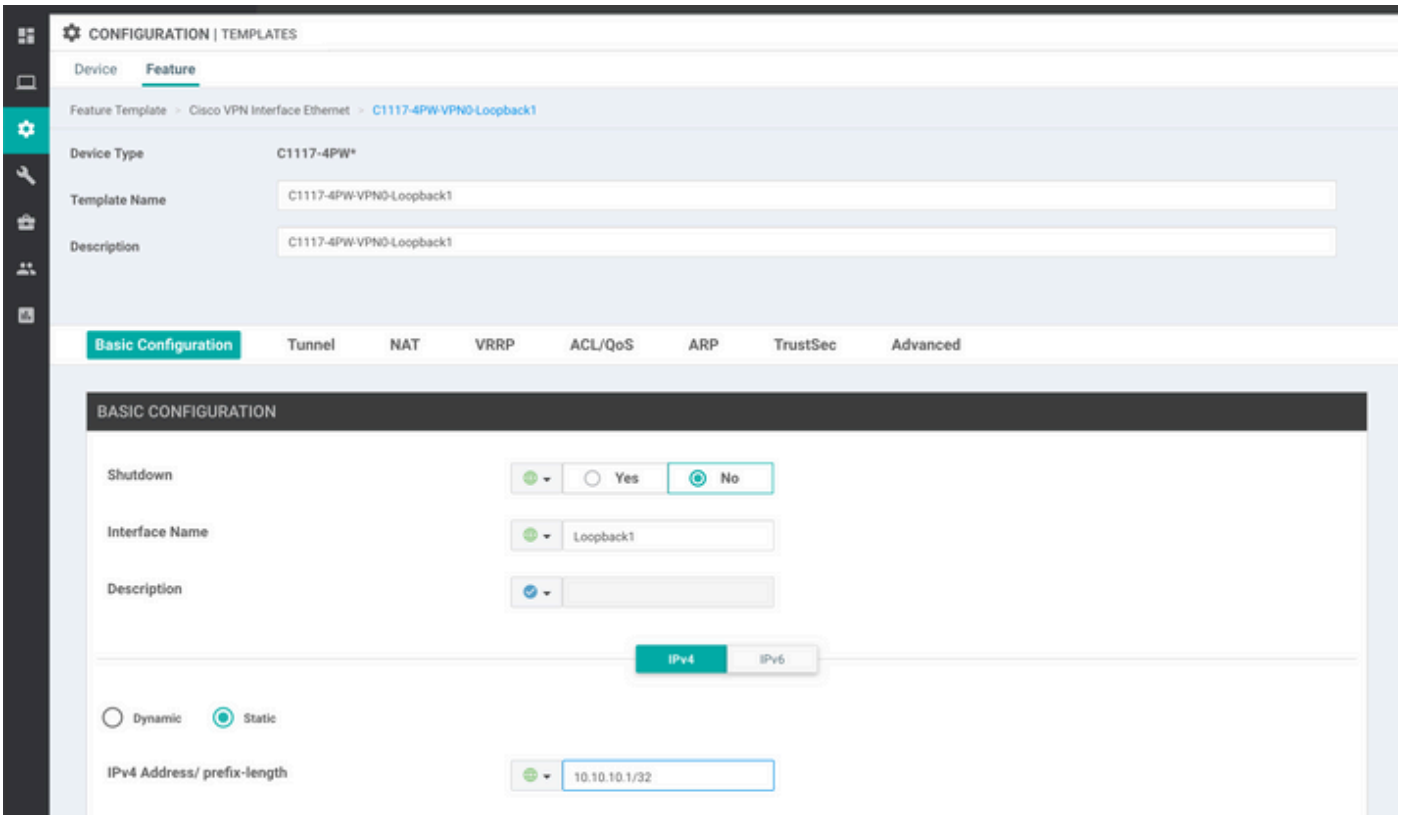
第二步：创建两个环回接口以链接SIG隧道。

注意：为活动模式下配置的每个SIG隧道创建环回接口，因为每个隧道都需要唯一的IKE ID，所以需要此接口。

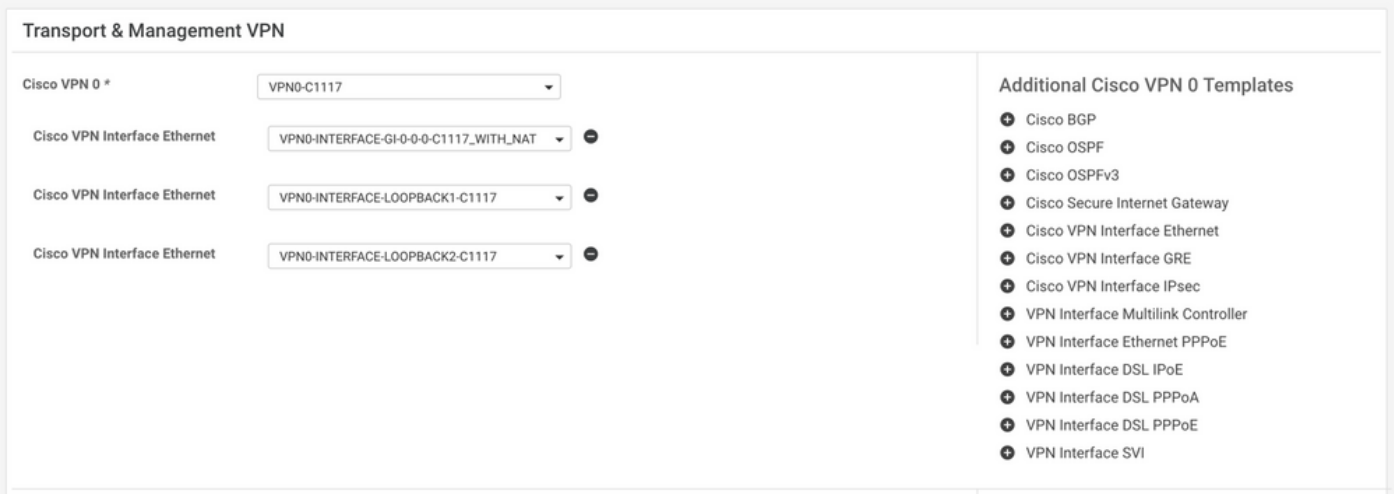
注意：此场景为Active/Active，因此创建了两个环回。

配置环回接口的接口名称和IPv4地址。

