

Configuration des tunnels SIG Umbrella pour les scénarios actifs/de sauvegarde ou actifs/actifs

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Présentation de Cisco Umbrella SIG](#)

[Limitation de la bande passante du tunnel Umbrella SIG](#)

[Obtenir les informations relatives au portail Cisco Umbrella](#)

[Obtenir la clé et la clé secrète](#)

[Obtenir votre ID d'entreprise](#)

[Créer des tunnels SIG de parapluie avec un scénario actif/de sauvegarde](#)

[Étape 1. Créer un modèle de fonction Informations d'identification SIG.](#)

[Étape 2. Créer un modèle de fonctionnalité SIG.](#)

[Étape 3. Sélectionnez votre fournisseur SIG pour le tunnel principal.](#)

[Étape 4. Ajoutez le tunnel secondaire.](#)

[Étape 5. Créez Une Paire Haute Disponibilité.](#)

[Étape 6. Modifier le modèle VPN côté service pour injecter une route de service.](#)

[Configuration du routeur de périphérie WAN pour le scénario actif/de sauvegarde](#)

[Créer des tunnels SIG de parapluie avec un scénario actif/actif](#)

[Étape 1. Créer un modèle de fonction Informations d'identification SIG.](#)

[Étape 2. Créez deux interfaces de bouclage pour relier les tunnels SIG.](#)

[Étape 3. Créer un modèle de fonctionnalité SIG.](#)

Introduction

Ce document décrit comment configurer **Cisco Umbrella Secure Internet Gateway (SIG)** tunnels avec IPsec dans les deux **Active/Active** et **Active/Standby**.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- **Cisco Umbrella**
- **Négociation IPsec**

- Réseau étendu défini par logiciel (SD-WAN) de Cisco

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco vManage version 20.4.2
- Routeur de périphérie WAN Cisco C117-4PW* 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Présentation de Cisco Umbrella SIG

Cisco **Umbrella** est un service de sécurité fourni dans le cloud qui rassemble des fonctions essentielles.

Umbrella unifie la passerelle web sécurisée, la sécurité DNS, le pare-feu fourni dans le cloud, la fonctionnalité de courtier de sécurité d'accès au cloud et les informations sur les menaces.

Une inspection et un contrôle approfondis garantissent la conformité avec les politiques d'utilisation acceptable du Web et protègent contre les menaces Internet.

Les routeurs SD-WAN peuvent s'intégrer aux passerelles Internet sécurisées (SIG) qui assurent la majorité du traitement pour sécuriser le trafic de l'entreprise.

Lorsque le SIG est configuré, tout le trafic client, en fonction des routes ou de la politique, est transféré au SIG.

Limitation de la bande passante du tunnel Umbrella SIG

Chaque tunnel IPsec IKEv2 vers le **Umbrella** La tête de réseau est limitée à environ 250 Mbits/s. Par conséquent, si plusieurs tunnels sont créés et que la charge équilibre le trafic, ils surmontent ces limitations au cas où une bande passante plus élevée serait nécessaire.

Jusqu'à quatre **High Availability** des paires de tunnels peuvent être créées.

Obtenir les informations relatives au portail Cisco Umbrella

Afin de procéder à l'intégration de SIG, un **Umbrella** Un compte avec le package SIG essentials est nécessaire.

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

Obtenir la clé et la clé secrète

La clé et la clé secrète peuvent être générées au moment où vous obtenez le **Umbrella Management API KEY** (cette clé se trouve sous « Clés héritées »). Si vous ne vous souvenez pas de la clé secrète ou si vous ne l'avez pas enregistrée, cliquez sur refresh.


 Attention : si vous cliquez sur le bouton d'actualisation, une mise à jour de ces touches est nécessaire sur tous les périphériques. Cette mise à jour n'est pas recommandée si des périphériques sont utilisés.

Umbrella Management

Key: [REDACTED] 36

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](#)


Key: Created:


Obtenir votre ID d'entreprise

L'ID d'organisation peut être facilement obtenu lorsque vous vous connectez à Umbrella dans la barre d'adresse du navigateur.

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

Créer des tunnels SIG de parapluie avec un scénario actif/de sauvegarde

 Remarque : Routage de tunnel IPsec/GRE et équilibrage de charge à l'aide d'ECMP : cette fonctionnalité est disponible dans vManage 20.4.1 et versions ultérieures, elle vous permet d'utiliser le modèle SIG pour diriger le trafic d'applications vers Cisco Umbrella ou un fournisseur SIG tiers

 Remarque : prise en charge du provisionnement automatique Zscaler : cette fonctionnalité est disponible sur vManage 20.5.1 et versions ultérieures. Elle automatise le provisionnement des tunnels des routeurs Cisco SD-WAN vers Zscaler, à l'aide des informations d'identification API des partenaires Zscaler.

