

Configuración de túneles Umbrella SIG para escenarios Activo/Copia de seguridad o Activo/Activo

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Descripción general de Cisco Umbrella SIG](#)

[Umbrella SIG Tunnel Bandwidth Limitation](#)

[Obtenga información sobre Cisco Umbrella Portal](#)

[Obtenga la clave y la clave secreta](#)

[Consiga su ID de organización](#)

[Creación de túneles Umbrella SIG con escenario activo/de respaldo](#)

[Paso 1. Cree una plantilla de función de credenciales SIG.](#)

[Paso 2. Cree una plantilla de función SIG.](#)

[Paso 3. Seleccione su proveedor SIG para el túnel principal.](#)

[Paso 4. Agregue el túnel secundario.](#)

[Paso 5. Cree Un Par De Alta Disponibilidad.](#)

[Paso 6. Edite la plantilla de VPN del lado de servicio para insertar una ruta de servicio.](#)

[Configuración del router de extremo de la WAN para el escenario activo/de copia de seguridad](#)

[Creación de túneles Umbrella SIG con escenario activo/activo](#)

[Paso 1. Cree una plantilla de función de credenciales SIG.](#)

[Paso 2. Cree dos interfaces de loopback para vincular los túneles SIG.](#)

[Paso 3. Cree una plantilla de función SIG.](#)

Introducción

Este documento describe cómo configurar Cisco Umbrella Secure Internet Gateway (SIG) túneles con IPsec en ambos *Active/Active* y *Active/Standby*.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Cisco Umbrella
- Negociación IPsec
- Red de área extensa definida por software de Cisco (SD-WAN)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco vManage versión 20.4.2
- Cisco WAN Edge Router C117-4PW* versión 17.4.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Descripción general de Cisco Umbrella SIG

Cisco Umbrella es un servicio de seguridad proporcionado a través de la nube que aúna funciones esenciales.

Umbrella unifica el gateway web seguro, la seguridad DNS, el firewall proporcionado en la nube, la funcionalidad de agente de seguridad de acceso a la nube y la inteligencia de amenazas.

La inspección y el control exhaustivos garantizan el cumplimiento de las políticas web de uso aceptable y protegen frente a las amenazas de Internet.

Los routers SD-WAN se pueden integrar con gateways de Internet seguros (SIG), que realizan la mayor parte del procesamiento para proteger el tráfico empresarial.

Cuando se configura el SIG, todo el tráfico del cliente, basado en rutas o políticas, se reenvía al SIG.

Umbrella SIG Tunnel Bandwidth Limitation

Cada túnel IKEv2 IPsec al Umbrella la cabecera está limitada a aproximadamente 250 Mbps, por lo que si se crean varios túneles y se equilibra la carga del tráfico, se superan dichas limitaciones en caso de que se requiera un ancho de banda mayor.

Hasta cuatro High Availability se pueden crear pares de túnel.

Obtenga información sobre Cisco Umbrella Portal

Con el fin de continuar con la integración de SIG, un Umbrella Se necesita una cuenta con el paquete 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.

Obtenga la clave y la clave secreta

La clave y la clave secreta se pueden generar en el momento en que se obtiene el Umbrella Management API KEY (esta clave se encuentra en 'Claves heredadas'). Si no recuerda o no guardó la clave secreta, haga clic en refresh.

 **Precaución:** si se hace clic en el botón de actualización, se necesita una actualización para estas teclas en todos los dispositivos, no se recomienda la actualización si hay dispositivos en uso.

Umbrella Management	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](#)


Consiga su ID de organización

La ID de la organización se puede obtener fácilmente al iniciar sesión en Umbrella desde la barra de direcciones del explorador.

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


Creación de túneles Umbrella SIG con escenario activo/de respaldo

 Nota: IPsec/GRE Tunnel Routing and Load-Balancing Using ECMP: Esta función está disponible en vManage 20.4.1 y versiones posteriores, le permite utilizar la plantilla SIG para dirigir el tráfico de aplicaciones a Cisco Umbrella o un proveedor de SIG de terceros

 Nota: Compatibilidad con el aprovisionamiento automático de Zscaler: esta función está disponible en vManage 20.5.1 y versiones posteriores, y automatiza el aprovisionamiento de túneles desde routers SD-WAN de Cisco hasta Zscaler, con el uso de credenciales de API de partners de Zscaler.