注意：为环回接口配置的IP地址是虚拟地址。



创建第二个环回模板并将其附加到设备模板。设备模板必须附加两个环回模板：

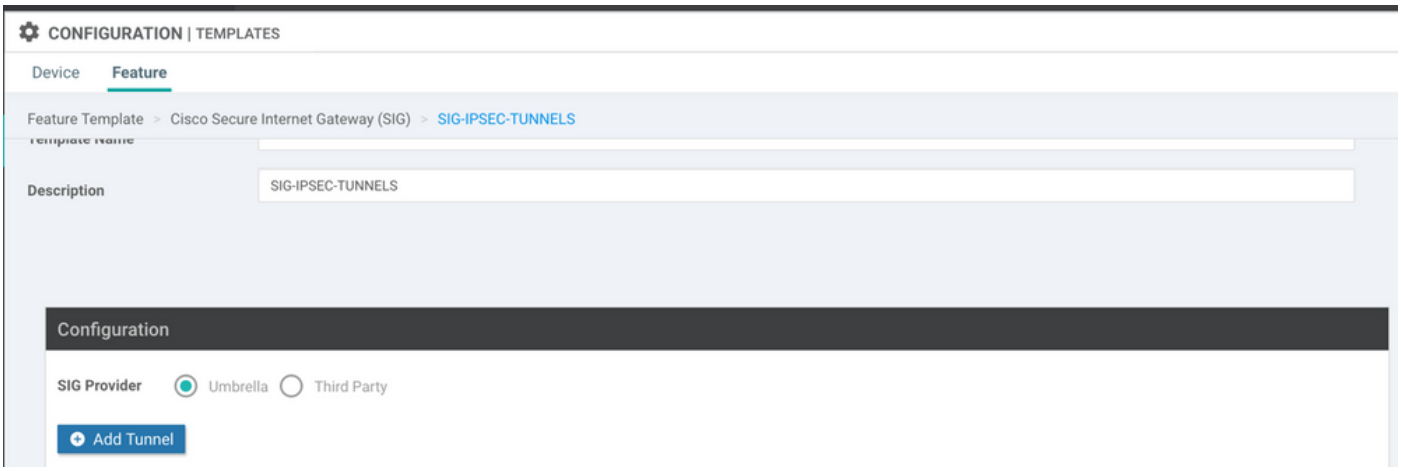


第三步：创建SIG功能模板。

导航至SIG功能模板，并在部分下方 **Transport & Management VPN** 选择 **Cisco Secure Internet Gateway** 功能模板。

