

Konfigurieren von Umbrella-SIG-Tunneln für Aktiv/Backup- oder Aktiv/Aktiv-Szenarien

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Cisco Umbrella SIG - Überblick](#)

[Umbrella-SIG-Tunnel-Bandbreitenbeschränkung](#)

[Informationen zum Cisco Umbrella Portal](#)

[Den Schlüssel und den geheimen Schlüssel](#)

[ID anfordern](#)

[Erstellung von Umbrella-SIG-Tunneln mit Aktiv/Backup-Szenario](#)

[Schritt 1: Erstellen einer Funktionsvorlage für SIG-Anmeldeinformationen](#)

[Schritt 2: Erstellen einer SIG-Funktionsvorlage](#)

[Schritt 3: Wählen Sie Ihren SIG-Anbieter für den primären Tunnel aus.](#)

[Schritt 4: Den sekundären Tunnel hinzufügen.](#)

[Schritt 5: Erstellen eines Hochverfügbarkeitspaars](#)

[Schritt 6: Bearbeiten Sie die serviceseitige VPN-Vorlage, um eine Serviceroute einzufügen.](#)

[WAN-Edge-Router-Konfiguration für Aktiv/Backup-Szenario](#)

[Erstellung von übergeordneten SIG-Tunneln mit Aktiv/Aktiv-Szenario](#)

[Schritt 1: Erstellen einer Funktionsvorlage für SIG-Anmeldeinformationen](#)

[Schritt 2: Erstellen Sie zwei Loopback-Schnittstellen, um die SIG-Tunnel zu verbinden.](#)

[Schritt 3: Erstellen einer SIG-Funktionsvorlage](#)

Einleitung

In diesem Dokument wird beschrieben, wie zwei Szenarien für Cisco **Umbrella Secure Internet Gateway** (SIG)-Tunnel mit IPsec auf einem **WAN-Edge-Router** konfiguriert werden:

- Zwei IPsec-Tunnel in einem Aktiv/Backup-Szenario.
- Zwei IPsec-Tunnel in einem Active/Active-Szenario.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Umbrella SIG - Überblick

Cisco **Umbrella** ist ein über die Cloud bereitgestellter Sicherheitservice, der alle wichtigen Funktionen zusammenführt.

Umbrella vereint sicheres Web-Gateway, DNS-Sicherheit, über die Cloud bereitgestellte Firewall, Cloud Access Security Broker-Funktionen und Threat-Intelligence.

Detaillierte Überprüfungen und Kontrollen gewährleisten die Einhaltung von Richtlinien für akzeptable Nutzung des Internets und den Schutz vor Bedrohungen aus dem Internet.

SD-WAN-Router können mit Secure Internet Gateways (SIG) integriert werden, die den Großteil der Verarbeitung zur Sicherung des Datenverkehrs in Unternehmen übernehmen.

Wenn die SIG eingerichtet ist, wird der gesamte Client-Datenverkehr auf Basis der Routen oder Richtlinien an die SIG weitergeleitet.

Umbrella-SIG-Tunnel-Bandbreitenbeschränkung

Jeder IPsec-IKEv2-Tunnel zum **Umbrella-Headend** ist auf ca. 250 Mbit/s beschränkt. Wenn also mehrere Tunnel erstellt werden und der Datenverkehr ausgeglichen wird, werden diese Einschränkungen überwunden, falls eine höhere Bandbreite erforderlich ist.

Es können bis zu vier Hochverfügbarkeits-Tunnelpaare erstellt werden.

Informationen zum Cisco Umbrella Portal

Für die SIG-Integration ist ein **Umbrella** Account mit dem SIG Essentials-Paket erforderlich.

Understand what Umbrella licensing has been purchased for your organization and your overall

Umbrella Package

Current Package	License Start Date	License End Date
Umbrella SIG Advantage + Multi-Org + RBI L3	June 30, 2021	June 30, 2031

Information listed here is not authoritative in regard to seat count for certain customers. Customers who do not have a traditional concept of seat count limitation and, as such, this page does not accurately reflect seat count.

The values in the graph below = (number of DNS queries in applicable month / number of currently licensed Users)

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

Support

Den Schlüssel und den geheimen Schlüssel

Der Schlüssel und der geheime Schlüssel können generiert werden, sobald Sie den **Umbrella Management API KEY** erhalten. Wenn Sie sich nicht an den geheimen Schlüssel erinnern oder diesen nicht gespeichert haben, klicken Sie auf **Aktualisieren**.

Vorsicht: Wenn Sie auf die Aktualisierungsschaltfläche klicken, ist ein Update für diese Tasten auf allen Geräten erforderlich. Das Update wird nicht empfohlen, wenn Geräte in Gebrauch sind.

Umbrella Management	Key:
	15... 36

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

Your Key: 15... 6

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

DELETE

ID anfordern

Die Organisations-ID erhalten Sie ganz einfach, wenn Sie sich bei **Umbrella** anmelden.

Erstellung von Umbrella-SIG-Tunneln mit Aktiv/Backup-Szenario

Hinweis: IPsec/GRE Tunnel Routing and Load-Balancing Using ECMP: Diese Funktion steht ab vManage 20.4.1 zur Verfügung. Sie ermöglicht Ihnen die Verwendung der SIG-Vorlage zur Steuerung des Anwendungsdatenverkehrs zu Cisco **Umbrella** oder einem Drittanbieter von SIG.

Hinweis: Unterstützung für die automatische Bereitstellung von Zscaler: Diese Funktion steht ab vManage 20.5.1 zur Verfügung und automatisiert die Bereitstellung von Tunneln von Cisco SD-WAN-Routern zu Zscaler unter Verwendung der API-Anmeldeinformationen des Zscaler-Partners.

Um die automatischen SIG-Tunnel zu konfigurieren, müssen einige Vorlagen erstellt/aktualisiert werden:

- Erstellen Sie eine Funktionsvorlage für SIG-Anmeldeinformationen.
 - Erstellen Sie zwei Loopback-Schnittstellen, um die SIG-Tunnel zu verbinden (nur bei mehr als einem aktiven Tunnel gleichzeitig anwendbar - Active/Active-Szenario).
 - Erstellen einer SIG-Funktionsvorlage
 - Bearbeiten Sie **die servicerspezifische VPN**-Vorlage, um eine Serviceroute einzufügen.
-

Hinweis: Stellen Sie sicher, dass UDP-4500- und -500-Ports von jedem Upstream-Gerät zugelassen werden.

Die Vorlagenkonfigurationen ändern sich mit den Szenarien "Aktiv/Backup" und "Aktiv/Aktiv", für die beide Szenarien separat erläutert und erläutert werden.

Schritt 1: Erstellen einer Funktionsvorlage für SIG-Anmeldeinformationen

Wechseln Sie zur Featurevorlage, und klicken Sie auf **Bearbeiten**.

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

Klicken Sie im Abschnitt "**Zusätzliche Vorlagen**" auf **Cisco SIG-Anmeldedaten**. Die Option wird im Bild angezeigt.

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

Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.

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  5 

Registration Key  1 

Secret 

[Get Keys](#)

Schritt 2: Erstellen einer SIG-Funktionsvorlage

Navigieren Sie zur Funktionsvorlage, und wählen Sie im Abschnitt **Transport & Management VPN** die Funktionsvorlage **Cisco Secure Internet Gateway aus**.

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

SIG-IPSEC-TUNNELS

Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.

Schritt 3: Wählen Sie Ihren SIG-Anbieter für den primären Tunnel aus.

Klicken Sie auf **Tunnel hinzufügen**.

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

Konfigurieren Sie die grundlegenden Details, und belassen Sie **das Rechenzentrum** als **primär**. Klicken

Sie dann auf **Hinzufügen**.