Para configurar los túneles automáticos SIG, es necesario crear/actualizar algunas plantillas:

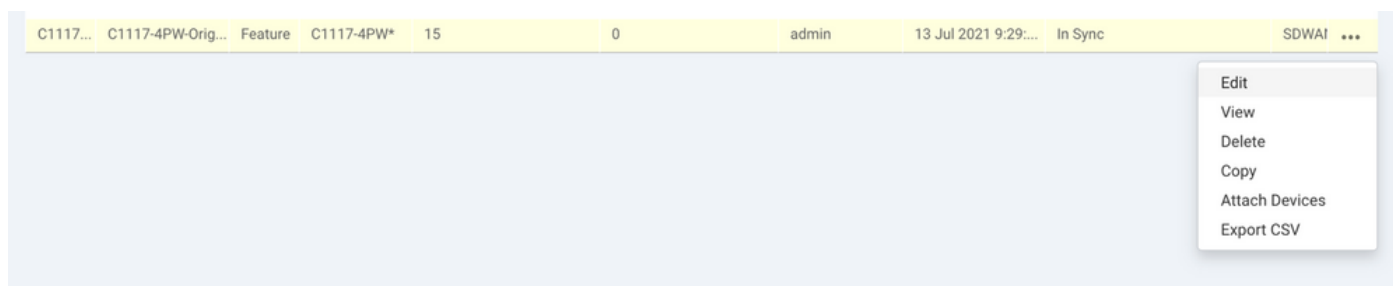
- Cree una plantilla de función de credenciales SIG.
- Cree dos interfaces de loopback para vincular los túneles SIG (solo aplicable con más de uno) *Active* túnel al mismo tiempo - *Active/Active* escenario).
- Cree una plantilla de función SIG.
- Edite la plantilla de VPN del lado del servicio para insertar una *Service Route*.

 Nota: Asegúrese de que se permiten los puertos UDP 4500 y 500 desde cualquier dispositivo ascendente.

Las configuraciones de las plantillas cambian con el *Active/Backup* y el *Active/Active* escenarios para los que ambos escenarios se explican y exponen por separado.

Paso 1. Cree una plantilla de función de credenciales SIG.

Vaya a la plantilla de función y haga clic en **Edit**.



En la sección de **Additional templates**, haga clic en **Cisco SIG Credentials**. La opción se muestra en la imagen.

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 ▼	

Dé un nombre y una descripción a la plantilla.

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](#)

Paso 2. Cree una plantilla de función SIG.

Desplácese hasta la plantilla de función y, en la sección **Transport & Management VPN** seleccione la plantilla de función 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

Dé un nombre y una descripción a la plantilla.

Paso 3. Seleccione su proveedor SIG para el túnel principal.

Haga clic en **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](#)

Configurar los detalles básicos y mantener **Data-Center** como **Primary**, haga clic en **Add**.

Update Tunnel ✕

Basic Settings

Tunnel Type **IPsec**

Interface Name (1..255)

Description

Tunnel Source Interface

Data-Center Primary Secondary

[Advanced Options](#) ▾

General

Shutdown Yes No

TCP MSS

IP MTU

Paso 4. Agregue el túnel secundario.

Agregar una segunda configuración de túnel, utilizar **Data-Center** como **Secondary** esta vez, y el nombre de la interfaz como ipsec2.

La configuración de vManage aparece como se muestra a continuación:

Configuration

SIG Provider Umbrella Third Party

[+ Add Tunnel](#)


Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300	<input checked="" type="checkbox"/> 1400	✎ ✖
ipsec2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300	<input checked="" type="checkbox"/> 1400	✎ ✖

Paso 5. Cree Un Par De Alta Disponibilidad.

Dentro de la **High Availability** , seleccione el ipsec1 como Active y el túnel ipsec2 como Backup.

