تكوين أنفاق Umbrella SIG للسيناريوهات النشطة/الاحتياطية أو النشطة/النشطة

المحتويات

المقدمة

يوضح هذا المستند كيفية التكوين **Cisco Umbrella Secure Internet Gateway (SIG)** أنفاق مع IPsec في كل ال **Active/Active** و **Active/Standby**.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- Cisco **Umbrella**
- تفاوض IPsec

- شبكة المنطقة الواسعة المعرفة من برنامج Cisco (SD-WAN)

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco vManage الإصدار 20.4.2
- موجه Cisco WAN Edge C1117-4PW*، الإصدار 17.4.2

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

نظرة عامة على Cisco Umbrella SIG

Cisco **Umbrella** عبارة عن خدمة أمان يتم توصيلها عبر السحابة تعمل على الجمع بين الوظائف الأساسية.

Umbrella يوحد بوابة الويب الآمنة وأمان DNS وجدار الحماية الذي يتم تسليمه عبر السحابة ووظائف وسيط أمان الوصول إلى السحابة واستخبارات التهديدات.

إن الفحص والرقابة العميقين يضمنان الامتثال لسياسات الويب ذات الاستخدام المقبول، ويحميان من تهديدات الإنترنت.

يمكن دمج موجهات SD-WAN مع بوابات الإنترنت الآمنة (SIG) التي تقوم بمعظم المعالجة لتأمين حركة مرور بيانات المؤسسة.

عند إعداد SIG، تتم إعادة توجيه جميع حركة مرور العملاء، استنادا إلى المسارات أو النهج، إلى SIG.

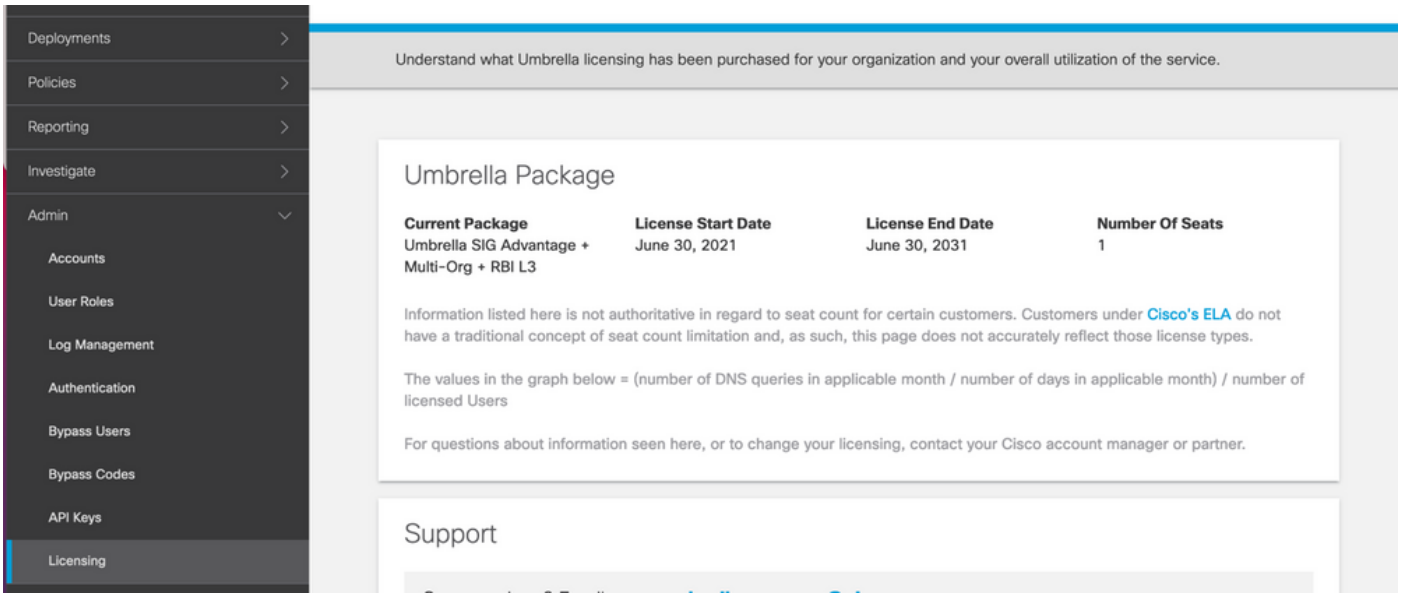
تحديد النطاق الترددي لنفق Umbrella SIG Tunnel

كل نفق IPsec IKEv2 إلى **Umbrella** تقتصر ميزة "طرف الرأس" على 250 ميجابت في الثانية تقريبا، لذلك إذا تم إنشاء عدة أنفاق وتوازن أحمال حركة المرور، فإنها تتغلب على هذه القيود في حالة الحاجة إلى نطاق ترددي أكبر.

يمكن إنشاء أزواج الأنفاق لما يصل إلى أربعة **High Availability**.

الحصول على معلومات بوابة Cisco Umbrella

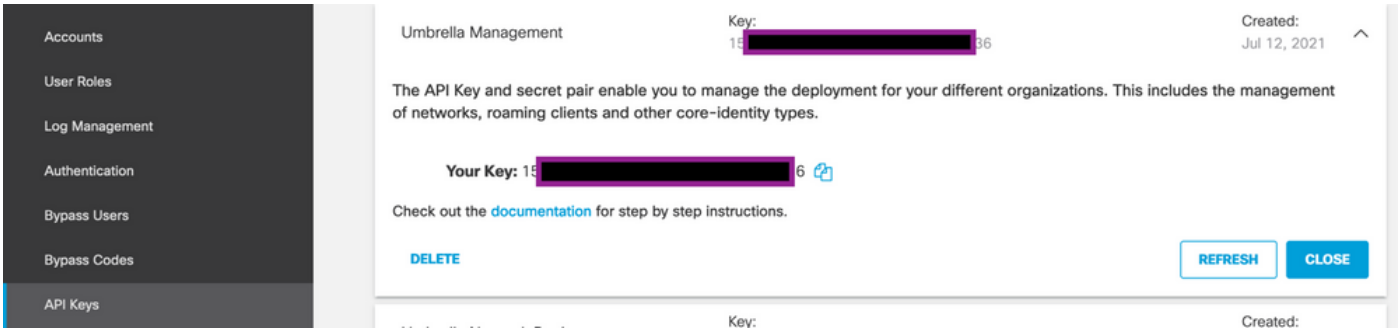
من أجل المضي قدما في عملية تكامل SIG، **Umbrella** يلزم وجود حساب مزود بحزمة SIG Essentials.



الحصول على المفتاح والمفتاح السري

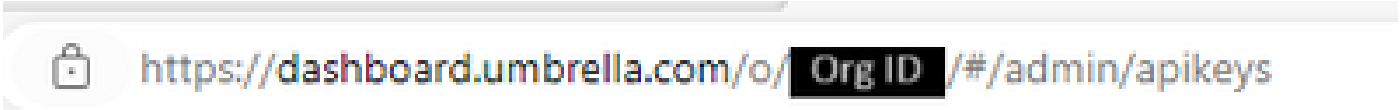
يمكن إنشاء المفتاح والمفتاح السري في اللحظة التي تحصل فيها على **Umbrella Management API KEY** (هذا المفتاح ضمن "المفاتيح القديمة"). إذا لم تذكر المفتاح السري أو لم تقم بحفظه، انقر فوق تحديث.

⚠ تحذير: في حالة النقر فوق الزر "تحديث"، يلزم تحديث هذه المفاتيح على جميع الأجهزة، لا يوصى بالتحديث في حالة وجود أجهزة قيد الاستخدام.



الحصول على معرف المؤسسة

يمكن الحصول على معرف المؤسسة بسهولة عند تسجيل الدخول إلى **Umbrella** من شريط عناوين المستعرض.



إنشاء أنفاق Umbrella SIG باستخدام سيناريو النسخ الاحتياطي/النشط

ملاحظة: توجيه النفق عبر بروتوكول IPsec/GRE وموازنة الحمل باستخدام بروتوكول ECMP: تتوفر هذه الميزة في الإصدار vManage 20.4.1 وفيما بعد، وهي تسمح لك باستخدام قالب SIG لتوجيه حركة مرور التطبيقات إلى Cisco Umbrella أو مزود SIG من جهة خارجية

ملاحظة: دعم الإمداد التلقائي ل Zscaler: تتوفر هذه الميزة على vManage 20.5.1 وفيما بعد، وتقوم هذه الميزة بأتمتة إمداد الأنفاق من موجهات Cisco SD-WAN إلى Zscaler، باستخدام بيانات اعتماد واجهة برمجة التطبيقات (API) الخاصة بشريك Zscaler.

لتكوين الأنفاق التلقائية ل SIG، يلزم إنشاء/تحديث بعض القوالب:

- قم بإنشاء قالب ميزة بيانات اعتماد SIG.
- قم بإنشاء واجهتي إسترجاع لربط أنفاق SIG (ينطبق فقط على أكثر من واحد Active في الوقت نفسه - Active/Active السيناريو).
- إنشاء قالب ميزة SIG.
- تحرير قالب VPN من جانب الخدمة لإدخال Service Route.

