

Configure Umbrella SIG Tunnels for Active/Backup or Active/Active Scenarios

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Cisco Umbrella SIG Overview](#)

[Umbrella SIG Tunnel Bandwidth Limitation](#)

[Get your Cisco Umbrella Portal Information](#)

[Get the Key and the Secret Key](#)

[Get Your Organization ID](#)

[Create Umbrella SIG Tunnels with Active/Backup Scenario](#)

[Step 1. Create a SIG Credentials Feature Template.](#)

[Step 2. Create a SIG Feature Template.](#)

[Step 3. Select Your SIG Provider for Primary Tunnel.](#)

[Step 4. Add the Secondary Tunnel.](#)

[Step 5. Create One High Availability Pair.](#)

[Step 6. Edit Service-side VPN Template to Inject a Service Route.](#)

[WAN Edge Router Configuration for Active/Backup Scenario](#)

[Create Umbrella SIG Tunnels with Active/Active Scenario](#)

[Step 1. Create a SIG Credentials Feature Template.](#)

[Step 2. Create Two Loopback Interfaces to Link the SIG Tunnels.](#)

[Step 3. Create a SIG Feature Template.](#)

Introduction

This document describes how to configure Cisco Umbrella Secure Internet Gateway (SIG) tunnels with IPsec in both Active/Active and Active/Standby.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cisco Umbrella
- IPsec negotiation
- Cisco Software-defined Wide Area Network (SD-WAN)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco vManage version 20.4.2
- Cisco WAN Edge Router C1117-4PW* version 17.4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Umbrella SIG Overview

Cisco **Umbrella** is a cloud-delivered security service that brings essential functions together.

Umbrella unifies secure web gateway, DNS security, cloud-delivered firewall, cloud access security broker functionality, and threat intelligence.

Deep inspection and control ensure compliance with acceptable-use web policies and protect against internet threats.

SD-WAN routers can integrate with Secure Internet Gateways (SIG) which do the majority of the processing to secure enterprise traffic.

When the SIG is set up, all client traffic, based on routes or policy, is forwarded to the SIG.

Umbrella SIG Tunnel Bandwidth Limitation

Each IPsec IKEv2 tunnel to the **Umbrella** head-end is limited to approximately 250 Mbps, so if multiple tunnels are created and load balance the traffic, they overcome such limitations in case a higher bandwidth is required.

Up to four **High Availability** tunnel pairs can be created.

Get your Cisco Umbrella Portal Information

In order to proceed with the SIG integration, an **Umbrella** Account with SIG essentials package is needed.

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

Get the Key and the Secret Key

The key and secret key can be generated at the moment you get the **Umbrella Management API KEY** (this key is under 'Legacy Keys'). If you do not remember or did not save the secret key, click **refresh**.

 **Caution:** If the refresh button is clicked, an update for these keys on all devices is needed, the update is not recommended if there are devices in use.

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.


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

Get Your Organization ID


The organization ID can be easily obtained when you log in to **Umbrella** from the browser address bar.

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

Create Umbrella SIG Tunnels with Active/Backup Scenario


 **Note:** IPsec/GRE Tunnel Routing and Load-Balancing Using ECMP: This feature is available in vManage 20.4.1 and onwards, it allows you to use the SIG template to steer application traffic to Cisco Umbrella or a Third-party SIG Provider

 **Note:** Support for Zscaler Automatic Provisioning: This feature is available on vManage 20.5.1 and

 onwards, this automates the provisioning of tunnels from Cisco SD-WAN routers to Zscaler, with the use of Zscaler partner API credentials.

To configure the SIG automatic tunnels, it is required to create/update a few templates:

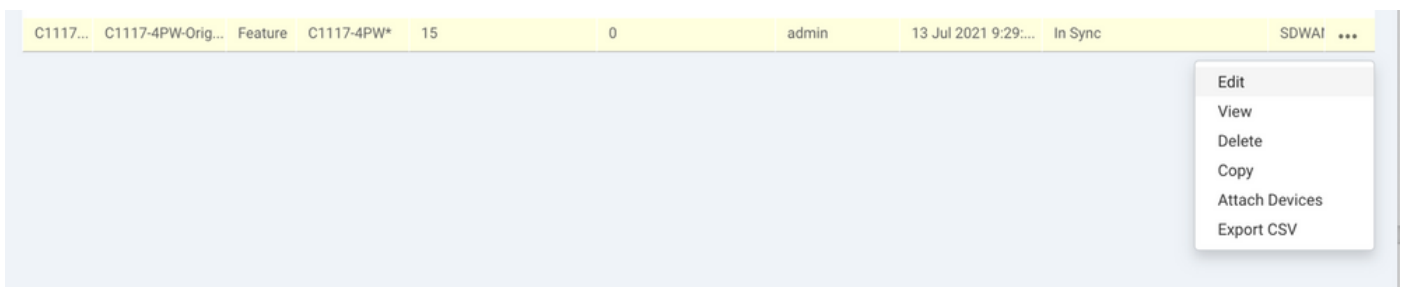
- Create a SIG Credentials feature template.
- Create two loopback interfaces in order to link the SIG tunnels (Only applicable with more than one Active tunnel at the same time - Active/Active scenario).
- Create a SIG feature template.
- Edit **service-side VPN** Template to inject a **Service Route**.