High Availability

	Active	Active Weight	Backup	Backup Weight
Pair-1	<input type="text" value="ipsec1"/>	<input type="text" value="1"/>	<input type="text" value="ipsec2"/>	<input type="text" value="1"/>

 Nota: hasta 4 **High Availability** se pueden crear simultáneamente pares de túneles y un máximo de 4 túneles activos.

Paso 6. Edite la plantilla de VPN del lado de servicio para insertar una ruta de servicio.

Desplácese hasta el **Service VPN** y, dentro de la **Service VPN** plantilla, desplácese a la sección **Service Route** y agregue un 0.0.0.0 con SIG **Service Route**. Para este documento, se utiliza el VRF/VPN 10.

SERVICE ROUTE

[+ New Service Route](#)

Prefix	Action
0.0.0.0	✎ ✖

Update Service Route

Prefix

Service SIG

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

GRE ROUTE

La ruta 0.0.0.0 SIG se muestra como se muestra aquí.

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	

Nota: Para que el tráfico del servicio se apague realmente, NAT debe configurarse en la interfaz WAN.

Adjunte esta plantilla al dispositivo e inserte la configuración:

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.
  
```

Configuración del router de extremo de la WAN para el escenario activo/de copia de seguridad

```

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
```

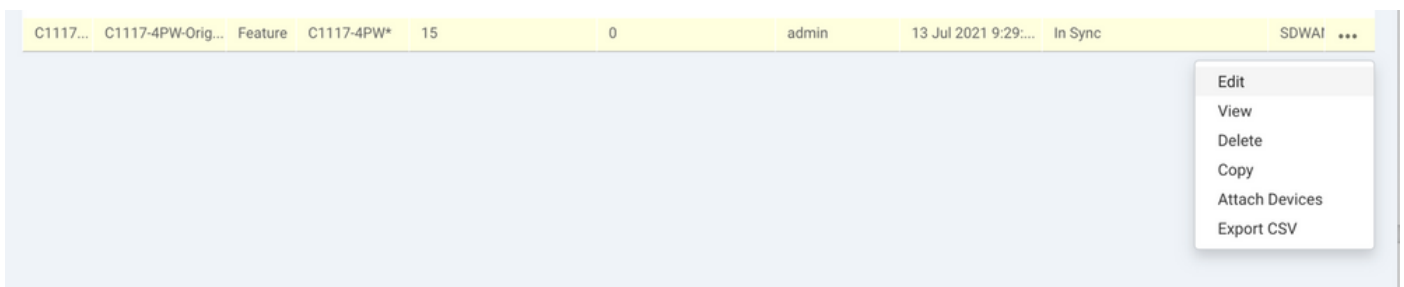
```
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
interface Tunnel100001
no shutdown
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
tunnel source GigabitEthernet0/0/0
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec1-ipsec-profile
tunnel vrf multiplexing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

Creación de túneles Umbrella SIG con escenario activo/activo

Paso 1. Cree una plantilla de función de credenciales SIG.

Desplácese hasta la plantilla de función y haga clic en **Edit**



En la sección de **Additional templates**, seleccione **Cisco SIG Credentials**. La opción se muestra en la imagen.

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 ▼	

Dé un nombre y una descripción a la plantilla.

