為活動/備份或活動/活動方案配置Umbrella SIG隧道

目錄

簡介

本檔案將說明如何設定 **Cisco Umbrella Secure Internet Gateway (SIG)** 兩個中均具有IPsec的隧道 **Active/Active** 和 **Active/Standby**.

必要條件

需求

思科建議瞭解以下主題：

- 思科 **Umbrella**
- IPsec交涉

- 思科軟體定義廣域網路(SD-WAN)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco vManage版本20.4.2
- Cisco WAN邊緣路由器C1117-4PW*版本17.4.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco Umbrella SIG概述

思科 **Umbrella** 是一項雲交付的安全服務，將基本功能整合在一起。

Umbrella 統一安全Web網關、DNS安全、雲交付的防火牆、雲訪問安全代理功能和威脅情報。

深入的檢測和控制，確保符合可接受使用的Web策略，並防範網際網路威脅。

SD-WAN路由器可以與安全網際網路網關(SIG)整合，後者執行大部分處理以保護企業流量。

設定SIG後，所有基於路由或策略的客戶端流量都會轉發到SIG。

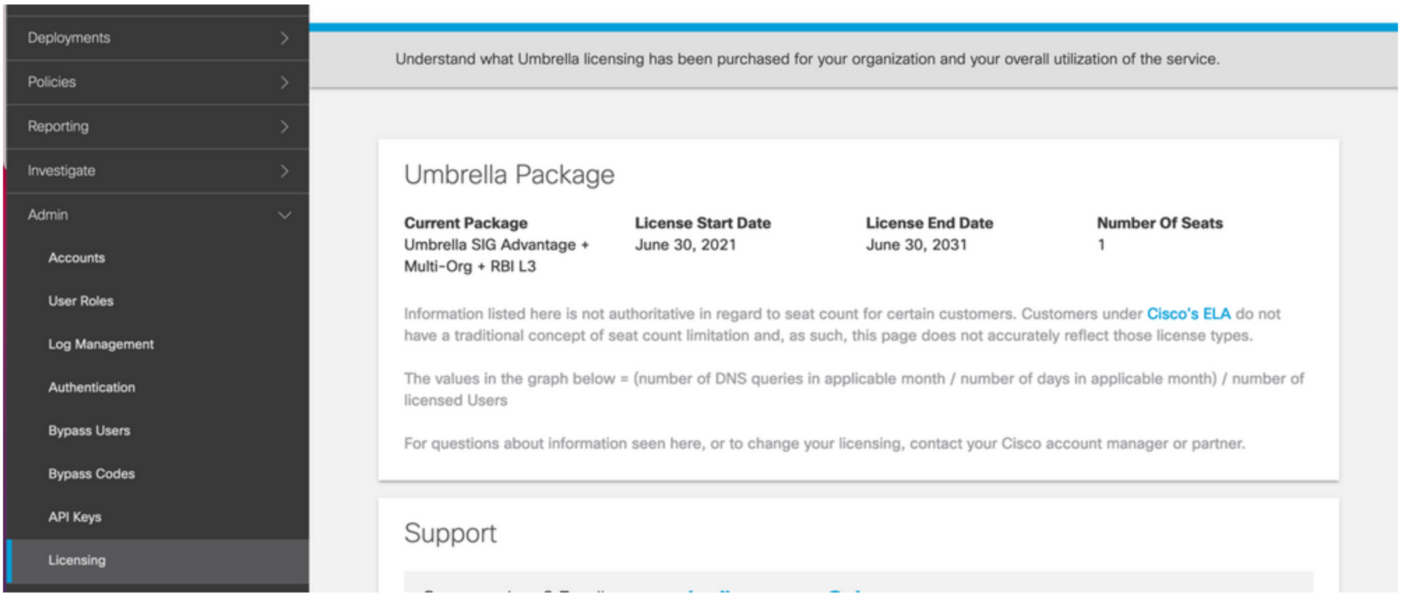
Umbrella SIG通道頻寬限制

到每個IPsec IKEv2隧道 **Umbrella** 頭端限製為大約250 Mbps，因此如果建立了多個隧道並對流量進行負載均衡，則它們可以克服此類限制，以防需要更高的頻寬。

最多四個 **High Availability** 可以建立隧道對。

獲取您的Cisco Umbrella門戶資訊

為了繼續實施SIG整合， **Umbrella** 需要具有SIG基本版包的帳戶。



Understand what Umbrella licensing has been purchased for your organization and your overall utilization of the service.

Umbrella Package

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

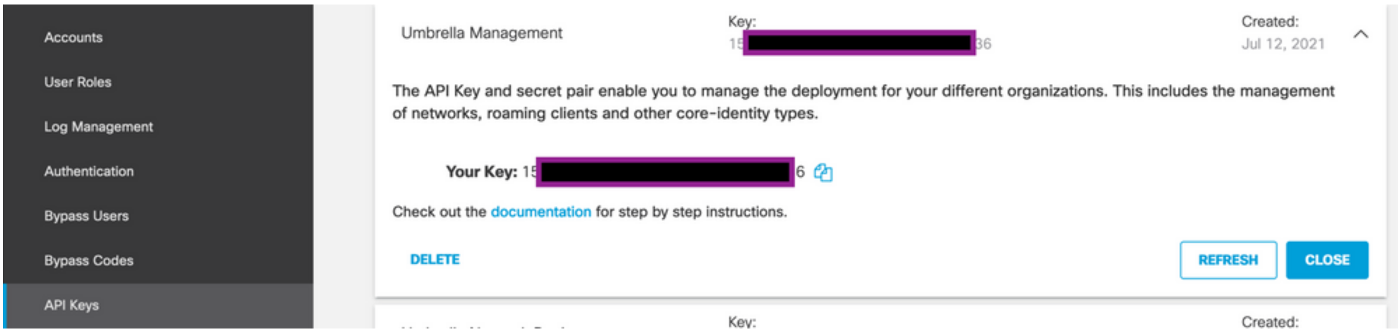
For questions about information seen here, or to change your licensing, contact your Cisco account manager or partner.

Support

獲取金鑰和金鑰

金鑰和金鑰可以在您獲得 Umbrella Management API KEY （此金鑰位於「Legacy Keys」下）。如果您不記得或沒有儲存金鑰，請按一下refresh。

⚠ 注意：如果按一下了刷新按鈕，則需要對所有裝置上的這些鍵進行更新，如果存在正在使用的裝置，則不建議進行更新。



Umbrella Management

Key: [redacted]

Created: Jul 12, 2021

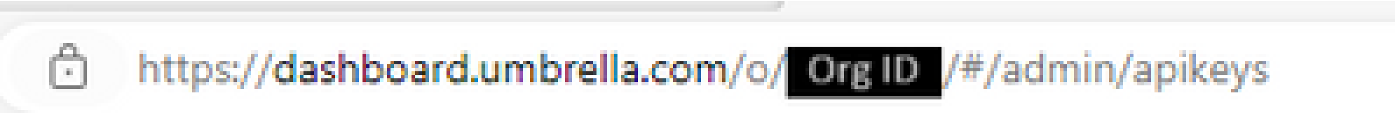
The API Key and secret pair enable you to manage the deployment for your different organizations. This includes the management of networks, roaming clients and other core-identity types.

Your Key: [redacted]

Check out the documentation for step by step instructions.

獲取您的組織ID

當您登入時，可以輕鬆獲取組織ID Umbrella 從瀏覽器位址列中。



https://dashboard.umbrella.com/o/ Org ID /#/admin/apikeys

使用活動/備份方案建立Umbrella SIG隧道

✎ 註：使用ECMP的IPsec/GRE通道路由和負載平衡：此功能在vManage 20.4.1及更高版本中可用，它允許您使用SIG模板將應用流量引導至Cisco Umbrella 或第三方SIG提供商

註：支援Zscaler自動調配：此功能在vManage 20.5.1及更高版本上可用，它使用Zscaler合作夥伴API憑證自動調配從Cisco SD-WAN路由器到Zscaler的隧道。

要配置SIG自動隧道，需要建立/更新幾個模板：

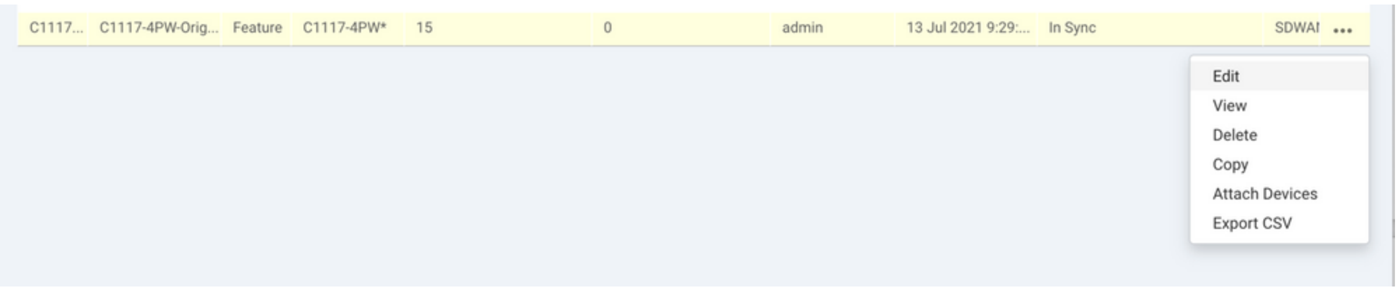
- 建立SIG憑證功能模板。
- 建立兩個回送介面以連結SIG通道（僅適用於多個通道） **Active** 同時使用通道 — **Active/Active** 場景)。
- 建立SIG功能模板。
- 編輯服務端VPN模板以插入 **Service Route**.