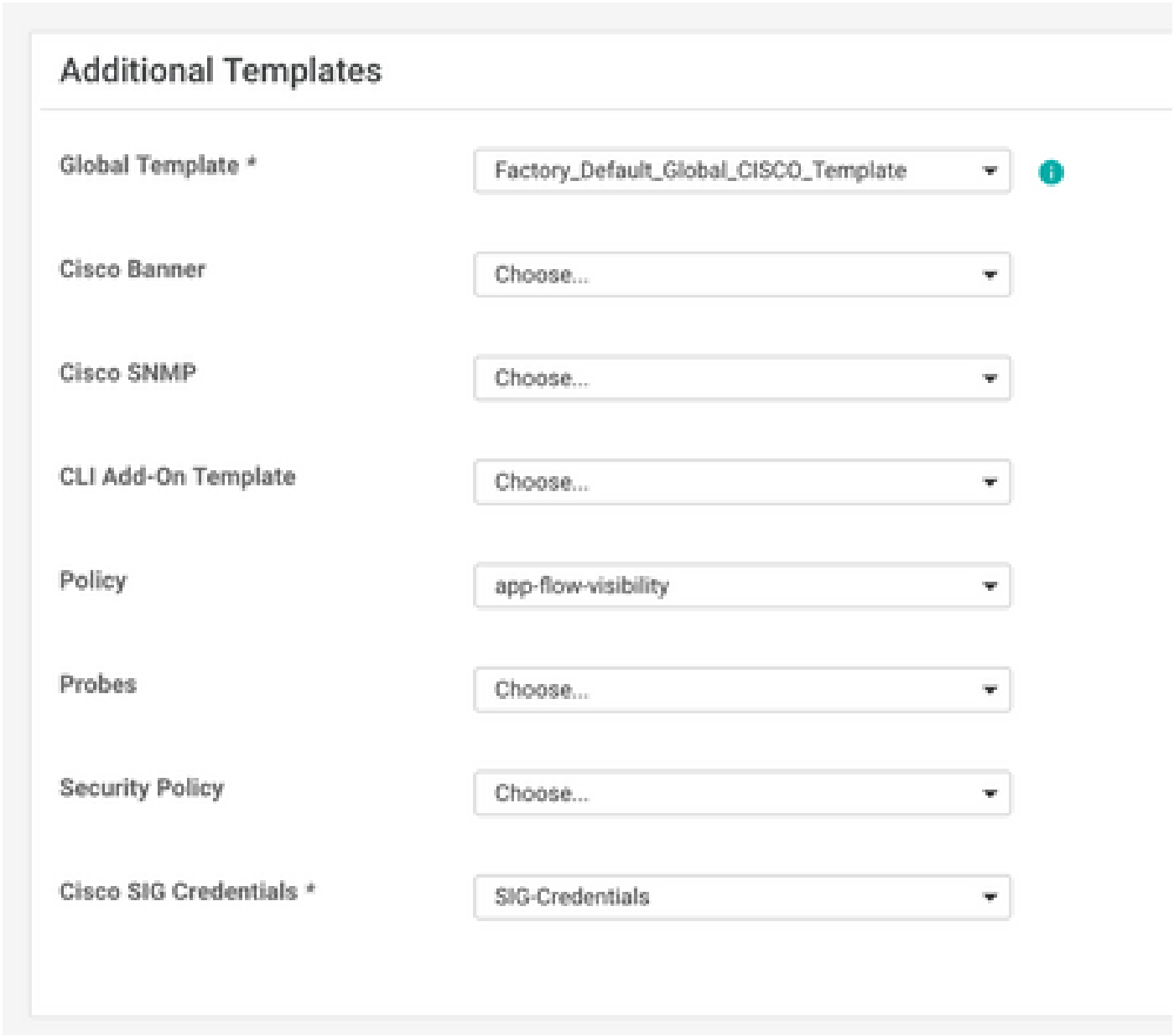
ملاحظة: تأكد من السماح بمنافذ UDP 4500 و 500 من أي جهاز للتحميل.

تتغير تكوينات القالب باستخدام Active/Backup و Active/Active السيناريوهات التي يتم من خلالها شرح السيناريوهين وكشفهما بشكل منفصل.

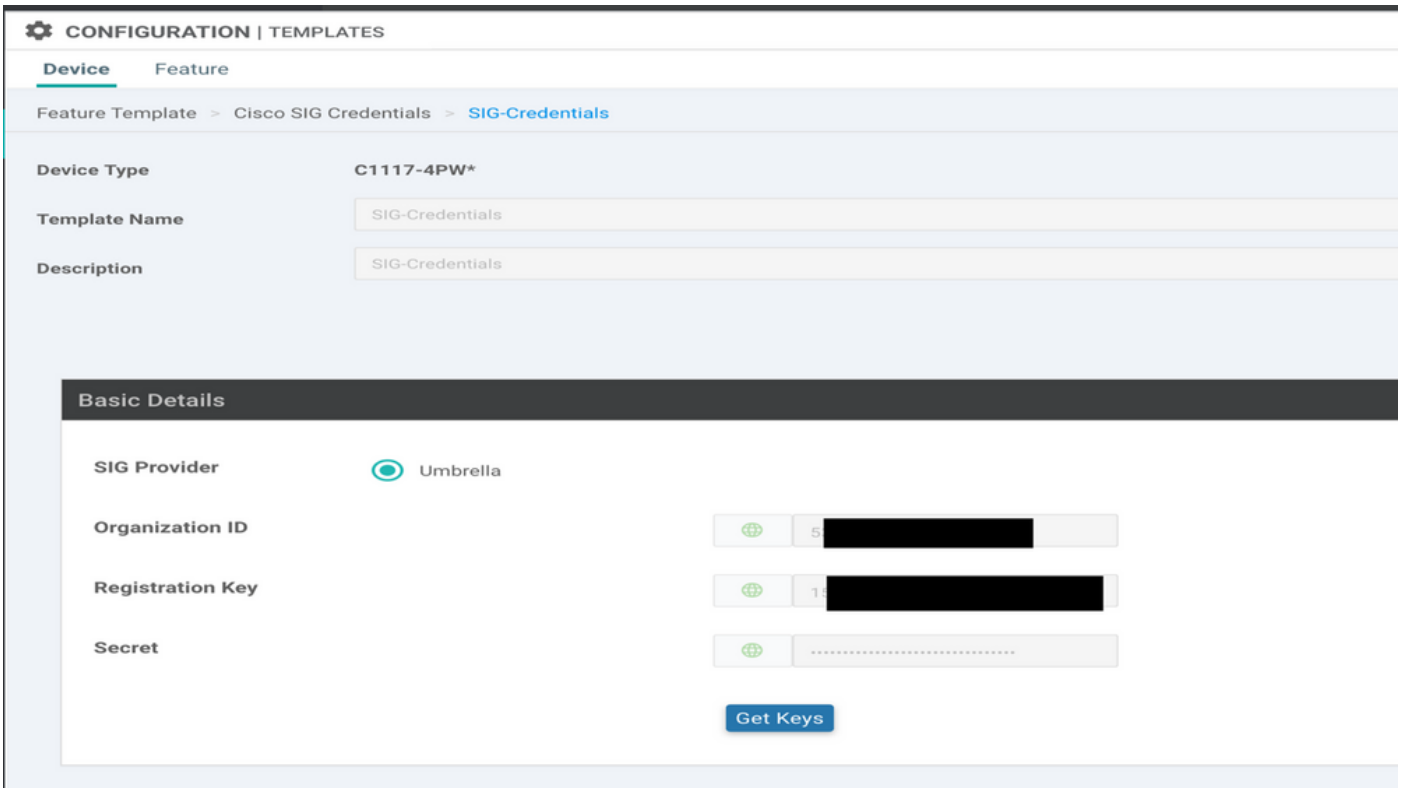
الخطوة 1. قم بإنشاء قالب ميزة بيانات اعتماد SIG.

انتقل إلى قالب الميزة وانقر فوق Edit.

بموجب قسم من Additional templates,انقر Cisco SIG Credentials. يظهر الخيار في الصورة.

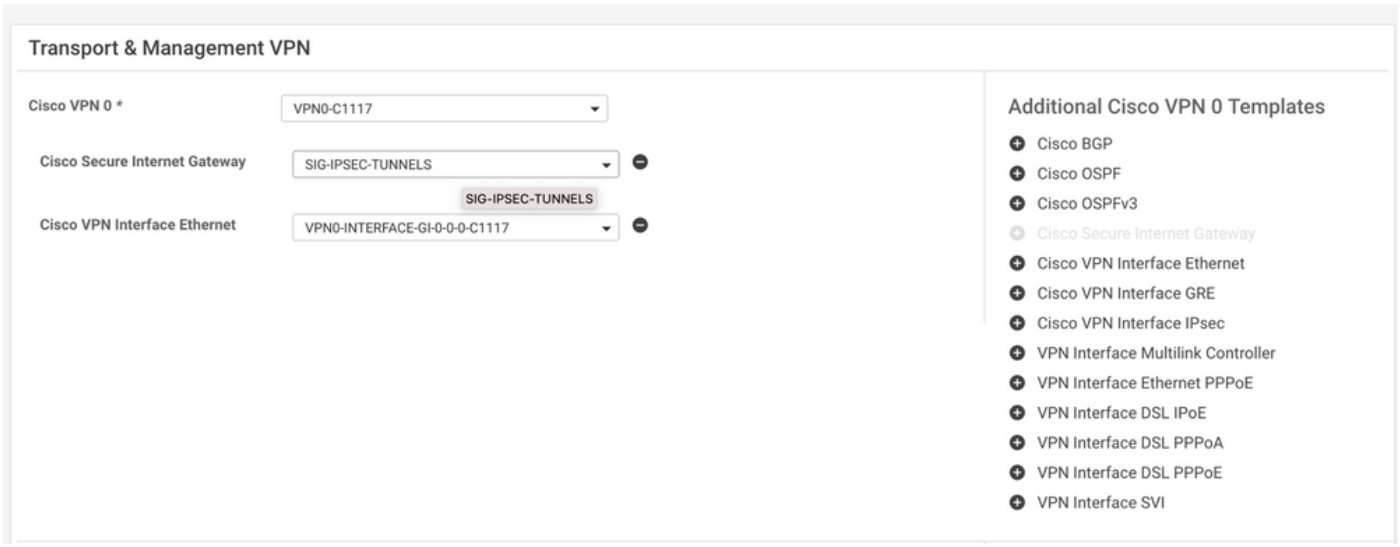


قم بإعطاء اسم ووصف للقالب.