Update Tunnel

Basic Settings


Tunnel Type

IPsec

Interface Name (1..255)

 ipsec1

Description

 ▾

Tunnel Source Interface

 ▾ GigabitEthernet0/0/0


Data-Center

Primary Secondary


Advanced Options ▾

General


Shutdown

 ▾ Yes No

TCP MSS

 ▾ 1300

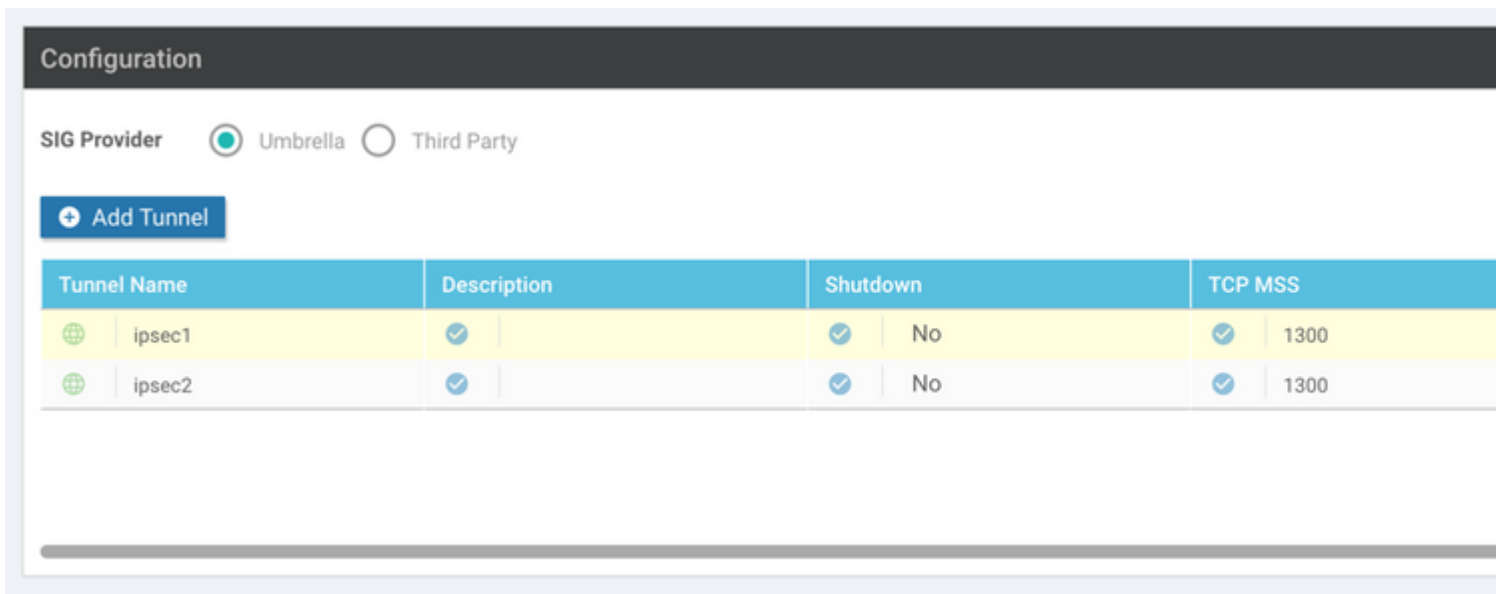
IP MTU

 ▾ 1400

Schritt 4: Den sekundären Tunnel hinzufügen.

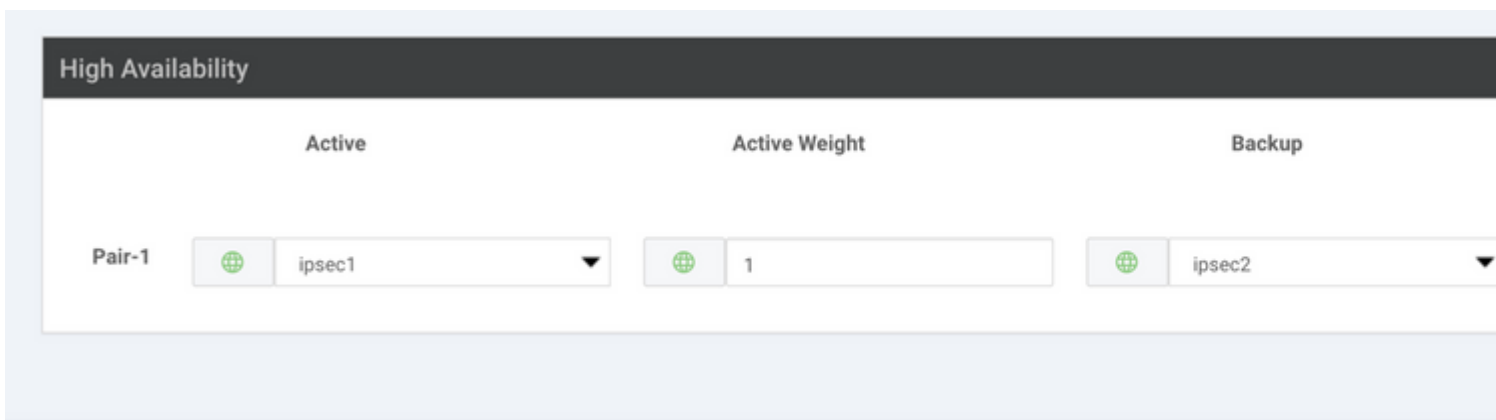
Fügen Sie eine zweite Tunnelkonfiguration hinzu, verwenden Sie diesmal **Data Center** als **Secondary** (**Sekundäres Rechenzentrum**) und den Schnittstellennamen als *ipsec2*.

Die vManage-Konfiguration wird wie folgt angezeigt:



Schritt 5: Erstellen eines Hochverfügbarkeitspaars

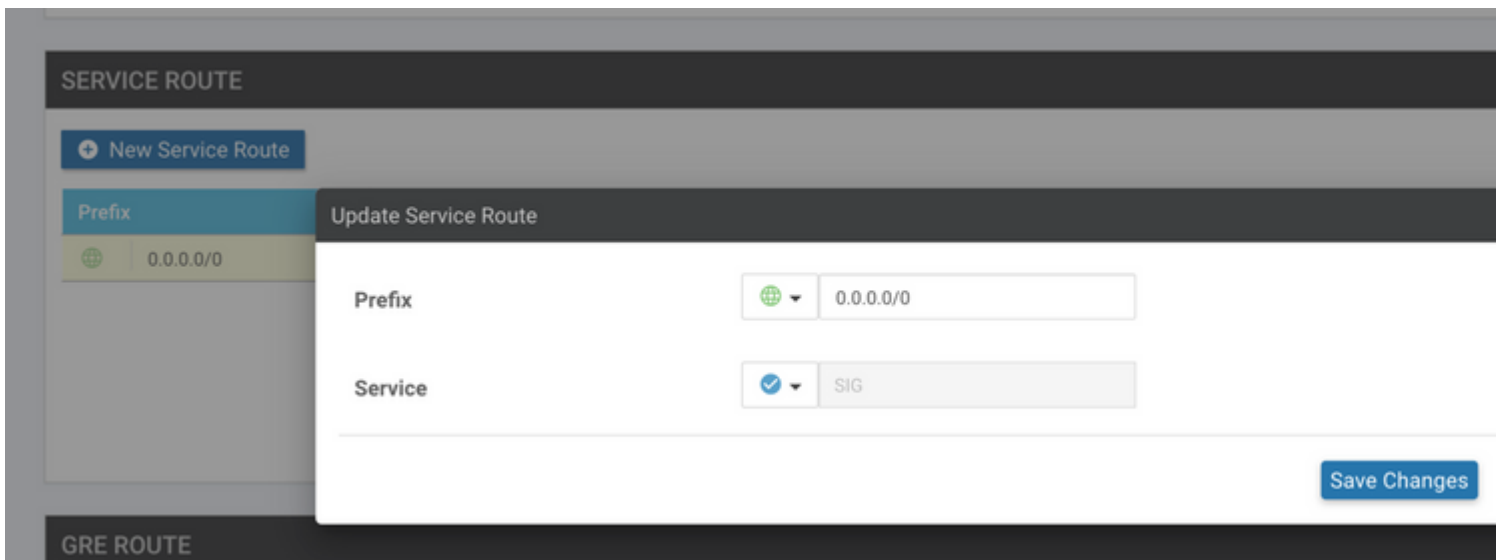
Wählen Sie im Abschnitt "Hohe Verfügbarkeit" **ipsec1** als **Aktiv** und den **ipsec2**-Tunnel als **Backup** aus.