 **Note:** Make sure UDP 4500 and 500 ports are allowed from any upstream device.

The template configurations change with the **Active/Backup** and the **Active/Active** scenarios for which both scenarios are explained and exposed separately.

Step 1. Create a SIG Credentials Feature Template.

Go to the feature template and click **Edit**.



Under the section of **Additional templates**, click **Cisco SIG Credentials**. The option is shown in the image.

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

Give a name and description to the template.

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](#)

Step 2. Create a SIG Feature Template.

Navigate to the feature template and, under the section **Transport & Management VPN** select the **Cisco Secure Internet Gateway** feature template.














Transport & Management VPN

Cisco VPN 0 * VPN0-C1117

Cisco Secure Internet Gateway SIG-IPSEC-TUNNELS

Cisco VPN Interface Ethernet VPN0-INTERFACE-GI-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

Give a name and description to the template.

Step 3. Select Your SIG Provider for Primary Tunnel.

Click **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 the basic details and keep **Data-Center** as **Primary**, then click **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

Step 4. Add the Secondary Tunnel.

Add a second tunnel configuration, use **Data-Center** as **Secondary** this time, and the interface name as *ipsec2*.

vManage configuration appears as shown here:

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	Edit Delete
ipsec2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> 1300	<input checked="" type="checkbox"/> 1400	Edit Delete

Step 5. Create One High Availability Pair.

Within the **High Availability** section, select the **ipsec1** as **Active** and the **ipsec2** tunnel as **Backup**.

High Availability

	Active	Active Weight	Backup	Backup Weight
Pair-1	<input checked="" type="checkbox"/> ipsec1	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> ipsec2	<input checked="" type="checkbox"/> 1

 **Note:** Up to 4 High Availability tunnel pairs and a maximum of 4 active tunnels can be created at the same time.

Step 6. Edit Service-side VPN Template to Inject a Service Route.

Navigate to the **Service VPN** section and, within the **Service VPN** template, navigate to the section **Service Route** and add a **0.0.0.0** with **SIG Service Route**. For this document, the VRF/VPN 10 is used.

SERVICE ROUTE

[+ New Service Route](#)

Prefix	Action
<input checked="" type="checkbox"/> 0.0.0.0	Edit Delete

Update Service Route

Prefix 0.0.0.0

Service SIG

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

GRE ROUTE

The **0.0.0.0 SIG route** is displayed as shown here.

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	

Note: For the Service traffic to actually go out, NAT has to be configured in the WAN interface.

Attach this template to the device and push the configuration:

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.

```

WAN Edge Router Configuration for Active/Backup Scenario

```

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 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
    !
    !
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
```

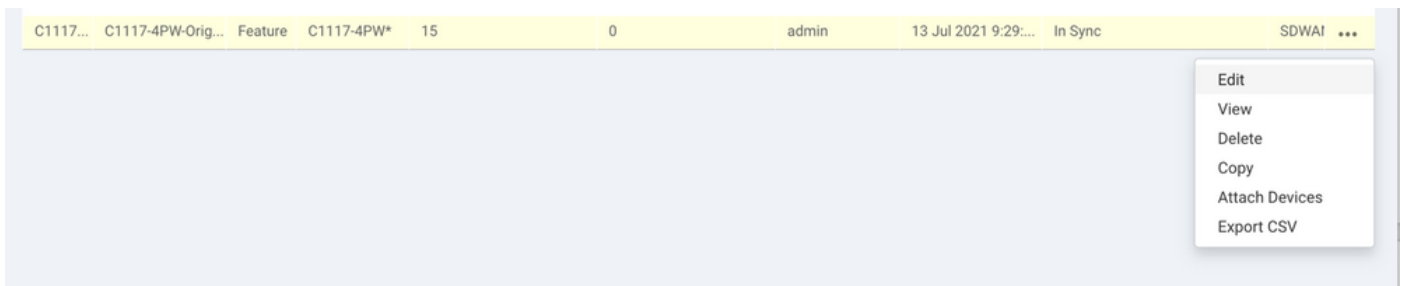
```
interface Tunnel100001
  no shutdown
  ip unnumbered GigabitEthernet0/0/0
  ip mtu 1400
  tunnel source GigabitEthernet0/0/0
  tunnel destination dynamic
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile if-ipsec1-ipsec-profile
  tunnel vrf multiplexing
exit
interface Tunnel100002
  no shutdown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

Create Umbrella SIG Tunnels with Active/Active Scenario

Step 1. Create a SIG Credentials Feature Template.