注意：確保允許來自任何上游裝置的UDP 4500和500埠。

模板配置會隨的 **Active/Backup** 和 **Active/Active** 兩種情景分別予以解釋和展示的情景。

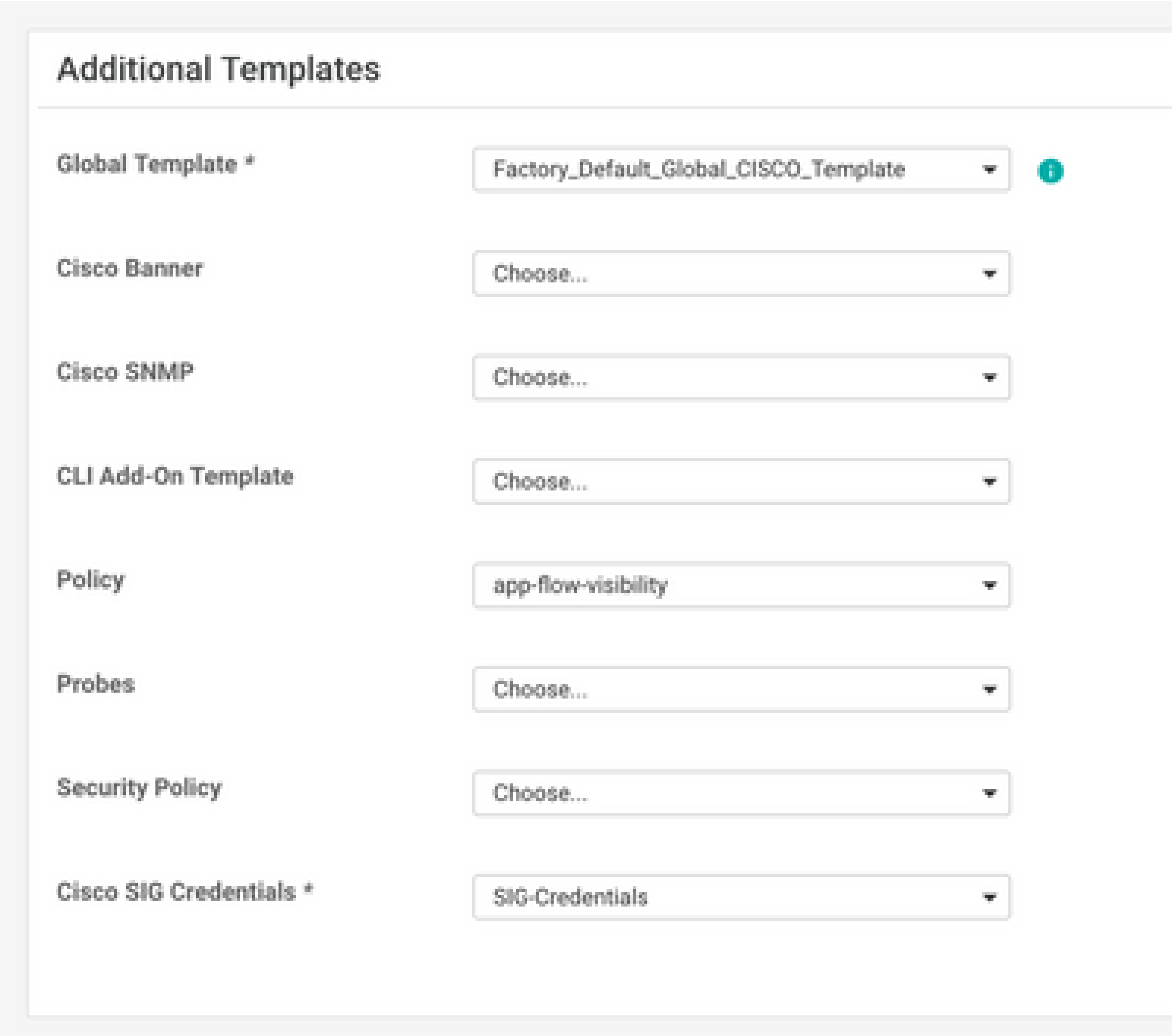
步驟 1.建立SIG憑證功能模板。

轉到功能模板並按一下 **Edit.**



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

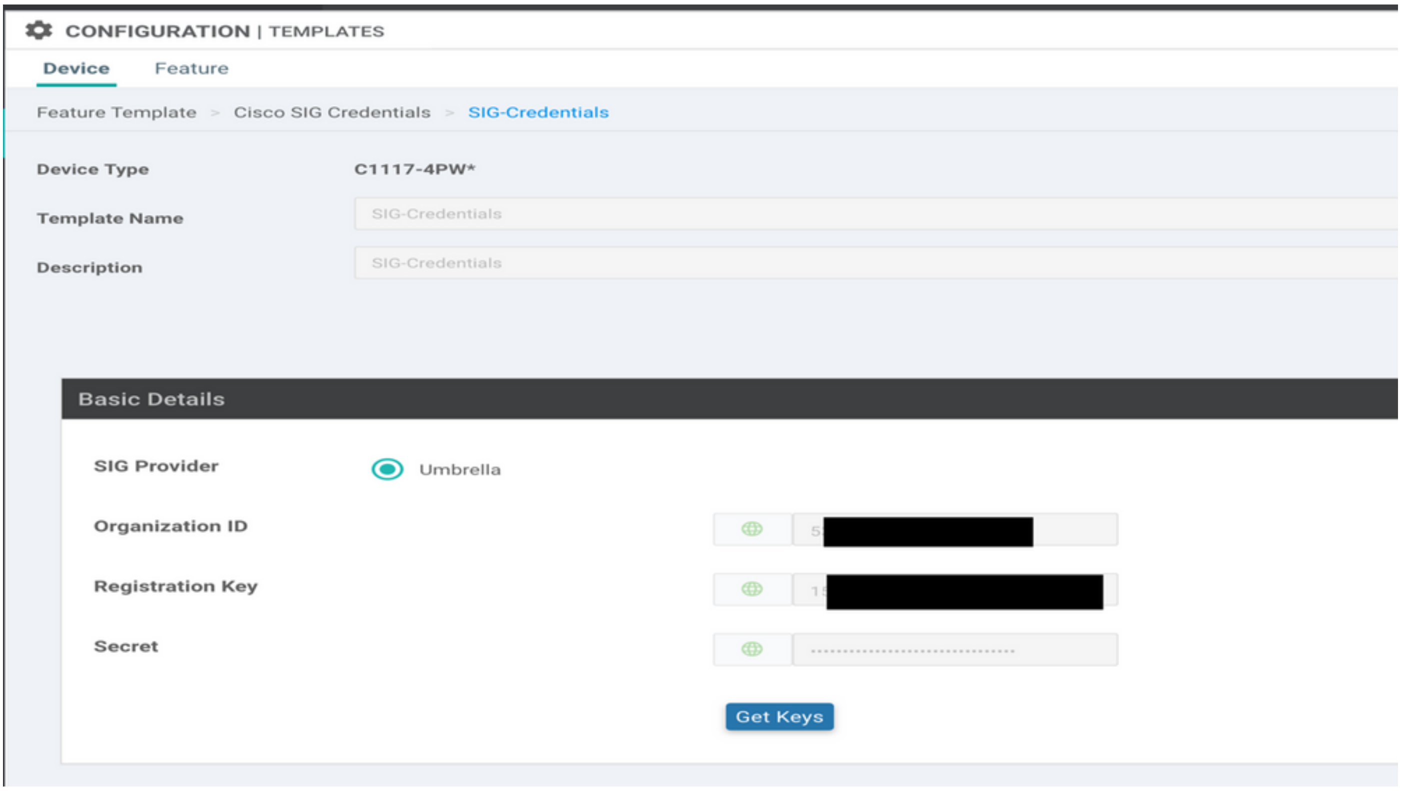
在 **Additional templates** ，按一下 **Cisco SIG Credentials.**該選項如下圖所示。



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

為模板提供名稱和說明。


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]

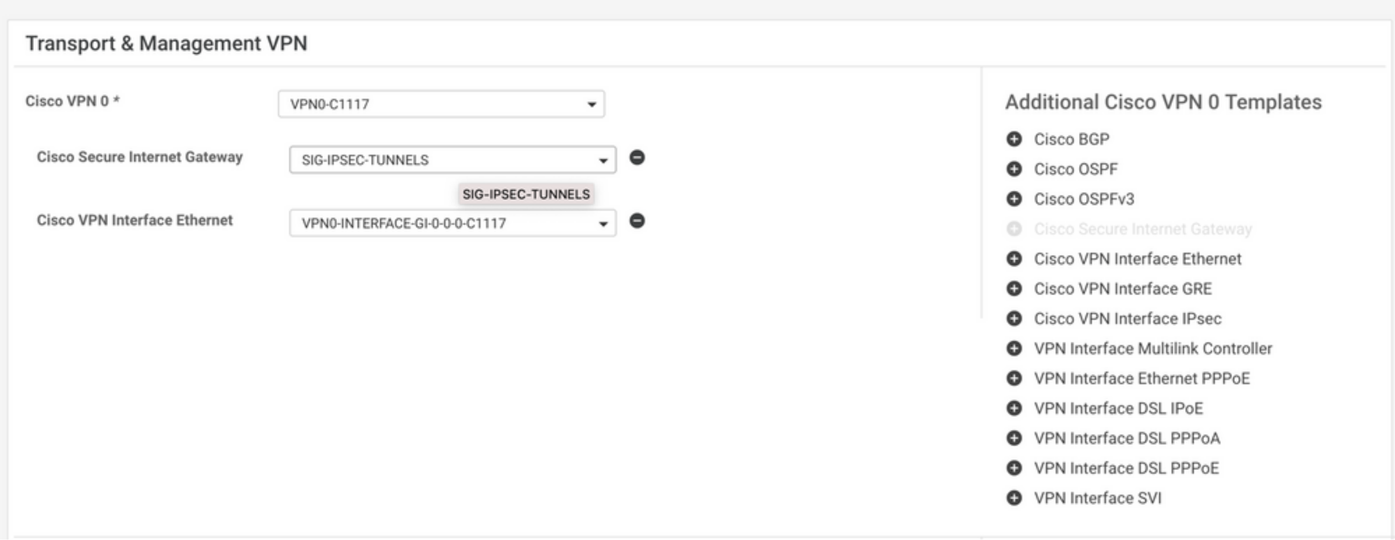
Registration Key: [redacted]

Secret: ································

Get Keys

步驟 2.建立SIG功能模板。

導航到功能模板，並在部分下方 **Transport & Management VPN** 選擇Cisco Secure Internet Gateway功能模板。