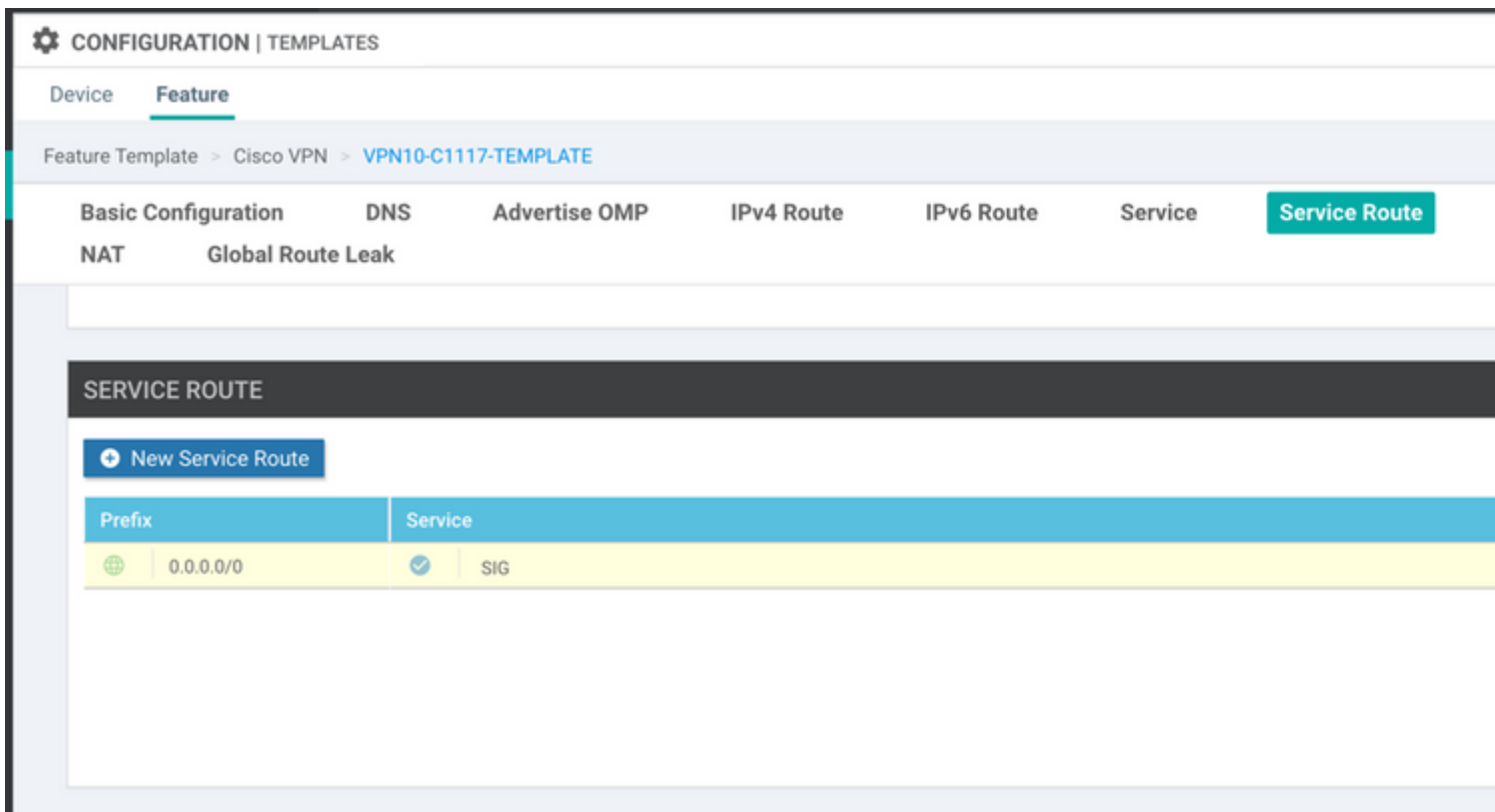
Hinweis: Es können bis zu 4 Hochverfügbarkeits-Tunnelpaare und maximal 4 aktive Tunnel gleichzeitig erstellt werden.

Schritt 6: Bearbeiten Sie die serviceseitige VPN-Vorlage, um eine Serviceroute einzufügen.

Navigieren Sie zum Abschnitt **Service-VPN**, und navigieren Sie innerhalb der Service-VPN-Vorlage zum Abschnitt **Service Route (Serviceroute)**, und fügen Sie eine **0.0.0.0** mit **SIG**-Serviceroute hinzu. Für dieses Dokument wird VRF/VPN 10 verwendet.



Die **SIG-Route 0.0.0.0** wird wie hier dargestellt angezeigt.



Hängen Sie diese Vorlage an das Gerät an, und verschieben Sie die Konfiguration:

TASK VIEW

Push Feature Template Configuration | ✔ Validation Success ▾

Total Task: 1 | In Progress : 1

🔍 Search Options ▾

	Status	Message	Chassis Number	Device Model	Hostname	System IP
▾	In progress	Pushing configuration t...	C1117-4PWE-FGL2149...	C1117-4PW*	C1117-4PWE-FGL2149...	10.10.10.10
<p>[19-Jul-2021 14:05:03 UTC] Configuring device with feature template: C1117-4PW-Original-Template</p> <p>[19-Jul-2021 14:05:03 UTC] Generating configuration from template</p> <p>[19-Jul-2021 14:05:03 UTC] Checking and creating device in vManage</p> <p>[19-Jul-2021 14:05:04 UTC] Device is online</p> <p>[19-Jul-2021 14:05:04 UTC] Updating device configuration in vManage</p> <p>[19-Jul-2021 14:05:10 UTC] Pushing configuration to device.</p>						

WAN-Edge-Router-Konfiguration für Aktiv/Backup-Szenario

```

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-in
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

```

Erstellung von übergeordneten SIG-Tunneln mit Aktiv/Aktiv-Szenario

Schritt 1: Erstellen einer Funktionsvorlage für SIG-Anmeldeinformationen

Navigieren Sie zur Featurevorlage, und klicken Sie auf **Bearbeiten**.

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

Wählen Sie im Abschnitt **Zusätzliche Vorlagen** die Option **Cisco SIG-Anmeldedaten** aus. Die Option wird im Bild angezeigt.

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	

Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.

