

# Configurazione dei tunnel Umbrella SIG per scenari attivi/di backup o attivi/attivi

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Panoramica di Cisco Umbrella SIG](#)

[Limitazione della larghezza di banda del tunnel Umbrella SIG](#)

[Ottieni le informazioni sul tuo Cisco Umbrella Portal](#)

[Ottieni la chiave e la chiave segreta](#)

[Ottieni ID organizzazione](#)

[Creazione di tunnel Umbrella SIG con scenario attivo/backup](#)

[Passaggio 1. Creare un modello di funzionalità per le credenziali SIG.](#)

[Passaggio 2. Create un modello di feature SIG.](#)

[Passaggio 3. Selezionare il provider SIG per il tunnel primario.](#)

[Passaggio 4. Aggiungere il tunnel secondario.](#)

[Passaggio 5. Creare Una Coppia Ad Alta Disponibilità.](#)

[Passaggio 6. Modificare il modello VPN sul lato servizio per inserire un route del servizio.](#)

[Configurazione di WAN Edge Router per scenario di backup/attivo](#)

[Crea tunnel Umbrella SIG con scenario attivo/attivo](#)

[Passaggio 1. Creare un modello di funzionalità per le credenziali SIG.](#)

[Passaggio 2. Creare due interfacce di loopback per collegare i tunnel SIG.](#)

[Passaggio 3. Create un modello di feature SIG.](#)

---

## Introduzione

In questo documento viene descritto come configurare i tunnel Cisco Umbrella Secure Internet Gateway (SIG) con IPsec in modalità attiva/attiva e attiva/standby

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Umbrella
- Negoziazione IPsec

- SD-WAN (Wide Area Network) definito dal software Cisco

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

### Panoramica di Cisco Umbrella SIG

Cisco Umbrella è un servizio di sicurezza fornito tramite cloud che riunisce funzioni essenziali.

Umbrella unifica gateway Web sicuro, sicurezza DNS, firewall fornito dal cloud, funzionalità di broker di sicurezza di accesso cloud e intelligence delle minacce.

Ispezione e controllo approfonditi garantiscono la conformità con le policy web ad uso accettabile e la protezione contro le minacce di Internet.

I router SD-WAN possono integrarsi con i gateway SIG (Secure Internet Gateway) che eseguono la maggior parte delle operazioni di elaborazione per proteggere il traffico aziendale.

Quando il SIG è configurato, tutto il traffico del client, basato su route o criteri, viene inoltrato al SIG.

### Limitazione della larghezza di banda del tunnel Umbrella SIG

Ogni tunnel IPsec IKEv2 tra l'headend Umbrella è limitato a circa 250 Mbps, quindi se vengono creati più tunnel e viene bilanciato il carico del traffico, questi superano queste limitazioni in caso sia necessaria una larghezza di banda più elevata.

È possibile creare fino a quattro coppie di tunnel ad alta disponibilità.

## Ottieni le informazioni sul tuo Cisco Umbrella Portal

Per procedere con l'integrazione SIG, è necessario un account Umbrella con pacchetto SIG Essentials.

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


## Otteni la chiave e la chiave segreta

La chiave e la chiave segreta possono essere generate nel momento in cui si ottiene la chiave API di gestione Umbrella (questa chiave si trova in 'Chiavi legacy'). Se non si ricorda o non si è salvata la chiave segreta, fare clic su aggiorna.

 **Attenzione:** se si fa clic sul pulsante di aggiornamento, è necessario aggiornare questi tasti su tutti i dispositivi. L'aggiornamento non è consigliato se sono presenti dispositivi in uso.

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: 15 [redacted] 6 

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

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

## Otteni ID organizzazione


L'ID organizzazione può essere facilmente ottenuto quando si accede a Umbrella dalla barra degli indirizzi del browser.

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


## Creazione di tunnel Umbrella SIG con scenario attivo/backup

 **Nota:** routing e bilanciamento del carico del tunnel IPsec/GRE tramite ECMP: questa

---

 funzione è disponibile in vManage versione 20.4.1 e successive e consente di utilizzare il modello SIG per indirizzare il traffico delle applicazioni verso Cisco Umbrella o un provider SIG di terze parti


---

 Nota: supporto per Zscaler Automatic Provisioning: questa funzione è disponibile su vManage 20.5.1 e versioni successive e consente di automatizzare il provisioning dei tunnel dai router Cisco SD-WAN a Zscaler, utilizzando le credenziali API del partner Zscaler.

---

Per configurare i tunnel automatici SIG, è necessario creare/aggiornare alcuni modelli:

- Creare un modello di funzionalità per le credenziali SIG.
  - Creare due interfacce di loopback per collegare i tunnel SIG (applicabile solo a più tunnel attivi contemporaneamente - scenario Attivo/Attivo).
  - Create un modello di feature SIG.
  - Modificare il modello VPN sul lato servizio per inserire una route del servizio.
- 