الخطوة 2. إنشاء قالب ميزة SIG.

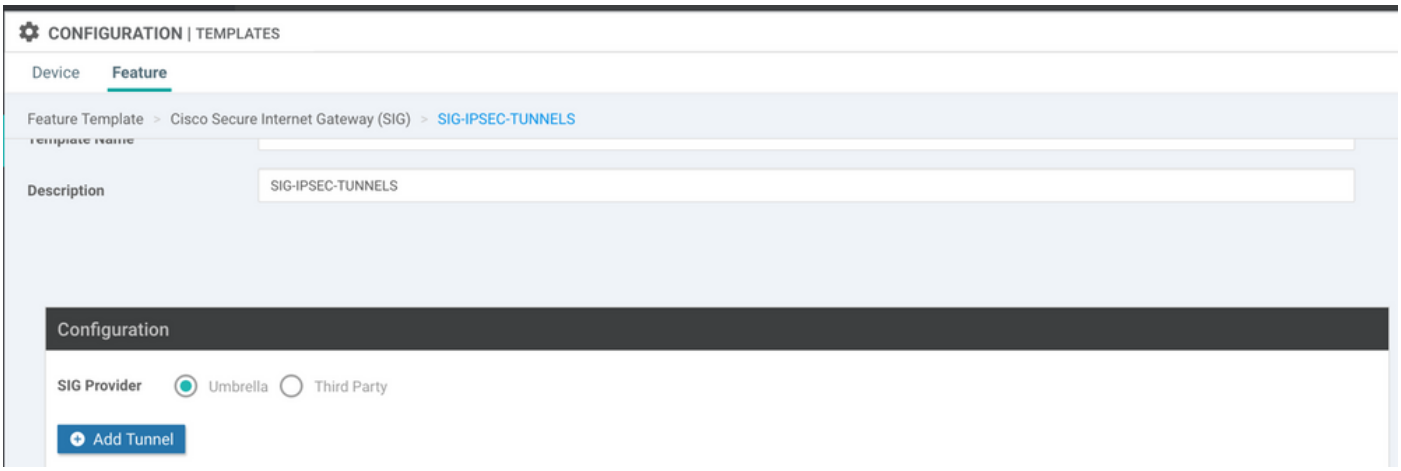
انتقل إلى قالب الميزة، وتحت القسم **Transport & Management VPN** حدد قالب ميزة عبارة الإنترنت الآمنة من Cisco.



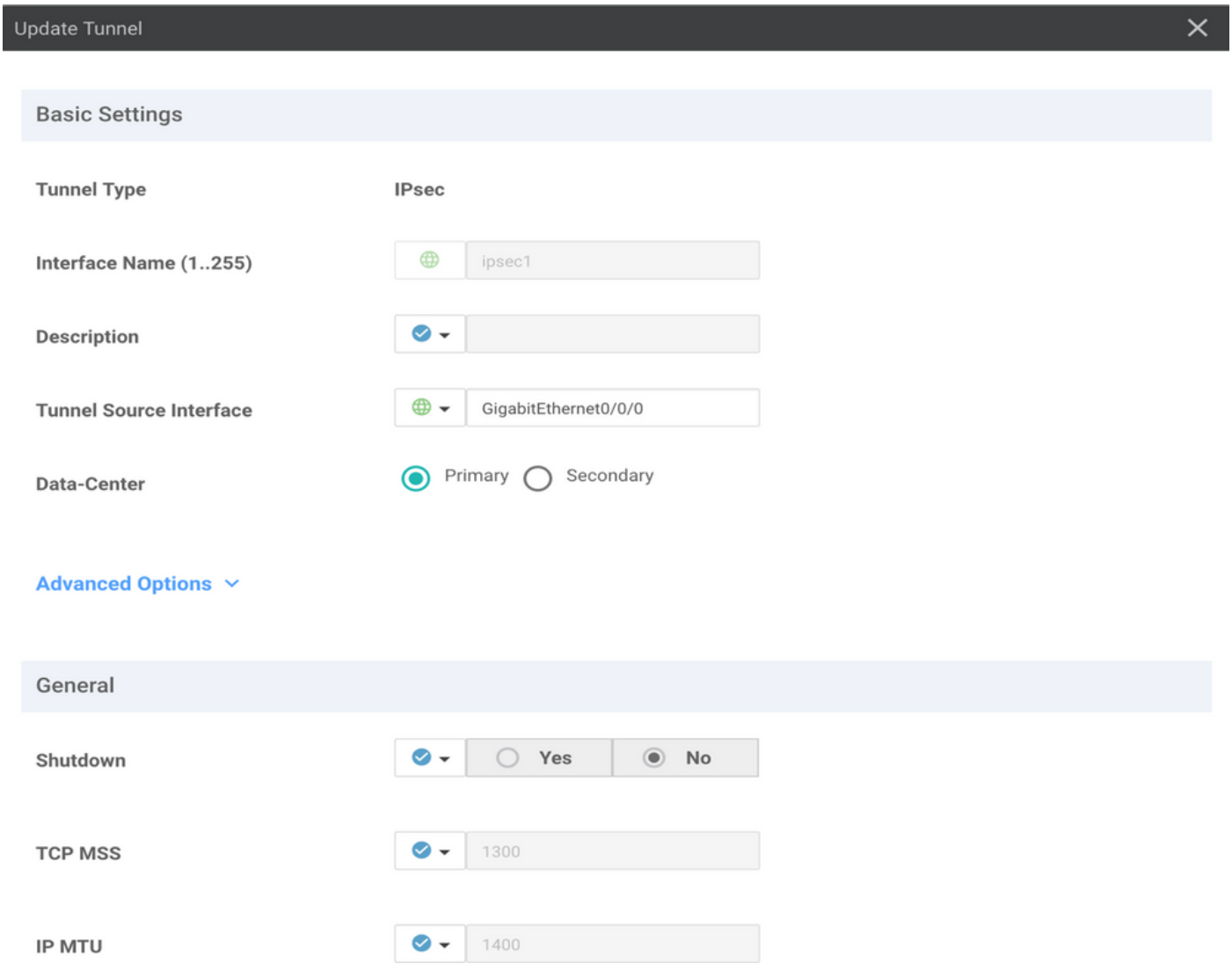
قم بإعطاء اسم ووصف للقالب.

الخطوة 3. حدد موفر SIG الخاص بك للنفق الأساسي.

انقر **Add Tunnel**.



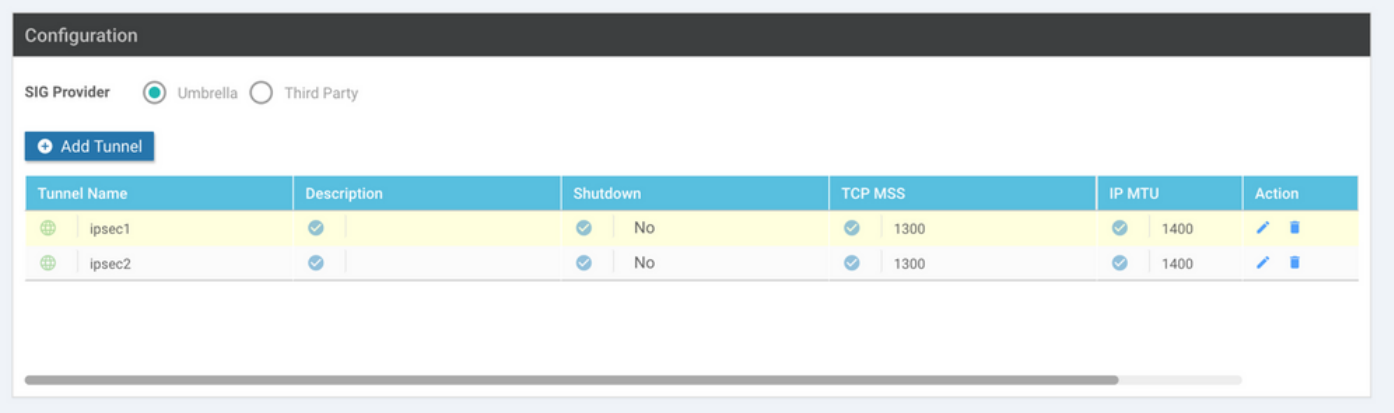
تكوين التفاصيل الأساسية والاحتفاظ **Data-Center** ك **Primary**، ثم انقر **Add**.



الخطوة 4. أضف النفق الثانوي.

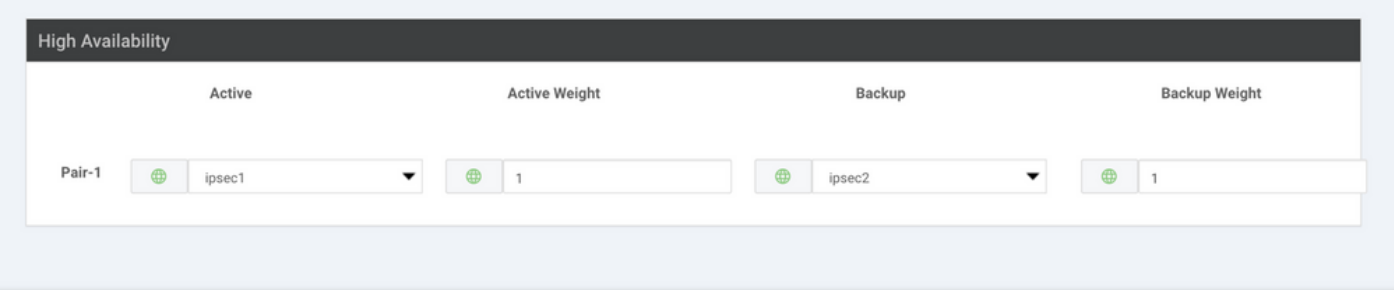
إضافة تكوين نفق ثان، إستخدام **Data-Center** ك **Secondary** هذه المرة، واسم الواجهة هو IPSec2.