CONFIGURATION | TEMPLATES

Device Feature

Feature Template > Cisco SIG Credentials > **SIG-Credentials**

Device Type C1117-4PW*

Template Name SIG-Credentials

Description SIG-Credentials

Basic Details

SIG Provider Umbrella

Organization ID [REDACTED]

Registration Key [REDACTED]

Secret

Get Keys

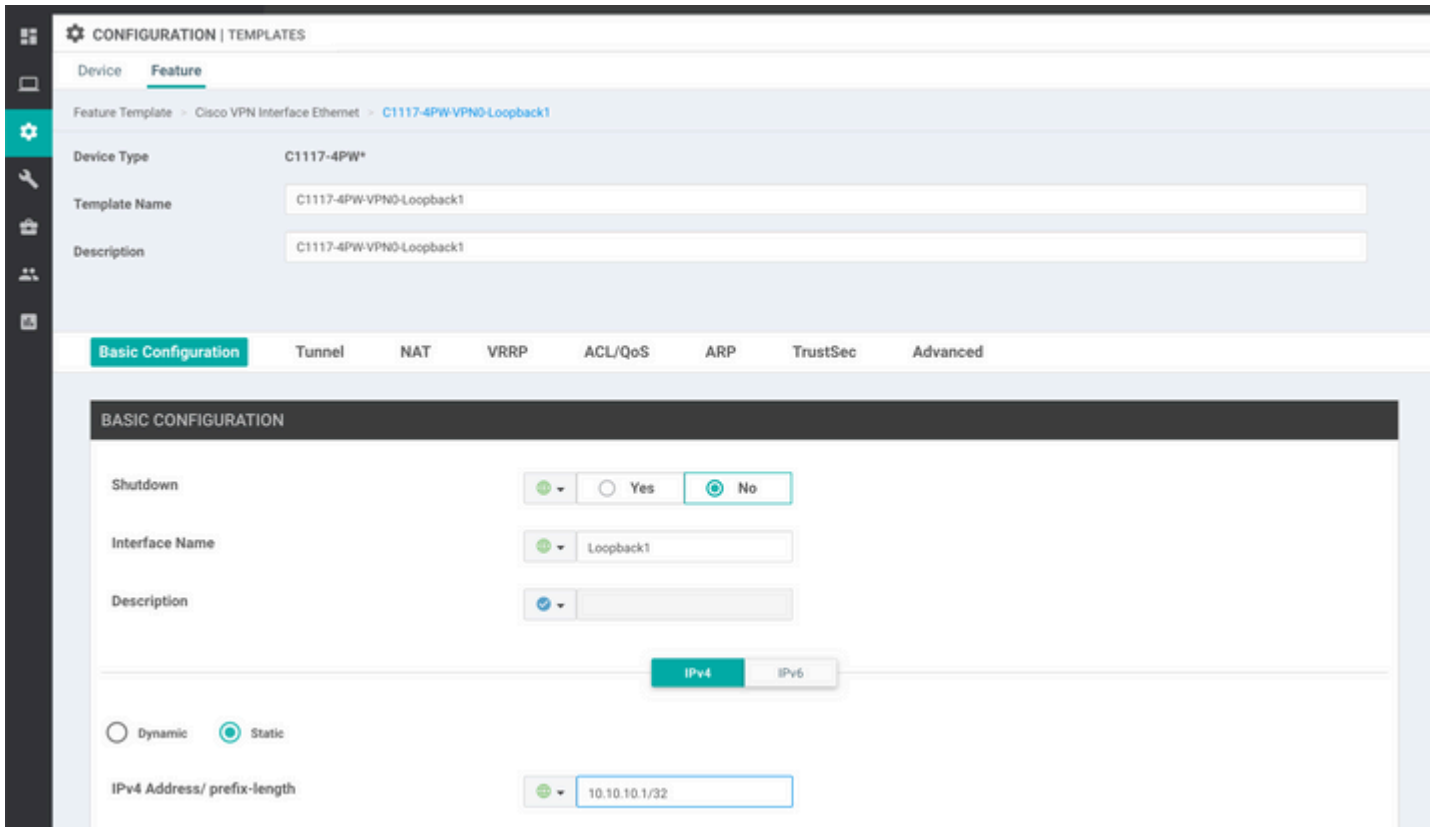
Schritt 2: Erstellen Sie zwei Loopback-Schnittstellen, um die SIG-Tunnel zu verbinden.

Hinweis: Erstellen Sie eine Loopback-Schnittstelle für jeden im aktiven Modus konfigurierten SIG-Tunnel. Dies ist erforderlich, da jeder Tunnel eine eindeutige IKE-ID benötigt.

Hinweis: Dieses Szenario ist "Aktiv/Aktiv", daher werden zwei Loopbacks erstellt.

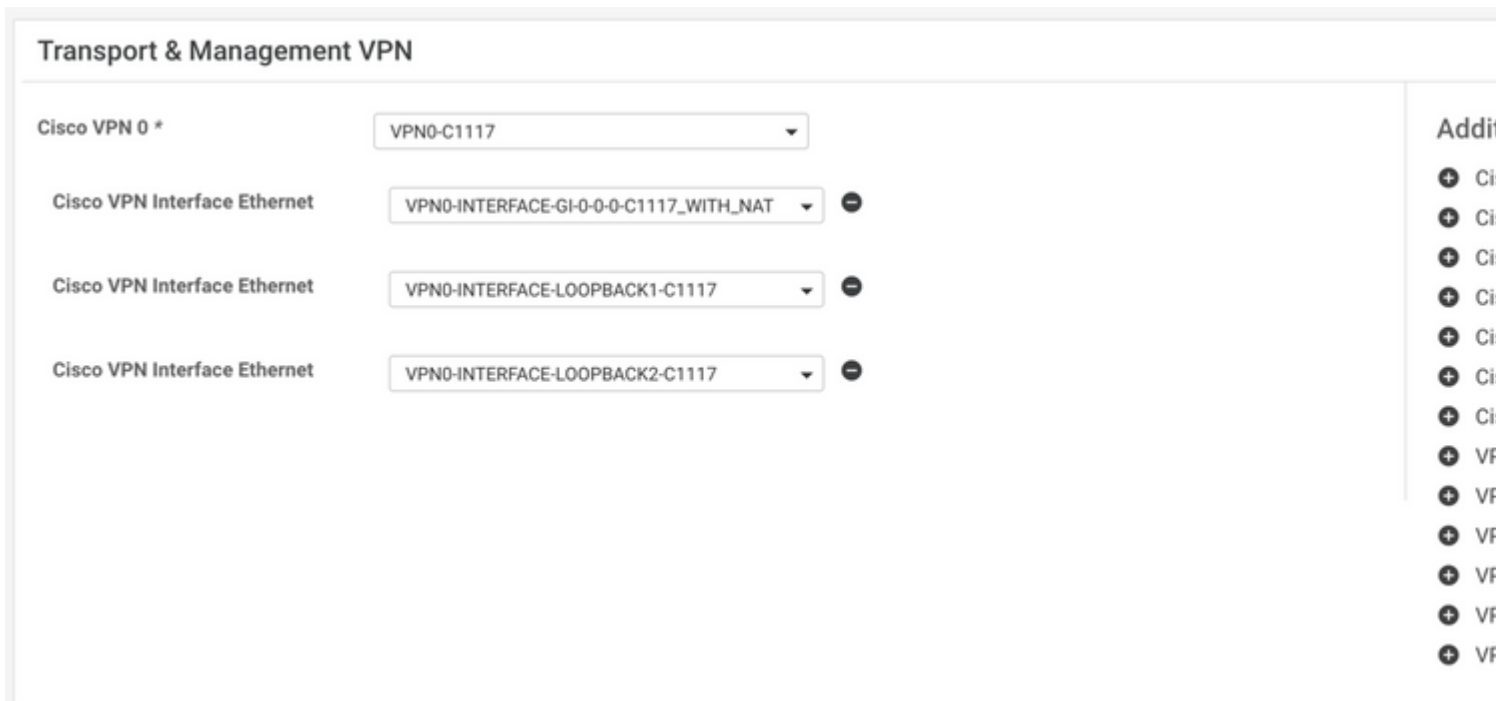
Konfigurieren Sie den Schnittstellennamen und die IPv4-Adresse für das Loopback.

Hinweis: Die für den Loopback konfigurierte IP-Adresse ist eine Scheinadresse.



