Konfiguration und Überprüfung des SD-WAN IPsec SIG-Tunnels mit Zscaler

Inhalt

Einleitung

In diesem Dokument werden die Konfigurationsschritte und die Überprüfung von SD-WAN-IPsec-SIG-Tunneln mit Zscaler beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Security Internet Gateway (SIG)
- Funktionsweise von IPsec-Tunneln, Phase 1 und Phase 2 auf Cisco IOS®

Zusätzliche Anforderungen

- NAT muss auf der Transportschnittstelle aktiviert werden, die mit dem Internet verbunden ist.
- Auf VPN 0 muss ein DNS-Server erstellt werden, und die Zscaler-Basis-URL muss mit diesem DNS-Server aufgelöst werden. Dies ist wichtig, da API-Aufrufe fehlschlagen, wenn dies nicht behoben wird. Layer-7-Integritätsprüfungen schlagen ebenfalls fehl, da die URL standardmäßig http://gateway.<zscalercloud>.net/vpntest lautet.

- NTP (Network Time Protocol) muss sicherstellen, dass die Uhrzeit des Cisco Edge-Routers korrekt ist und API-Anrufe nicht fehlschlagen.
- Eine Service-Route, die auf SIG verweist, muss in der Service-VPN-Funktionsvorlage oder CLI konfiguriert werden:
  ip sdwan route vrf 1 0.0.0.0/0 service sig

Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- Cisco Edge Router Version 17.6.6a
- vManage, Version 20.9.4

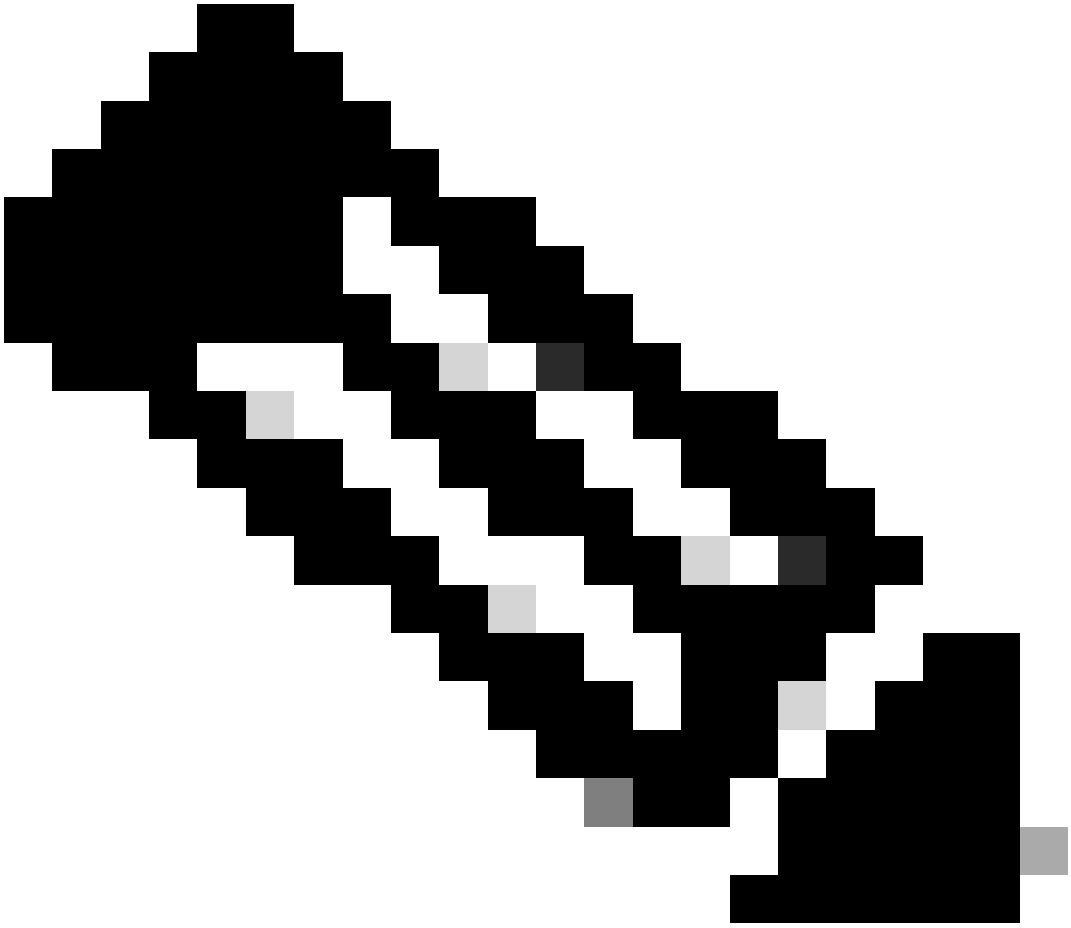
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

Optionen für das Netzwerkdesign

Nachfolgend sind die verschiedenen Bereitstellungsarten in einer Aktiv/Standby-Kombinationskonfiguration aufgeführt. Die Tunnelkapselung kann entweder über GRE oder IPsec bereitgestellt werden.