Pour configurer les tunnels automatiques SIG, il est nécessaire de créer/mettre à jour quelques modèles :

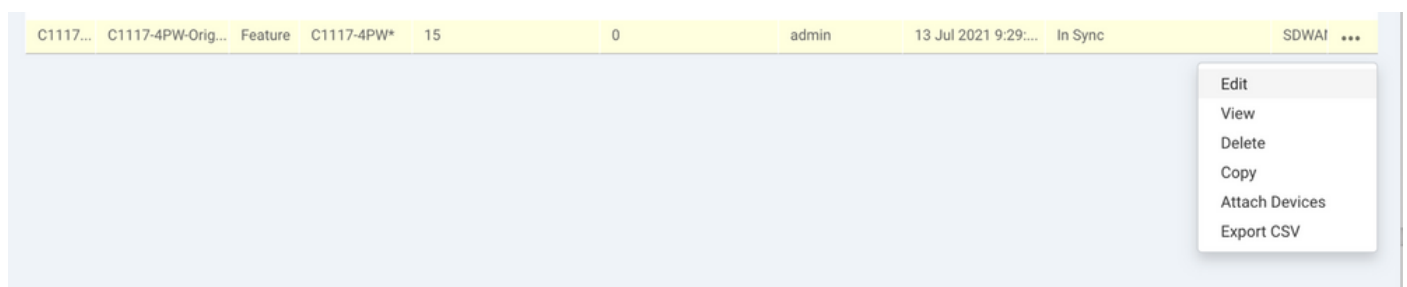
- Créez un modèle de fonction Informations d'identification SIG.
 - Créez deux interfaces de bouclage afin de relier les tunnels SIG (Applicable uniquement avec plusieurs *Active* tunnel en même temps - *Active/Active* scénario).
 - Créez un modèle de fonctionnalité SIG.
 - Modifier le modèle VPN côté service pour injecter un *Service Route*.
-

 Remarque : assurez-vous que les ports UDP 4500 et 500 sont autorisés à partir de tout périphérique en amont.

Les configurations des modèles changent avec la *Active/Backup* et la *Active/Active* scénarios pour lesquels les deux scénarios sont expliqués et exposés séparément.

Étape 1. Créer un modèle de fonction Informations d'identification SIG.

Accédez au modèle de fonction et cliquez sur **Edit**.



Dans la section de **Additional templates**, cliquez sur **Cisco SIG Credentials**. L'option est affichée dans l'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 ▼	

Donnez un nom et une description au modèle.

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](#)

Étape 2. Créer un modèle de fonctionnalité SIG.

Accédez au modèle de fonction et, sous la section **Transport & Management VPN** sélectionnez le modèle de fonctionnalité 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

Donnez un nom et une description au modèle.

Étape 3. Sélectionnez votre fournisseur SIG pour le tunnel principal.

Cliquer **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](#)

Configurez les détails de base et conservez **Data-Center** comme **Primary**, puis cliquez sur **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

Étape 4. Ajout du tunnel secondaire

Ajoutez une deuxième configuration de tunnel, utilisez **Data-Center** comme **Secondary** cette fois, et le nom de l'interface est ipsec2.

La configuration vManage apparaît comme suit :

Configuration

SIG Provider Umbrella Third Party

[+ Add Tunnel](#)

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

Étape 5. Créez Une Paire Haute Disponibilité.

Dans le **High Availability** , sélectionnez ipsec1 comme actif et le tunnel ipsec2 comme sauvegarde.

High Availability

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

 Remarque : jusqu'à 4 **High Availability** des paires de tunnels et un maximum de 4 tunnels actifs peuvent être créés simultanément.

Étape 6. Modifier le modèle VPN côté service pour injecter une route de service.

Accédez à la page **Service VPN** et, dans la section **Service VPN** , accédez à la section **Service Route** et ajoutez un 0.0.0.0 avec SIG **Service Route**. Pour ce document, le VRF/VPN 10 est utilisé.

SERVICE ROUTE

[+ New Service Route](#)

Prefix	Action
0.0.0.0/0	✎ ✖

Update Service Route

Prefix

Service SIG

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

GRE ROUTE

La route SIG 0.0.0.0 s'affiche comme indiqué ici.