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

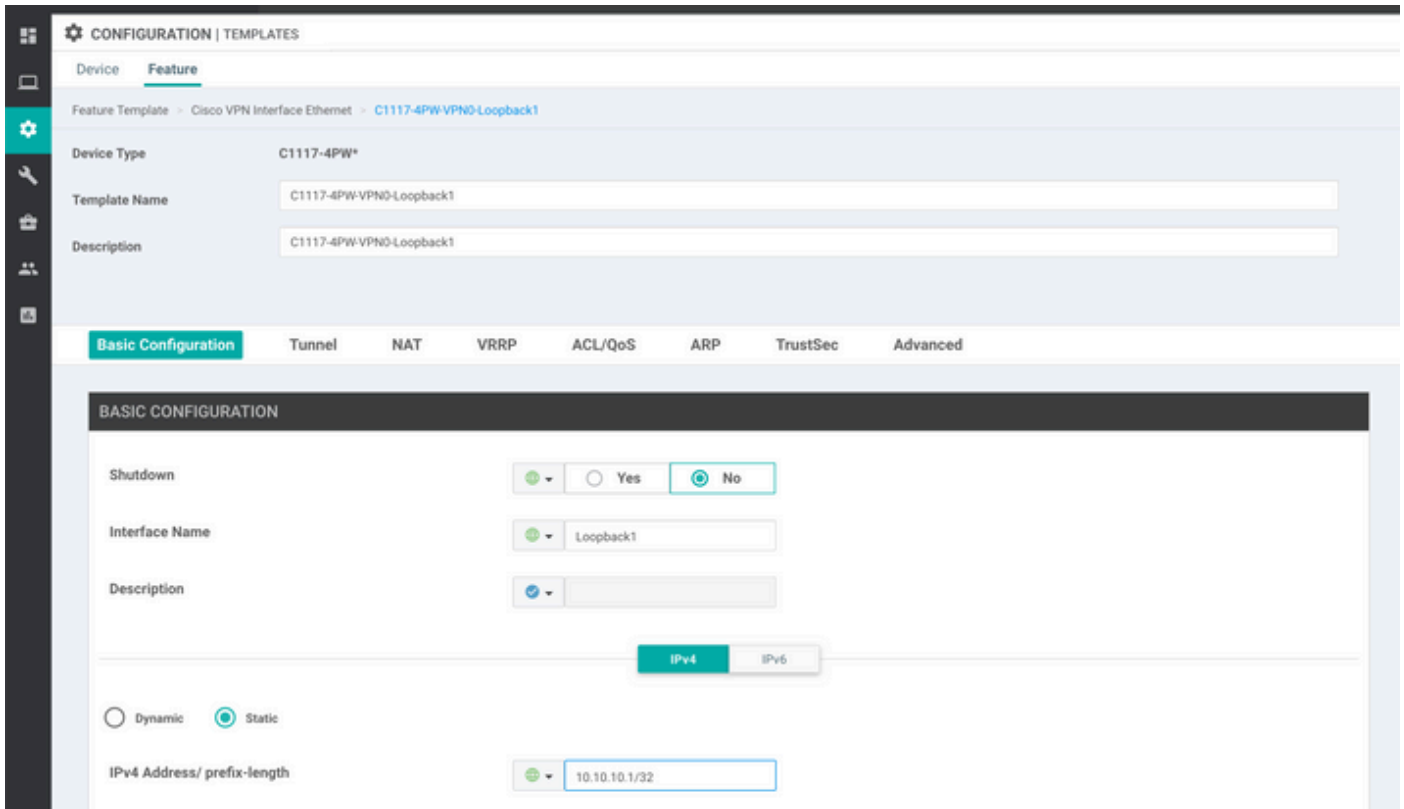
Paso 2. Cree dos interfaces de loopback para vincular los túneles SIG.

 Nota: Cree una interfaz de loopback para cada túnel SIG configurado en modo activo; esto es necesario porque cada túnel necesita un ID IKE único.