â€f

Erstellen Sie die zweite Loopback-Vorlage, und hängen Sie sie an die Gerätevorlage an. Der Gerätevorlage müssen zwei Loopback-Vorlagen angefügt sein:

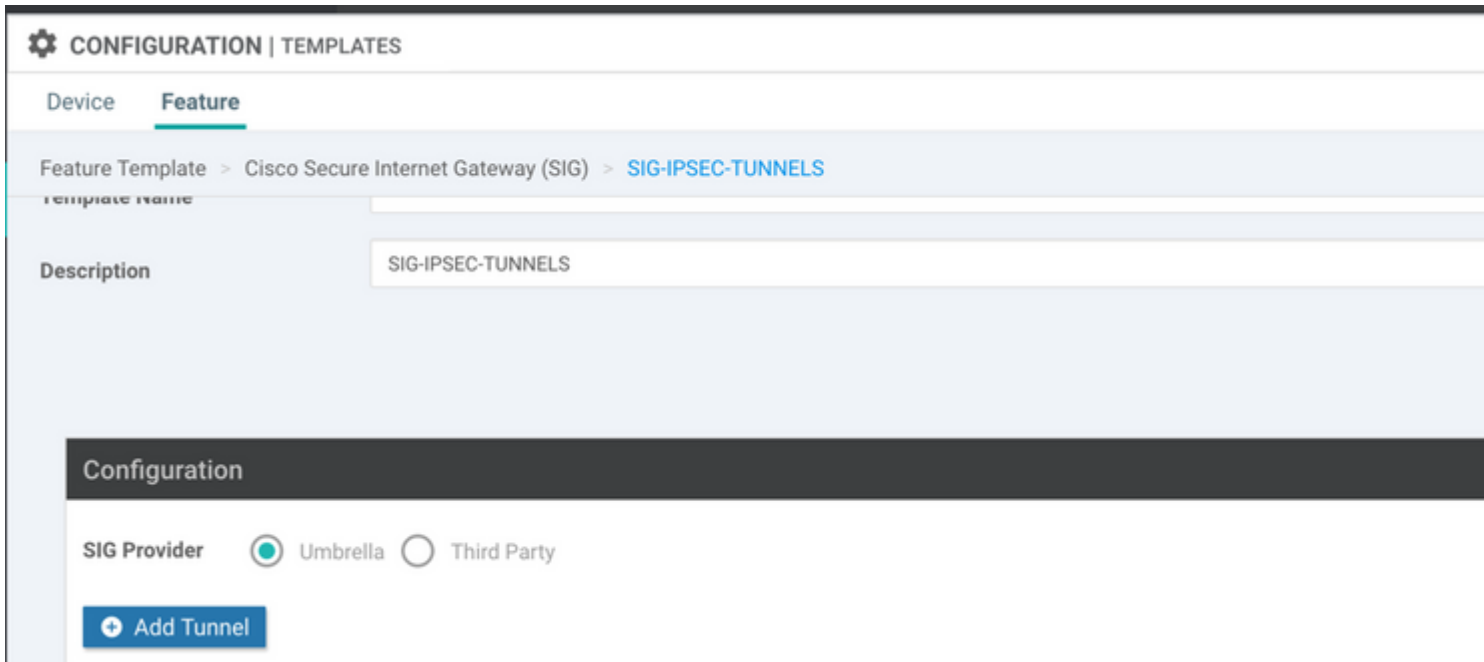


Schritt 3: Erstellen einer SIG-Funktionsvorlage

Navigieren Sie zur SIG-Funktionsvorlage, und wählen Sie im Abschnitt **Transport & Management VPN** die Funktionsvorlage **Cisco Secure Internet Gateway** aus.

Schritt 4: Wählen Sie den SIG-Anbieter für den primären Tunnel aus.

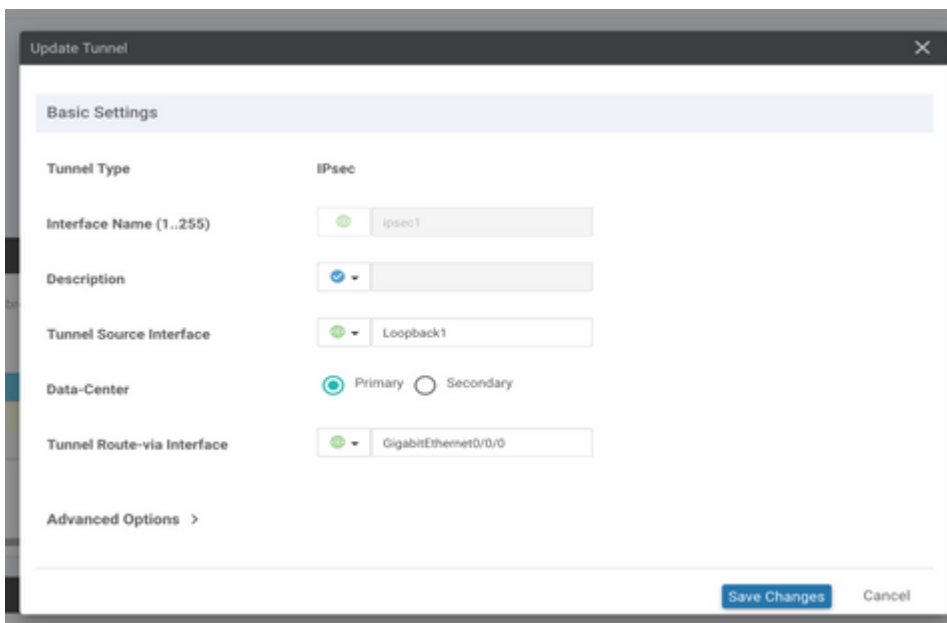
Klicken Sie auf **Tunnel hinzufügen**.



The screenshot shows the 'CONFIGURATION | TEMPLATES' page. Under the 'Feature' tab, the breadcrumb is 'Feature Template > Cisco Secure Internet Gateway (SIG) > SIG-IPSEC-TUNNELS'. The 'Description' field contains 'SIG-IPSEC-TUNNELS'. In the 'Configuration' section, the 'SIG Provider' is set to 'Umbrella' (selected with a radio button) and 'Third Party' is unselected. A blue 'Add Tunnel' button is visible at the bottom left of the configuration area.

Konfigurieren Sie die grundlegenden Details, und belassen Sie das **Rechenzentrum** als **primär**.

Hinweis: Der Parameter "Tunnel Source Interface" ist das Loopback (für dieses Dokument Loopback1) und als Tunnel Route-via Interface die physische Schnittstelle (für dieses Dokument GigabitEthernet0/0/0).