يظهر تكوين vManage كما هو موضح هنا:



الخطوة 5. إنشاء زوج واحد عالي التوفر.

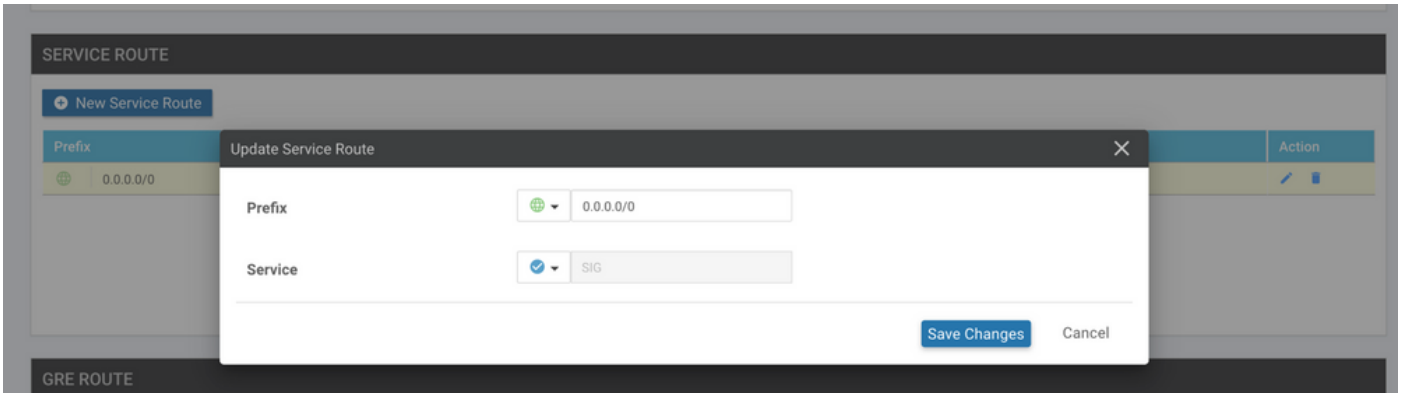
داخل **High Availability** أختر القسم ipSec1 على أنه نشط ونفق IPSec2 على أنه نسخ إحتياطي.



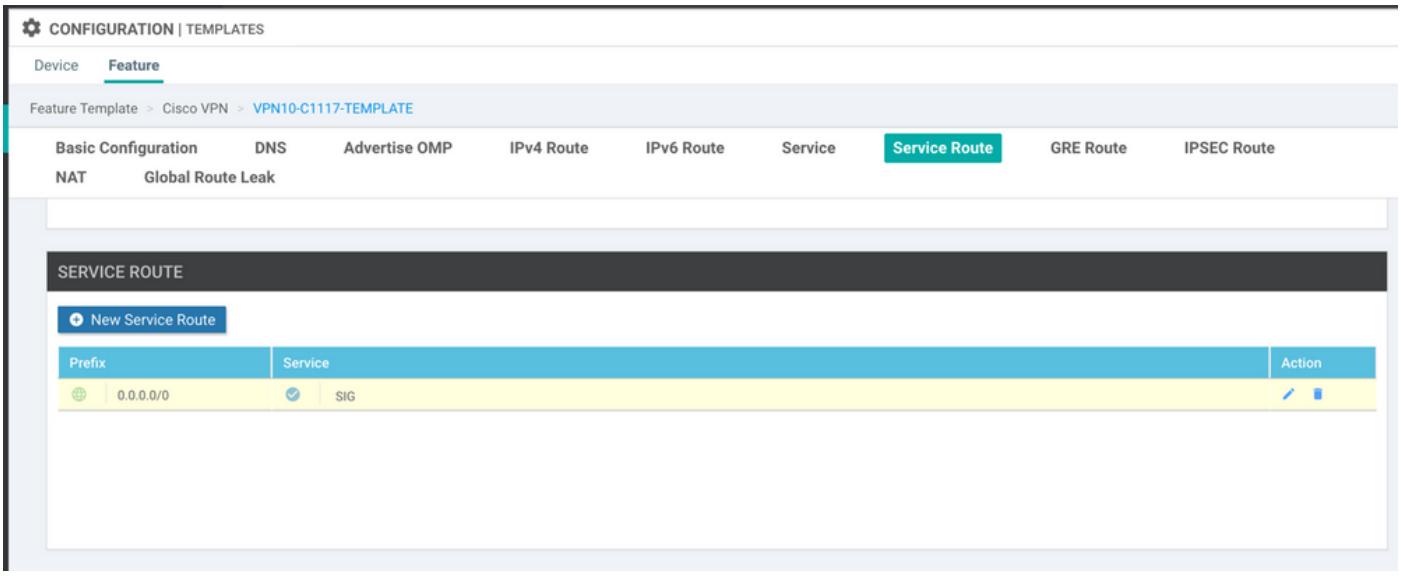
ملاحظة: ما يصل إلى 4 **High Availability** يمكن إنشاء أزواج من الأنفاق بحد أقصى من 4 أنفاق نشطة في نفس الوقت.

الخطوة 6. تحرير قالب VPN من جانب الخدمة لإدخال مسار خدمة.

انتقل إلى **Service VPN** و، ضمن **Service VPN** القالب، انتقل إلى المقطع **Service Route** وإضافة 0.0.0.0 مع SIG **Service Route**. ل هذا وثيقة، ال VRF/VPN 10 استعملت.

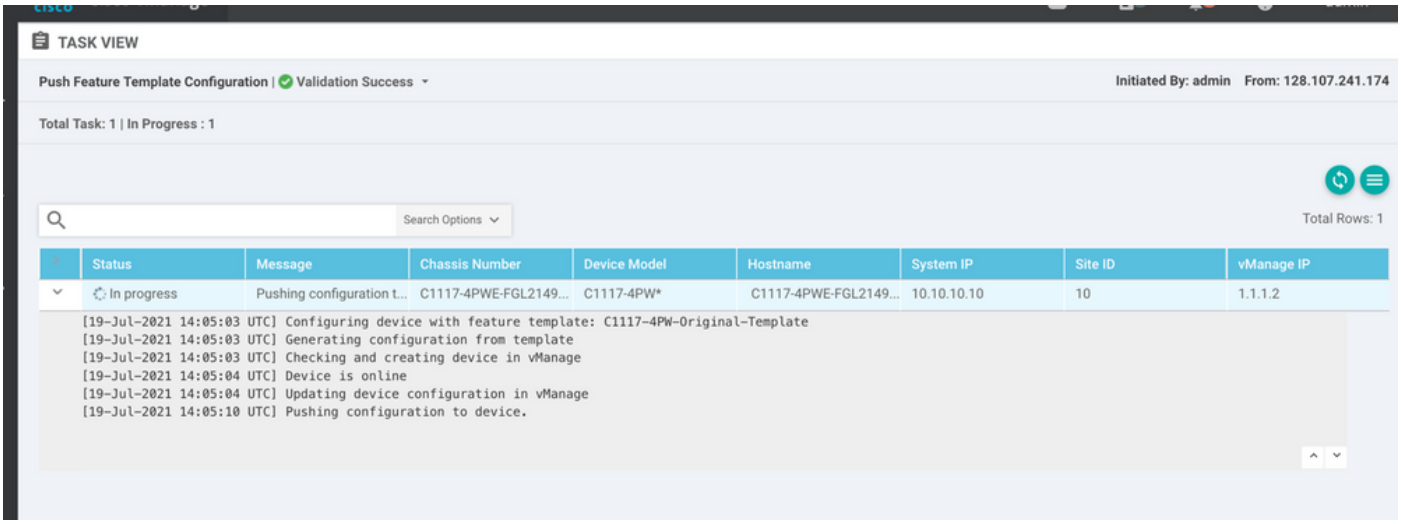


يتم عرض مسار 0.0.0.0 SIG كما هو موضح هنا.



ملاحظة: للخروج الفعلي لحركة مرور الخدمة، يجب تكوين NAT في واجهة WAN.