Navigate to the feature template and click **Edit**



Under the section of **Additional templates**, select **Cisco SIG Credentials**. The option is shown on the image.

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

Give a name and description to the template.

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](#)

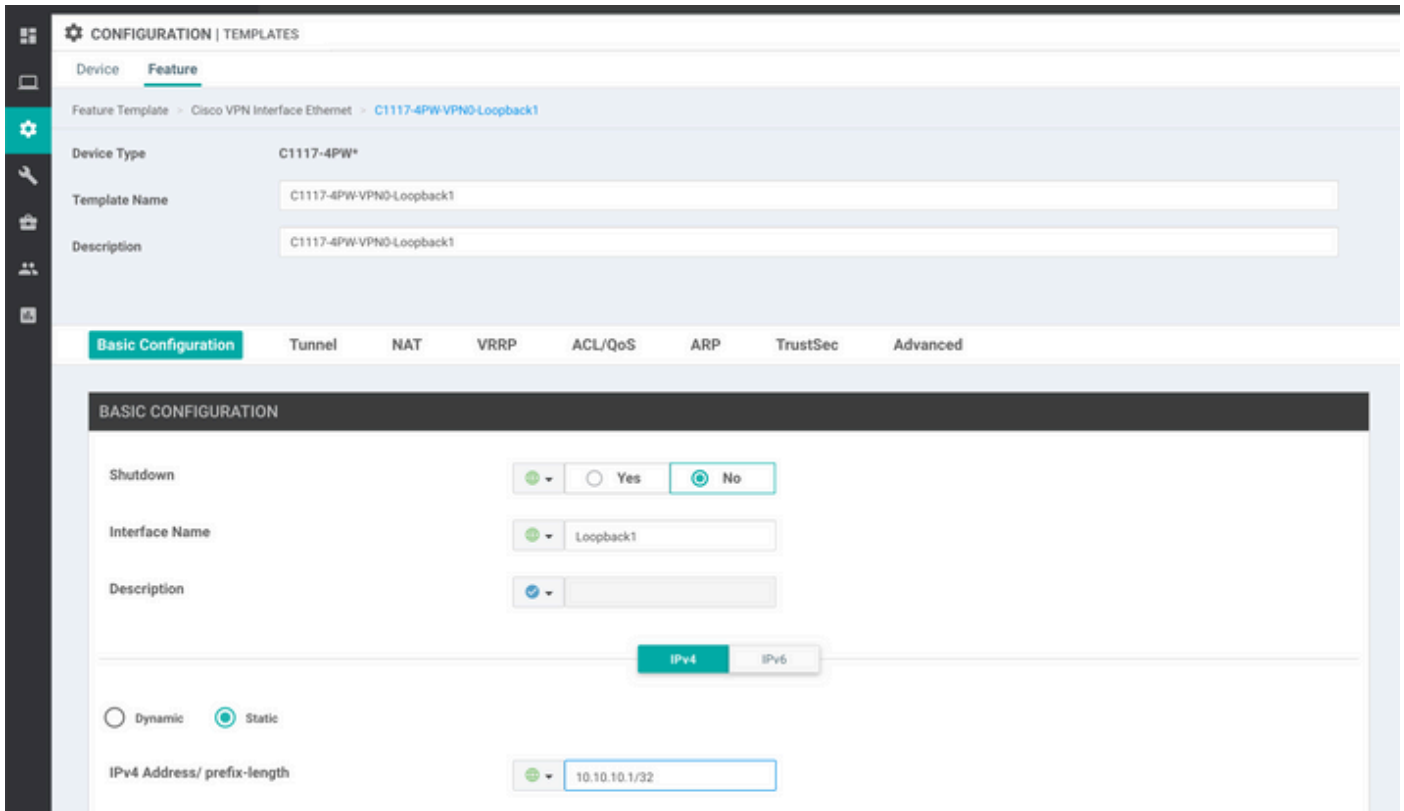
Step 2. Create Two Loopback Interfaces to Link the SIG Tunnels.