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	

Remarque : pour que le trafic du service sorte, la fonction NAT doit être configurée dans l'interface WAN.

Fixez ce modèle au périphérique et poussez la configuration :

TASK VIEW

Push Feature Template Configuration | Validation Success

Initiated By: admin From: 128.107.241.174

Total Task: 1 | In Progress: 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.

Configuration du routeur de périphérie WAN pour le scénario actif/de sauvegarde

```

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
```

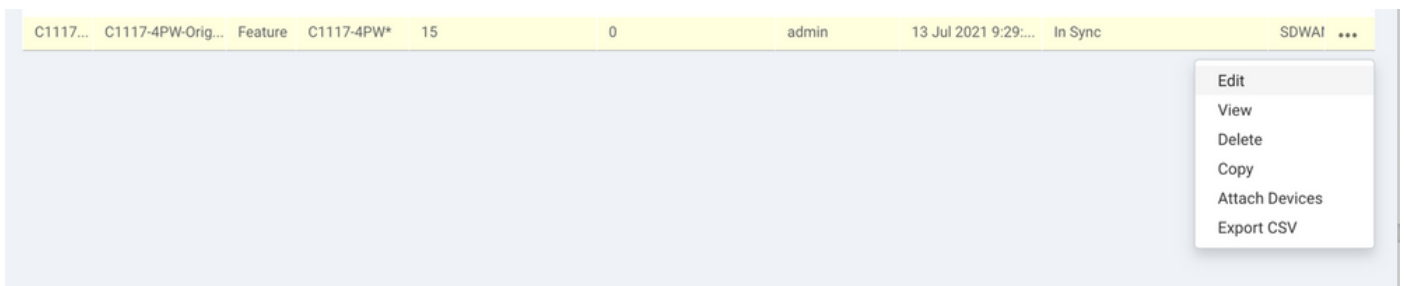
```
tunnel mode sdwan
exit
interface Tunnel100001
no shutdown
ip unnumbered GigabitEthernet0/0/0
ip mtu 1400
tunnel source GigabitEthernet0/0/0
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec1-ipsec-profile
tunnel vrf multiplexing
exit
interface Tunnel100002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

Créer des tunnels SIG de parapluie avec un scénario actif/actif

Étape 1. Créer un modèle de fonction Informations d'identification SIG.