- Ein Aktiv/Standby-Tunnelpaar
- Ein Aktiv/Aktiv-Tunnelpaar
- Mehrere aktive/Standby-Tunnelpaare.
- Mehrere aktive/aktive Tunnelpaare.



Hinweis: Auf Cisco Edge-Routern mit SD-WAN können Sie eine oder mehrere mit dem Internet verbundene Transportschnittstellen verwenden, damit diese effektiv funktionieren.

Konfigurationen

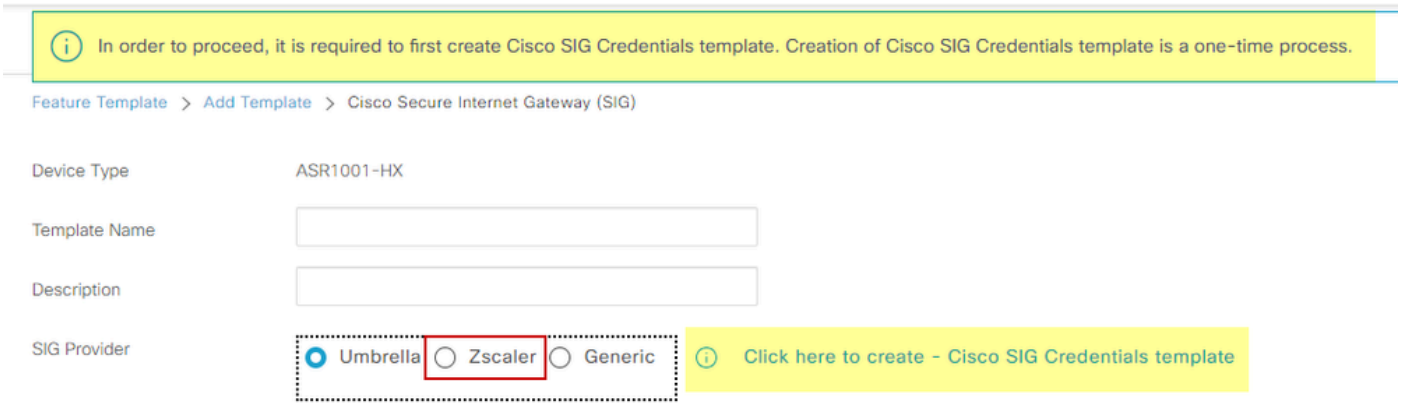
Fahren Sie mit der Konfiguration dieser Vorlagen fort:

- SIG-Vorlage (Security Internet Gateway) für Anmeldeinformationen:
  - Sie benötigen einen für alle Cisco Edge-Router. Informationen zum Ausfüllen der erforderlichen Felder der Vorlage müssen im Zscaler-Portal erstellt werden.
- SIG-Funktionsvorlage (Security Internet Gateway):
  - Unter dieser Funktionsvorlage konfigurieren Sie IPsec-Tunnel, stellen eine hohe Verfügbarkeit sicher, entweder im Aktiv/Aktiv- oder im Aktiv/Standby-Modus, und wählen das Zscaler-Rechenzentrum entweder automatisch oder manuell aus.

Um eine Vorlage mit Zscaler-Anmeldeinformationen zu erstellen, navigieren Sie zu Configuration

> Template > Feature Template > Add Template.

Wählen Sie das Gerätemodell aus, das Sie für diesen Zweck verwenden möchten, und suchen Sie nach SIG. Wenn Sie es zum ersten Mal erstellen, zeigt das System, dass Zscaler-Anmeldeinformationen zuerst erstellt werden müssen, wie in diesem Beispiel:
Sie müssen Zscaler als SIG-Anbieter auswählen und auf die Vorlage Klicken Sie hier, um die Cisco SIG-Anmeldeinformationen zu erstellen klicken.



Signaturanmeldevorlage

"

Sie werden zur Vorlage mit den Anmeldeinformationen weitergeleitet. In dieser Vorlage müssen Sie die Werte für alle Felder eingeben:

- Vorlagenname
- Beschreibung
- SIG-Anbieter (automatisch aus dem vorherigen Schritt ausgewählt)
- Organisation
- Partner Base-URI
- Benutzername
- Kennwort
- Partner-API-Schlüssel

Klicken Sie auf Speichern.