قم بإرفاق هذا القالب بالجهاز واضغط على التكوين:



تكوين موجه WAN Edge للسيناريو النشط/الاحتياطي

```
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
```

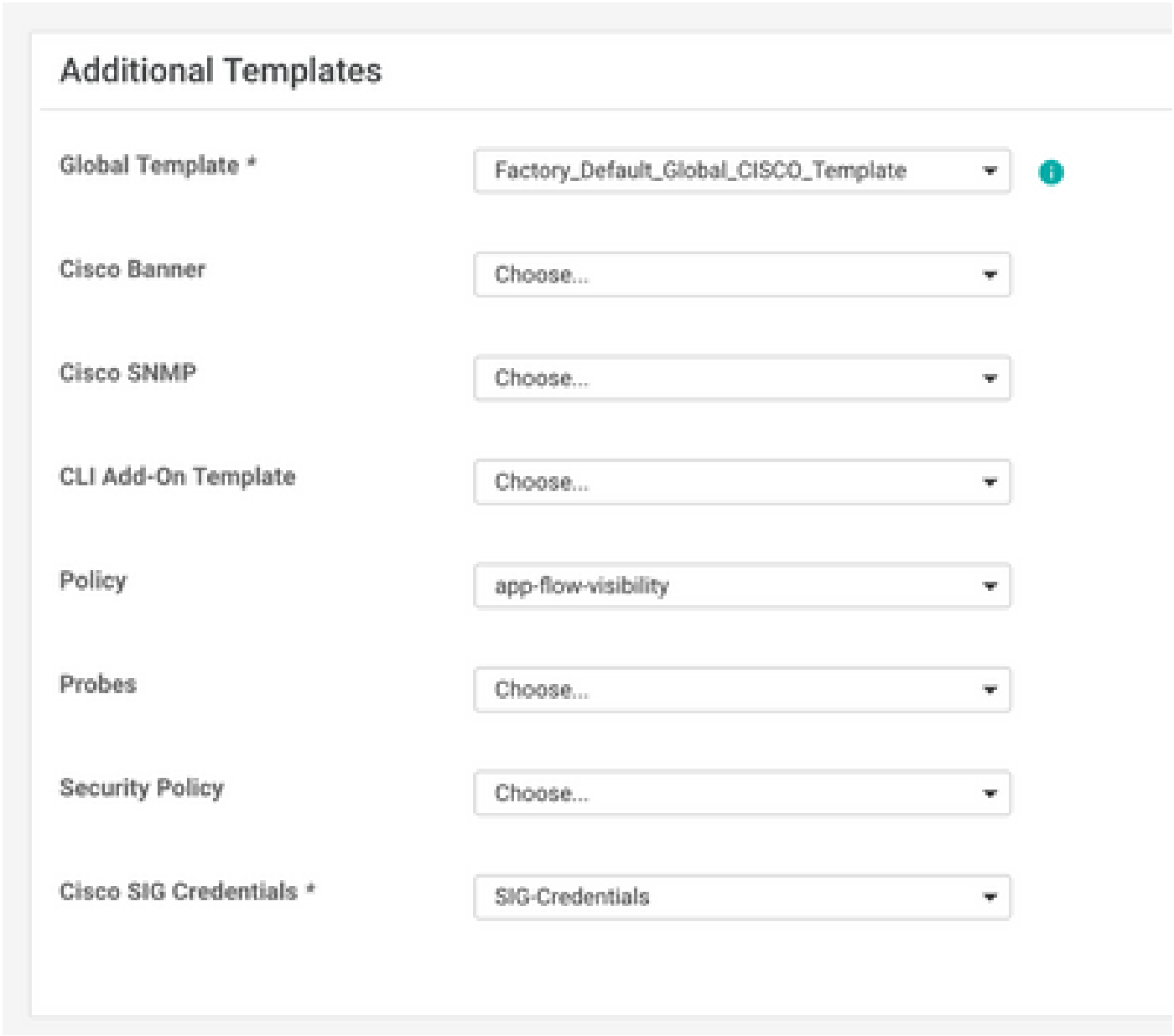
```
 set security-association replay window-size 512
!
crypto ipsec profile if-ipsec2-ipsec-profile
 set ikev2-profile if-ipsec2-ikev2-profile
 set transform-set if-ipsec2-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
no crypto isakmp diagnose error
no network-clock revertive
```

إنشاء أنفاق Umbrella SIG باستخدام سيناريو نشط/نشط

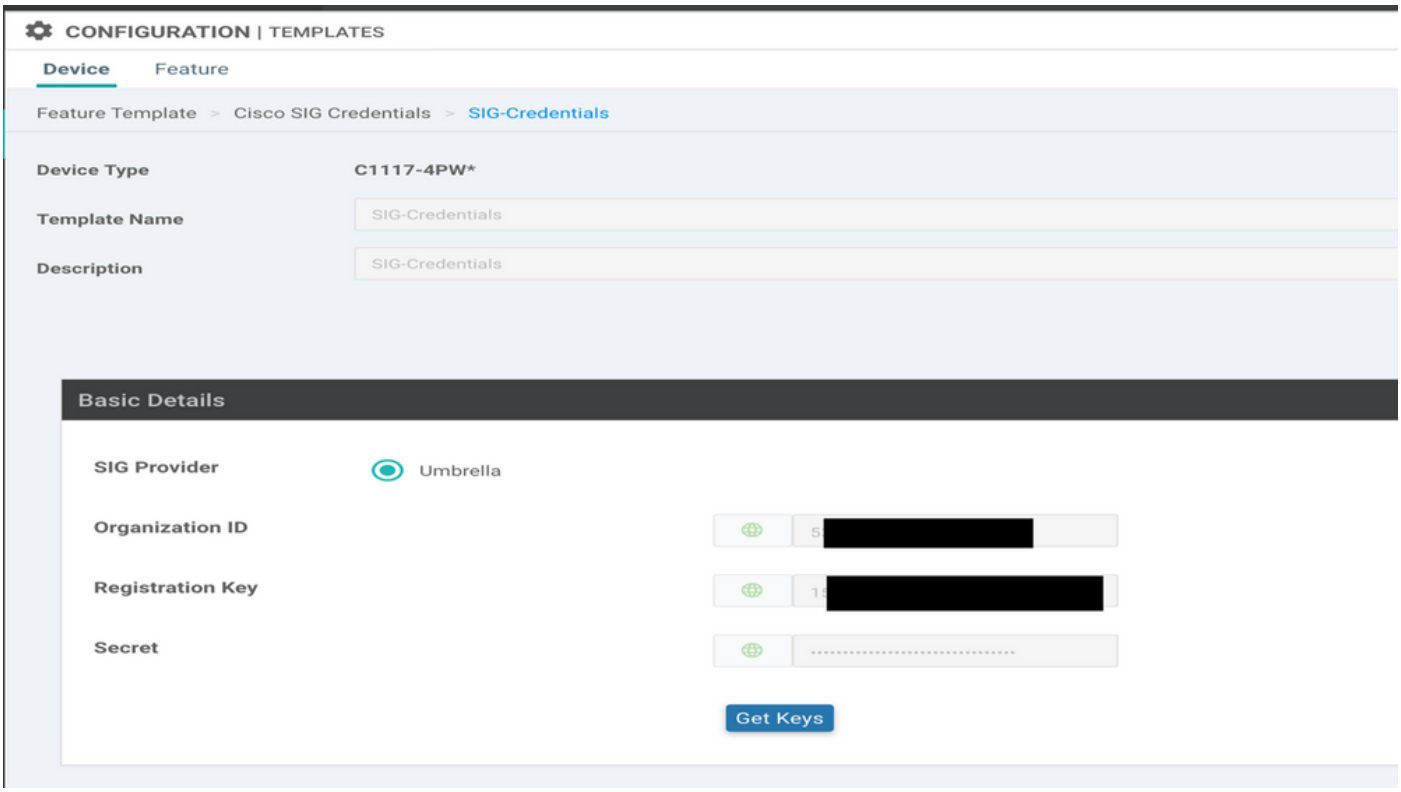
الخطوة 1. قم بإنشاء قالب ميزة بيانات اعتماد SIG.

انتقل إلى قالب الميزة وانقر فوق **Edit**

بموجب قسم من **Additional templates**، حدد **Cisco SIG Credentials**. يظهر الخيار على الصورة.



قم بإعطاء اسم ووصف للقالب.



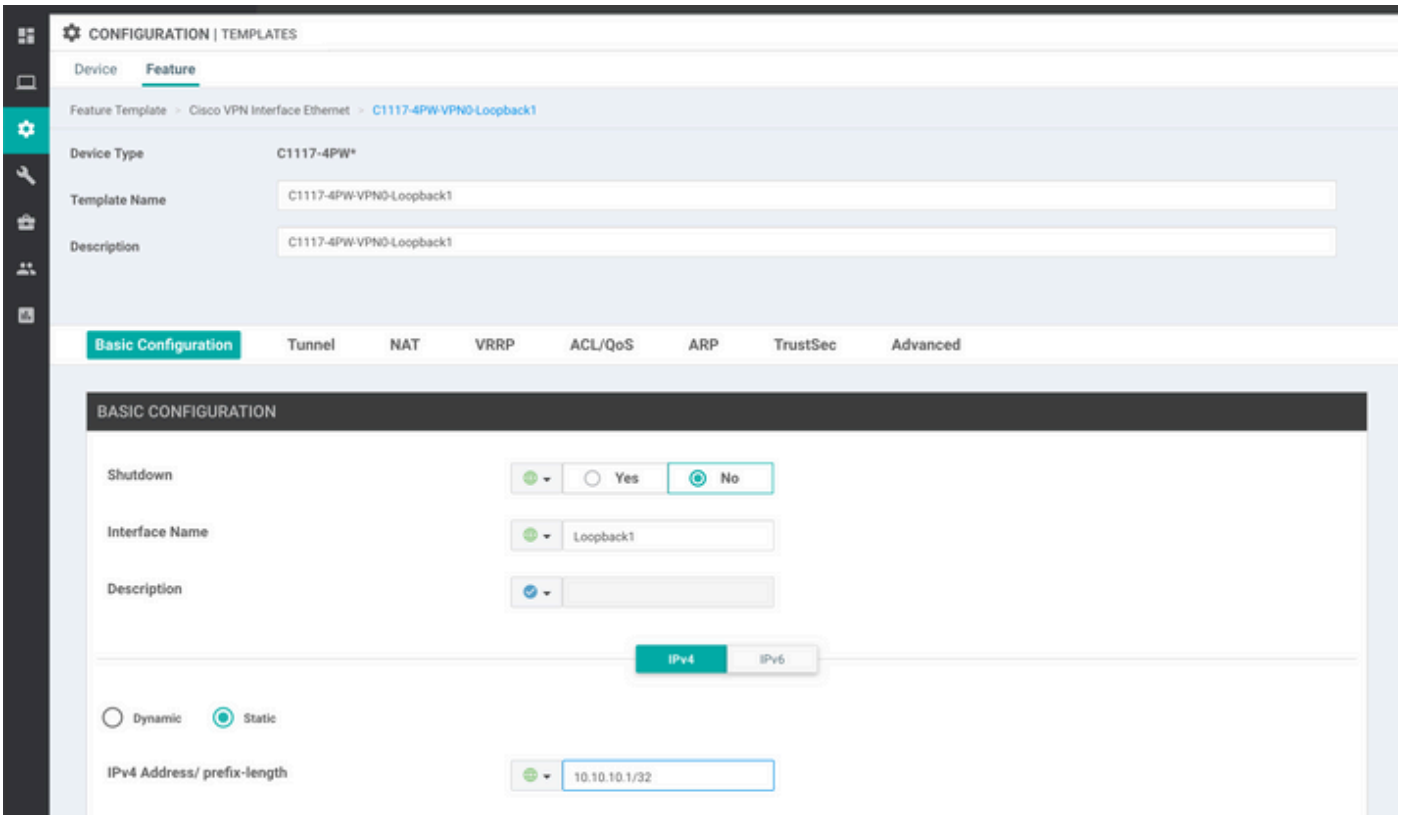
الخطوة 2. قم بإنشاء واجهة إسترجاع لربط أنفاق SIG.