Accédez au modèle de fonction et cliquez sur **Edit**



Dans la section de **Additional templates**, sélectionnez **Cisco SIG Credentials**. L'option est affichée sur l'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 ▼	

Donnez un nom et une description au modèle.

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](#)

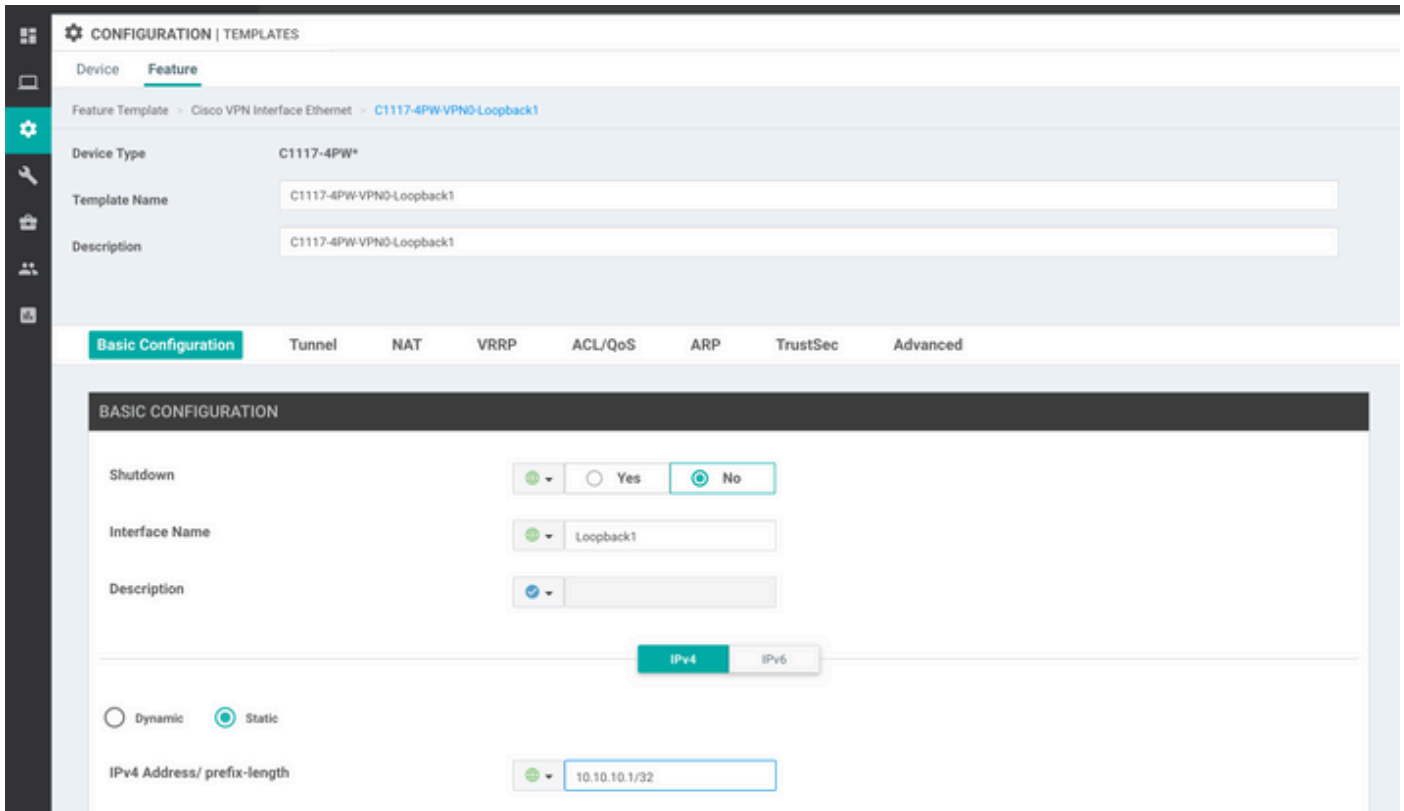
Étape 2. Créez deux interfaces de bouclage pour relier les tunnels SIG.

 Remarque : créez une interface de bouclage pour chaque tunnel SIG configuré en mode actif, car chaque tunnel nécessite un ID IKE unique.

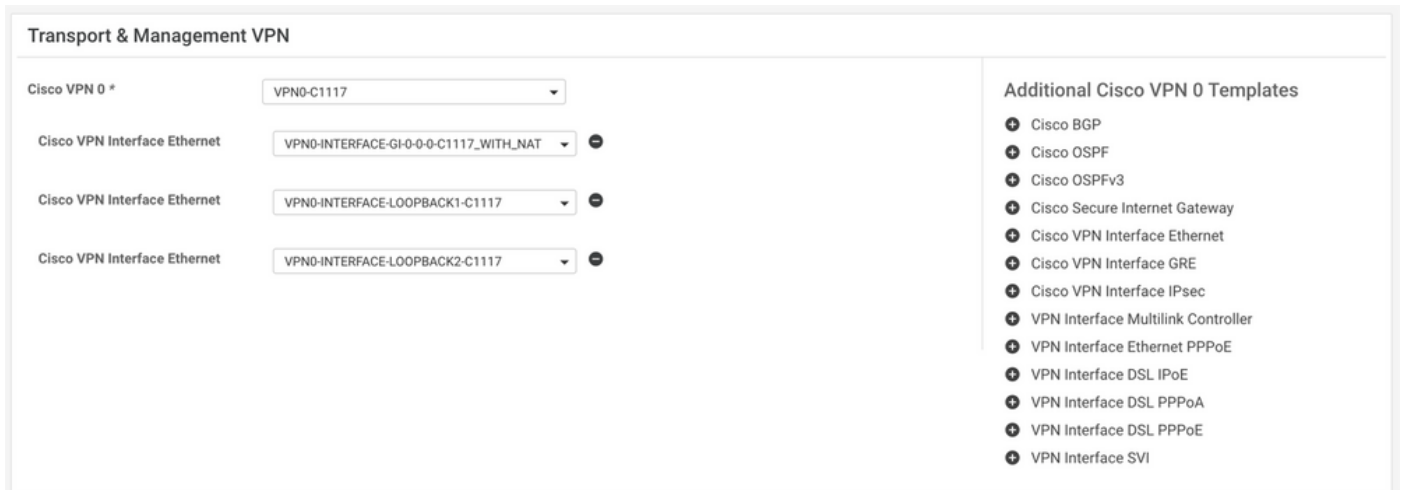
 Remarque : ce scénario est actif/actif. Par conséquent, deux boucles sont créées.

Configurez le nom d'interface et l'adresse IPv4 pour le bouclage.

 Remarque : l'adresse IP configurée pour le bouclage est une adresse fictive.



Créez le deuxième modèle de bouclage et attachez-le au modèle de périphérique. Le modèle de périphérique doit être associé à deux modèles de bouclage :



Étape 3. Créer un modèle de fonctionnalité SIG.