Transport & Management VPN

Cisco VPN 0 *: VPN0-C1117

Cisco Secure Internet Gateway: SIG-IPSEC-TUNNELS

SIG-IPSEC-TUNNELS

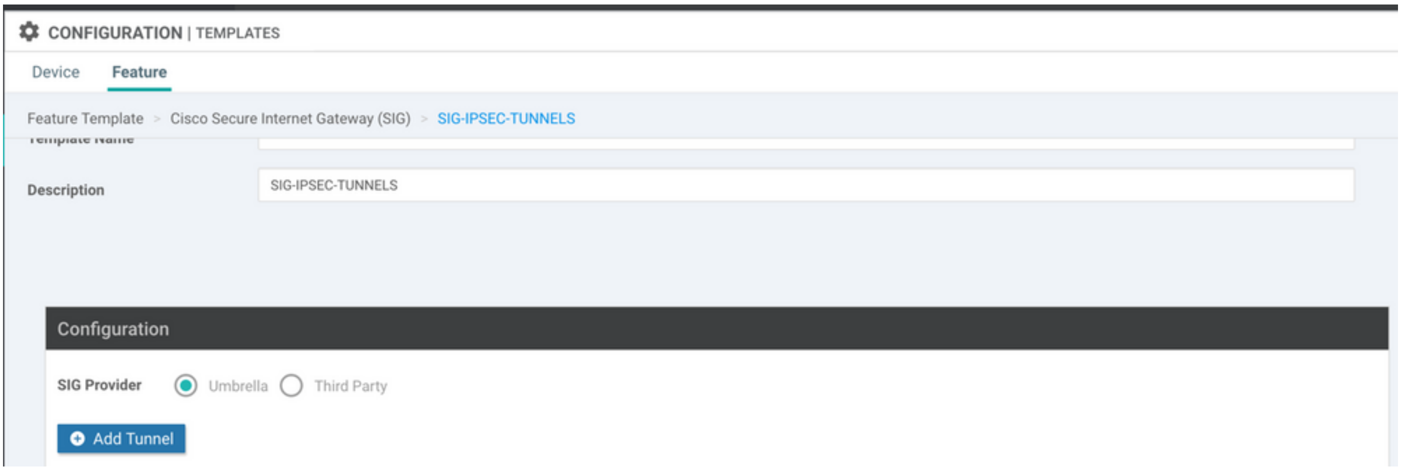
Cisco VPN Interface Ethernet: VPN0-INTERFACE-GI-0-0-0-C1117

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

為模板提供名稱和說明。

步驟 3.選擇主隧道的SIG提供商。

按一下 **Add Tunnel.**



CONFIGURATION | TEMPLATES

Device Feature

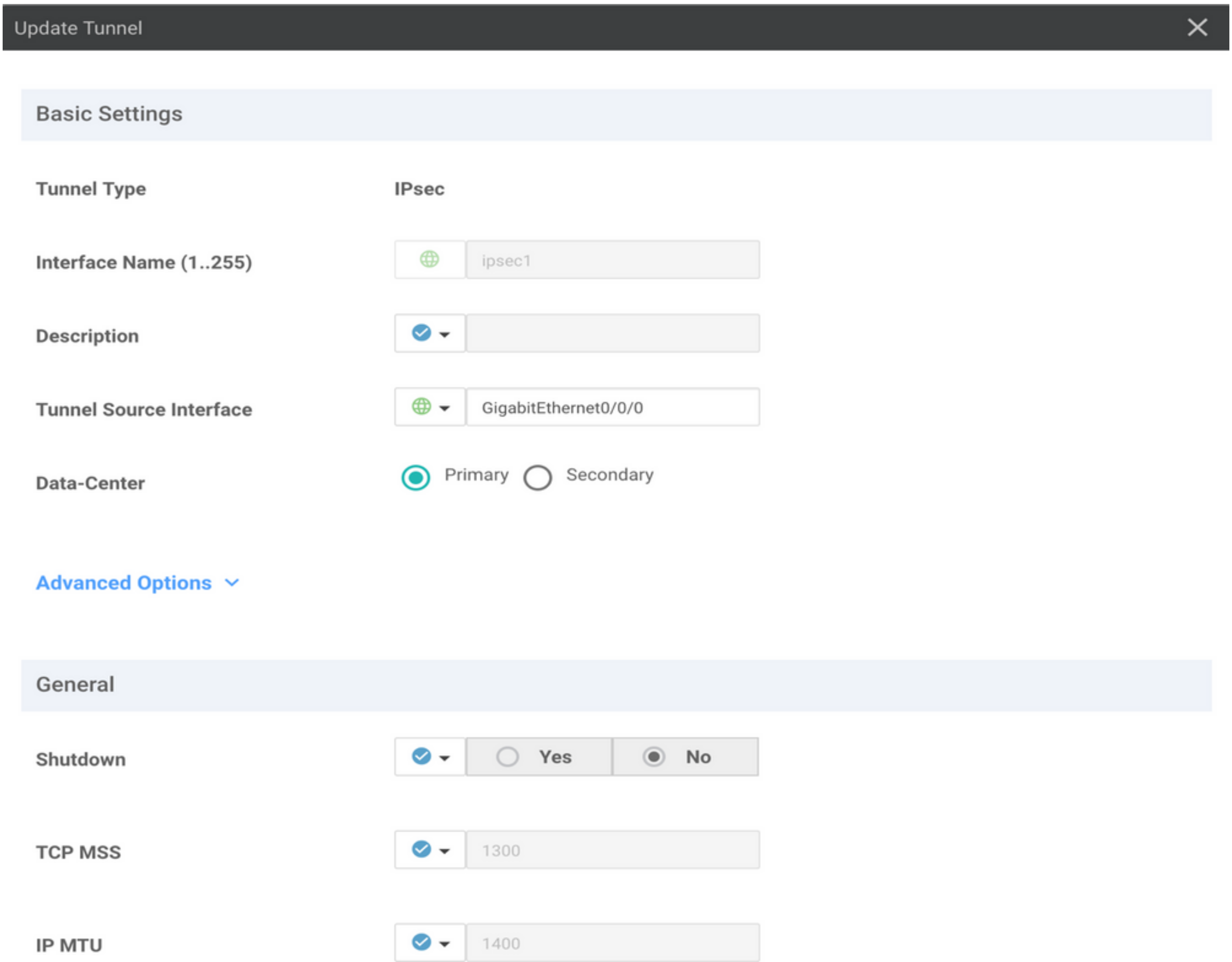
Feature Template > Cisco Secure Internet Gateway (SIG) > SIG-IPSEC-TUNNELS

Description: SIG-IPSEC-TUNNELS

Configuration

SIG Provider ● Umbrella ○ Third Party

配置基本詳細資訊並保留 **Data-Center** 作為 **Primary**，然後按一下 **Add.**



Update Tunnel

Basic Settings

Tunnel Type: IPsec

Interface Name (1..255): ipsec1

Description:

Tunnel Source Interface: GigabitEthernet0/0/0

Data-Center ● Primary ○ Secondary

General

Shutdown ○ Yes ● No

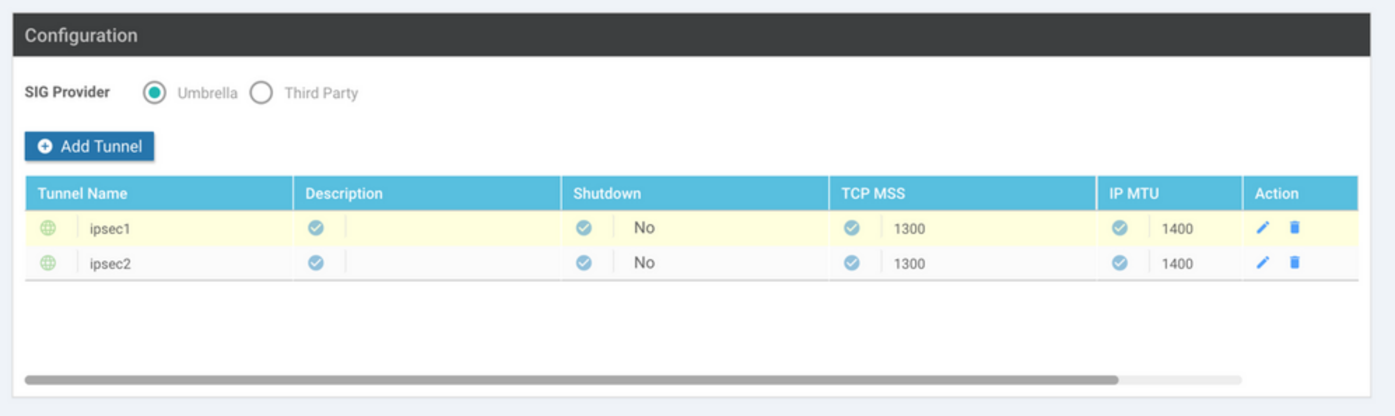
TCP MSS: 1300

IP MTU: 1400

步驟4.新增輔助隧道。

新增第二個隧道配置，使用 **Data-Center** 作為 **Secondary** 這一次，並將介面名稱命名為ipsec2。

vManage配置如下所示：



Configuration

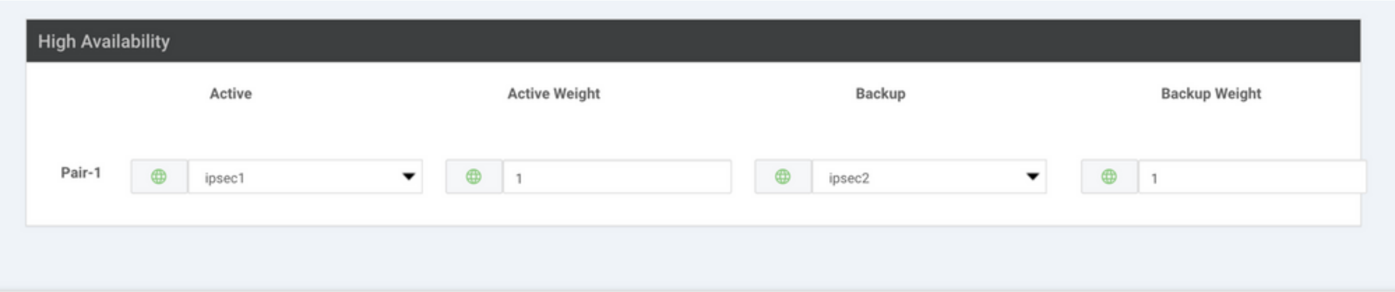
SIG Provider ● Umbrella ○ Third Party

Add Tunnel

Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1	✓	✓ No	✓ 1300	✓ 1400	✎ 🗑
ipsec2	✓	✓ No	✓ 1300	✓ 1400	✎ 🗑