 **Note:** Create a Loopback interface for each SIG tunnel configured in active mode, this is needed because each tunnel needs a unique IKE ID.

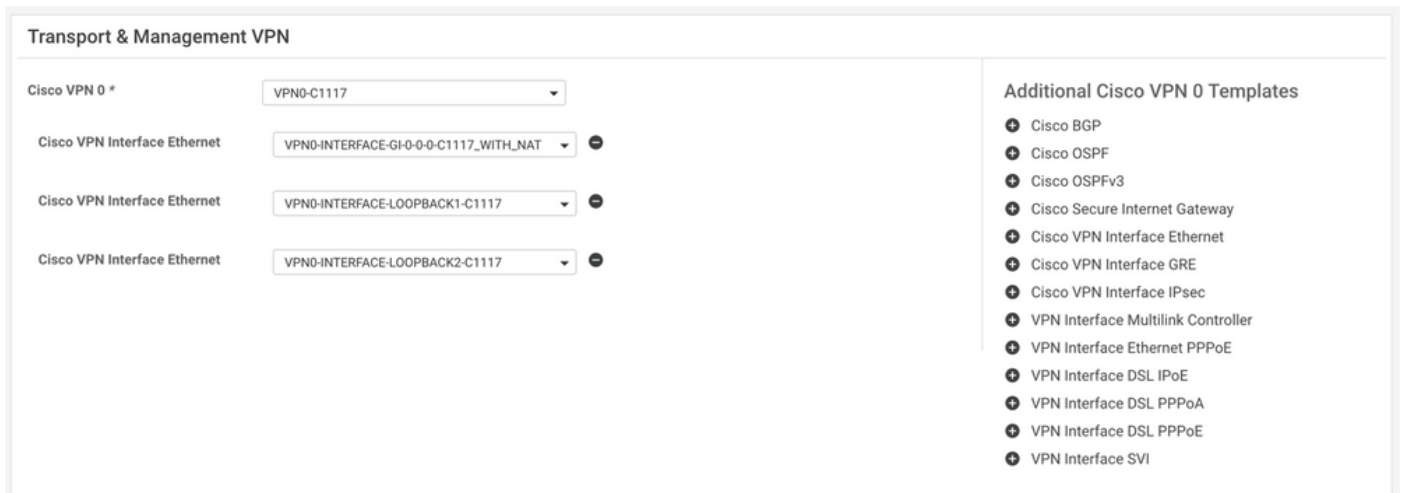
 **Note:** This scenario is Active/Active, therefore two Loopbacks are created.

Configure the interface name and IPv4 address for the Loopback.

 **Note:** The IP address configured for the loopback is a dummy address.



Create the second Loopback template and attach it to the device template. The device template must have two Loopback templates attached:



Step 3. Create a SIG Feature Template.

Navigate to the SIG feature template and, under the section **Transport & Management VPN** select **Cisco Secure Internet Gateway** feature template.

Step 4. Select the SIG Provider for the Primary Tunnel.

Click **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 the basic details and keep **Data-Center** as **Primary**.

 **Note:** The Tunnel Source Interface parameter is the Loopback (for this document Loopback1) and as Tunnel Route-via Interface the physical interface (for this document GigabitEthernet0/0/0)

Update Tunnel

Basic Settings

Tunnel Type IPsec

Interface Name (1..255)