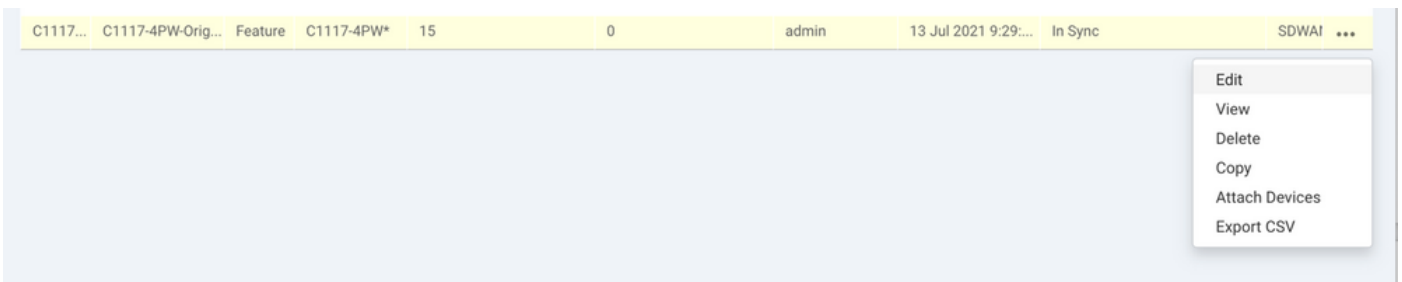
 Nota: verificare che le porte UDP 4500 e 500 siano consentite da qualsiasi dispositivo upstream.

---

Le configurazioni dei modelli cambiano con gli scenari Attivo/Backup e Attivo/Attivo per i quali entrambi gli scenari vengono spiegati ed esposti separatamente.

## Passaggio 1. Creare un modello di funzionalità per le credenziali SIG.

Andare al modello di feature e fare clic su Modifica (Edit).



ID	Name	Type	Feature	Status	Version	Admin	Last Sync	Sync Status	Location
C1117...	C1117-4PW-Orig...	Feature	C1117-4PW*	15	0	admin	13 Jul 2021 9:29:...	In Sync	SDWAN ...

Nella sezione Modelli aggiuntivi, fare clic su Cisco SIG Credentials. L'opzione è mostrata nell'immagine.

## 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 ▼	

Assegnare un nome e una descrizione al modello.

**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](#)

Passaggio 2. Create un modello di feature SIG.

Passare al modello di funzionalità e, nella sezione VPN di trasporto e gestione, selezionare il modello di funzionalità 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

Assegnare un nome e una descrizione al modello.

Passaggio 3. Selezionare il provider SIG per il tunnel primario.

Fare clic su Aggiungi 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](#)

Configurare i dettagli di base e mantenere il centro dati come principale, quindi fare clic su Aggiungi.

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

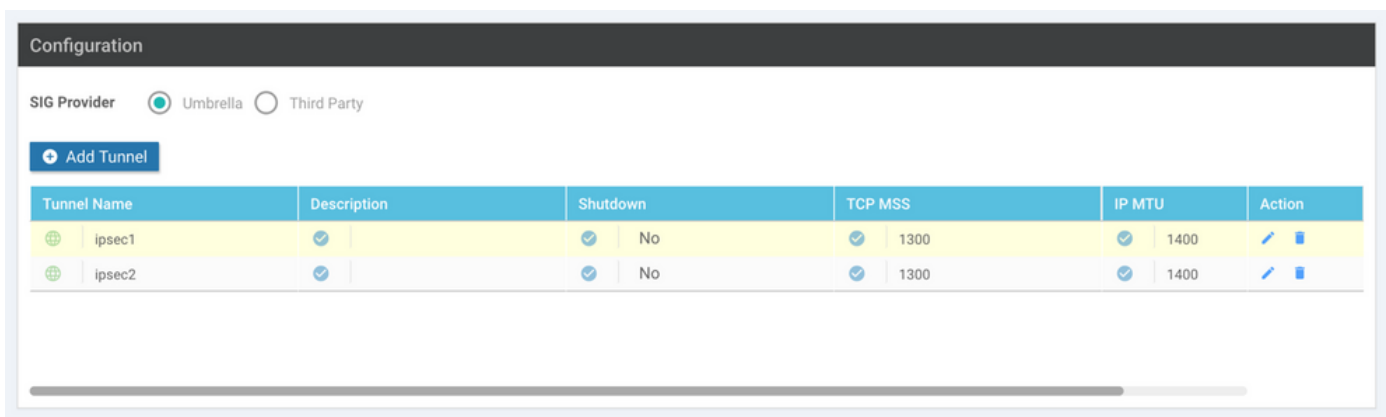
TCP MSS

IP MTU

Passaggio 4. Aggiungere il tunnel secondario.

Aggiungere una seconda configurazione del tunnel, utilizzare Data-Center come Secondario questa volta e il nome dell'interfaccia come ipsec2.

La configurazione di vManage viene visualizzata come illustrato di seguito:

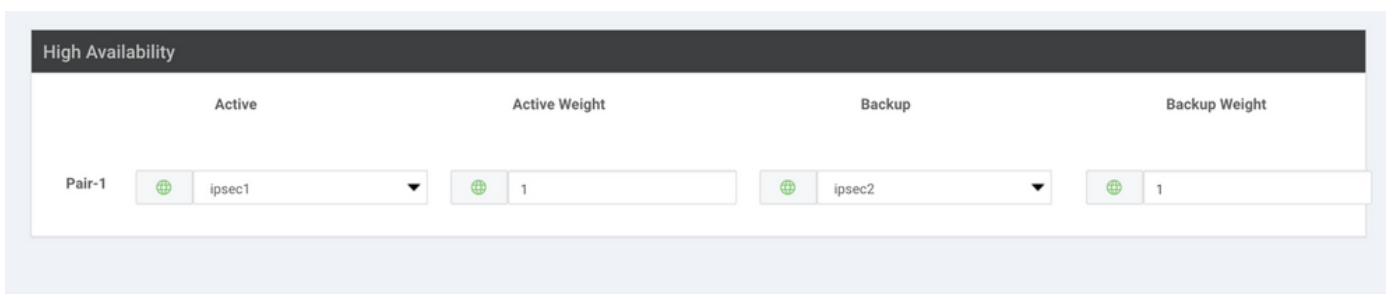


The screenshot shows the 'Configuration' page in vManage. At the top, there are radio buttons for 'SIG Provider' with 'Umbrella' selected and 'Third Party' unselected. Below this is a blue button labeled '+ Add Tunnel'. The main part of the page is a table with the following columns: Tunnel Name, Description, Shutdown, TCP MSS, IP MTU, and Action. There are two rows of tunnels listed: 'ipsec1' and 'ipsec2'. Both have a checkmark in the Description column, a checkmark and 'No' in the Shutdown column, a checkmark and '1300' in the TCP MSS column, and a checkmark and '1400' in the IP MTU column. The Action column contains edit and delete icons for each tunnel.


Tunnel Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1	✓	✓ No	✓ 1300	✓ 1400	[edit] [delete]
ipsec2	✓	✓ No	✓ 1300	✓ 1400	[edit] [delete]

## Passaggio 5. Creare Una Coppia Ad Alta Disponibilità.

Nella sezione Alta disponibilità selezionare ipsec1 come Attivo e il tunnel ipsec2 come Backup.

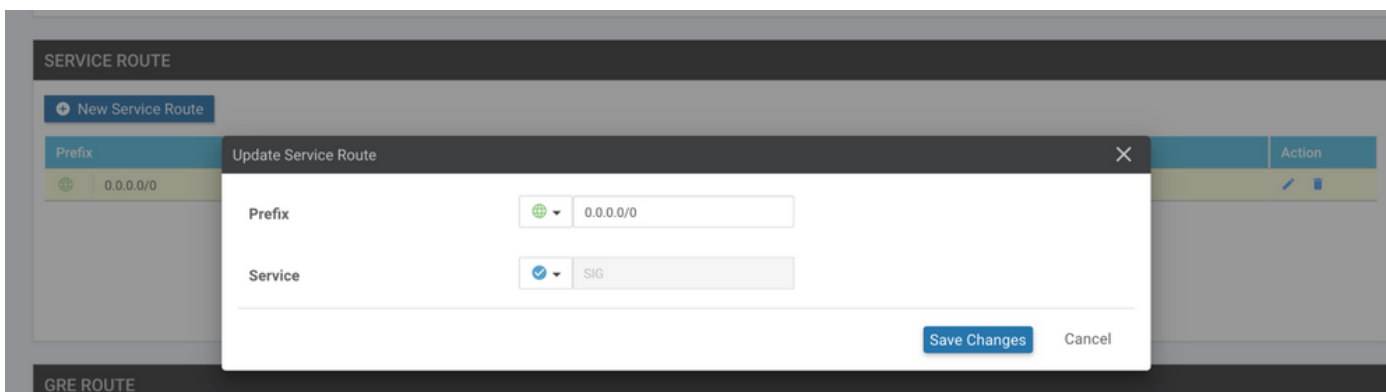


The screenshot shows the 'High Availability' configuration page. It features four input fields: 'Active', 'Active Weight', 'Backup', and 'Backup Weight'. The 'Active' field has a dropdown menu with 'ipsec1' selected. The 'Active Weight' field has the value '1'. The 'Backup' field has a dropdown menu with 'ipsec2' selected. The 'Backup Weight' field has the value '1'. There is a 'Pair-1' label on the left side of the configuration area.

 Nota: è possibile creare contemporaneamente fino a 4 coppie di tunnel ad alta disponibilità e un massimo di 4 tunnel attivi.

## Passaggio 6. Modificare il modello VPN sul lato servizio per inserire un route del servizio.

Passare alla sezione Service VPN e, all'interno del modello Service VPN, passare alla sezione Service Route, quindi aggiungere uno 0.0.0.0 con il percorso del servizio SIG. Per questo documento, viene usato il VRF/VPN 10.



The screenshot shows the 'SERVICE ROUTE' configuration page. A modal dialog titled 'Update Service Route' is open in the foreground. The dialog has two input fields: 'Prefix' with the value '0.0.0.0/0' and 'Service' with a dropdown menu showing 'SIG' selected. At the bottom of the dialog are two buttons: 'Save Changes' and 'Cancel'. In the background, the 'SERVICE ROUTE' table is visible, showing a row for the prefix '0.0.0.0/0' with an edit icon in the 'Action' column.

Viene visualizzata la route 0.0.0.0 SIG, come mostrato di seguito.



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: per consentire l'effettiva uscita del traffico di servizio, è necessario configurare NAT nell'interfaccia WAN.