步驟 5.建立一個高可用性對。

在 **High Availability** 部分，選擇ipsec1作為Active，選擇ipsec2隧道作為Backup。



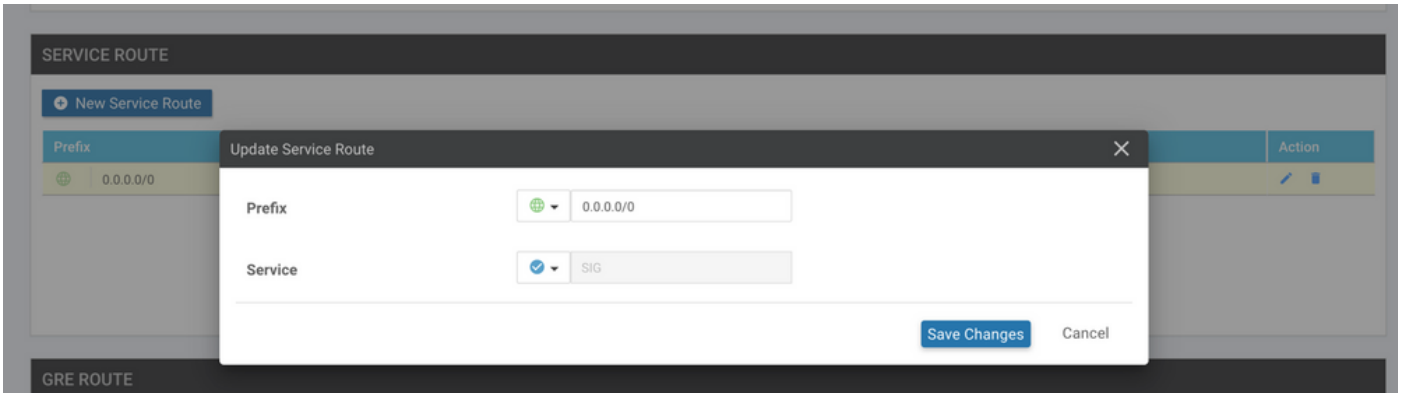
High Availability

	Active	Active Weight	Backup	Backup Weight
Pair-1	ipsec1	1	ipsec2	1

註：最多4個 **High Availability** 可以同時建立隧道對和最多4個活動隧道。

步驟 6.編輯服務端VPN模板以插入服務路由。

導航至 **Service VPN** 部分和，在 **Service VPN** 模板，導航到相應部分 **Service Route** 並新增0.0.0.0和SIG **Service Route**.本文檔使用VRF/VPN 10。