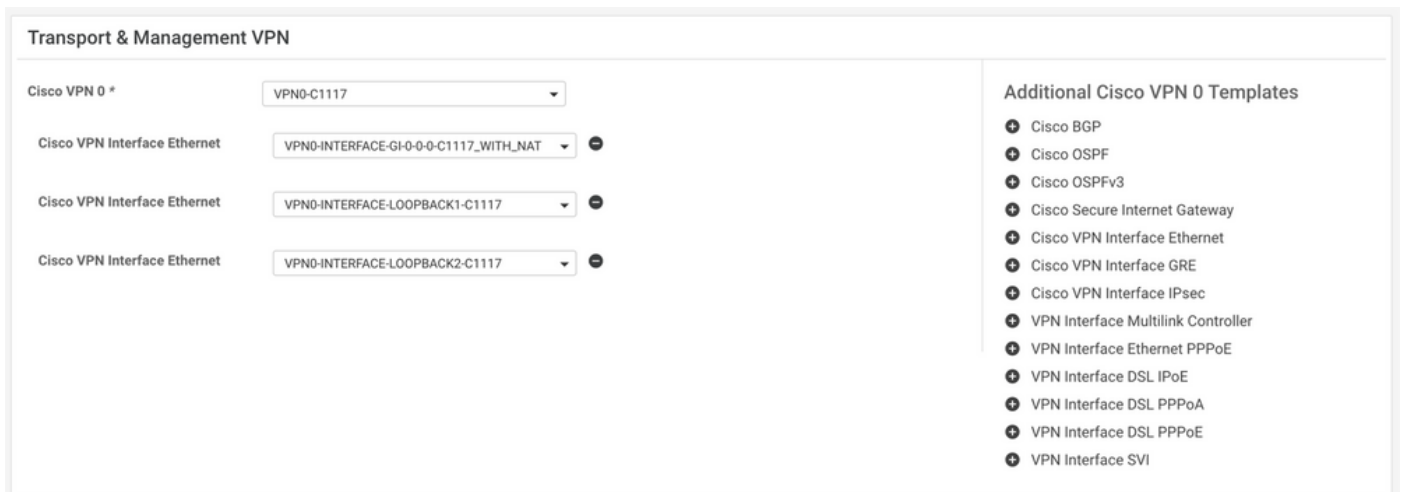
 Nota: Este escenario es Activo/Activo, por lo tanto se crean dos loopbacks.

Configure el nombre de la interfaz y la dirección IPv4 para el bucle invertido.

 Nota: La dirección IP configurada para el loopback es una dirección ficticia.



Cree la segunda plantilla de bucle invertido y conéctela a la plantilla de dispositivo. La plantilla de dispositivo debe tener dos plantillas de bucle invertido conectadas:



Paso 3. Cree una plantilla de función SIG.

Desplácese hasta la plantilla de función SIG y, en la sección **Transport & Management VPN** seleccionar **Cisco Secure Internet Gateway** plantilla de función.

Paso 4. Seleccione el proveedor SIG para el túnel principal.

Haga clic en **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](#)

Configurar los detalles básicos y mantener **Data-Center** como **Primary**.

 Nota: El parámetro Tunnel Source Interface es el Loopback (para este documento Loopback1) y como Tunnel Route-via Interface la interfaz 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](#)

Paso 5. Agregue el túnel secundario.

Agregar una segunda configuración de túnel, utilizar **Data-Center** como **Primary** y el nombre de la interfaz como ipsec2.

La configuración de vManage aparece como se muestra a continuación:

Configuration

SIG Provider Umbrella Third Party

[+ Add Tunnel](#)

Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300	<input checked="" type="checkbox"/> 1400	✎ ✖
ipsec2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300	<input checked="" type="checkbox"/> 1400	✎ ✖

Paso 6. Cree Dos Pares De Alta Disponibilidad.

Dentro de la **High Availability** sección, crear dos **High Availability** pares.

- En el primer par HA, seleccione el ipsec1 como Activo y seleccione **None** para copia de seguridad.
- En el segundo par HA, seleccione el ipsec2 como Active select **None** y para copias de seguridad.

La configuración de vManage para **High Availability** aparece como se muestra:

High Availability

	Active	Active Weight	Backup	Backup Weight
Pair-1	<input type="text" value="ipsec1"/>	<input type="text" value="1"/>	<input type="text" value="None"/>	<input type="text" value="1"/>
Pair-2	<input type="text" value="ipsec2"/>	<input type="text" value="1"/>	<input type="text" value="None"/>	<input type="text" value="1"/>

La plantilla de dispositivo tiene las dos plantillas de bucle invertido y la plantilla de función SIG conectadas también.