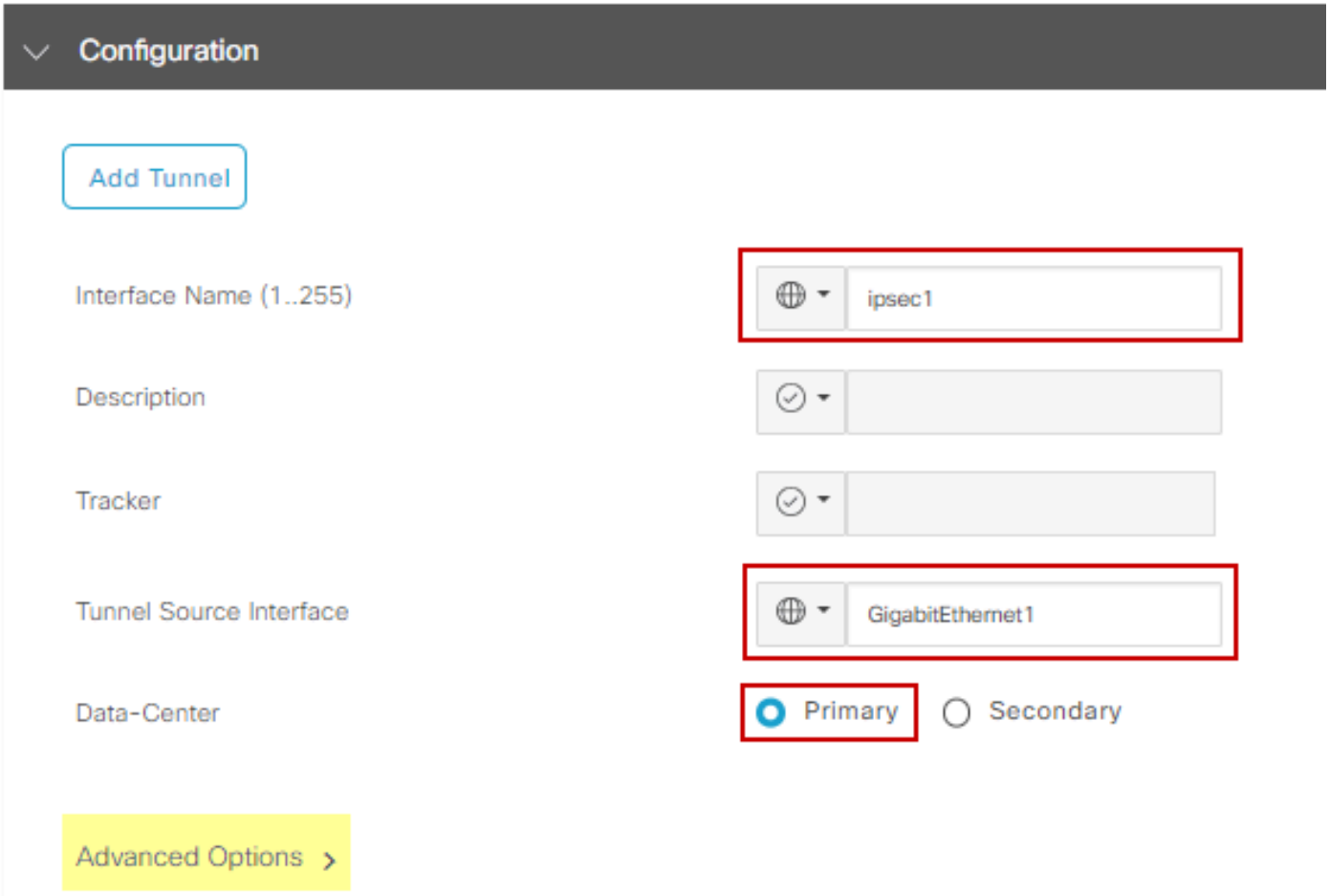
Sie werden zur Vorlage für ein sicheres Internet-Gateway (SIG) umgeleitet. Mit dieser Vorlage können Sie alle notwendigen Einstellungen für SD-WAN IPsec SIG mit Zscaler vornehmen.

Geben Sie im ersten Abschnitt der Vorlage einen Namen und eine Beschreibung an. Der Standard-Tracker wird automatisch aktiviert. Die für die Zscaler Layer 7-Integritätsprüfung verwendete API-URL lautet: zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest.

In Cisco IOS XE müssen Sie eine IP-Adresse für den Tracker festlegen. Jede private IP innerhalb des /32-Bereichs ist zulässig. Die eingestellte IP-Adresse kann von der Loopback 6530-Schnittstelle verwendet werden, die automatisch für die Durchführung von Zscaler-Zustandsinspektionen erstellt wird.