SERVICE ROUTE

New Service Route

Prefix	Action
0.0.0.0/0	✎ 🗑

Update Service Route

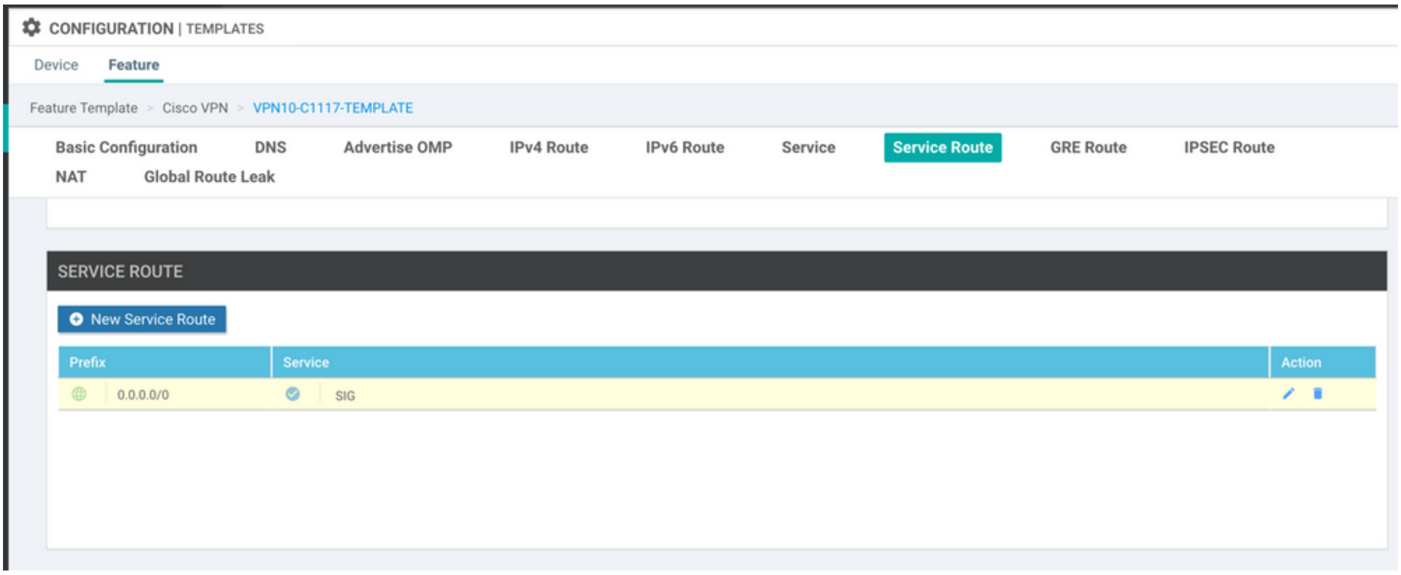
Prefix: 0.0.0.0/0

Service: SIG

Save Changes   Cancel

GRE ROUTE

0.0.0.0 SIG路由顯示，如下所示。


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

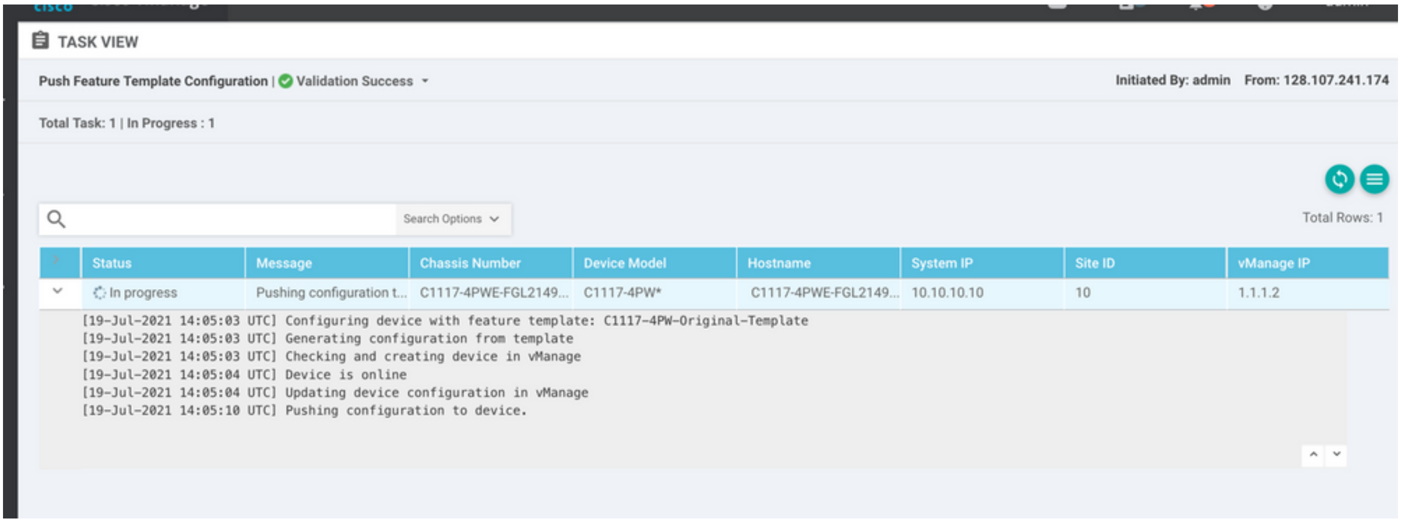
SERVICE ROUTE

New Service Route

Prefix	Service	Action
0.0.0.0/0	SIG	

註：要使服務流量實際出去，必須在WAN介面中配置NAT。

將此模板連線到裝置並推送配置：


TASK VIEW

Push Feature Template Configuration | Validation Success

Initiated By: admin From: 128.107.241.174

Total Task: 1 | In Progress : 1

Search Options

Total Rows: 1

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.
```

活動/備份方案的WAN邊緣路由器配置

```
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
```

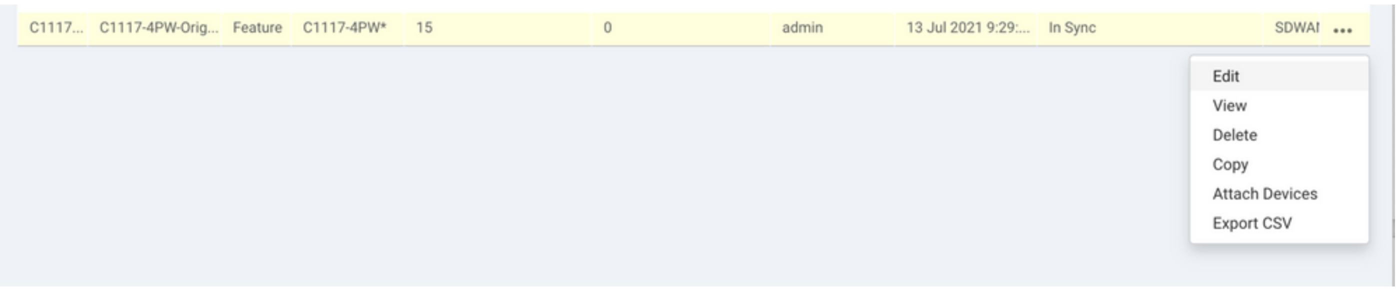
```
  route-target export 1:10
  route-target import 1:10
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 description Transport VPN
 rd          1:512
 address-family ipv4
  route-target export 1:512
  route-target import 1:512
  exit-address-family
 !
 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
```

使用活動/活動方案建立Umbrella SIG隧道

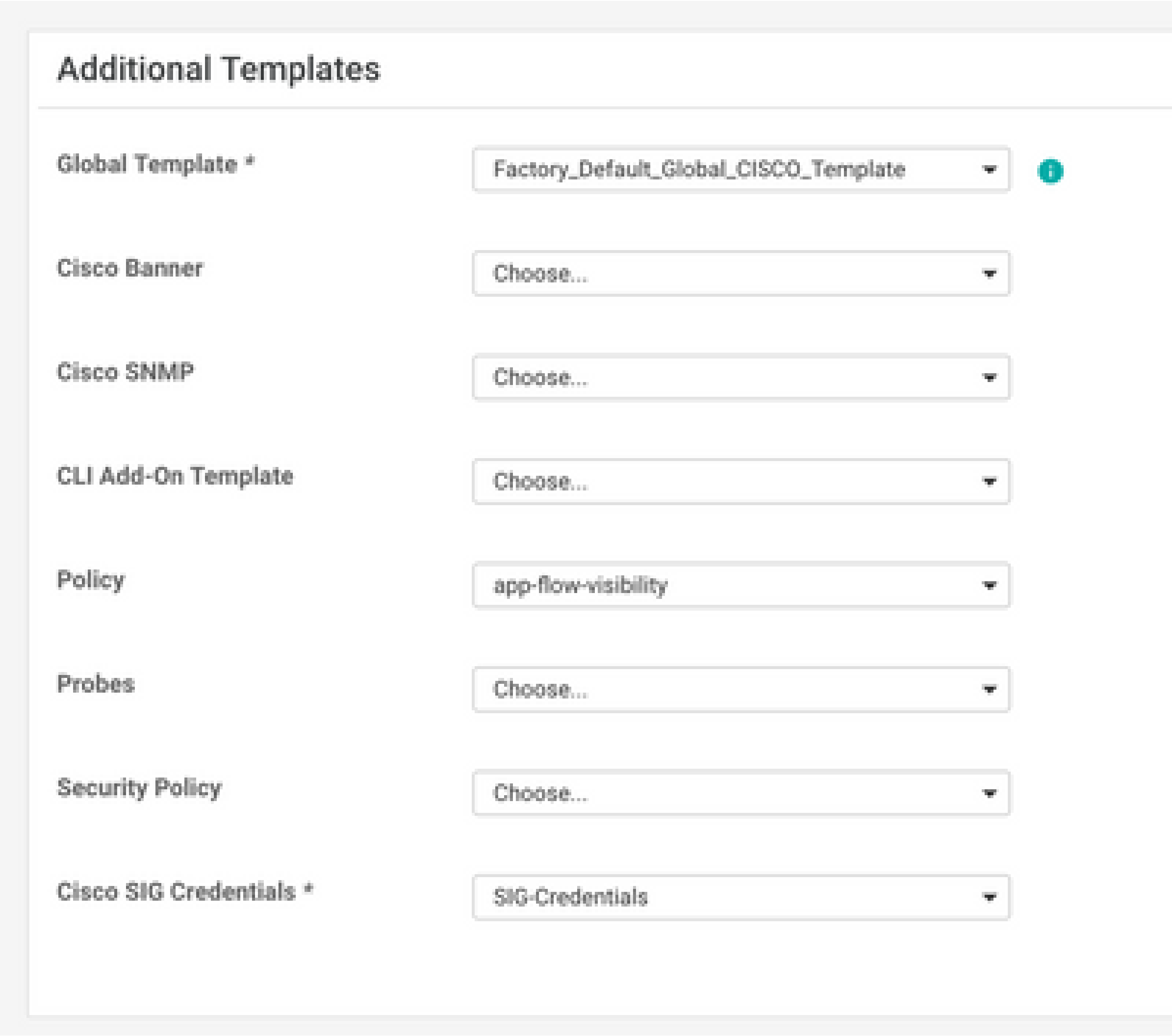
步驟 1.建立SIG憑證功能模板。

導航到功能模板並按一下 **Edit**



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

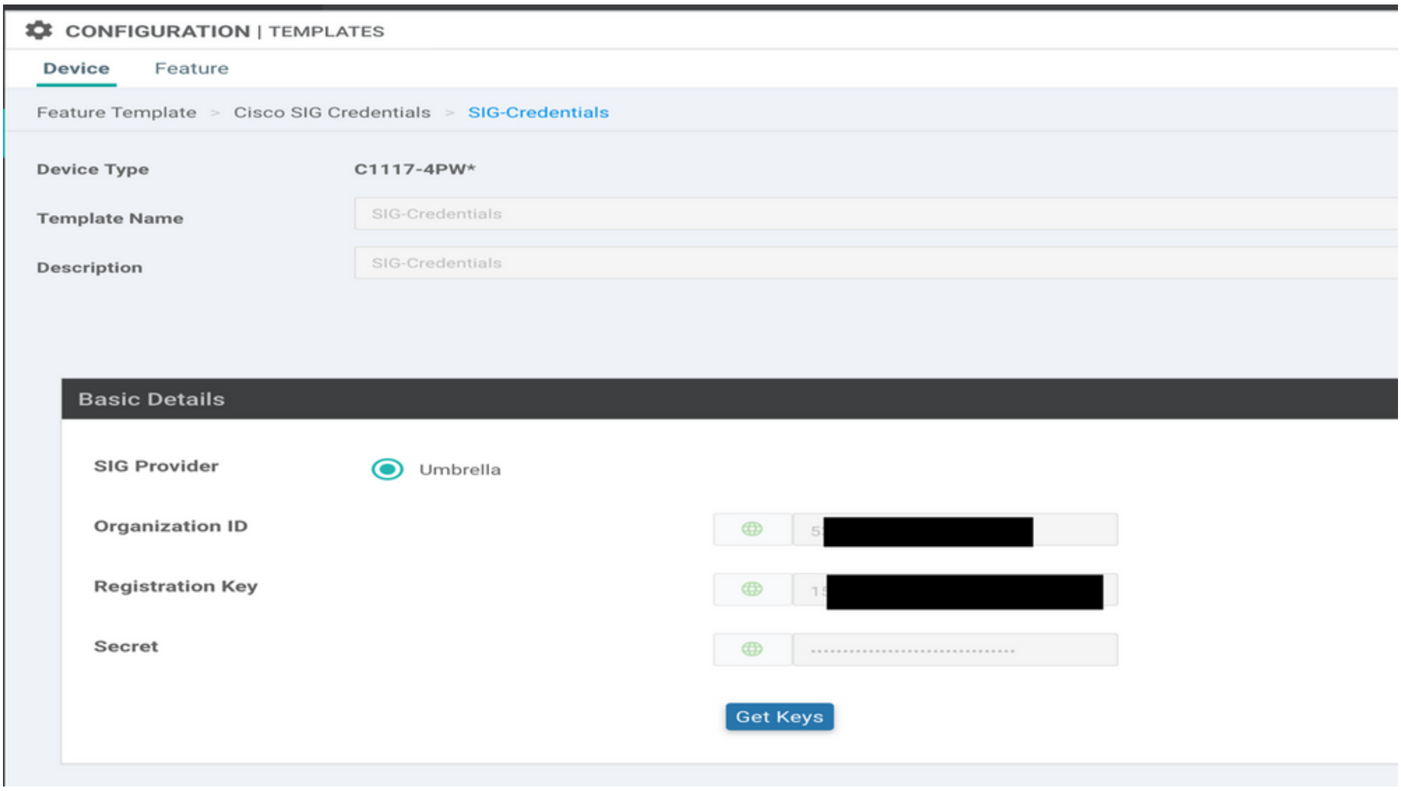
在 **Additional templates**，選擇 **Cisco SIG Credentials.**選項如下圖所示。



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

為模板提供名稱和說明。



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 ....

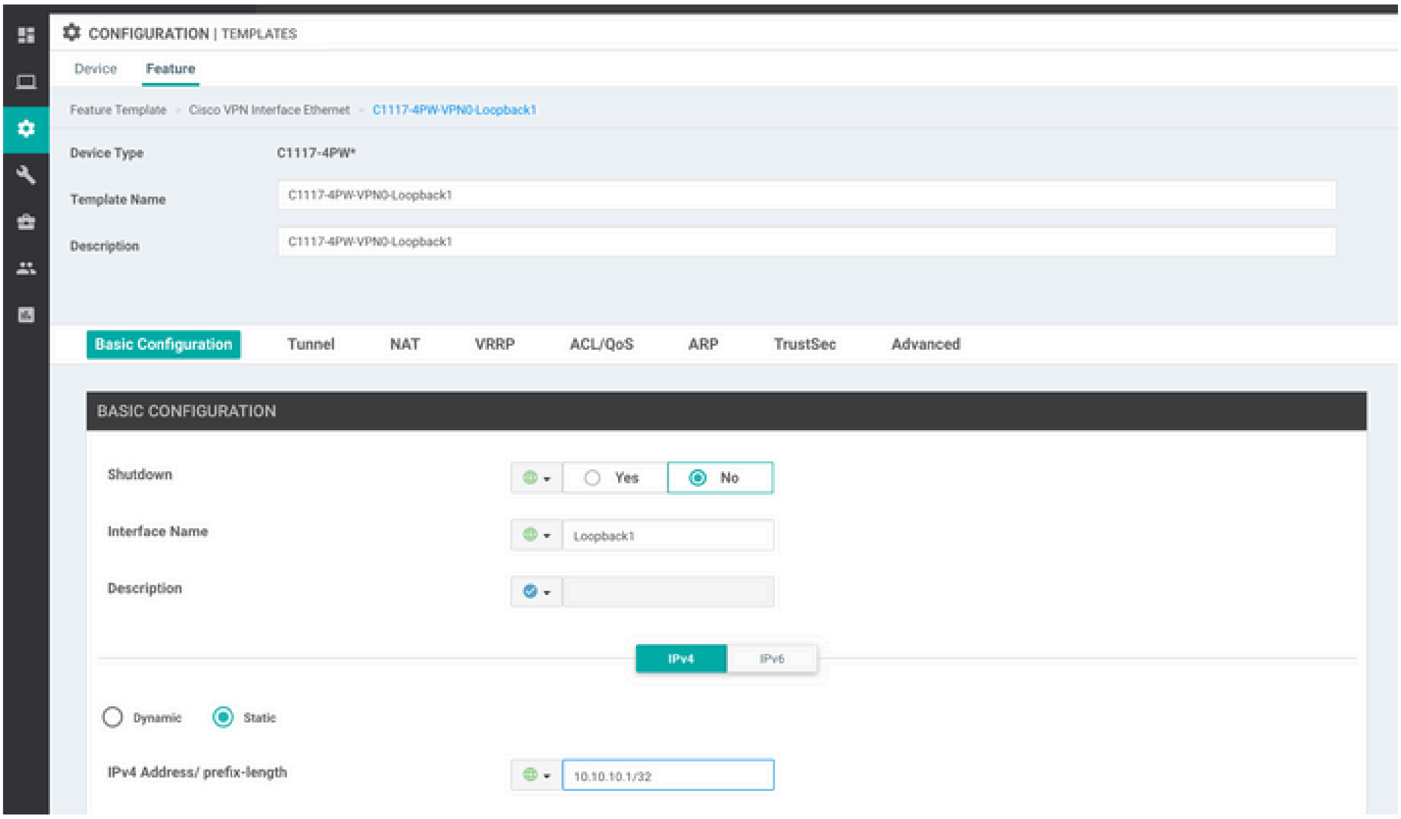
步驟 2.建立兩個環回介面以連結SIG隧道。

注意：為以活動模式配置的每個SIG隧道建立環回介面，因為每個隧道都需要唯一的IKE ID，所以需要這樣做。