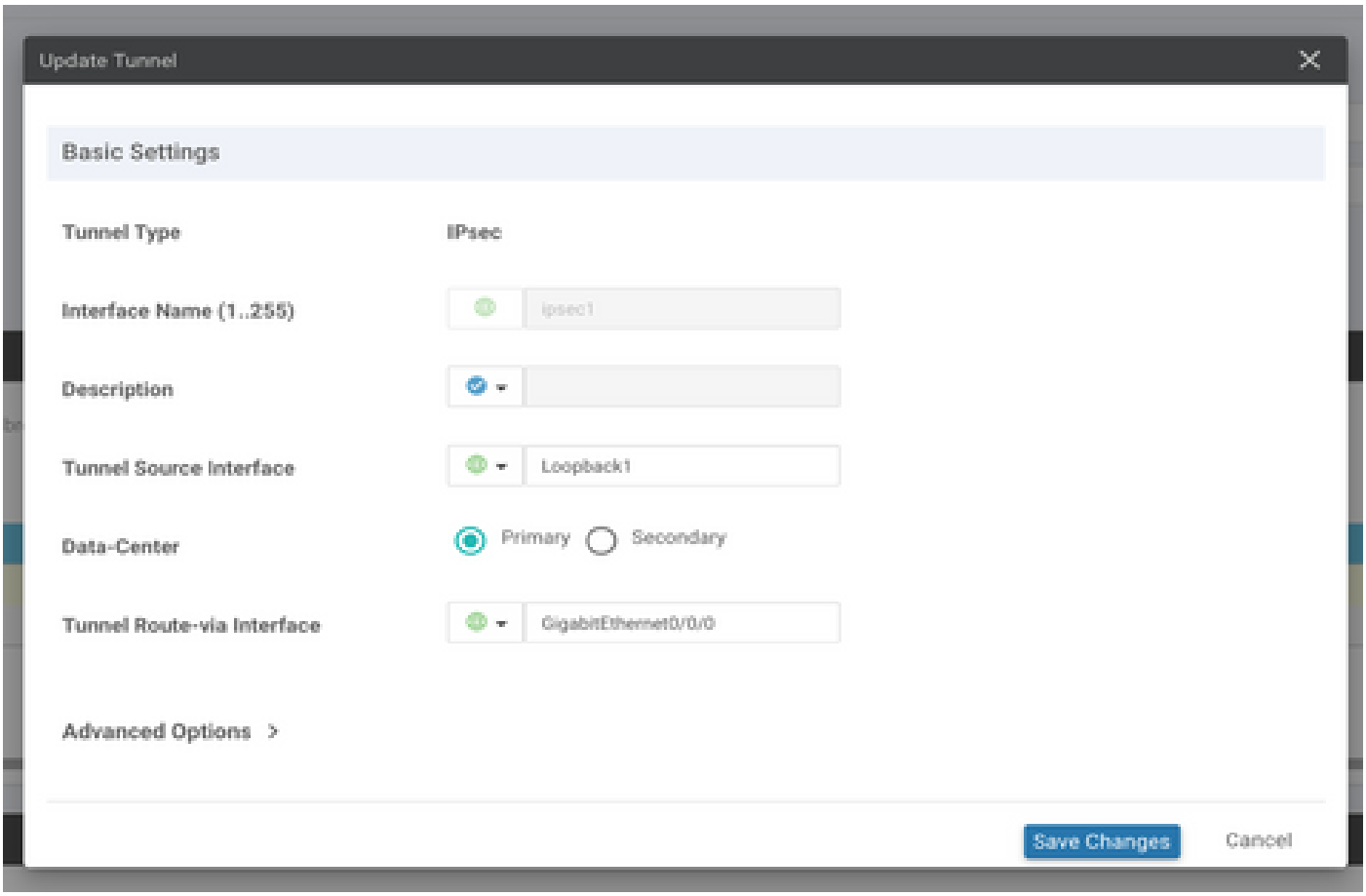
第四步：选择主隧道的SIG提供程序。

点击 **Add Tunnel.**



配置基本详细信息并保留 **Data-Center** 作为 **Primary**.