Collegare questo modello al dispositivo e spingere la configurazione:

**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.

```

## Configurazione di WAN Edge Router per scenario di backup/attivo

```

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
```

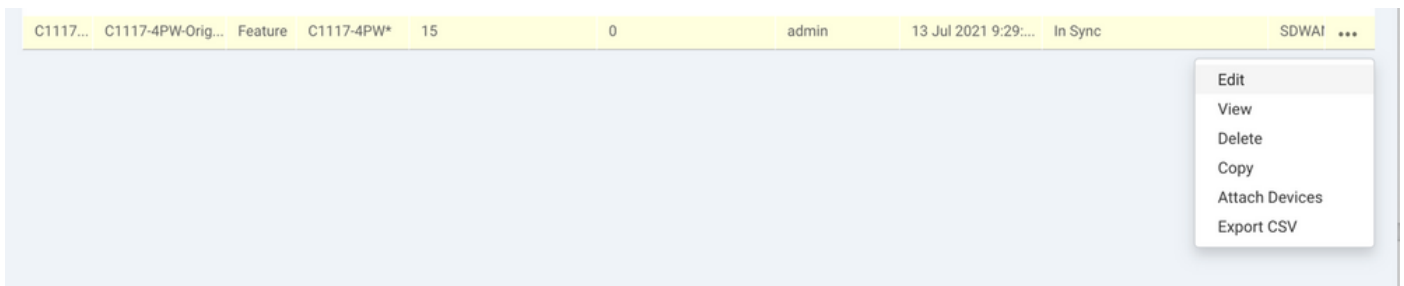
```
tunnel mode sdwan
exit
interface Tunnel100001
no shutdown
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
tunnel source GigabitEthernet0/0/0
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec1-ipsec-profile
tunnel vrf multiplexing
exit
interface Tunnel100002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

## Crea tunnel Umbrella SIG con scenario attivo/attivo

Passaggio 1. Creare un modello di funzionalità per le credenziali SIG.

Passate al modello di feature e fate clic su Modifica (Edit).



Nella sezione Modelli aggiuntivi, selezionare Cisco SIG Credentials. L'opzione viene visualizzata sull'immagine.

## 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 ▼	

Assegnare un nome e una descrizione al modello.

**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](#)

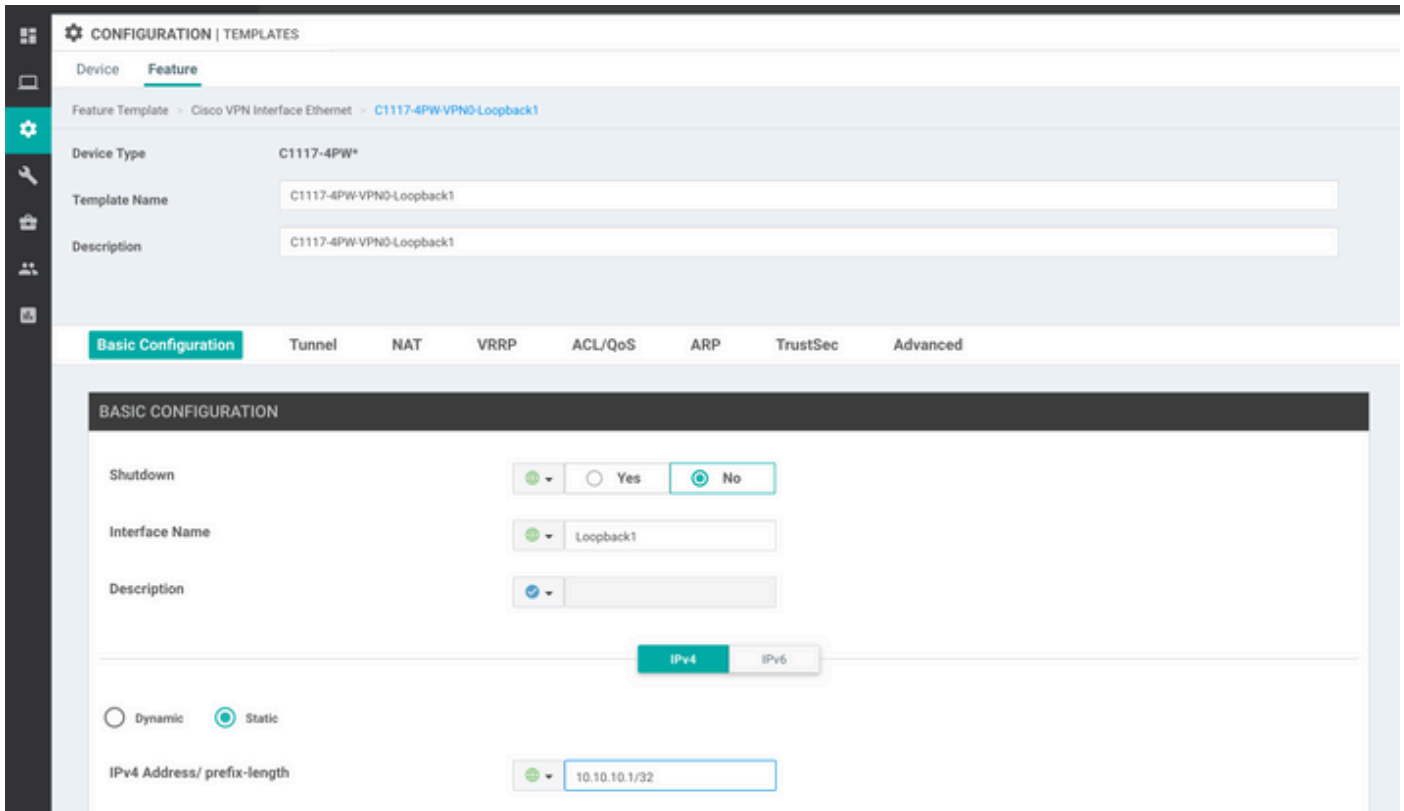
Passaggio 2. Creare due interfacce di loopback per collegare i tunnel SIG.