Description

Tunnel Source Interface

Data-Center Primary Secondary

Tunnel Route-via Interface

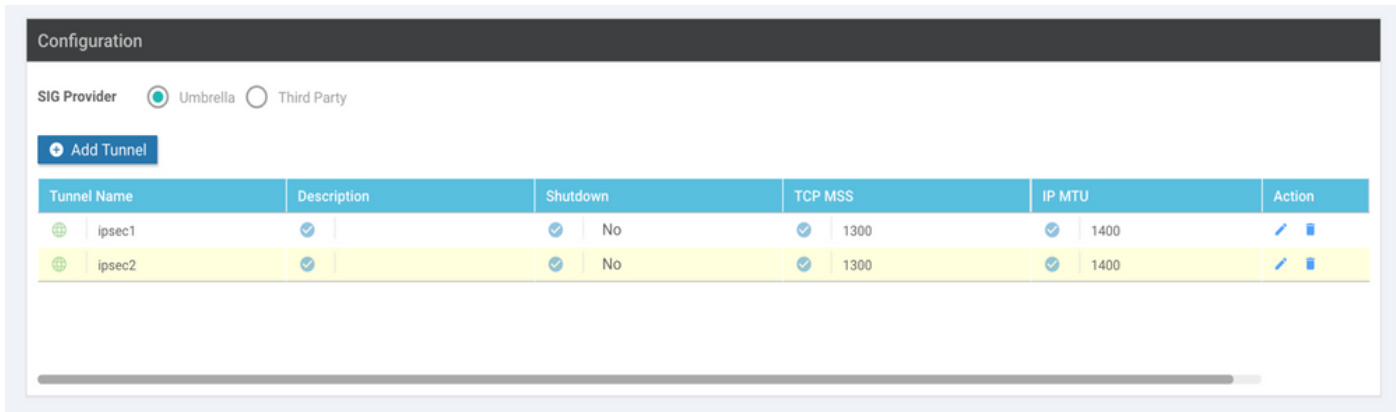
Advanced Options >

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

Step 5. Add the Secondary Tunnel.

Add a second tunnel configuration, use **Data-Center** as **Primary** as well, and the interface name as *ipsec2*.

vManage configuration appears as shown here:

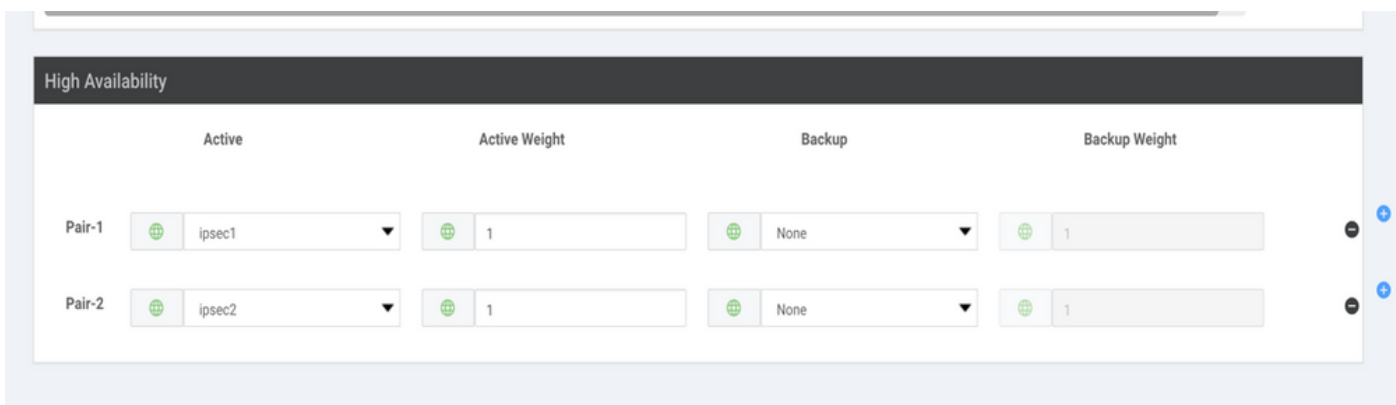


Step 6. Create Two High Availability Pairs.

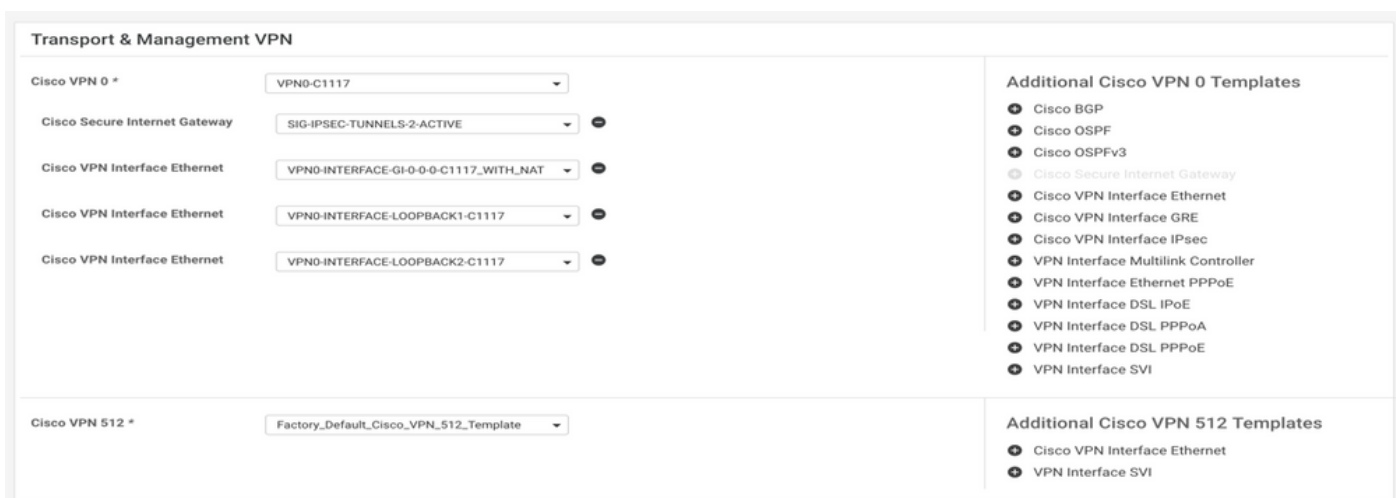
Within the **High Availability** section, create two **High Availability** pairs.