Accédez au modèle de fonction SIG et, sous la section **Transport & Management VPN** sélectionnez **Cisco Secure Internet Gateway** modèle de fonction.

Étape 4. Sélectionnez le fournisseur SIG pour le tunnel principal.

Cliquer **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](#)

Configurez les détails de base et conservez **Data-Center** comme **Primary**.

 Remarque : le paramètre Tunnel Source Interface est Loopback (pour ce document Loopback1) et Tunnel Route-via Interface est l'interface physique (pour ce document 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

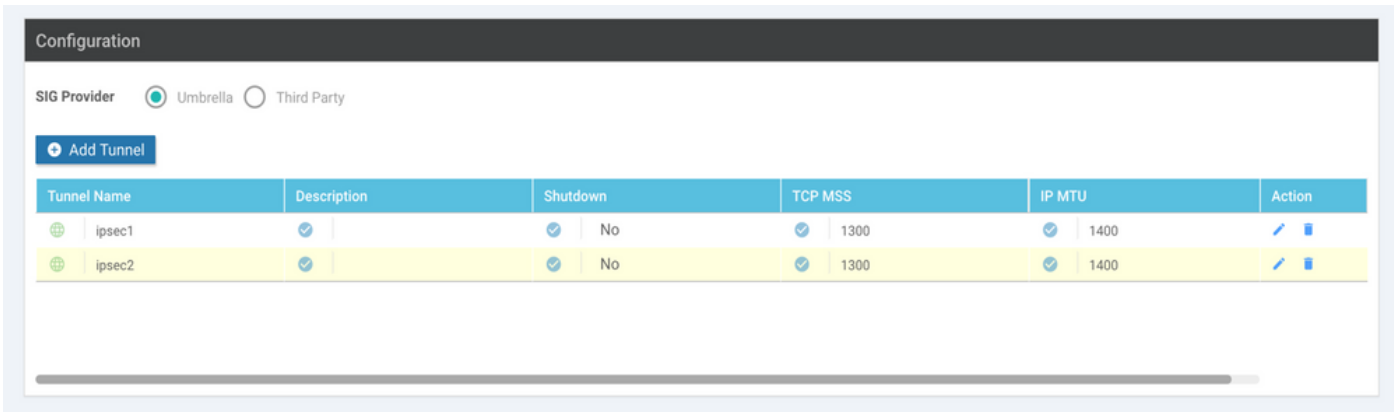
Advanced Options >

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

Étape 5. Ajout du tunnel secondaire

Ajoutez une deuxième configuration de tunnel, utilisez **Data-Center** comme **Primary** et le nom de l'interface comme ipsec2.

La configuration vManage apparaît comme suit :

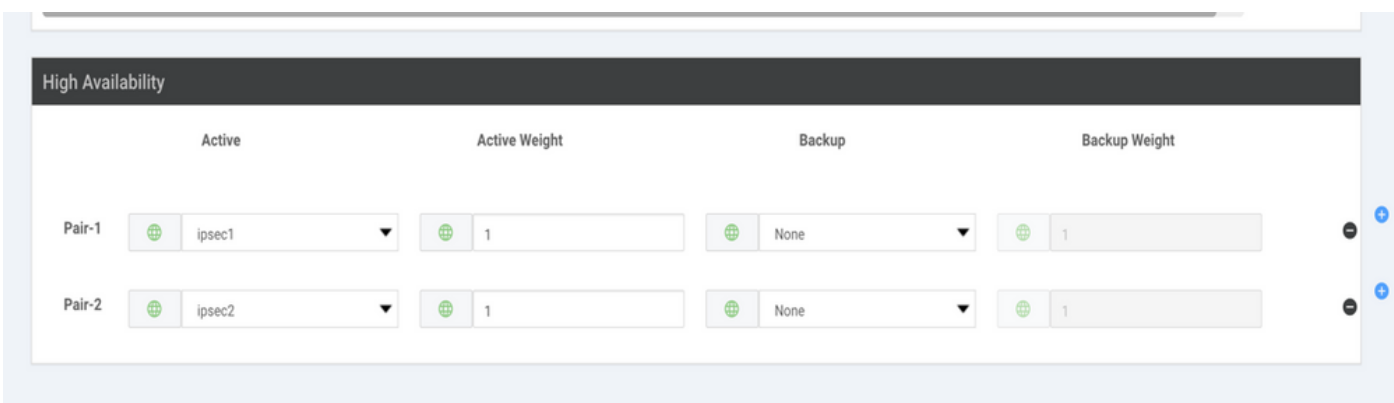


Étape 6. Créez Deux Paires Haute Disponibilité.

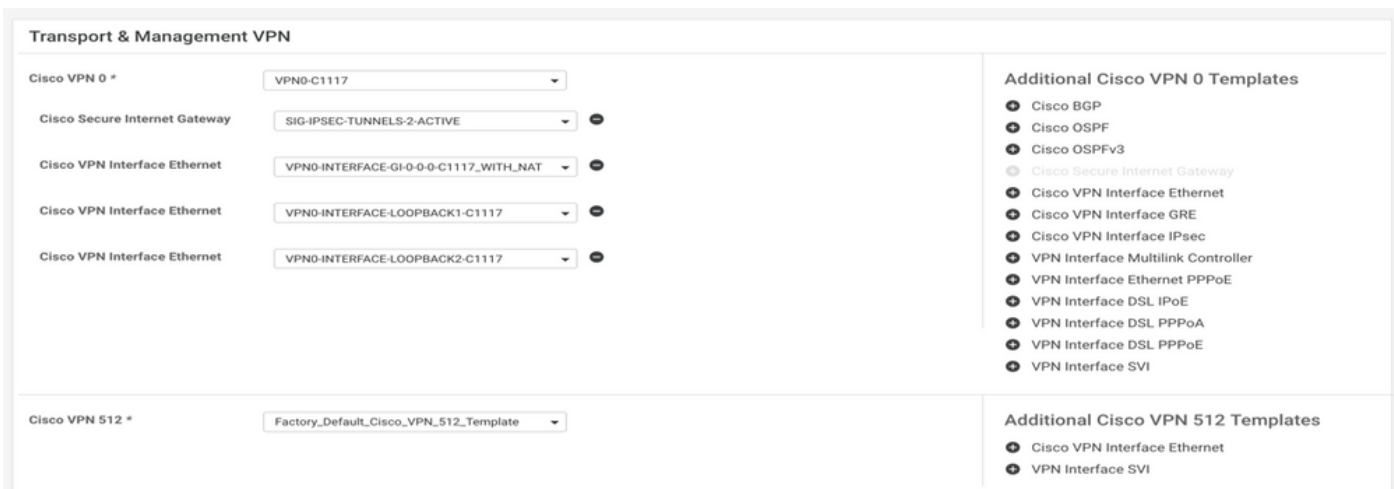