ملاحظة: إنشاء واجهة إسترجاع لكل نفق SIG تم تكوينه في الوضع النشط، يلزم ذلك لأن كل نفق يحتاج إلى معرف IKE فريد.

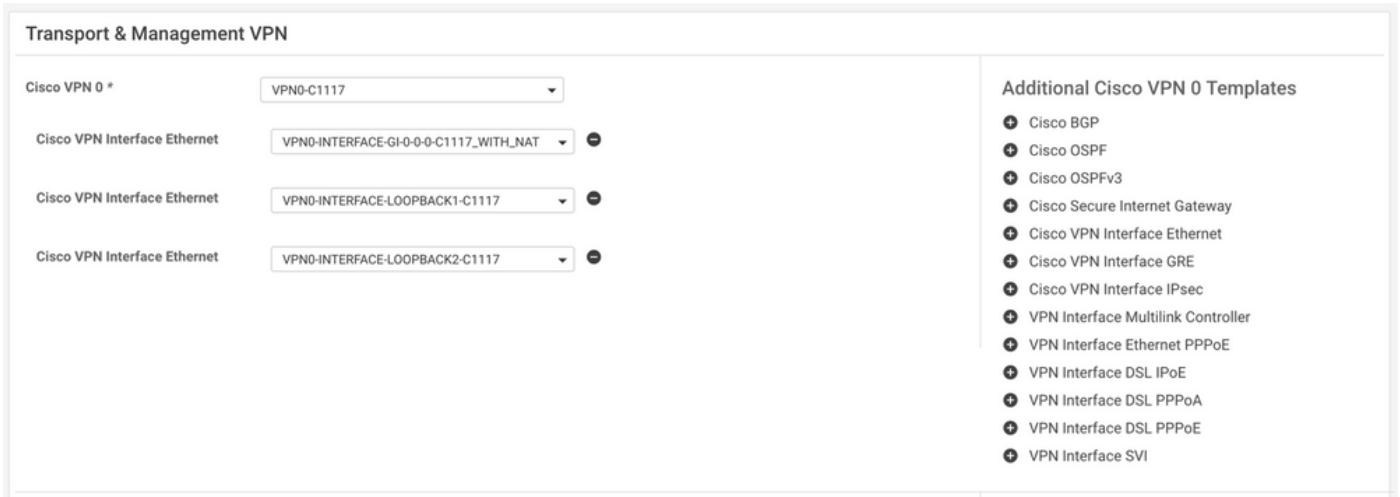
ملاحظة: هذا السيناريو نشط/نشط، لذلك يتم إنشاء استعراضين.

قم بتكوين اسم الواجهة وعنوان IPv4 للاستدراد.

ملاحظة: عنوان IP الذي تم تكوينه لإعادة الاسترجاع هو عنوان وهمي.



قم بإنشاء قالب الاسترجاع الثاني وإرفاقه بقالب الجهاز. يجب أن يحتوي قالب الجهاز على إثنين من قوالب الاسترجاع المرفقة:

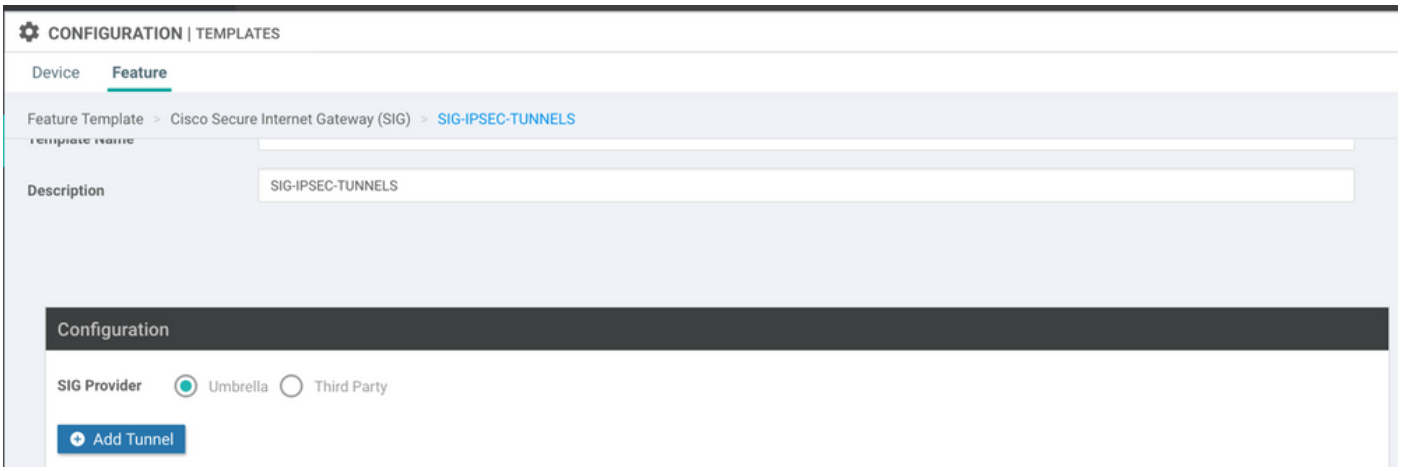


الخطوة 3. إنشاء قالب ميزة SIG.

انتقل إلى قالب ميزة SIG، وتحت القسم **Transport & Management VPN** تحديد **Cisco Secure Internet Gateway** قالب الميزة.

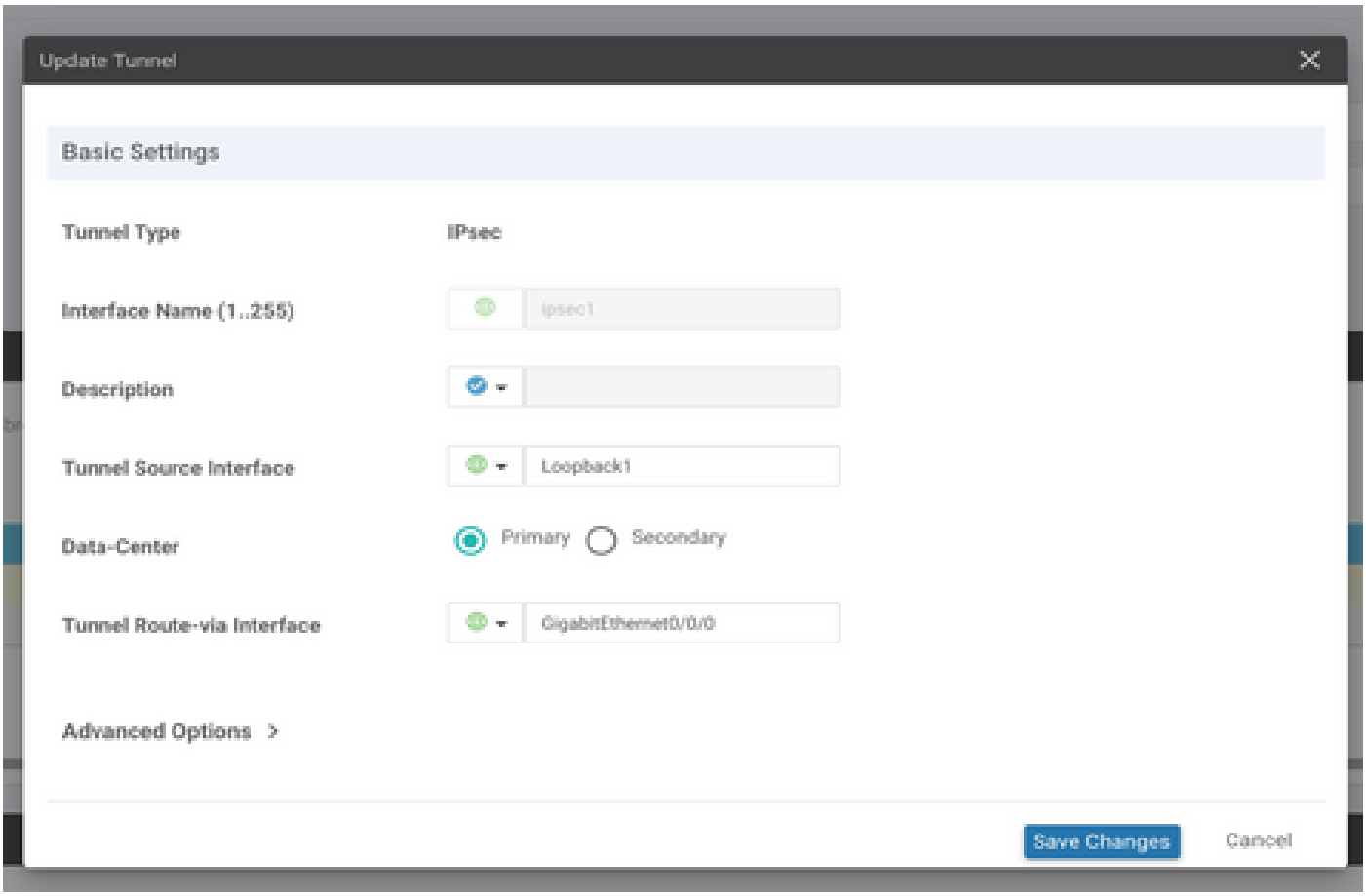
الخطوة 4. حدد موفر SIG للنفق الأساسي.