 Nota: creare un'interfaccia di loopback per ciascun tunnel SIG configurato in modalità attiva. Questa operazione è necessaria perché ciascun tunnel ha bisogno di un ID IKE univoco.

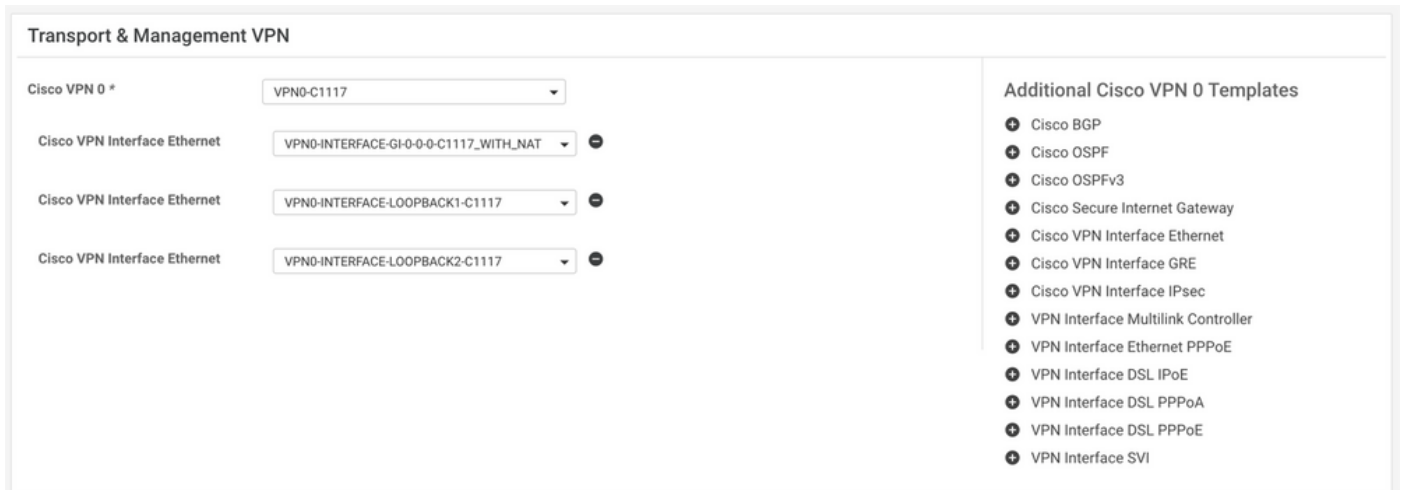
 Nota: poiché questo scenario è Attivo/Attivo, vengono creati due loopback.

Configurare il nome dell'interfaccia e l'indirizzo IPv4 per il loopback.

 Nota: l'indirizzo IP configurato per il loopback è un indirizzo fittizio.



Creare il secondo modello di loopback e allegarlo al modello di dispositivo. Al modello di dispositivo devono essere collegati due modelli di loopback:



Passaggio 3. Create un modello di feature SIG.

Andare al modello della funzionalità SIG e, nella sezione VPN di trasporto e gestione, selezionare Cisco Secure Internet Gateway feature template.

Passaggio 4. Selezionare il provider SIG per il tunnel primario.

Fare clic su Aggiungi 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](#)

Configurare i dettagli di base e mantenere il centro dati come principale.

 Nota: il parametro Tunnel Source Interface è il loopback (per questo documento Loopback1) e come Tunnel Route-via Interface l'interfaccia fisica (per questo documento Gigabit Ethernet0/0/0)

Update Tunnel

**Basic Settings**

Tunnel Type IPsec

Interface Name (1..255)