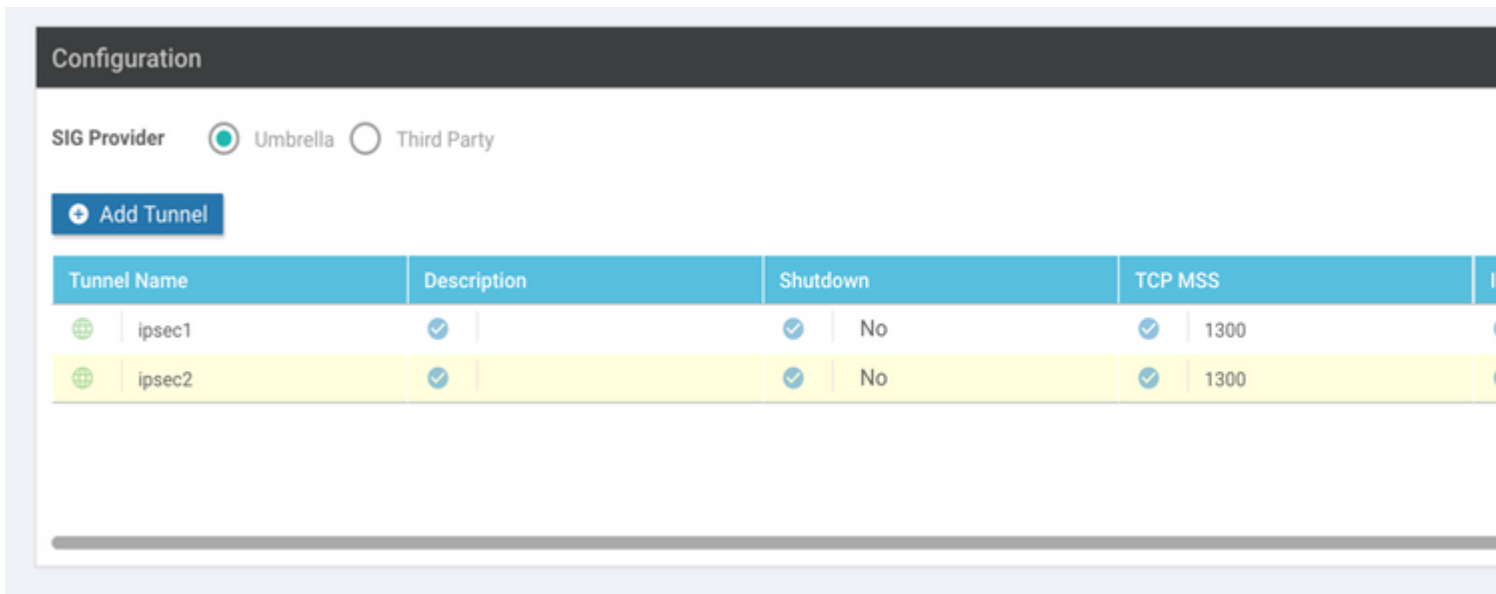


The 'Update Tunnel' dialog box shows the following settings under 'Basic Settings':
- Tunnel Type: IPsec
- Interface Name (1..255): ipsec1
- Description: (empty field)
- Tunnel Source Interface: Loopback1
- Data-Center: Primary (selected with a radio button), Secondary (unselected)
- Tunnel Route-via Interface: GigabitEthernet0/0/0
At the bottom right, there are 'Save Changes' and 'Cancel' buttons.

Schritt 5: Den sekundären Tunnel hinzufügen.

Fügen Sie eine zweite Tunnelkonfiguration hinzu, verwenden Sie ebenfalls **Data Center** als **Primary** (**Primäres Rechenzentrum**) und den Schnittstellennamen als *ipsec2*.

Die vManage-Konfiguration wird wie folgt angezeigt:



The screenshot shows the 'Configuration' page in vManage. At the top, there is a 'SIG Provider' section with two radio buttons: 'Umbrella' (selected) and 'Third Party'. 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, and TCP MSS. Two rows are visible, both highlighted in yellow.

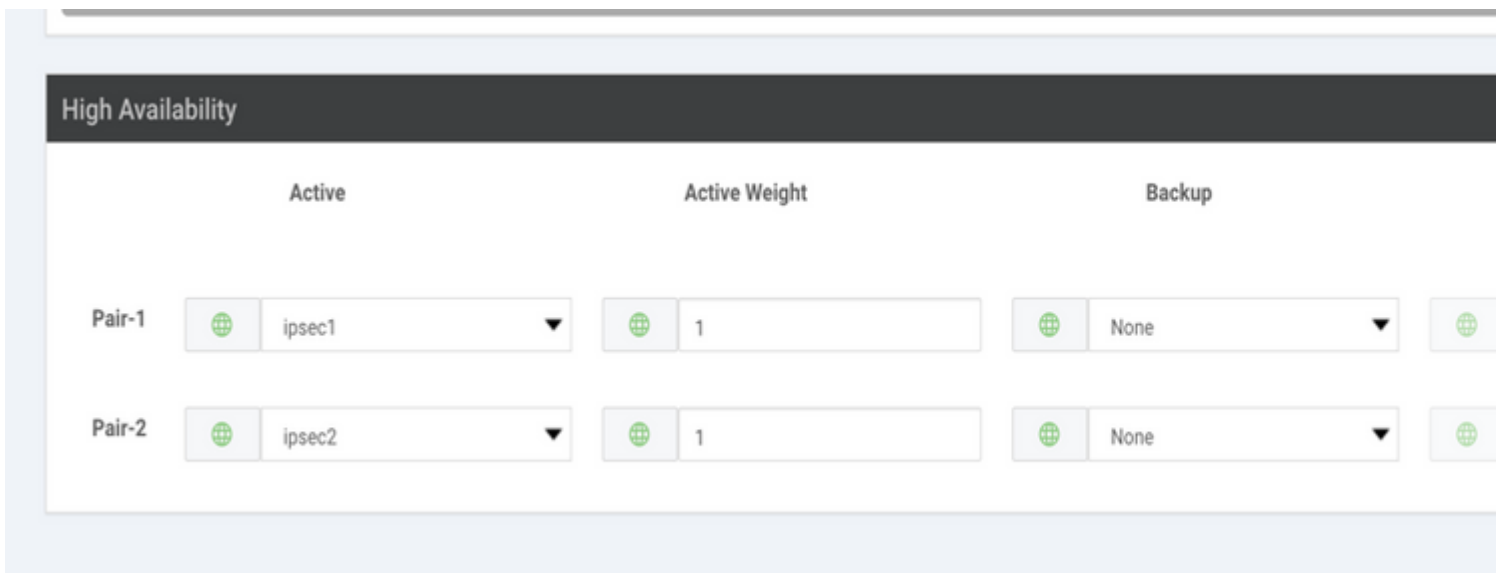
Tunnel Name	Description	Shutdown	TCP MSS
ipsec1		No	1300
ipsec2		No	1300

Schritt 6: Erstellen Sie zwei Hochverfügbarkeitspaare.

Erstellen Sie im Abschnitt **High Availability** zwei Hochverfügbarkeitspaare.

- Wählen Sie im ersten HA-Paar ipsec1 als Aktiv und **Keine** als Backup aus.
- Wählen Sie im zweiten HA-Paar ipsec2 als Aktiv, wählen Sie **Keine** und als Backup aus.

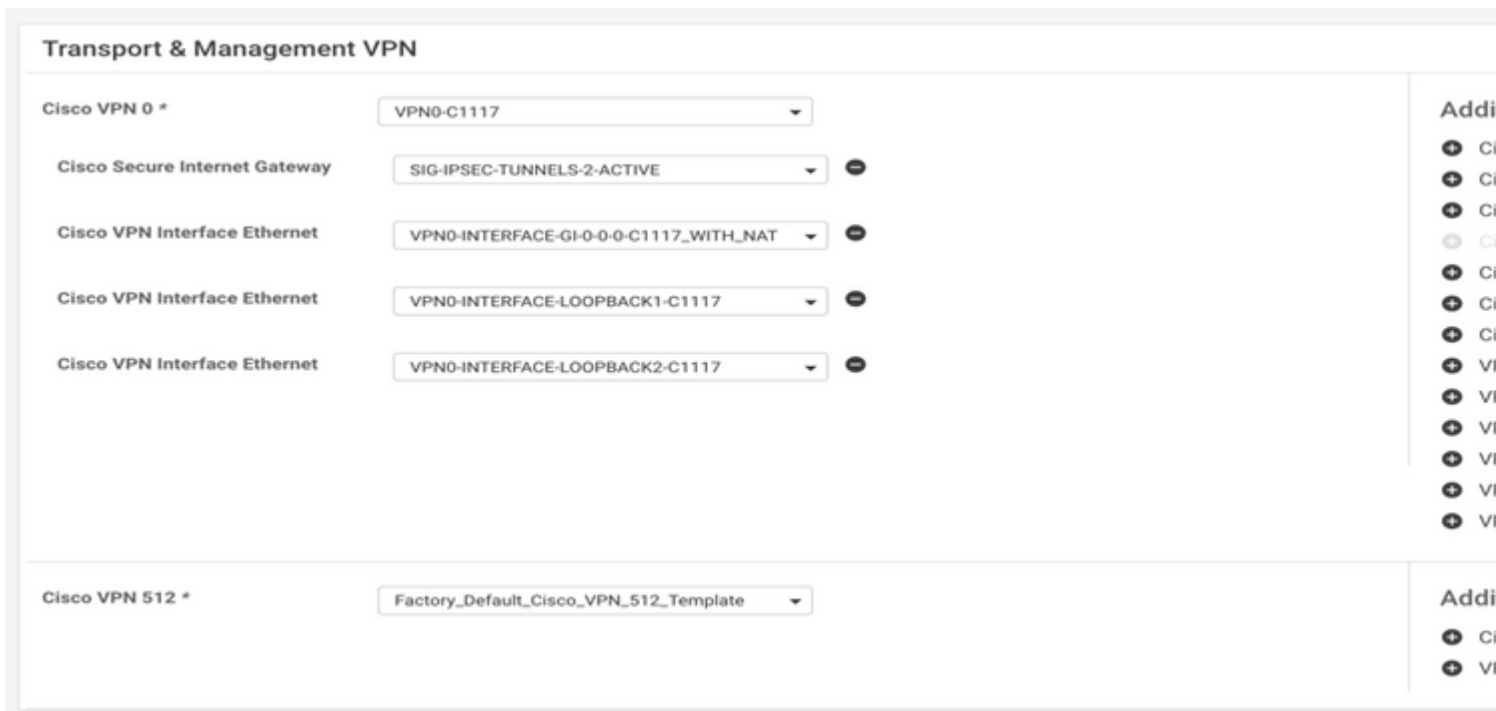
Die vManage-Konfiguration für Hochverfügbarkeit wird wie folgt angezeigt:



The screenshot shows the 'High Availability' configuration page. It features two rows of configuration for 'Pair-1' and 'Pair-2'. Each row has three main sections: 'Active', 'Active Weight', and 'Backup'. Each section contains a globe icon, a dropdown menu, and a plus icon.

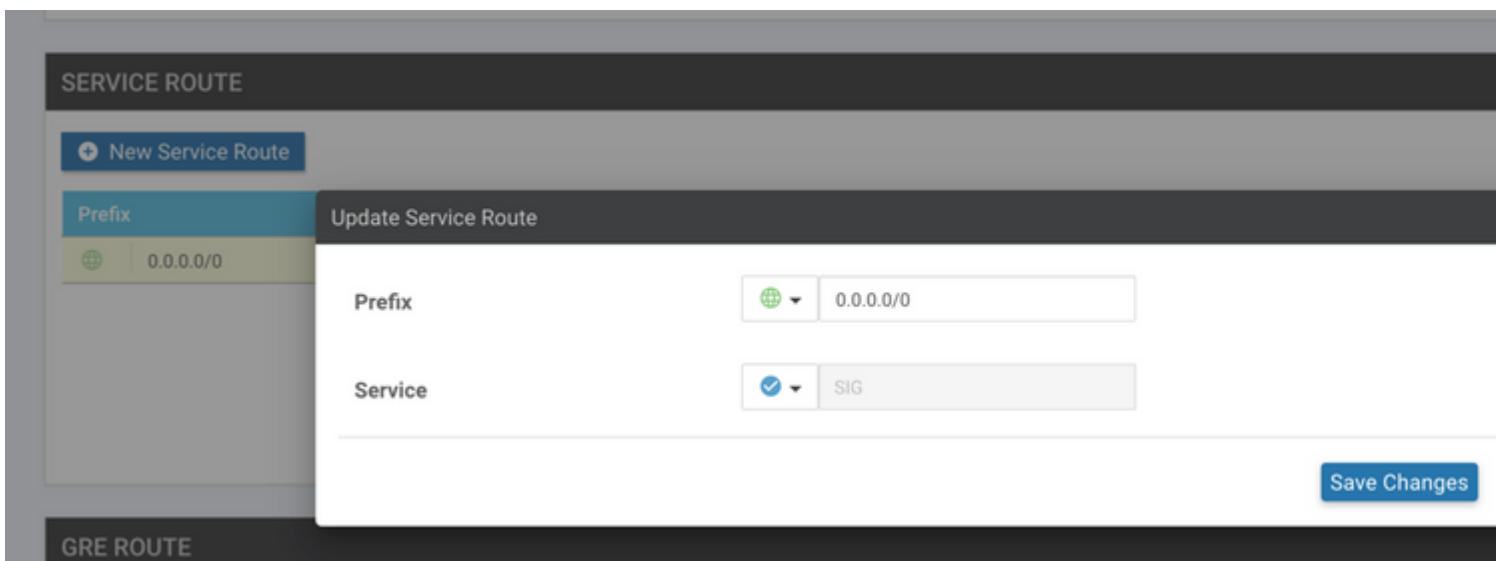
	Active	Active Weight	Backup
Pair-1	ipsec1	1	None
Pair-2	ipsec2	1	None

Der Gerätevorlage sind die beiden Loopback-Vorlagen und die SIG-Funktionsvorlage zugeordnet.



Schritt 7. Bearbeiten Sie die serviceseitige VPN-Vorlage, um eine Serviceroute einzufügen.

Navigieren Sie zum Abschnitt "Service-VPN" und innerhalb der VPN-Vorlage für den Service, navigieren Sie zum Abschnitt "Service Route", und fügen Sie eine **0.0.0.0** mit **SIG-Service-Route** hinzu.



Die SIG-Route 0.0.0.0 wird wie hier dargestellt angezeigt.

Hinweis: Damit der Service-Datenverkehr tatsächlich ausgeht, muss NAT in der WAN-Schnittstelle konfiguriert werden.

Hängen Sie diese Vorlage an das Gerät an, und verschieben Sie die Konfiguration.

WAN-Edge-Router-Konfiguration für Aktiv/Aktiv-Szenario

```
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-inter
exit
interface Tunnel100002
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-inter
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  
!
```

Hinweis: Obwohl sich dieses Dokument auf **Umbrella** konzentriert, gelten die gleichen Szenarien für Azure- und Drittanbieter-SIG-Tunnel.