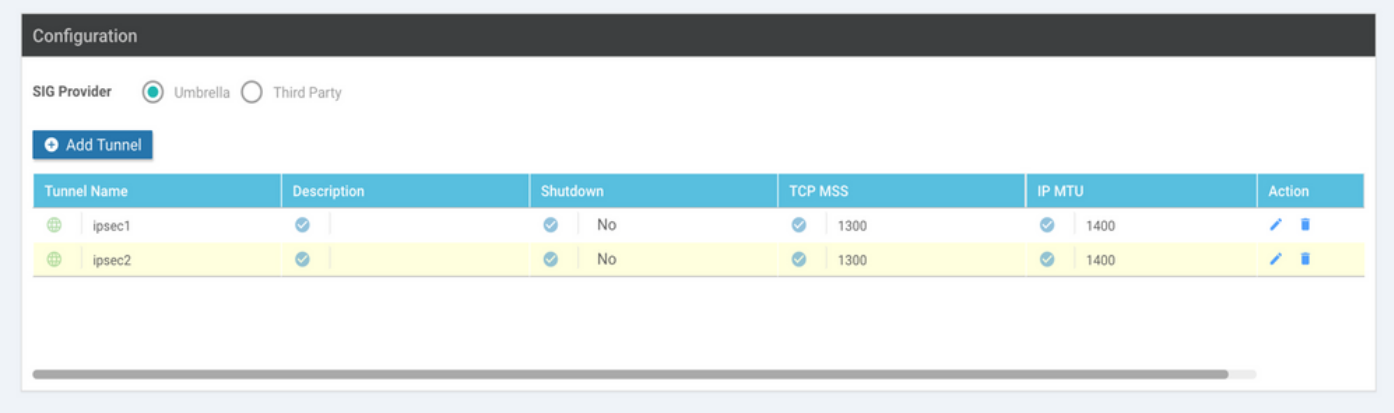
注:Tunnel Source Interface参数是Loopback（对于本文档Loopback1），物理接口作为Tunnel Route-via Interface（对于本文档GigabitEthernet0/0/0）