Description

Tunnel Source Interface

Data-Center  Primary  Secondary

Tunnel Route-via Interface

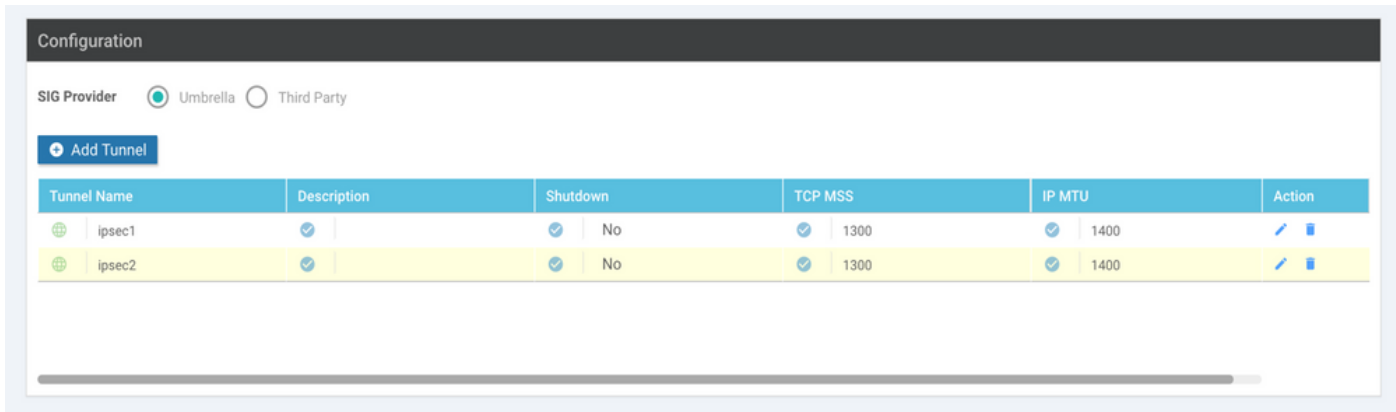
Advanced Options >

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

Passaggio 5. Aggiungere il tunnel secondario.

Aggiungere una seconda configurazione del tunnel, utilizzare anche Data-Center come primario e il nome dell'interfaccia come ipsec2.

La configurazione di vManage viene visualizzata come illustrato di seguito:

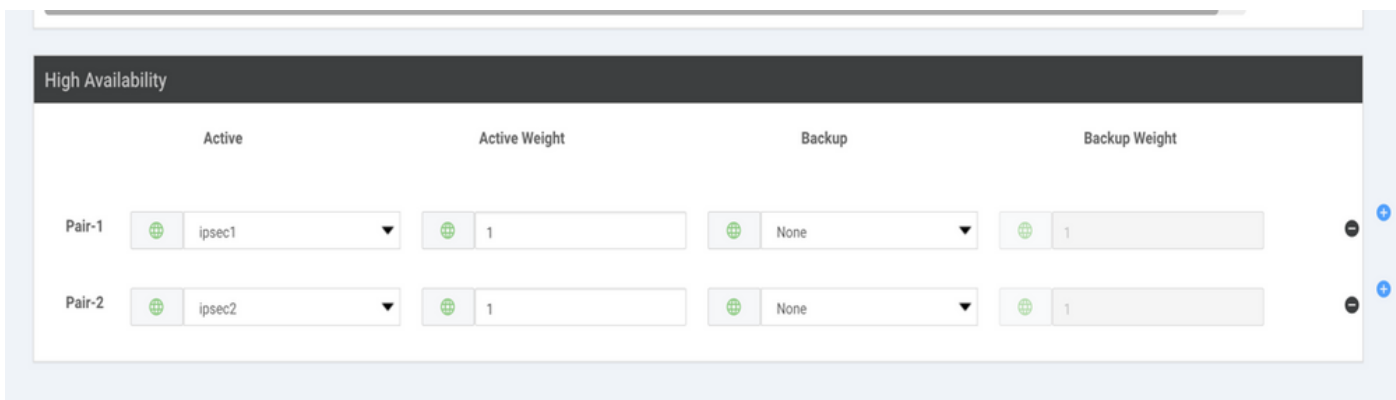


## Passaggio 6. Creare Due Coppie Di Disponibilità Elevata.

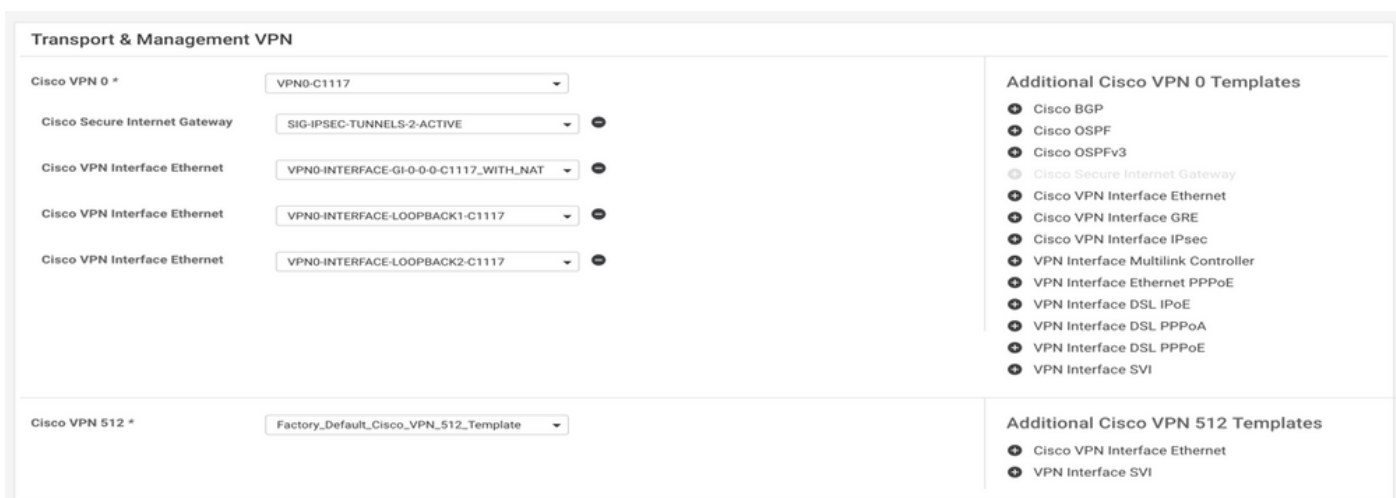
All'interno della sezione Alta disponibilità, creare due coppie Alta disponibilità.