注意：此方案為活動/活動，因此建立了兩個環回。

為環回配置介面名稱和IPv4地址。

注意：為環回配置的IP地址是一個虛擬地址。



Feature Template > Cisco VPN Interface Ethernet > C1117-4PW-VPN0-Loopback1

Device Type	C1117-4PW*
Template Name	C1117-4PW-VPN0-Loopback1
Description	C1117-4PW-VPN0-Loopback1

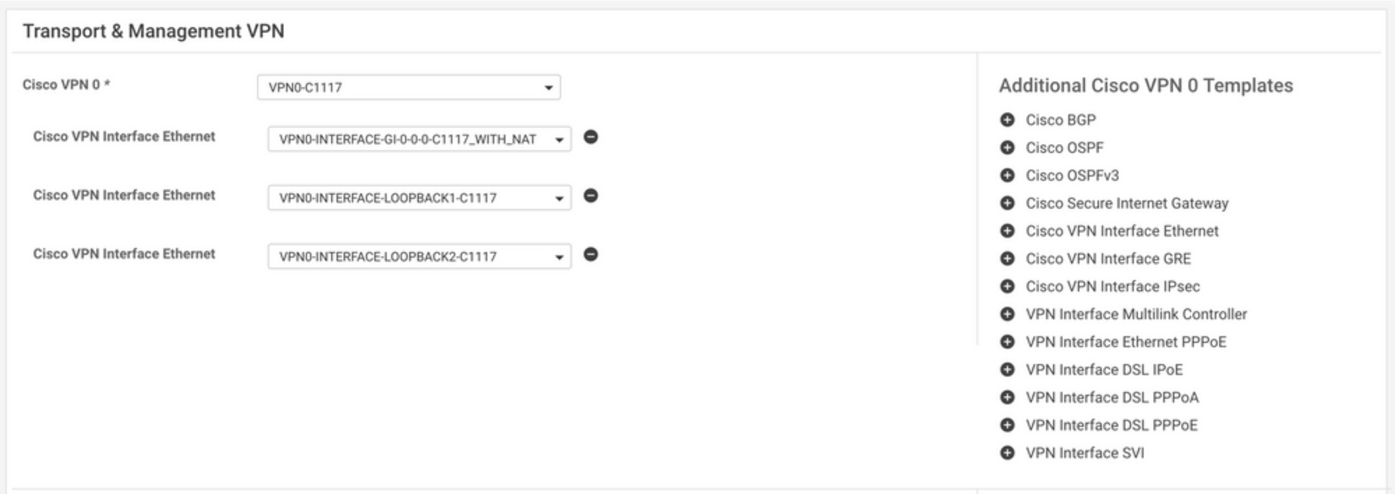
BASIC CONFIGURATION

Shutdown	○ Yes ● No
Interface Name	Loopback1
Description	

○ Dynamic ● Static

IPv4 Address/ prefix-length: 10.10.10.1/32

建立第二個環回模板並將其連線到裝置模板。裝置模板必須附加兩個環回模板：



Transport & Management VPN

Cisco VPN 0 *	VPN0-C1117
Cisco VPN Interface Ethernet	VPN0-INTERFACE-GI-0-0-0-C1117_WITH_NAT
Cisco VPN Interface Ethernet	VPN0-INTERFACE-LOOPBACK1-C1117
Cisco VPN Interface Ethernet	VPN0-INTERFACE-LOOPBACK2-C1117

Additional Cisco VPN 0 Templates

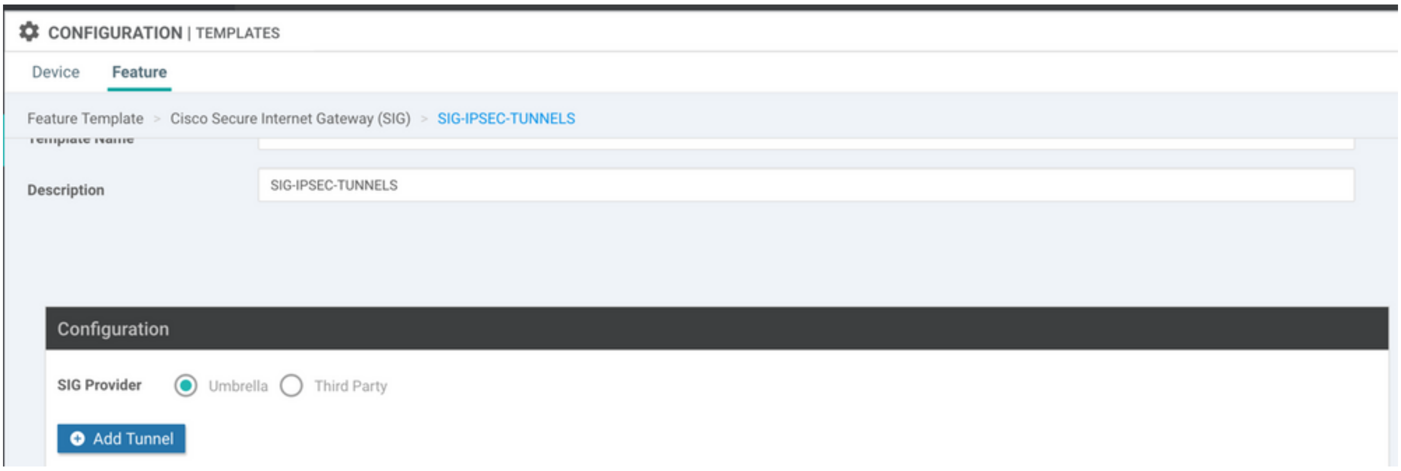
- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco Secure Internet Gateway
- Cisco VPN Interface Ethernet
- Cisco VPN Interface GRE
- Cisco VPN Interface IPsec
- VPN Interface Multilink Controller
- VPN Interface Ethernet PPPoE
- VPN Interface DSL IPoE
- VPN Interface DSL PPPoA
- VPN Interface DSL PPPoE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

步驟 3.建立SIG功能模板。

導航至SIG功能模板，並在部分下方 **Transport & Management VPN** 選擇 **Cisco Secure Internet Gateway** 功能模板。

步驟 4.選擇主隧道的SIG提供程式。

按一下 **Add Tunnel.**



CONFIGURATION | TEMPLATES

Device Feature

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

Description: SIG-IPSEC-TUNNELS

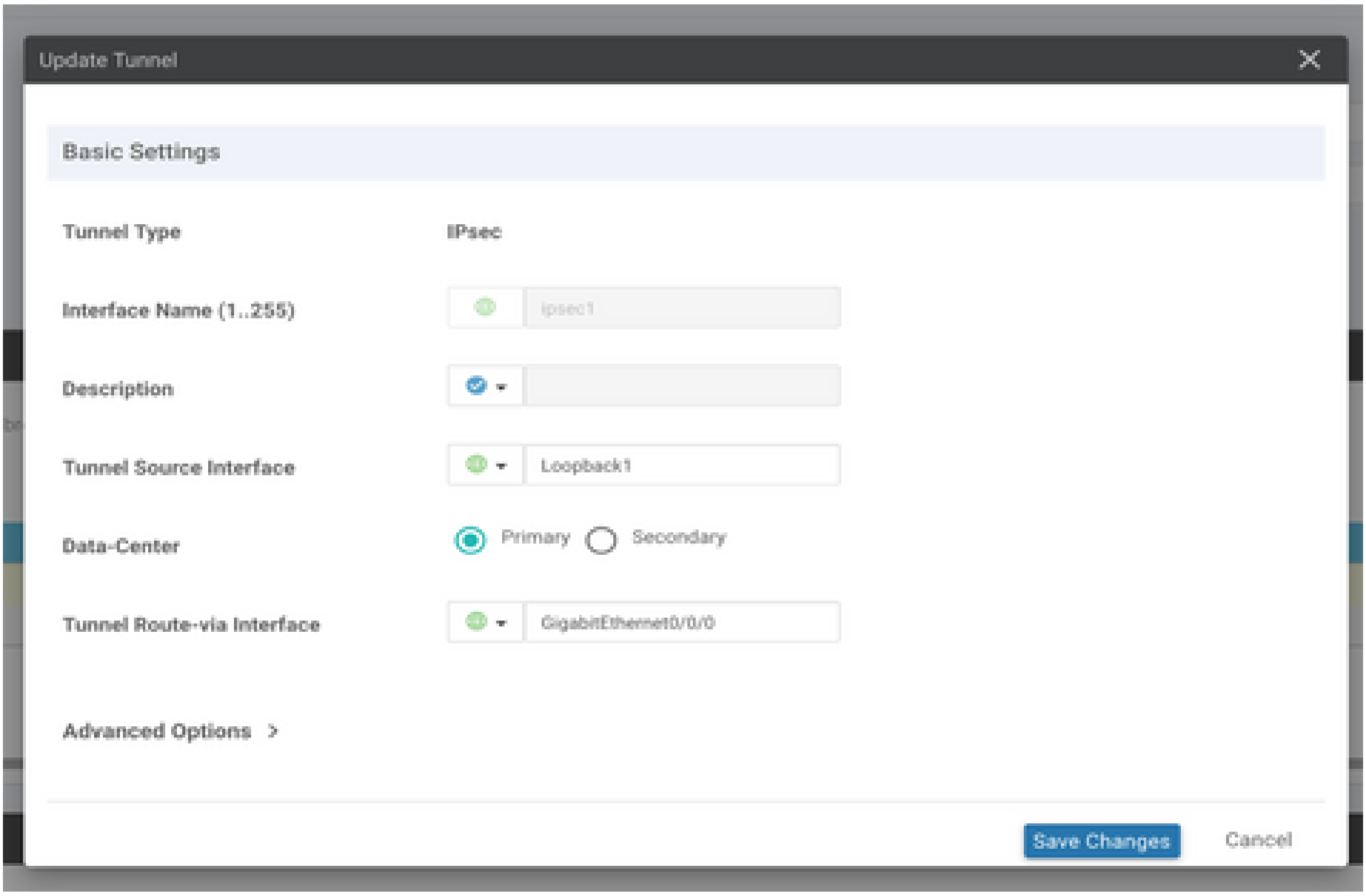
Configuration

SIG Provider ● Umbrella ○ Third Party

Add Tunnel

配置基本詳細資訊並保留 **Data-Center** 作為 **Primary.**