Transport & Management VPN

Cisco VPN 0 *

Cisco Secure Internet Gateway

Cisco VPN Interface Ethernet

Cisco VPN Interface Ethernet

Cisco VPN Interface Ethernet

Cisco VPN 512 *

Additional Cisco VPN 0 Templates

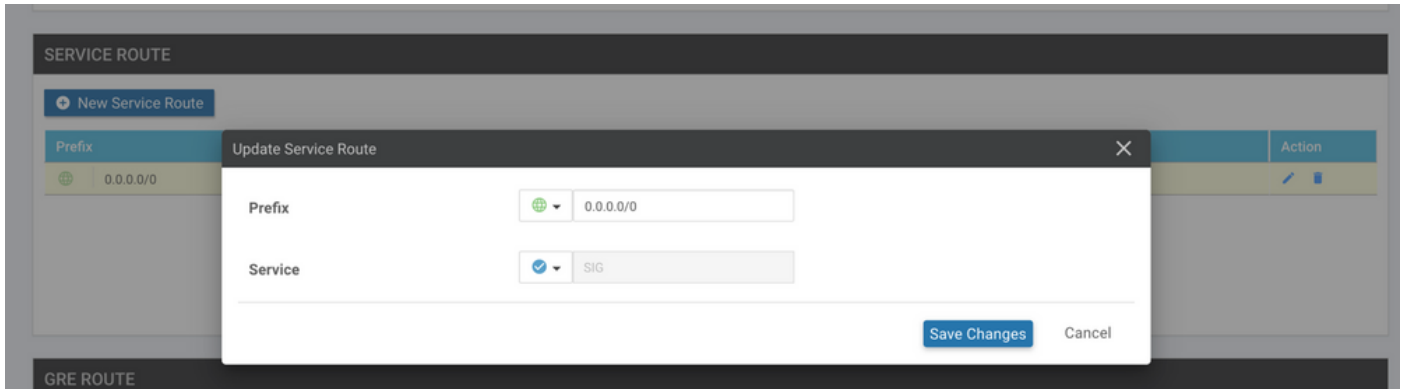
- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco Secure Internet Gateway
- Cisco VPN Interface Ethernet
- Cisco VPN Interface GRE
- Cisco VPN Interface IPsec
- VPN Interface Multilink Controller
- VPN Interface Ethernet PPPoE
- VPN Interface DSL IPoE
- VPN Interface DSL PPPoA
- VPN Interface DSL PPPoE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

Additional Cisco VPN 512 Templates


- Cisco VPN Interface Ethernet
- VPN Interface SVI

Paso 7. Edite la plantilla de VPN del lado de servicio para insertar una ruta de servicio.

Desplácese hasta el **Service VPN** y, dentro de la plantilla **VPN of service**, vaya a la sección **Service Route** y agregue un **0.0.0.0** con **SIGService Route**



La ruta SIG 0.0.0.0 aparece como se muestra aquí.

 **Nota:** Para que el tráfico del servicio se apague realmente, NAT debe configurarse en la interfaz WAN.

Adjunte esta plantilla al dispositivo e inserte la configuración.

Configuración del router de extremo de la WAN para el escenario activo/activo


```
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 tcptopt 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
!
```

 Nota: aunque este documento se centra en Umbrella, las mismas situaciones se aplican a los túneles SIG de Azure y de terceros.