Dans le **High Availability** , créez deux **High Availability** paires.

- Dans la première paire haute disponibilité, sélectionnez ipsec1 comme actif et sélectionnez **None** pour la sauvegarde.
- Dans la deuxième paire de haute disponibilité, sélectionnez ipsec2 comme actif et sélectionnez **None** et pour la sauvegarde.

La configuration vManage pour **High Availability** s'affiche comme suit :

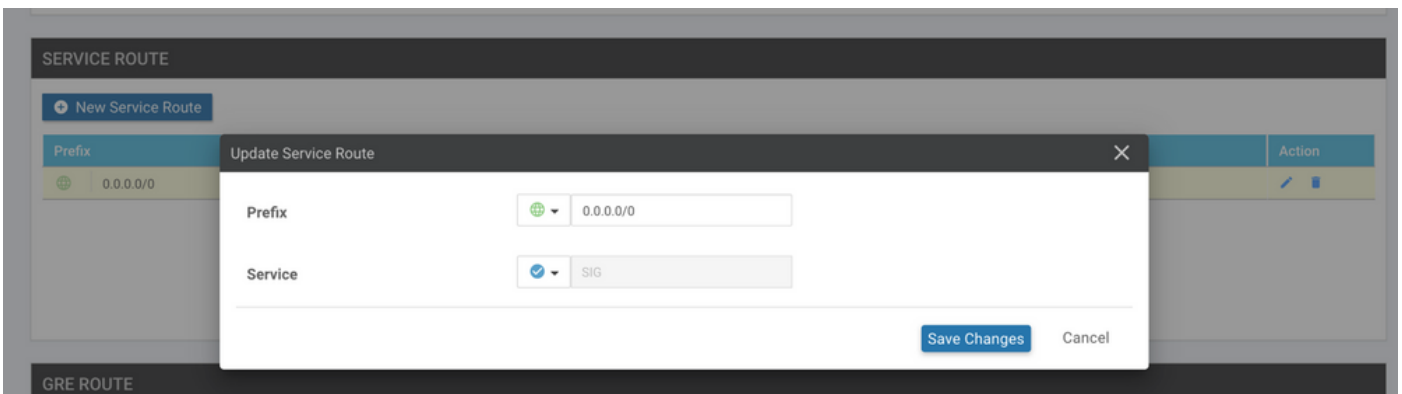


Les deux modèles de bouclage et le modèle de fonctionnalité SIG sont également associés au modèle de périphérique.




Étape 7. Modifier le modèle VPN côté service pour injecter une route de service.

Accédez à la page **Service VPN** et dans le modèle VPN de service, accédez à la section **Service Route** et ajoutez un 0.0.0.0 avec SIG



La route SIG 0.0.0.0 apparaît comme illustré ici.

 **Remarque :** pour que le trafic du service sorte, la fonction NAT doit être configurée dans l'interface WAN.

Fixez ce modèle au périphérique et poussez la configuration.

Configuration du routeur de périphérie WAN pour le scénario actif/actif