- Nella prima coppia HA, selezionare ipsec1 come Attivo e Nessuno per il backup.
- Nella seconda coppia HA, selezionare ipsec2 come Attivo, selezionare Nessuno e per il backup.

La configurazione di vManage per l'alta disponibilità viene visualizzata come illustrato di seguito:



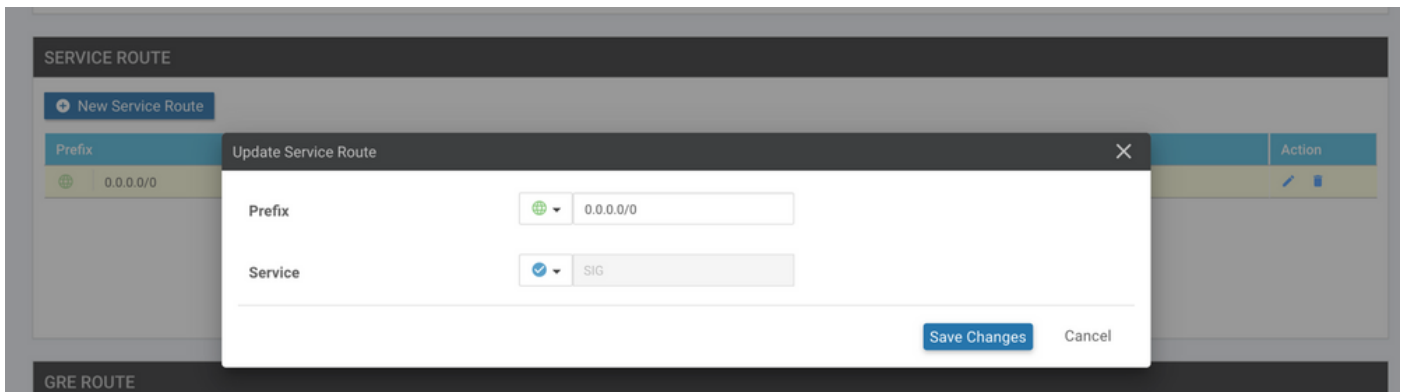
Al modello di dispositivo sono allegati i due modelli di loopback e il modello di funzionalità SIG.




Passaggio 7. Modificare il modello VPN sul lato servizio per inserire un route del

servizio.

Passare alla sezione Service VPN e, all'interno del modello VPN of service, passare alla sezione Service Route e aggiungere un percorso di servizio 0.0.0.0 con SIG.



Il percorso SIG 0.0.0 viene visualizzato come mostrato di seguito.

 Nota: per consentire l'effettiva uscita del traffico di servizio, è necessario configurare NAT nell'interfaccia WAN.

Collegare questo modello al dispositivo e premere la configurazione.

## Configurazione di WAN Edge Router per uno scenario attivo/attivo


```
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: anche se questo documento è incentrato su Umbrella, gli stessi scenari si applicano ai tunnel SIG di Azure e di terze parti.

## Verifica

### Verifica scenario attivo/backup

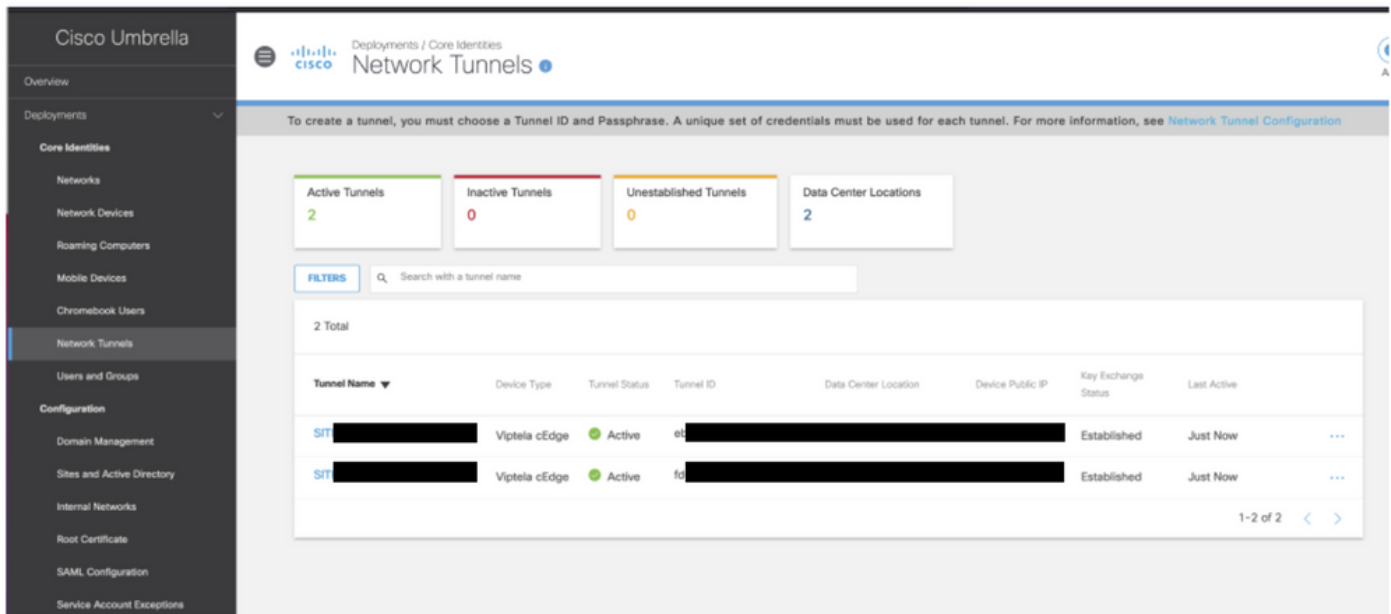
In vManage è possibile monitorare lo stato dei tunnel IPsec SIG. Selezionare Monitor > Network (Monitor > Rete), quindi selezionare il dispositivo periferico WAN desiderato.

Fare clic sulla scheda Interfacce sul lato sinistro; viene visualizzato un elenco di tutte le interfacce nel dispositivo. incluse le interfacce ipsec1 e ipsec2.

Nell'immagine viene mostrato come il tunnel ipsec1 inoltri tutto il traffico e come ipsec2 non lo passi.



È anche possibile verificare i tunnel sul portale Cisco Umbrella come mostrato nell'immagine.



Usare il comando `show sdwan secure-internet-gateway tunnel` sulla CLI per visualizzare le informazioni sui tunnel.