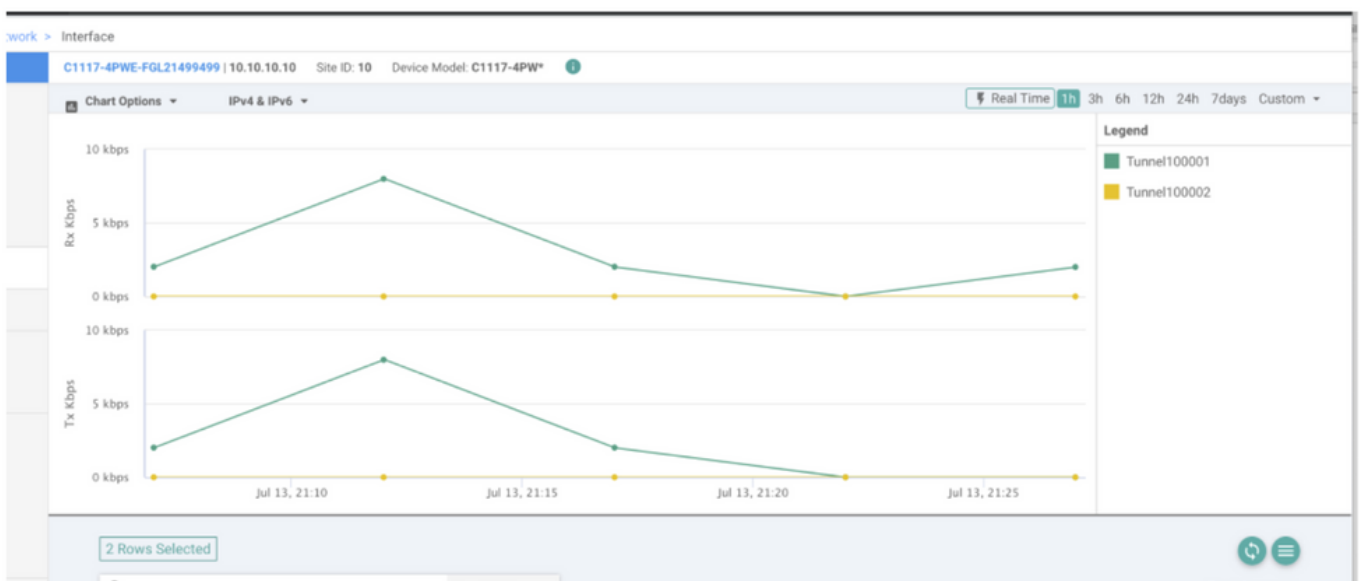
Verificación

Verificar escenario activo/de respaldo

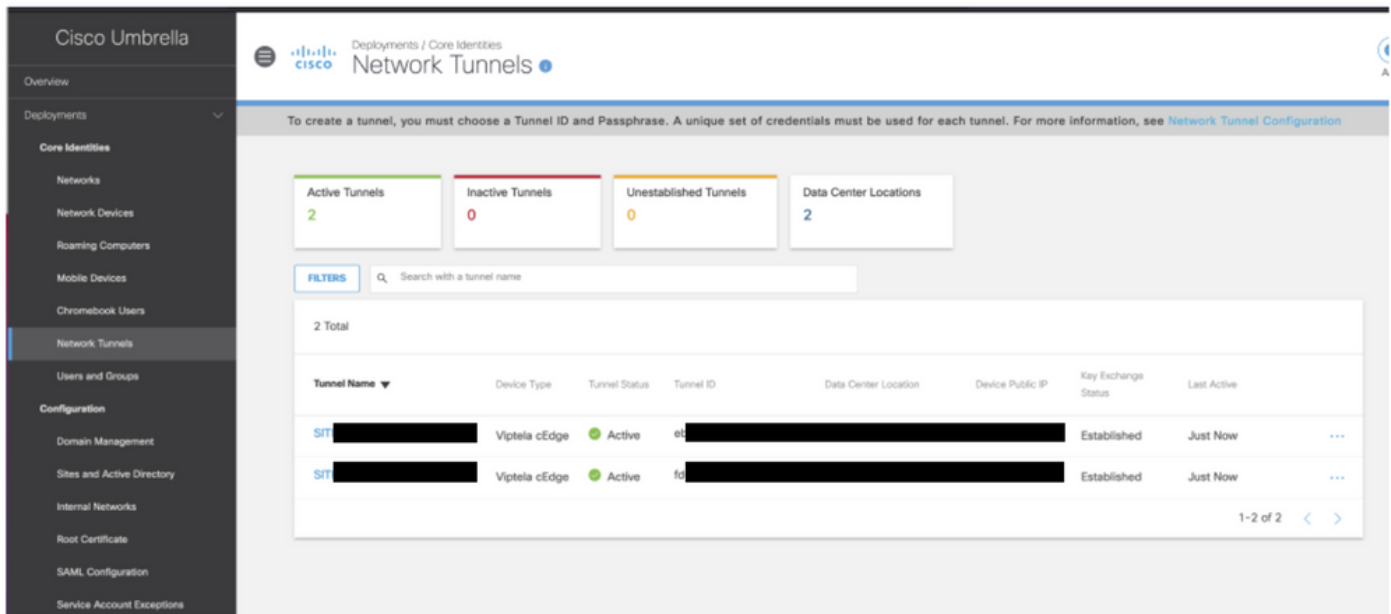
En vManage, es posible supervisar el estado de los túneles IPsec de SIG. Desplácese hasta **Monitor > Network**, seleccione el dispositivo de extremo de la WAN que desee.