```
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
!
```

 Remarque : bien que ce document soit axé sur Umbrella, les mêmes scénarios s'appliquent aux tunnels Azure et SIG tiers.

Vérifier

Vérification du scénario actif/de sauvegarde

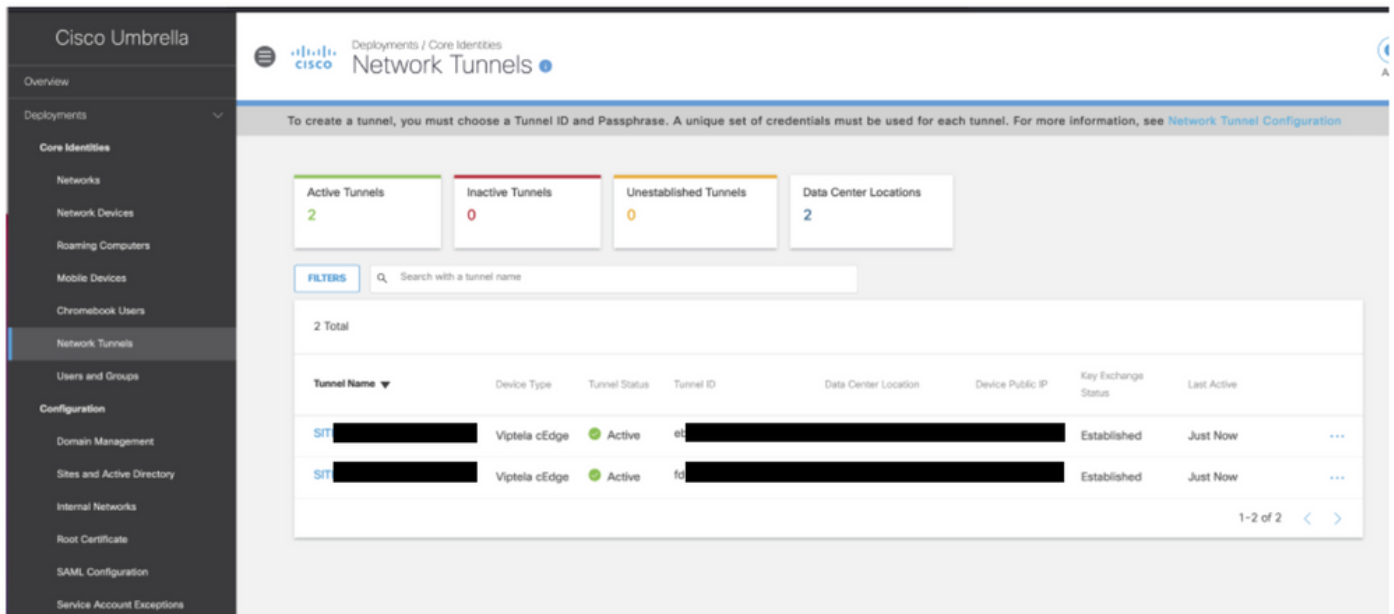
Dans vManage, il est possible de surveiller l'état des tunnels IPsec SIG. Naviguez jusqu'à **Monitor > Network**, sélectionnez le périphérique de périphérie WAN souhaité.

Cliquez sur le bouton **Interfaces** sur le côté gauche ; une liste de toutes les interfaces du périphérique s'affiche. Cela inclut les interfaces ipsec1 et ipsec2.

L'image montre que le tunnel ipsec1 transfère tout le trafic et que ipsec2 ne transmet pas le trafic.



Il est également possible de vérifier les tunnels sur le routeur Cisco Umbrella. Le portail est illustré dans l'image.



Utilisez `show sdwan secure-internet-gateway tunnels` sur l'interface de ligne de commande afin d'afficher les informations relatives aux tunnels.