步骤5.添加辅助隧道。

添加第二个隧道配置，使用 **Data-Center** 作为 **Primary** 以及接口名称ipsec2。

vManage配置如下所示：

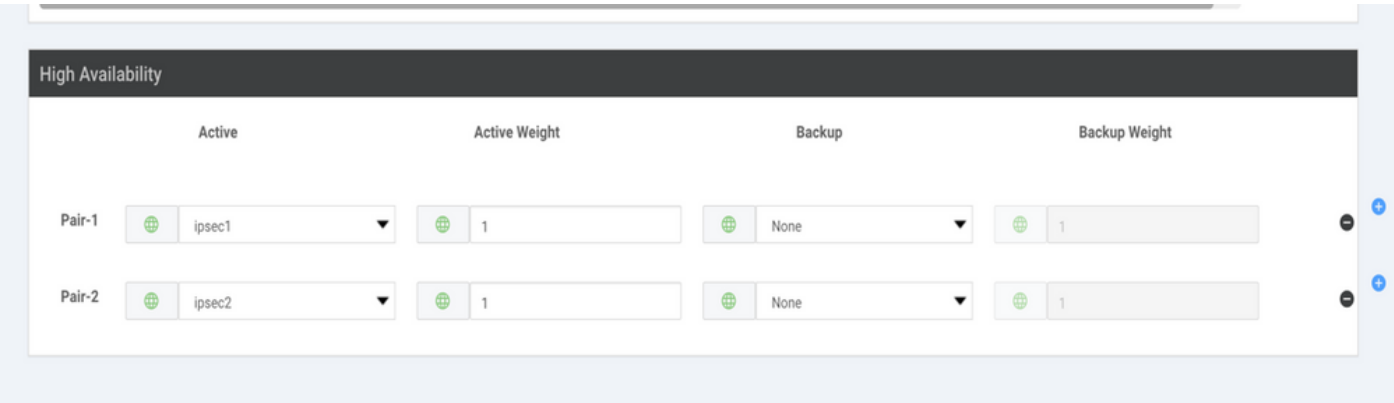


第六步：创建两个高可用性对。

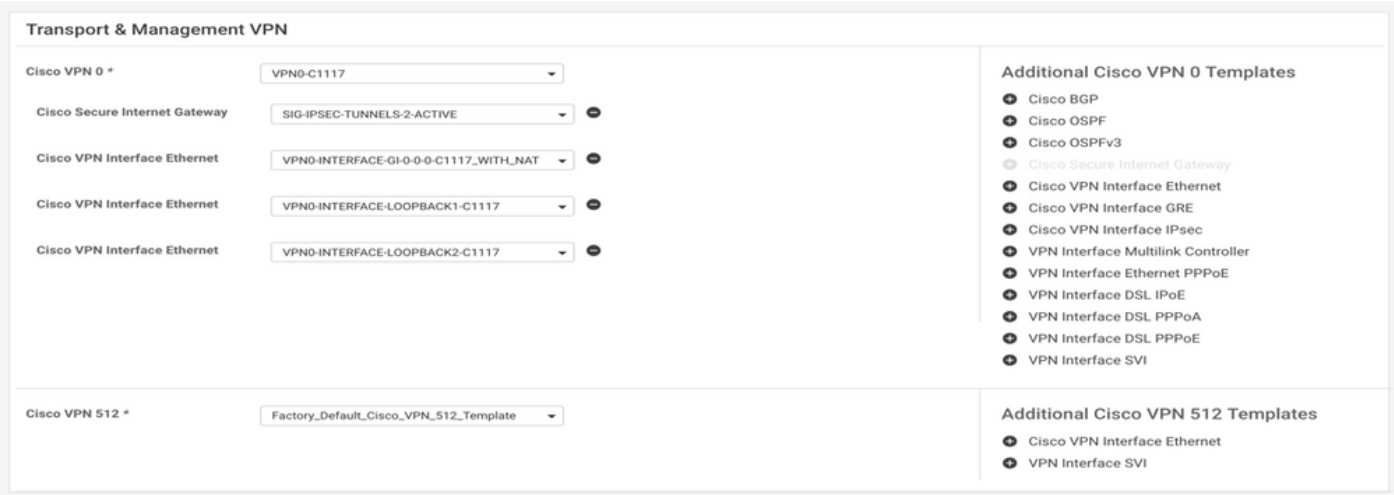
在 **High Availability** 部分，创建两个 **High Availability** 线对。

- 在第一个HA对中，选择ipsec1作为Active，然后选择 **None** 用于备份。
- 在第二个HA对中，选择ipsec2作为活动选择 **None** 和备份。

vManage配置 **High Availability** 如下所示：

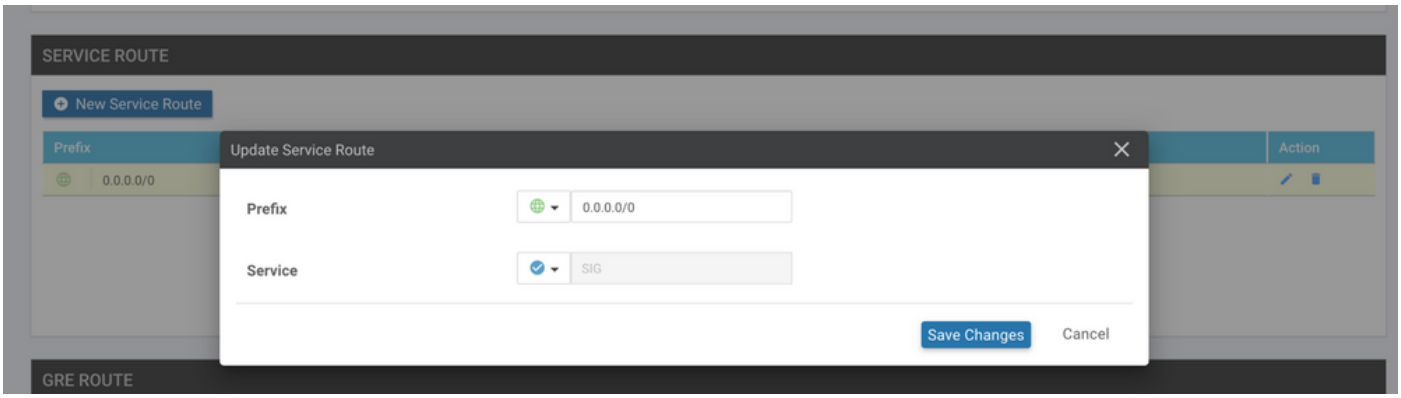


设备模板还附加了两个环回模板和SIG功能模板。



步骤 7.编辑服务端VPN模板以注入服务路由。

导航至 **Service VPN** 部分，并在服务模板的VPN中，导航至 **Service Route** 并添加带SIG的0.0.0.0**Service Route**