- In the first HA pair, select the ipsec1 as Active and select **None** for backup.
- In the second HA pair, select the ipsec2 as Active select **None** and for backup.

The vManage configuration for **High Availability** appears as shown:



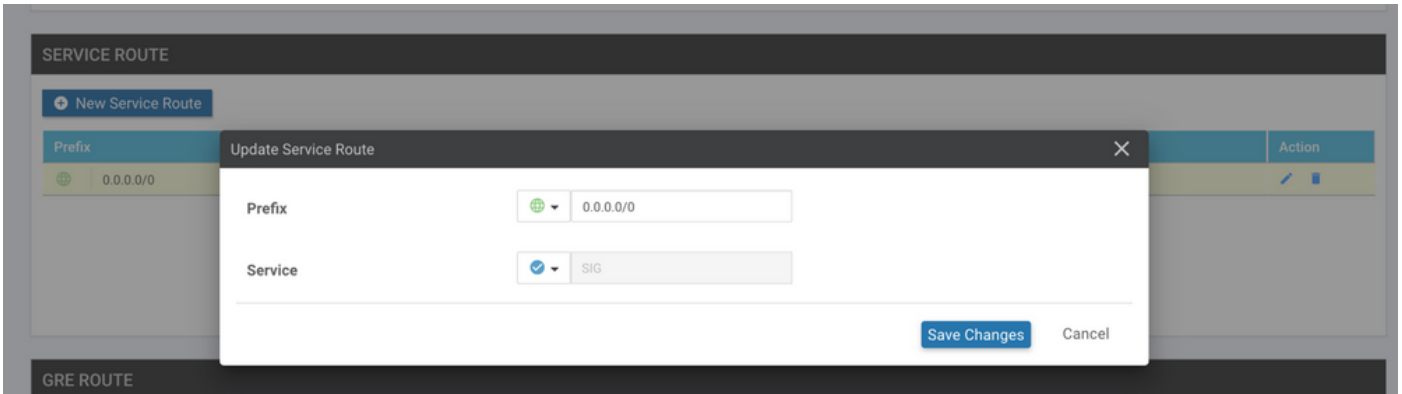
The device template has the two Loopback templates and the SIG feature template attached as well.




Step 7. Edit Service-side VPN Template to Inject a Service Route.

Navigate to the **Service VPN** section and within the VPN of service template, navigate to the section **Service Route**

and add a **0.0.0.0** with **SIG** Service Route



The 0.0.0.0 SIG route appears as shown here.

 **Note:** For the Service traffic to actually go out, NAT has to be configured in the WAN interface.

Attach this template to the device and push the configuration.


WAN Edge Router Configuration for Active/Active Scenario

```
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
!
```

 **Note:** Although this document is **Umbrella** focused, the same scenarios apply for Azure and Third-party SIG tunnels.