انقر **Add Tunnel**.



تكوين التفاصيل الأساسية والاحتفاظ **Data-Center** ك **Primary**.

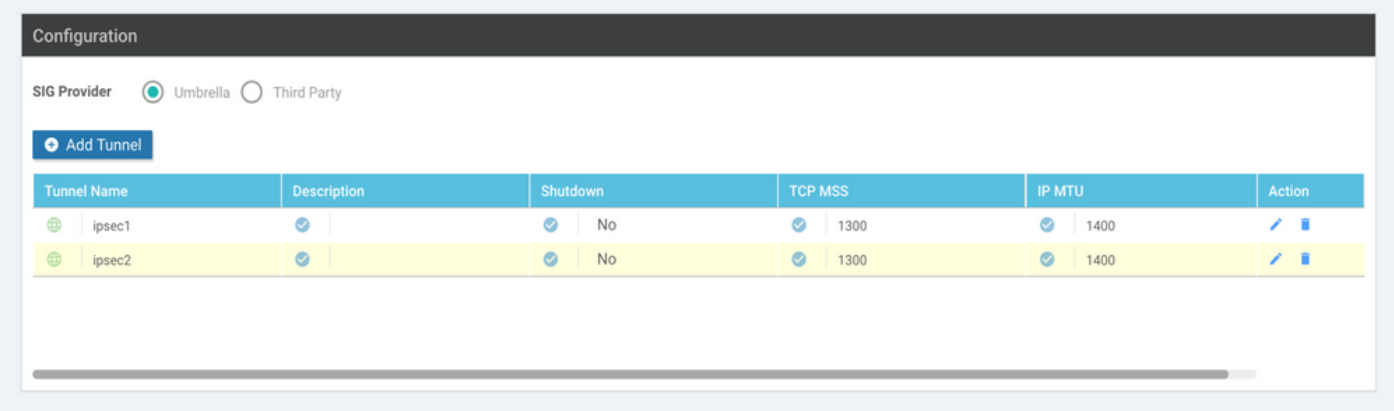
ملاحظة: معلمة واجهة مصدر النفق هي الاسترجاع (لهذا المستند الاسترجاع1) وبوصفها مسار النفق عبر الواجهة المادية (لهذا المستند GigabitEthernet0/0/0)



الخطوة 5. أضف النفق الثانوي.

إضافة تكوين نفق ثان، إستخدام **Data-Center** ك **Primary** كذلك، واسم الواجهة وهو IPSec2.

يظهر تكوين vManage كما هو موضح هنا:

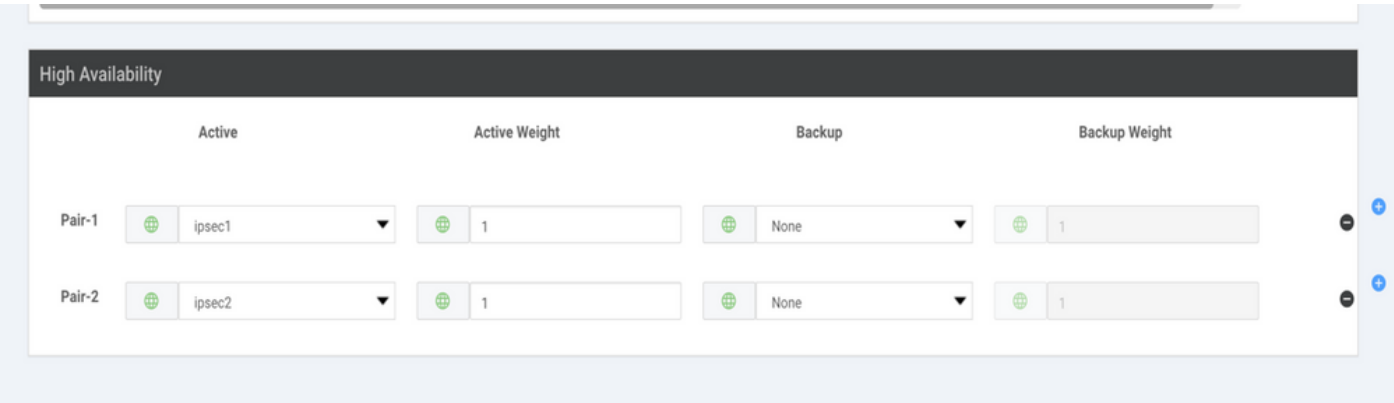


الخطوة 6. إنشاء إثنين من أزواج التوفر العالي.

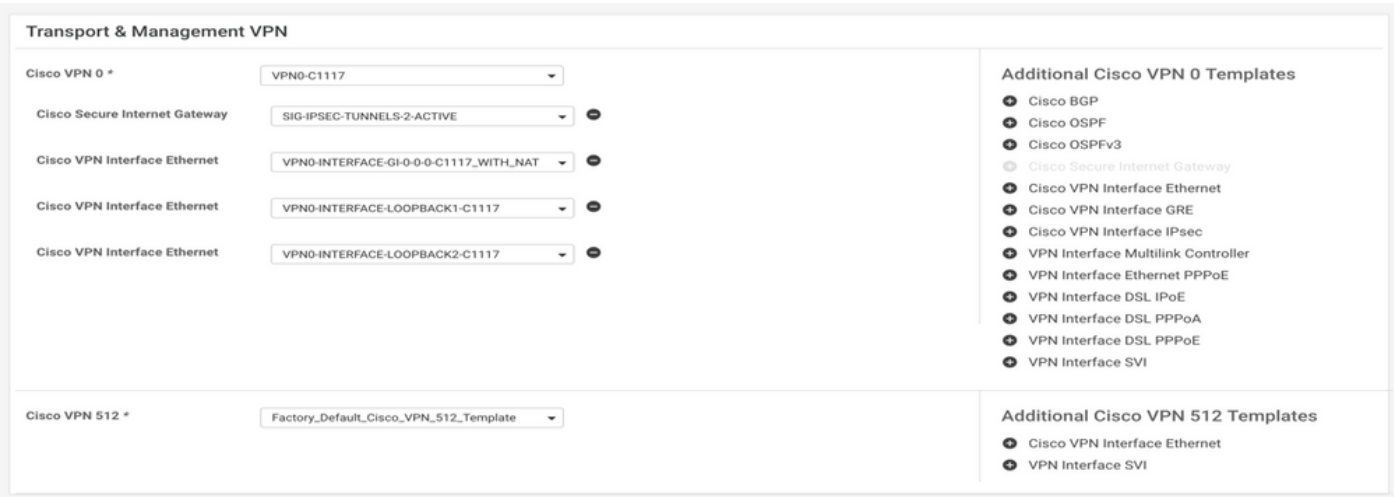
داخل **High Availability** قسم، إنشاء إثنان **High Availability** أزواج.

- في زوج HA الأول، حدد IPSec1 كنشاط وحدد **None** للنسخ الاحتياطي.
- في زوج HA الثاني، حدد IPSec2 كتحديد نشط **None** ومشان الدعم.

تكوين vManage ل **High Availability** يظهر كما هو موضح:

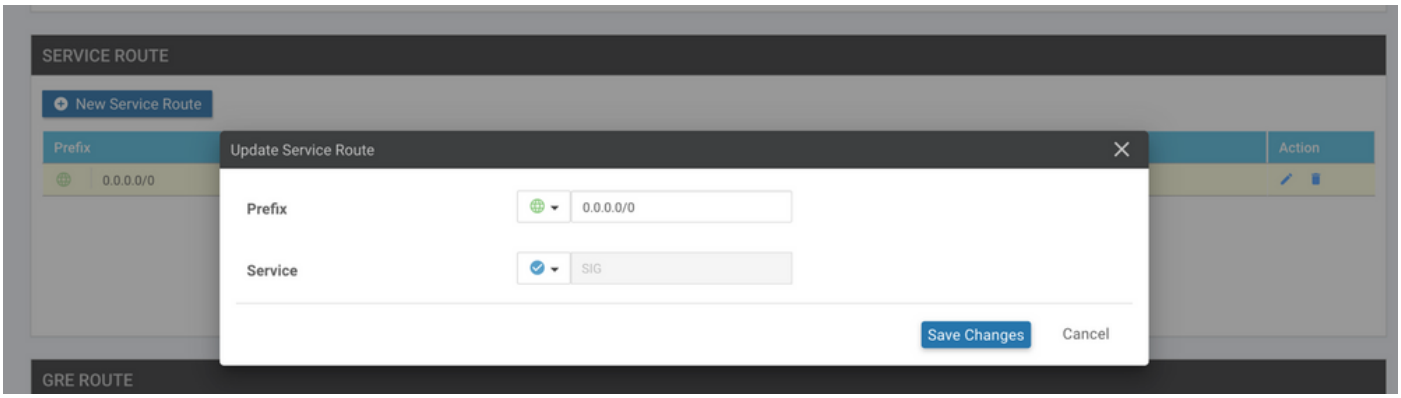


يحتوي قالب الجهاز على كل القالبين Loopback وقالب ميزة SIG المرفق أيضا.