此时将显示0.0.0.0 SIG路由，如下所示。

注：要使服务流量实际传出，必须在WAN接口中配置NAT。

将此模板附加到设备并推送配置。

主用/主用场景的WAN边缘路由器配置

```
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
!
```

注意：虽然本文档以Umbrella为重点，但适用于Azure和第三方SIG隧道的方案相同。

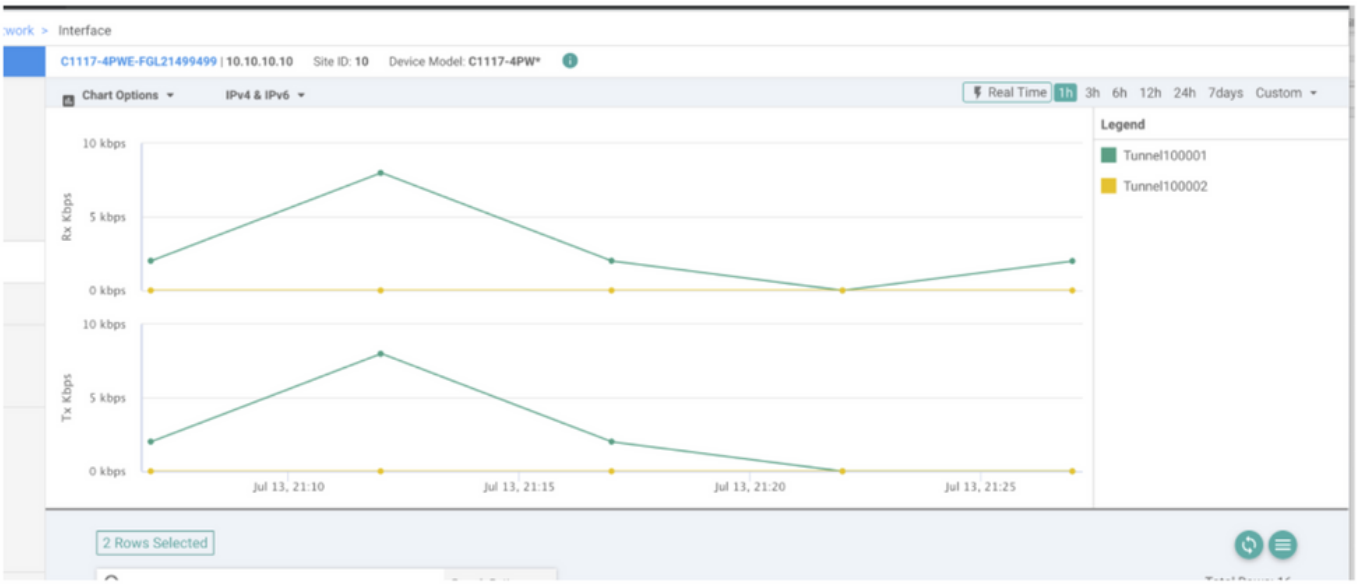
验证

检验活动/备份方案

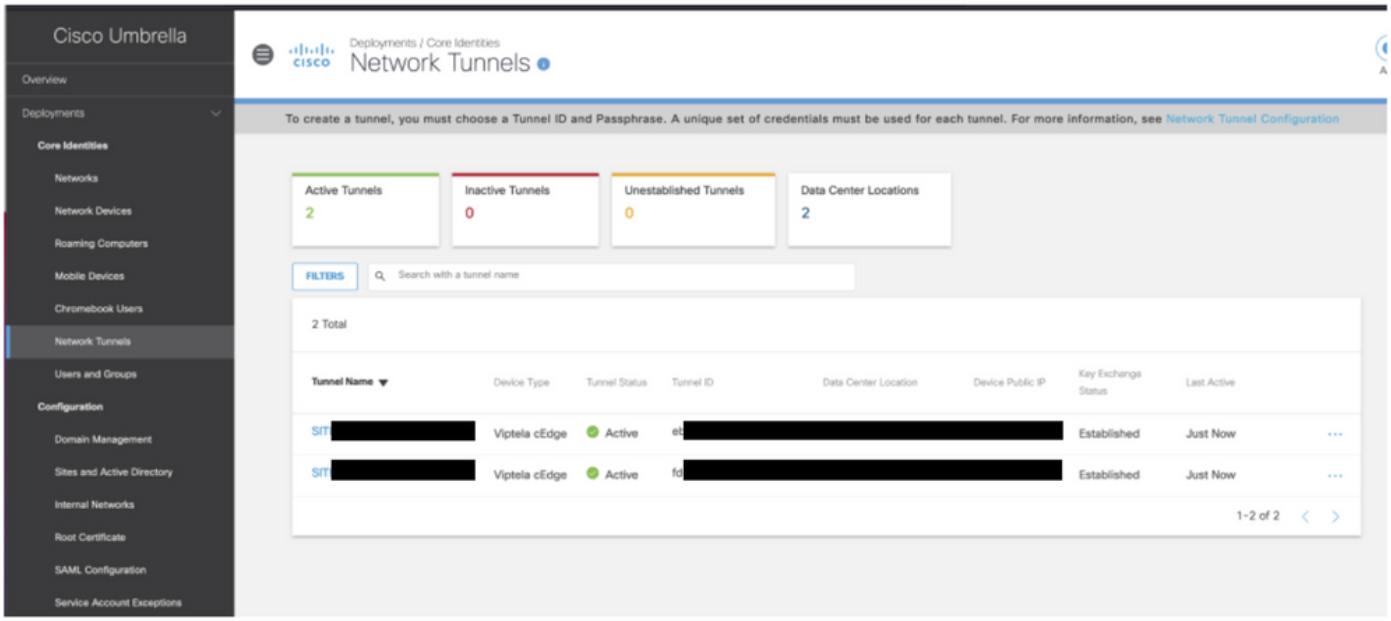
在vManage中，可以监控SIG IPSec隧道的状态。导航至 **Monitor** > **Network,** 选择所需的WAN边缘设备。

单击 **Interfaces** 选项卡；显示设备中所有接口的列表。其中包括ipsec1和ipsec2接口。

该图显示，ipsec1隧道转发所有流量，而ipsec2不传输流量。



也可以验证思科上的隧道 **Umbrella** 门户如图所示。



请使用 **show sdwan secure-internet-gateway tunnels** 命令，以显示隧道信息。

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
                                                                                    API   LAST
TUNNEL IF                                                                           HTTP  SUCCESSFUL
NAME          TUNNEL ID  TUNNEL NAME                          FSM STATE             CODE  REQ
-----------------------------------------------------------------------------------------------------
Tunnel100001  540798313  SITE10SYS10x10x10x10IFTunnel100001  st-tun-create-notif  200   create-tunnel
Tunnel100002  540798314  SITE10SYS10x10x10x10IFTunnel100002  st-tun-create-notif  200   create-tunnel
```

请使用 **show endpoint-tracker** 和 **show ip sla summary** 命令，以显示有关自动生成的跟踪器和SLA的信息。

```
cEdge_Site1_East_01#show endpoint-tracker
Interface              Record Name            Status          RTT in msecs    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      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