```
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

Usare i comandi `show endpoint-tracker` e `show ip sla summary` sulla CLI per visualizzare informazioni sui tracker e sugli SLA generati automaticamente.

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

Interface	Record Name	Status	RTT in msec	Probe ID	Next Hop
Tunnel100001	#SIGL7#AUTO#TRACKER	Up	8	14	None
Tunnel100002	#SIGL7#AUTO#TRACKER	Up	2	12	None

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

IPSLAs Latest Operation Summary

Codes: \* active, ^ inactive, ~ pending

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

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

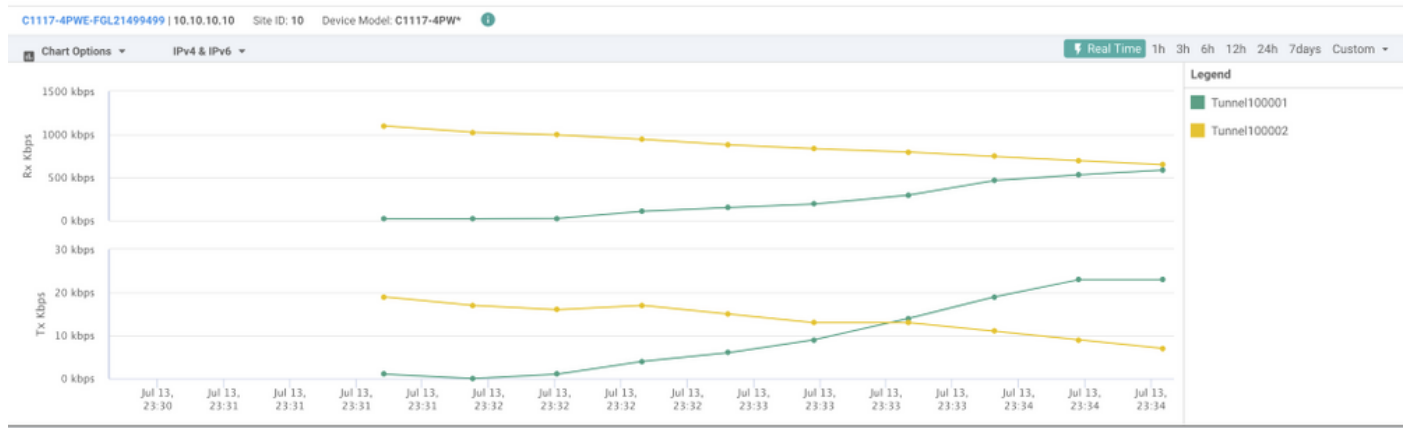


## Verifica scenario attivo/attivo

In vManage è possibile monitorare lo stato dei tunnel IPsec SIG. Selezionare Monitor > Network (Monitor > Rete), quindi selezionare il dispositivo periferico WAN desiderato.

Fare clic sulla scheda Interfacce sul lato sinistro. Viene visualizzato un elenco di tutte le interfacce presenti nel dispositivo, incluse le interfacce ipsec1 e ipsec2.

Nell'immagine viene mostrato come i tunnel ipsec1 e ipsec2 inoltrino il traffico.



Usare il comando `show sdwan secure-internet-gateway tunnel` sulla CLI per visualizzare le informazioni sui tunnel.

```
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

Usare i comandi `show endpoint-tracker` e `show ip sla summary` sulla CLI per visualizzare informazioni sui tracker e sugli SLA generati automaticamente.

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

Interface	Record Name	Status	RTT in msec	Probe ID	Next Hop
Tunnel100001	#SIGL7#AUTO#TRACKER	Up	8	14	None
Tunnel100002	#SIGL7#AUTO#TRACKER	Up	2	12	None

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

IPSLAs Latest Operation Summary

Codes: \* active, ^ inactive, ~ pending

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

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

## Informazioni correlate

- [Integrazione dei dispositivi con gateway Internet sicuri - Cisco IOS® XE release 17.x](#)
- [http://Network Configurazione tunnel - Umbrella SIG](#)
- [Guida introduttiva a Umbrella](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).