Haga clic en el **Interfaces** a la izquierda; se muestra una lista de todas las interfaces del dispositivo. Esto incluye las interfaces ipsec1 e ipsec2.

La imagen muestra que el túnel ipsec1 reenvía todo el tráfico y el ipsec2 no pasa el tráfico.



También es posible verificar los túneles en el Cisco Umbrella portal se muestra en la imagen.



Use el comando `show sdwan secure-internet-gateway tunnels` en la CLI para mostrar la información de los túneles.

```
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 el comando `show endpoint-tracker` y `show ip sla summary` comandos en la CLI para mostrar información sobre los rastreadores generados automáticamente y los SLA.

```
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

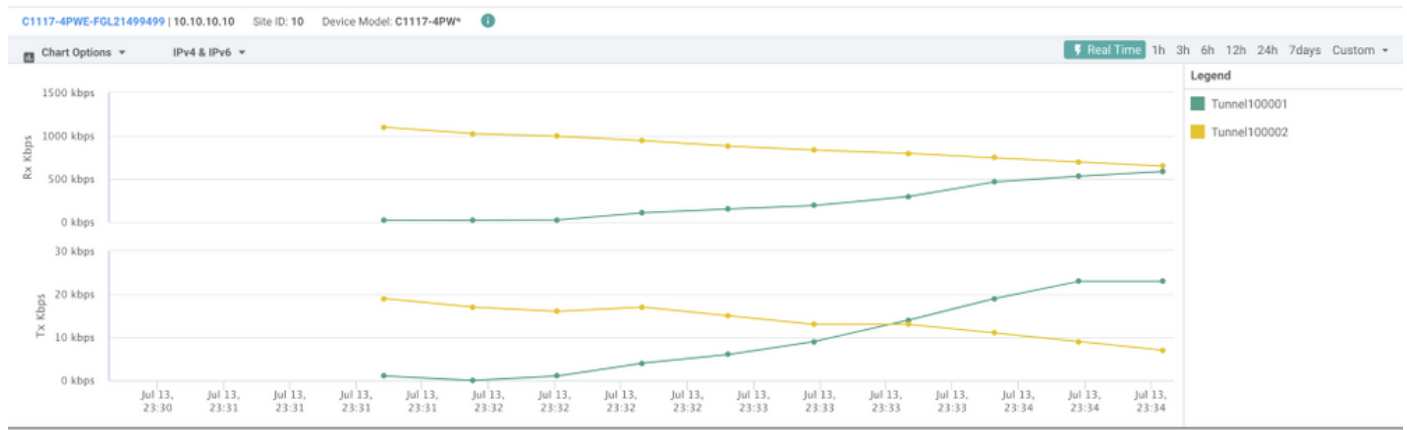
ID	Type	Destination	Stats	Return Code	Last Run
*12	http	10.10.10.10	RTT=6	OK	8 seconds ago
*14	http	10.10.10.10	RTT=17	OK	3 seconds ago

Verificar escenario activo/activo

En vManage es posible supervisar el estado de los túneles IPsec de SIG. Desplácese hasta **Monitor > Network**, seleccione el dispositivo de extremo de la WAN que desee.

Haga clic en el **Interfaces** a la izquierda y se muestra una lista de todas las interfaces del dispositivo. Esto incluye las interfaces ipsec1 e ipsec2.

La imagen muestra que los túneles ipsec1 e ipsec2 reenvían el tráfico.



Use el comando `show sdwan secure-internet-gateway tunnels` en la CLI para mostrar la información de los túneles.

```
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 el comando `show endpoint-tracker` y `show ip sla summary` comandos en la CLI para mostrar información sobre los rastreadores generados automáticamente y los SLA.

```
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

Información Relacionada

- [Integre sus dispositivos con gateways de Internet seguros: Cisco IOS® XE versión 17.x](#)
- [http://Network Configuración del túnel - Umbrella SIG](#)
- [Introducción a Umbrella](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).