```

验证主用/主用方案

在vManage中，可以监控SIG IPSec隧道的状态。导航至 **Monitor** > **Network,** 选择所需的WAN边缘设备。

单击 **Interfaces** 选项卡 — 设备中的所有接口列表都会显示。其中包括ipsec1和ipsec2接口。

该图显示，ipsec1和ipsec2隧道都转发流量。

请使用 **show sdwan secure-internet-gateway tunnels** 命令，以显示隧道信息。

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
                                                                                    API    LAST
TUNNEL IF                                                                            HTTP   SUCCESSFUL
NAME          TUNNEL ID  TUNNEL NAME                          FSM STATE              CODE   REQ
-----------------------------------------------------------------------------------------------------------
Tunnel100001  540798313  SITE10SYS10x10x10x10IFTunnel100001  st-tun-create-notif  200    create-tunnel
Tunnel100002  540798314  SITE10SYS10x10x10x10IFTunnel100002  st-tun-create-notif  200    create-tunnel
```

请使用 **show endpoint-tracker** 和 **show ip sla summary** 命令，以显示有关自动生成的跟踪器和SLA的信息。

```
cEdge_Site1_East_01#show endpoint-tracker
Interface              Record Name            Status          RTT in msecs    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      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
```

相关信息

- 将您的设备与安全的互联网网关集成 — Cisco IOS® XE版本17.x
- http://Network隧道配置 — Umbrella SIG
- Umbrella入门
- 技术支持和文档 - Cisco Systems

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。