註: Tunnel Source Interface引數是Loopback（對於本文檔為Loopback1）以及物理介面（對於本文檔為GigabitEthernet0/0/0）作為Tunnel Route-via Interface



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

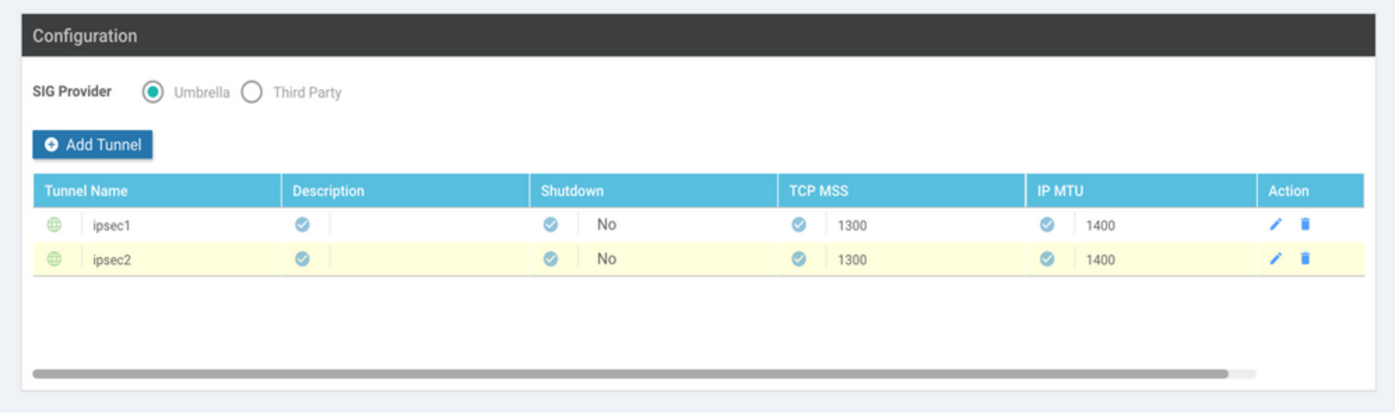
Advanced Options >

Save Changes Cancel

步驟5.新增輔助通道。

新增第二個隧道配置，使用 **Data-Center** 作為 **Primary** 以及介面名稱ipsec2。

vManage配置如下所示：



Configuration

SIG Provider ● Umbrella ○ Third Party

Add Tunnel

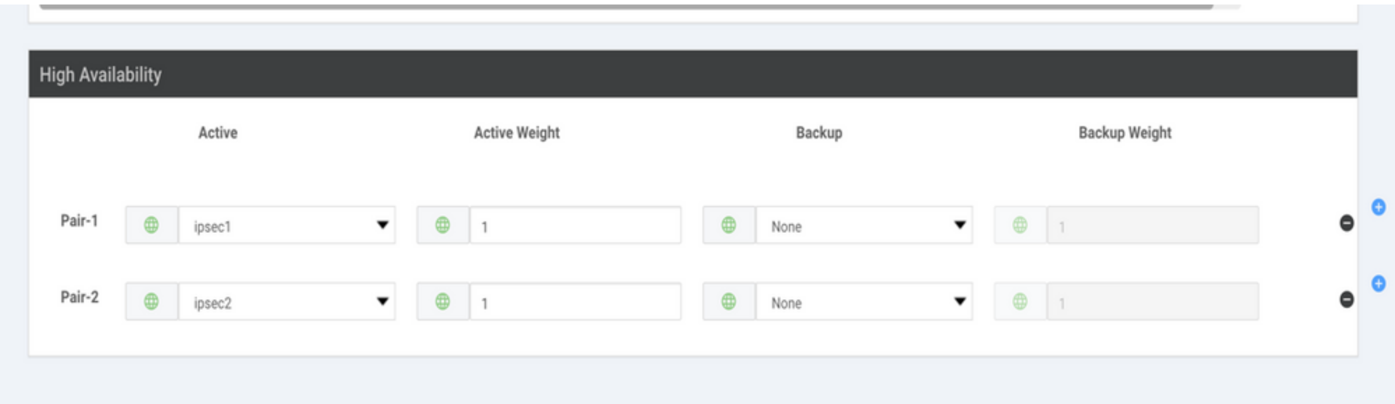
Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		No	1300	1400	
ipsec2		No	1300	1400	

步驟 6.建立兩個高可用性對。

在 **High Availability** 部分，建立兩個 **High Availability** 配對。

- 在第一個HA對中，選擇ipsec1作為活動，然後選擇 **None** 作為後援。
- 在第二個HA配對中，選擇ipsec2作為活動選擇 **None** 和備用的。

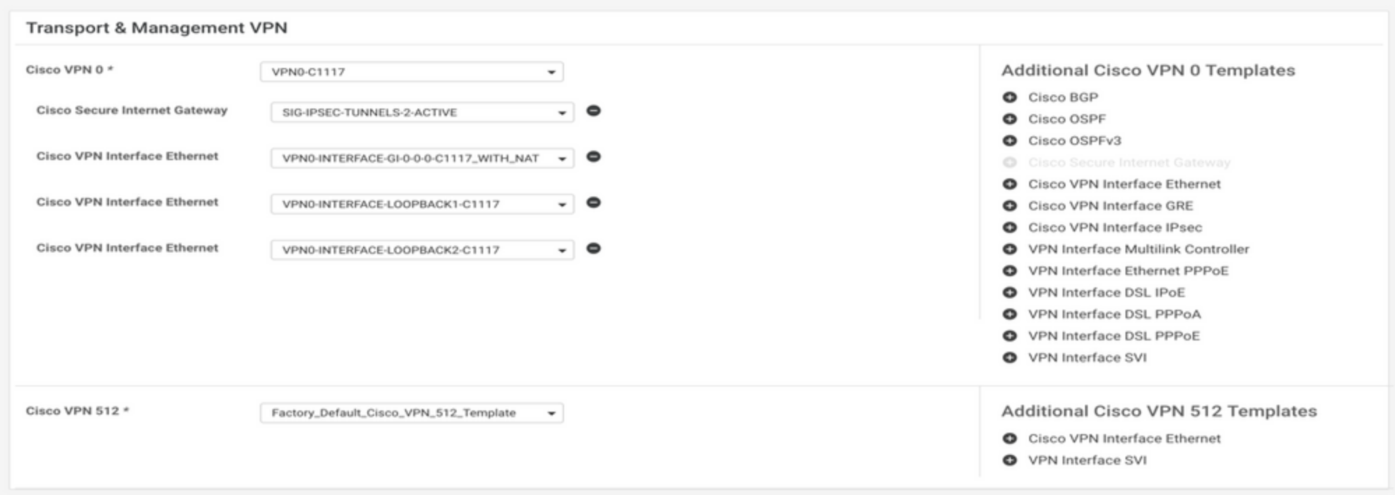
vManage配置 **High Availability** 如下所示顯示：



High Availability

	Active	Active Weight	Backup	Backup Weight
Pair-1	ipsec1	1	None	1
Pair-2	ipsec2	1	None	1

裝置模板還附加了兩個環回模板和SIG功能模板。



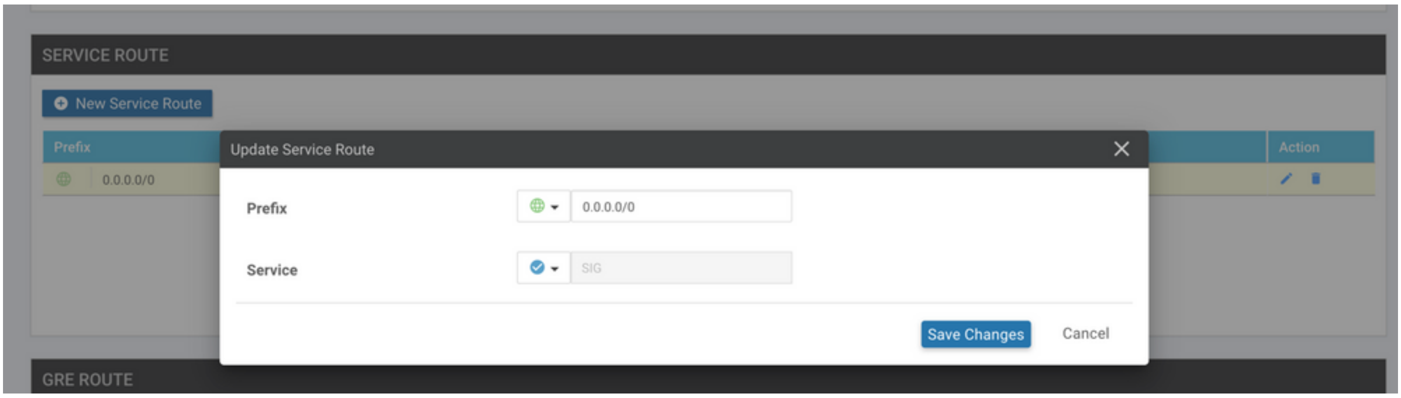
Transport & Management VPN

Cisco VPN 0 *	VPN0-C1117
Cisco Secure Internet Gateway	SIG-IPSEC-TUNNELS-2-ACTIVE
Cisco VPN Interface Ethernet	VPN0-INTERFACE-GI-0-0-0-C1117_WITH_NAT
Cisco VPN Interface Ethernet	VPN0-INTERFACE-LOOPBACK1-C1117
Cisco VPN Interface Ethernet	VPN0-INTERFACE-LOOPBACK2-C1117
Cisco VPN 512 *	Factory_Default_Cisco_VPN_512_Template

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
Additional Cisco VPN 512 Templates
Cisco VPN Interface Ethernet
VPN Interface SVI

步驟 7.編輯服務端VPN模板以插入服務路由。

導航至 Service VPN 部分，在服務VPN模板中，導航到部分 Service Route 並新增0.0.0.0和SIGService Route



Prefix: 0.0.0.0/0

Service: SIG

此時會顯示0.0.0.0 SIG路由，如下所示。

註：要使服務流量實際出去，必須在WAN介面中配置NAT。

將此模板連線到裝置並推送配置。

主用/主用方案的WAN邊緣路由器配置