الخطوة 7. تحرير قالب VPN من جانب الخدمة لإدخال مسار خدمة.

انتقل إلى Service VPN انتقل إلى القسم وضمن شبكة VPN الخاصة بقالب الخدمة Service Route وإضافة 0.0.0.0 مع SIGService Route



يظهر مسار 0.0.0.0 SIG كما هو موضح هنا.

ملاحظة: للخروج الفعلي لحركة مرور الخدمة، يجب تكوين NAT في واجهة WAN.

قم بإرفاق هذا القالب بالجهاز واضغط على التكوين.

تكوين موجه WAN Edge لسيناريو نشط/نشط

```
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
!
```

ملاحظة: على الرغم من أن هذه المستندات تركز على Umbrella، إلا أن السيناريوهات نفسها تنطبق على أنفاق Azure و SIG الخاصة بالطرف الثالث.

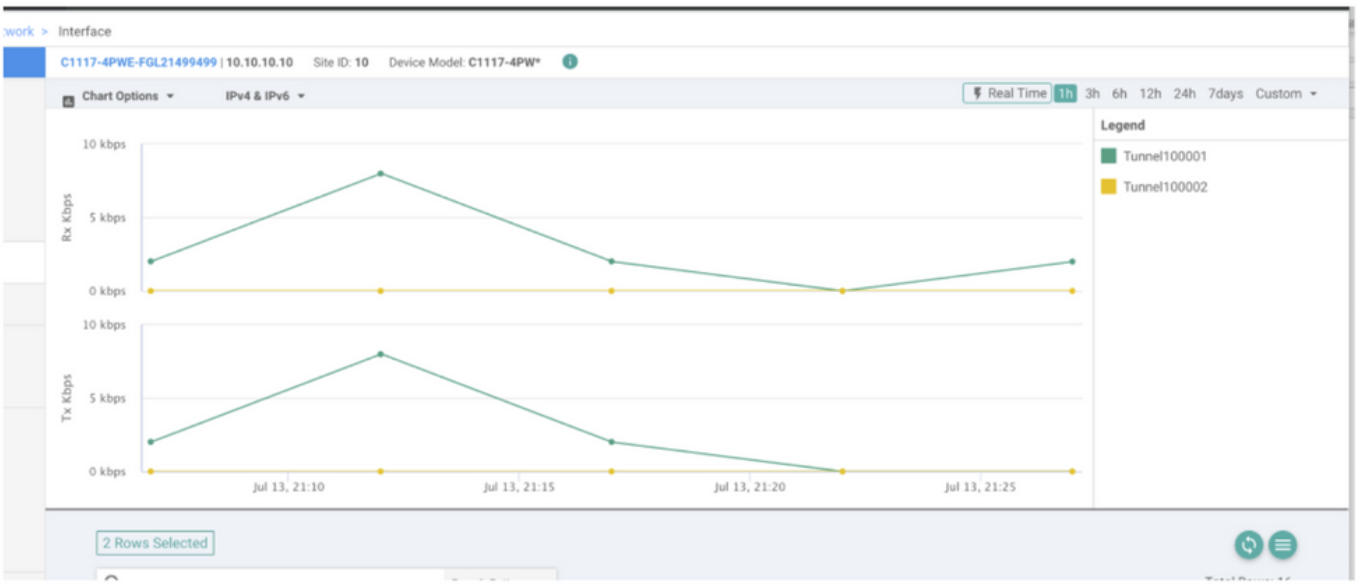
التحقق من الصحة

التحقق من السيناريو النشط/الاحتياطي

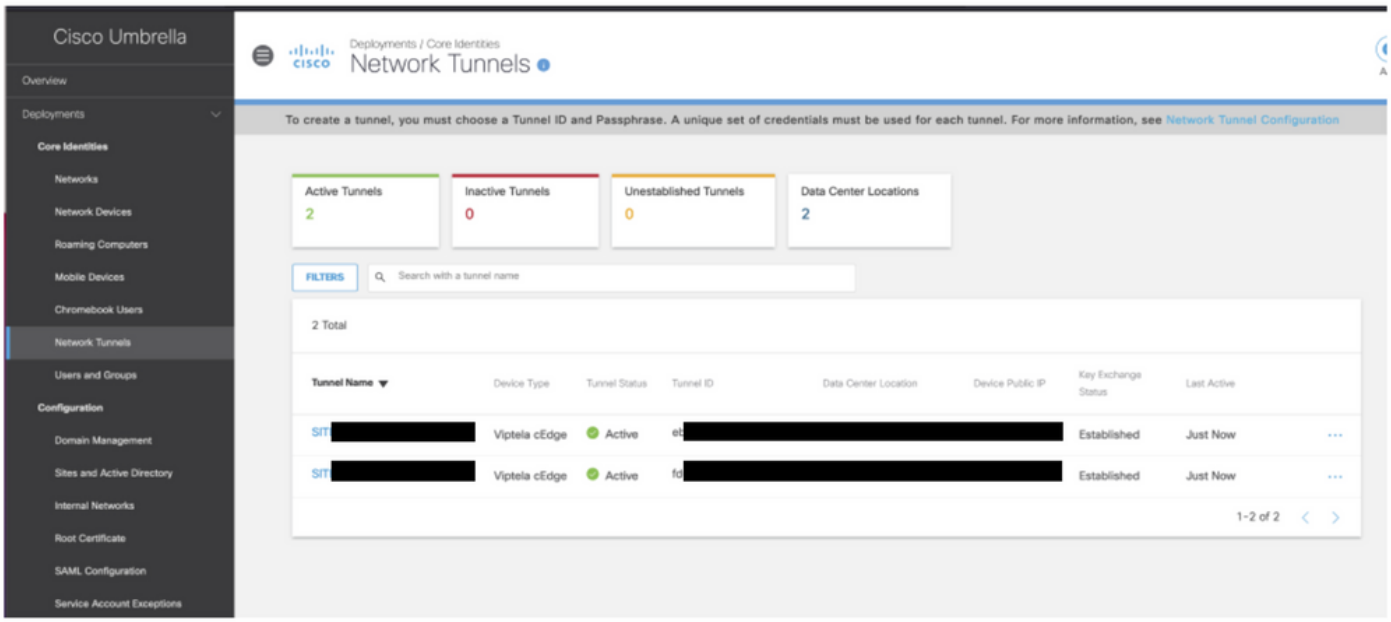
في vManage، من الممكن مراقبة حالة أنفاق SIG IPSec. انتقل إلى **Monitor** > **Network**، حدد جهاز حافة WAN المطلوب.

انقر فوق **Interfaces** على الجانب الأيسر، يتم عرض قائمة بجميع الواجهات في الجهاز. ويتضمن ذلك واجهات IPSec1 و IPSec2.

توضح الصورة أن نفق IPSec1 يقوم بإعادة توجيه حركة مرور البيانات والنفق IPSec2 يقوم بتمرير حركة مرور البيانات.



من الممكن أيضا التحقق من الأنفاق على Cisco **Umbrella** المدخل ظاهرة في الصورة.



أستخدم **show sdwan secure-internet-gateway tunnels** أمر على ال CLI in order to عرض النفق معلومة.

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
                                                                                                API   LAST
TUNNEL IF
NAME           TUNNEL ID  TUNNEL NAME                                FSM STATE                 HTTP  SUCCESSFUL
                                                                                                CODE  REQ
-------------------------------------------------------------------------------------------------------------
Tunnel100001   540798313  SITE10SYS10x10x10x10IFTunnel100001  st-tun-create-notif  200   create-tunnel
Tunnel100002   540798314  SITE10SYS10x10x10x10IFTunnel100002  st-tun-create-notif  200   create-tunnel
```

أستخدم **show endpoint-tracker** و **show ip sla summary** أوامر على واجهة سطر الأوامر (CLI) لعرض المعلومات حول أجهزة التعقب التي تم إنشاؤها تلقائيا ووحدات التحكم في الوصول (SLAs).

```
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      Last
                                                       Code        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
```

التحقق من السيناريو النشط/النشط

من الممكن أن يراقب vManage حالة أنفاق SIG IPSec. انتقل إلى **Monitor** > **Network**, حدد جهاز حافة WAN المطلوب.

انقر فوق **Interfaces** علامة التبويب على الجانب الأيسر - ويتم عرض قائمة بجميع الواجهات في الجهاز. ويتضمن ذلك واجهات IPSec1 و IPSec2.

توضح الصورة أن كل من نفق IPSec1 و IPSec2 يؤدي إلى إعادة توجيه حركة مرور البيانات.

أستخدم **show sdwan secure-internet-gateway tunnels** أمر على ال CLI in order to عرض النفق معلومة.

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
                                                                                API   LAST
TUNNEL IF                                                                        HTTP  SUCCESSFUL
NAME          TUNNEL ID  TUNNEL NAME                          FSM STATE          CODE  REQ
-------------------------------------------------------------------------------------------------
Tunnel100001  540798313  SITE10SYS10x10x10x10IFTunnel100001  st-tun-create-notif  200   create-tunnel
Tunnel100002  540798314  SITE10SYS10x10x10x10IFTunnel100002  st-tun-create-notif  200   create-tunnel
```

أستخدم **show endpoint-tracker** و **show ip sla summary** أوامر على واجهة سطر الأوامر (CLI) لعرض المعلومات حول أجهزة التعقب التي تم إنشاؤها تلقائيا ووحدات التحكم في الوصول (SLAs).

```
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      Last
```

```
                                                        Code        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
```

معلومات ذات صلة

- تمتع بدمج أجهزتك مع بوابات الإنترنت الآمنة - الإصدار 17.x من Cisco IOS® XE
- http://Network Tunnel Configuration - Umbrella SIG
- بدء تشغيل Umbrella
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).