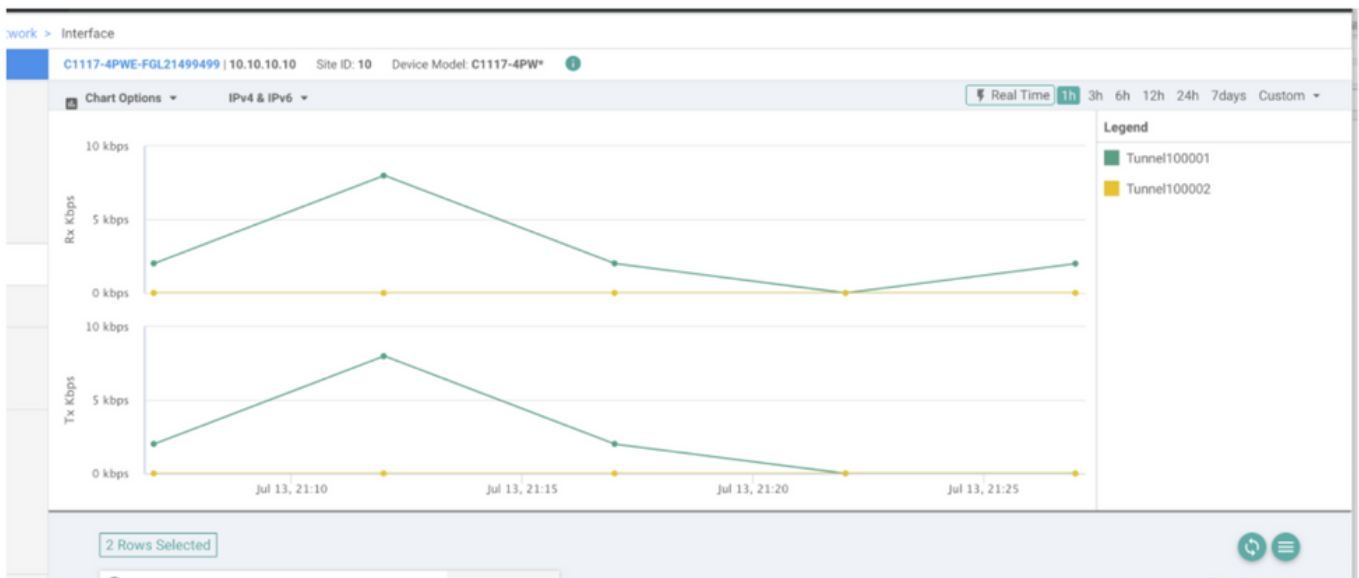
Verify

Verify Active/Backup Scenario

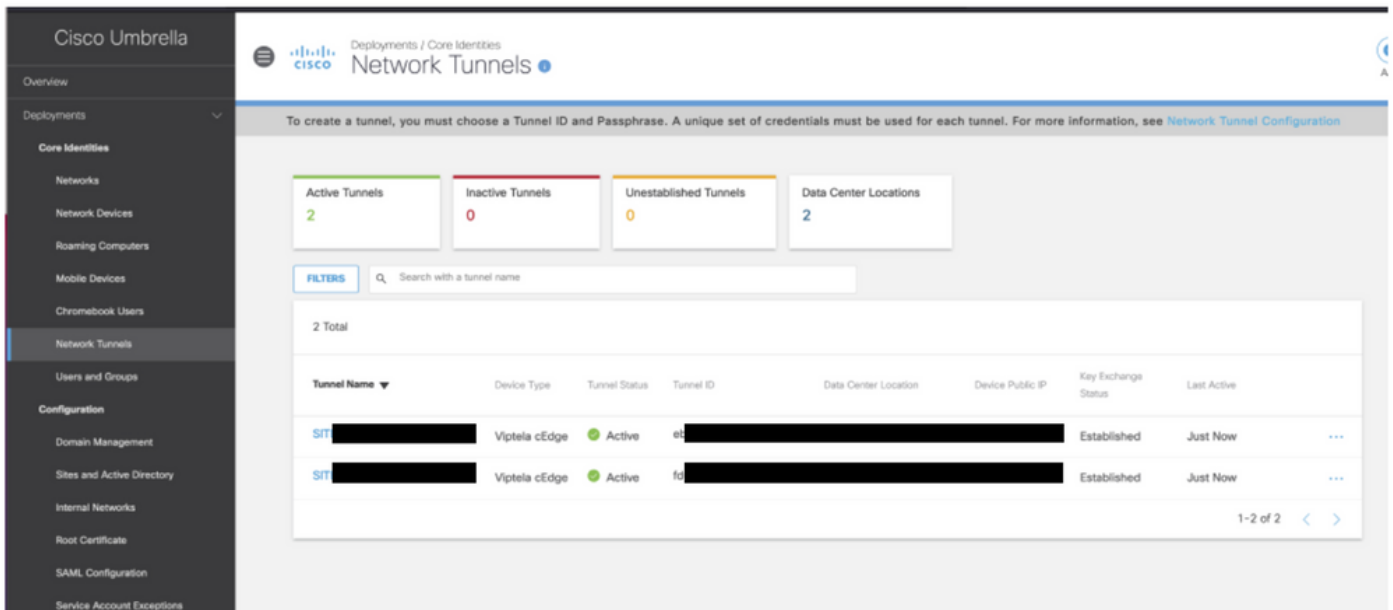
In the vManage, it is possible to monitor the status of the SIG IPsec tunnels. Navigate to **Monitor > Network**, select the WAN edge device desired.

Click the **Interfaces** tab on the left side; a list of all interfaces in the device is displayed. This includes the ipsec1 and ipsec2 interfaces.