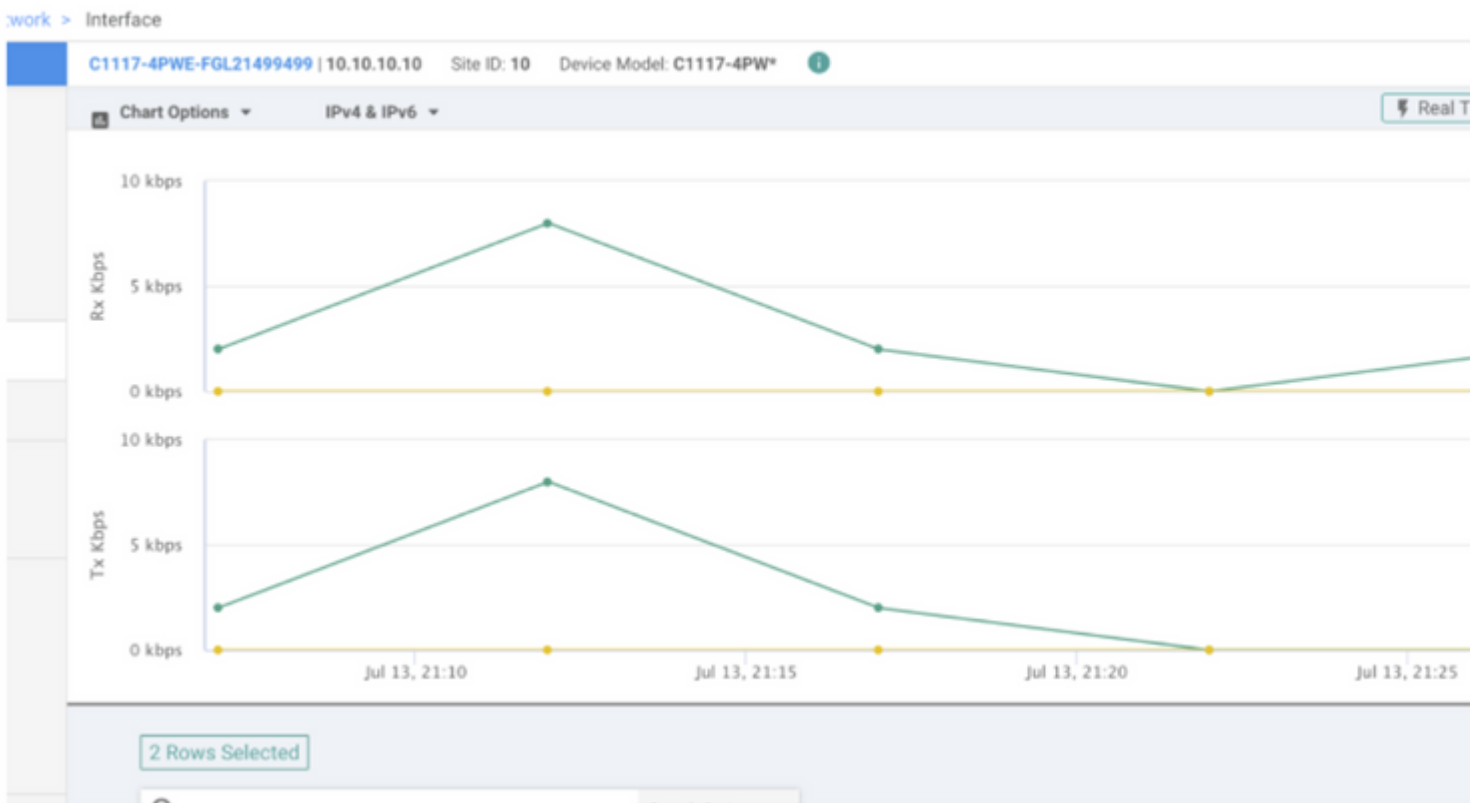
Überprüfung

Überprüfung des Aktiv/Backup-Szenarios

Im vManage ist es möglich, den Status der SIG IPsec-Tunnel zu überwachen. Navigieren Sie zu **Monitor > Network**, und wählen Sie das gewünschte WAN-Edge-Gerät aus.

Klicken Sie auf der linken Seite auf die Registerkarte **Interfaces (Schnittstellen)**. Eine Liste aller Schnittstellen im Gerät wird angezeigt. Dies schließt die Schnittstellen ipsec1 und ipsec2 ein.

Das Bild zeigt, dass der ipsec1-Tunnel den gesamten Datenverkehr weiterleitet und dass ipsec2 den Datenverkehr nicht weiterleitet.



Es ist auch möglich, die Tunnel auf dem Cisco **Umbrella** Portal wie im Bild gezeigt zu überprüfen.

Cisco Umbrella

Overview

Deployments

Core Identities

- Networks
- Network Devices
- Roaming Computers
- Mobile Devices
- Chromebook Users
- Network Tunnels
- Users and Groups

Configuration

- Domain Management
- Sites and Active Directory
- Internal Networks
- Root Certificate
- SAML Configuration
- Service Account Exceptions

Deployments / Core Identities

Network Tunnels

To create a tunnel, you must choose a Tunnel ID and Passphrase. A unique set of credentials must be used for each tunnel. For more information, see the Cisco Umbrella documentation.

Active Tunnels: 2

Inactive Tunnels: 0

Unestablished Tunnels: 0

Data Center Locations: 2

FILTERS Search with a tunnel name

2 Total

Tunnel Name	Device Type	Tunnel Status	Tunnel ID	Data Center Location	Device Public IP
SIT [REDACTED]	Viptela cEdge	Active	et [REDACTED]		
SIT [REDACTED]	Viptela cEdge	Active	fd [REDACTED]		

Verwenden Sie den Befehl `show sdwan secure-internet-gateway tunnels` in der CLI, um die

Tunnelinformationen anzuzeigen.

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
```

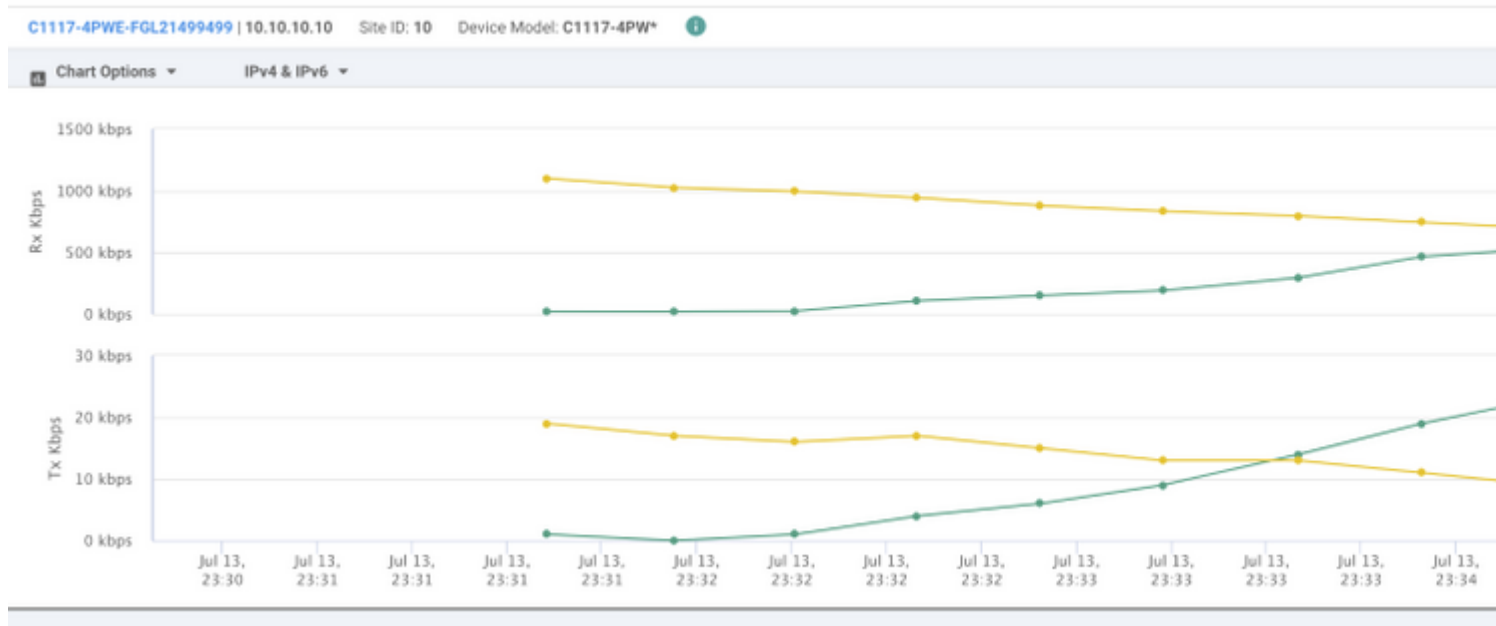
TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	540798313	SITE10SYS10x10x10x10IFTunnel100001	st-tun-create-notif	200	create-tunnel
Tunnel100002	540798314	SITE10SYS10x10x10x10IFTunnel100002	st-tun-create-notif	200	create-tunnel

Überprüfung des Szenarios "Aktiv/Aktiv"

Im vManage kann der Status der SIG IPsec-Tunnel überwacht werden. Navigieren Sie zu **Monitor > Network**, und wählen Sie das gewünschte WAN-Edge-Gerät aus.

Klicken Sie auf der linken Seite auf die Registerkarte **Interfaces (Schnittstellen)**. Daraufhin wird eine Liste aller Schnittstellen im Gerät angezeigt. Dies schließt die Schnittstellen ipsec1 und ipsec2 ein.

Das Bild zeigt, dass sowohl ipsec1- als auch ipsec2-Tunnel Datenverkehr weiterleiten.



Verwenden Sie den Befehl **show sdwan secure-internet-gateway tunnels** in der CLI, um die Tunnelinformationen anzuzeigen.

```
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

Zugehörige Informationen

- [Integration Ihrer Geräte mit sicheren Internet-Gateways - Cisco IOS® XE Version 17.x](#)
- [http://Network Tunnelkonfiguration - Umbrella SIG](#)
- [Umbrella Erste Schritte](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.