```
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

Utilisez `show endpoint-tracker` et `show ip sla summary` sur l'interface de ligne de commande afin d'afficher des informations sur les trackers et les SLA générés automatiquement.

```
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

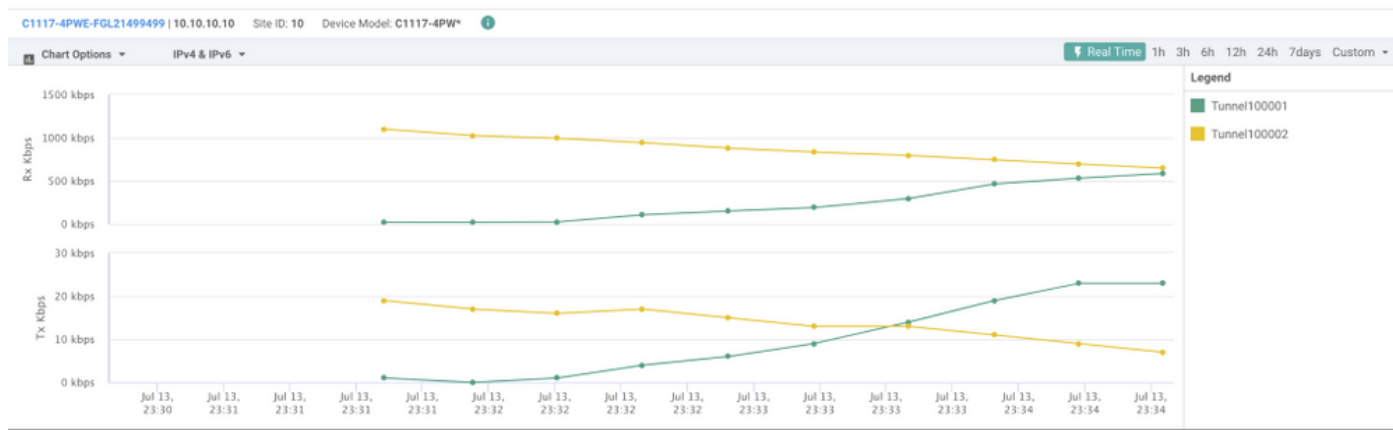
ID	Type	Destination	Stats	Return Code	Last Run
*12	http	10.10.10.10	RTT=6	OK	8 seconds ago
*14	http	10.10.10.10	RTT=17	OK	3 seconds ago

Vérification du scénario actif/actif

Dans vManage, il est possible de surveiller l'état des tunnels IPsec SIG. Naviguez jusqu'à **Monitor > Network**, sélectionnez le périphérique de périphérie WAN souhaité.

Cliquez sur le bouton **Interfaces** sur le côté gauche - et une liste de toutes les interfaces dans le périphérique s'affiche. Cela inclut les interfaces ipsec1 et ipsec2.

L'image montre que les tunnels ipsec1 et ipsec2 transfèrent le trafic.



Utilisez `show sdwan secure-internet-gateway tunnels` sur l'interface de ligne de commande afin d'afficher les informations relatives aux tunnels.

```
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

Utilisez `show endpoint-tracker` et `show ip sla summary` sur l'interface de ligne de commande afin d'afficher des informations sur les trackers et les SLA générés automatiquement.

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

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

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

```
IPSLAs Latest Operation Summary
```

```
Codes: * active, ^ inactive, ~ pending
```

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

ID	Type	Destination	Stats	Return 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

Informations connexes

- [Intégration de vos périphériques avec des passerelles Internet sécurisées - Cisco IOS® XE version 17.x](#)
- [http://Network Configuration du tunnel - Umbrella SIG](#)
- [Mise en route de Umbrella](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.