The image shows that the ipsec1 tunnel forwards all the traffic and the ipsec2 does not pass traffic.



It is also possible to verify the Tunnels on the Cisco **Umbrella** portal s shown in the image.



The screenshot shows the Cisco Umbrella Network Tunnels portal. The left sidebar contains navigation options: Overview, Deployments, Core Identities, Networks, Network Devices, Roaming Computers, Mobile Devices, Chromebook Users, Network Tunnels (selected), Users and Groups, and Configuration. The main content area displays 'Network Tunnels' with a summary of tunnel status: Active Tunnels (2), Inactive Tunnels (0), Unestablished Tunnels (0), and Data Center Locations (2). Below this is a search bar and a table listing the tunnels.

Tunnel Name	Device Type	Tunnel Status	Tunnel ID	Data Center Location	Device Public IP	Key Exchange Status	Last Active	
SIT [REDACTED]	Viptela cEdge	Active	et [REDACTED]			Established	Just Now	...
SIT [REDACTED]	Viptela cEdge	Active	fo [REDACTED]			Established	Just Now	...

1-2 of 2 < >

Use the `show sdwan secure-internet-gateway tunnels` command on the CLI in order to display the Tunnels information.

```
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 the `show endpoint-tracker` and `show ip sla summary` commands on the CLI in order to display information on the auto-generated trackers and SLAs.

```
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

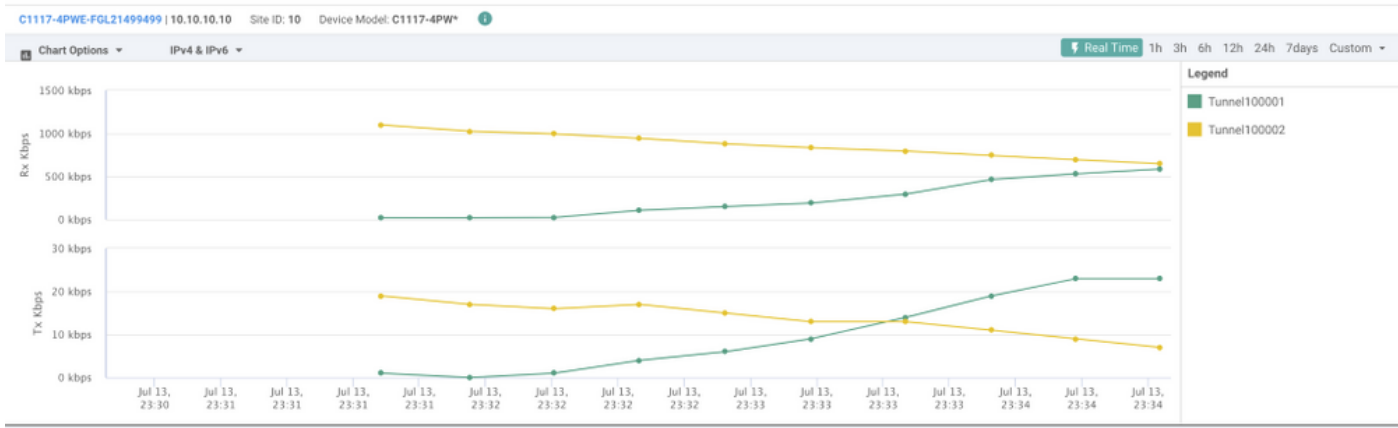
ID	Type	Destination	Stats	Return Code	Last Run
*12	http	10.10.10.10	RTT=6	OK	8 seconds ago
*14	http	10.10.10.10	RTT=17	OK	3 seconds ago

Verify Active/Active Scenario

In the vManage is possible to monitor the status of the SIG IPsec tunnels. Navigate to **Monitor > Network**, select the WAN edge device desired.

Click the **Interfaces** tab on the left side - and a list of all interfaces in the device is displayed. This includes the ipsec1 and ipsec2 interfaces.

The image shows that both ipsec1 and ipsec2 tunnels forward traffic.



Use the `show sdwan secure-internet-gateway tunnels` command on the CLI in order to display the Tunnels information.

```
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 the `show endpoint-tracker` and `show ip sla summary` commands on the CLI in order to display information on the auto-generated trackers and SLAs.

```
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

Related Information

- [Integrate Your Devices With Secure Internet Gateways- Cisco IOS® XE Release 17.x](#)
- [http://Network Tunnel Configuration - Umbrella SIG](#)
- [Umbrella Getting Started](#)
- [Technical Support & Documentation - Cisco Systems](#)