```
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：雖然此文檔以Umbrella為重點，但適用於Azure和第三方SIG隧道的方案相同。

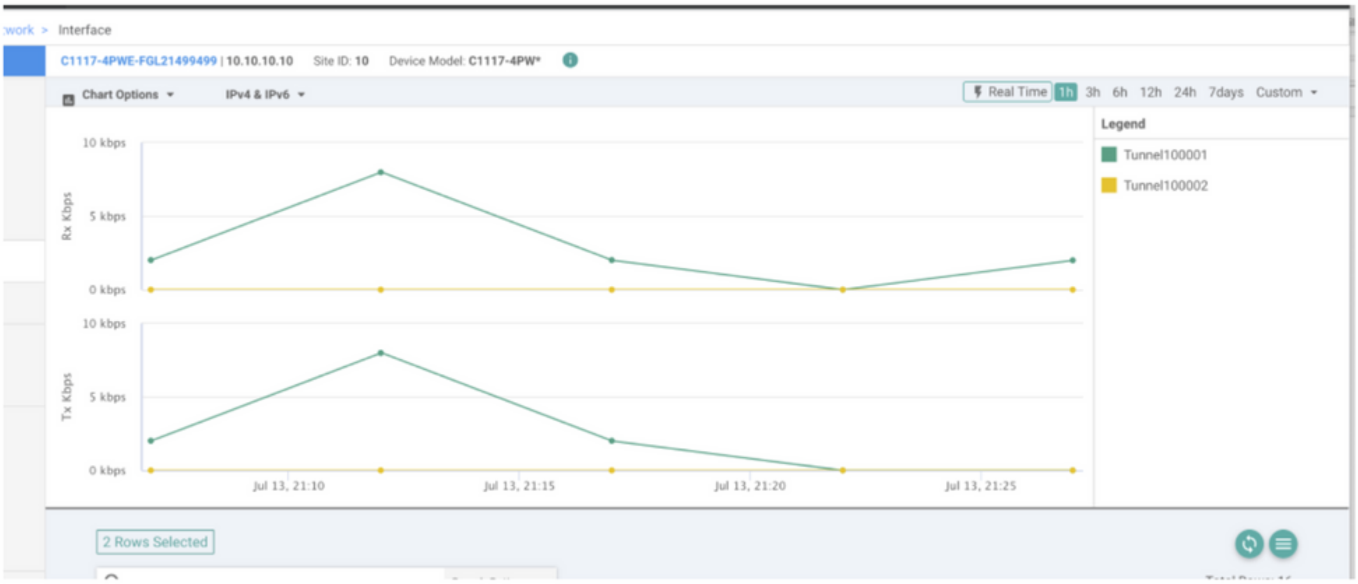
驗證

驗證活動/備份方案

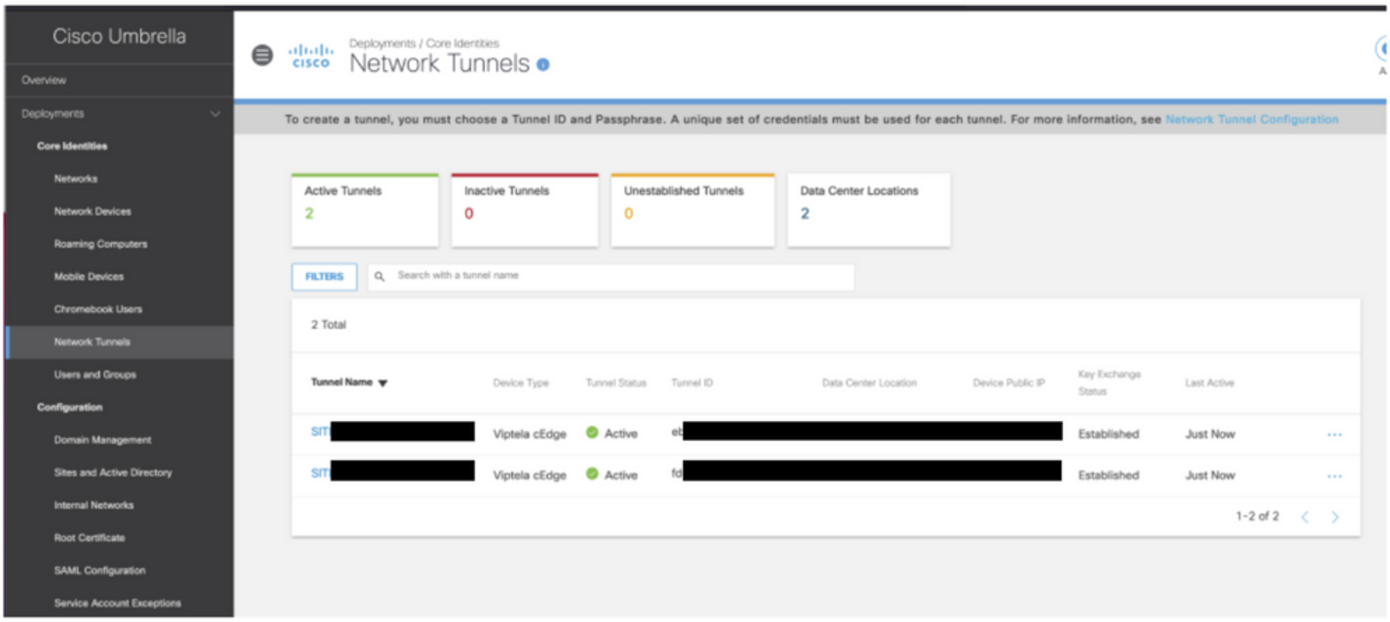
在vManage中，可以監控SIG IPSec通道的狀態。導航至 **Monitor** > **Network**, 選擇所需的WAN邊緣裝置
。

按一下 **Interfaces** 頁籤；顯示裝置中所有介面的清單。其中包括ipsec1和ipsec2介面。

圖顯示，ipsec1通道轉送所有流量，而ipsec2不傳遞流量。



也可以驗證思科上的通道 **Umbrella** 門戶如圖所示。



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 Network Tunnel Configuration

Active Tunnels	Inactive Tunnels	Unestablished Tunnels	Data Center Locations
2	0	0	2

2 Total

Tunnel Name	Device Type	Tunnel Status	Tunnel ID	Data Center Location	Device Public IP	Key Exchange Status	Last Active
SIT[redacted]	Viptela cEdge	● Active	eb[redacted]	[redacted]	[redacted]	Established	Just Now
SIT[redacted]	Viptela cEdge	● Active	fd[redacted]	[redacted]	[redacted]	Established	Just Now

1-2 of 2

使用 **show sdwan secure-internet-gateway tunnels** 命令以顯示通道資訊。

```
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
```

使用 **show endpoint-tracker** 和 **show ip sla summary** 命令，以顯示自動生成的跟蹤程式和SLA的資訊。

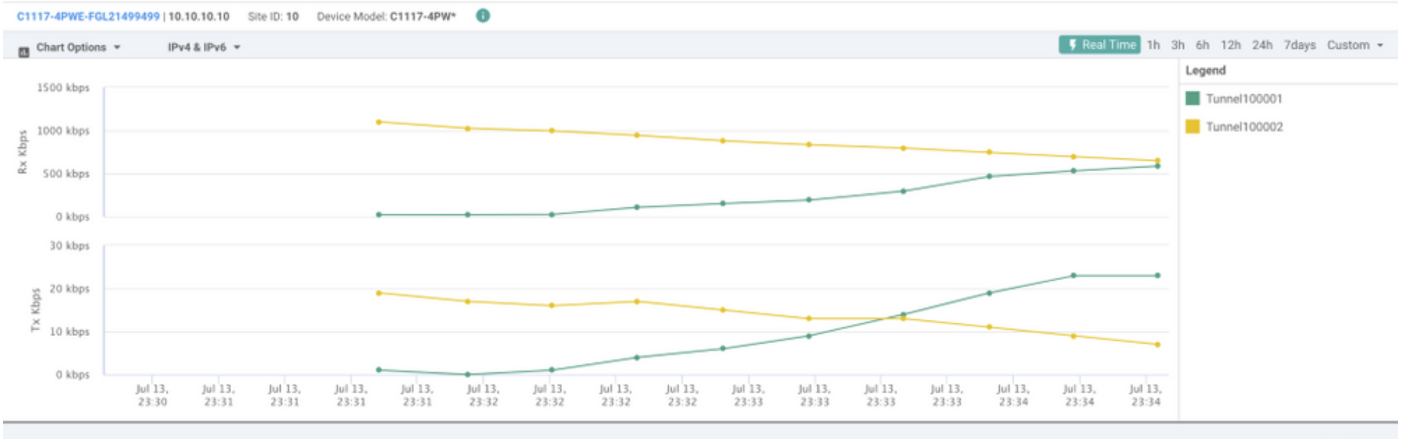
```
cEdge_Site1_East_01#show endpoint-tracker
Interface               Record Name             Status          RTT in msecs    Probe ID        Next Hop
Tunnel100001            #SIGL7#AUTO#TRACKER     Up              8               14              None
Tunnel100002            #SIGL7#AUTO#TRACKER     Up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

驗證活動/活動方案

在vManage中，可以監控SIG IPSec通道的狀態。導航至 **Monitor** > **Network,** 選擇所需的WAN邊緣裝置。

按一下 **Interfaces** 頁籤的左側 — 並且顯示裝置中所有介面的清單。其中包括ipsec1和ipsec2介面。

該圖顯示，ipsec1和ipsec2均通過隧道轉發流量。



使用 **show sdwan secure-internet-gateway tunnels** 命令以顯示通道資訊。

```
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
```

使用 **show endpoint-tracker** 和 **show ip sla summary** 命令，以顯示自動生成的跟蹤程式和SLA的資訊。

```
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
```

相關資訊

- 將您的裝置與安全的網際網路網關整合 — Cisco IOS® XE版本17.x
- http://Network隧道配置 — Umbrella SIG
- Umbrella入門
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。