Im Abschnitt "Konfiguration" können Sie die IPsec-Tunnel erstellen, indem Sie auf Tunnel hinzufügen klicken. Wählen Sie im neuen Popup-Fenster eine Auswahl basierend auf Ihren Anforderungen aus.

In diesem Beispiel wurde die Schnittstelle IPsec1 erstellt, wobei die WAN-Schnittstelle GigabitEthernet1 als Tunnelquelle verwendet wurde. Anschließend kann eine Verbindung mit dem primären Rechenzentrum der Zcaler-Klasse hergestellt werden.
Es wird empfohlen, die Standardwerte für die erweiterten Optionen beizubehalten.

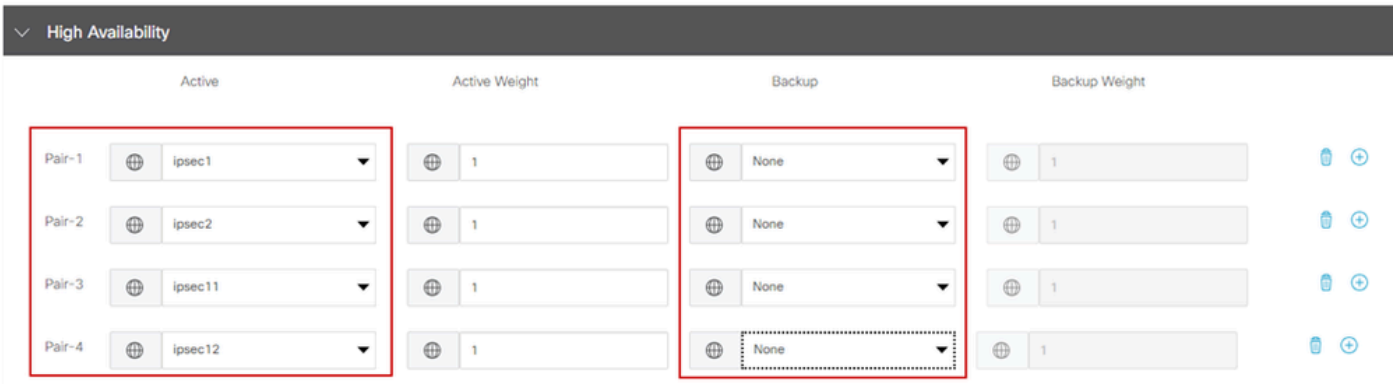


IPsec-Schnittstellenkonfiguration

Hohe Verfügbarkeit

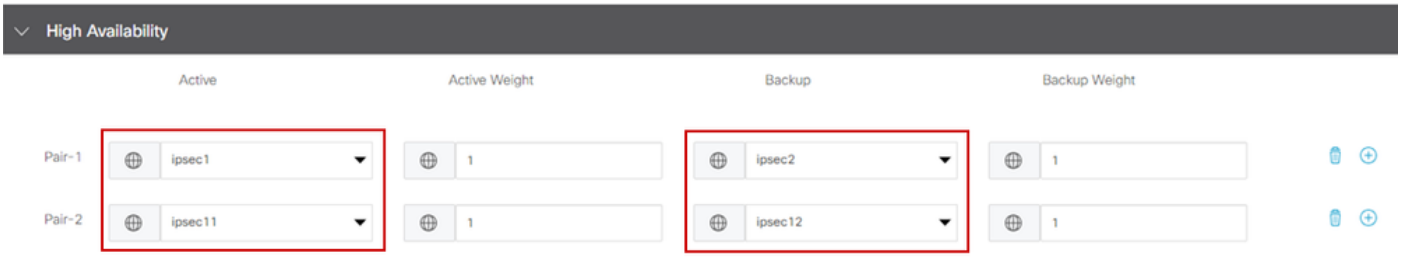
In diesem Abschnitt wählen Sie, ob das Design "Aktiv/Aktiv" oder "Aktiv/Standby" sein soll, und legen fest, welche IPsec-Schnittstelle aktiv sein soll.

Dies ist ein Beispiel für ein Aktiv/Aktiv-Design. Alle Schnittstellen sind unter Aktiv ausgewählt, Sicherung bleibt ohne ausgewählt.



Aktives/aktives Design

Dieses Beispiel zeigt ein Aktiv/Standby-Design. IPsec1 und IPsec11 werden als aktive Schnittstellen ausgewählt, während IPsec2 und IPsec12 als Standby-Schnittstellen festgelegt werden.



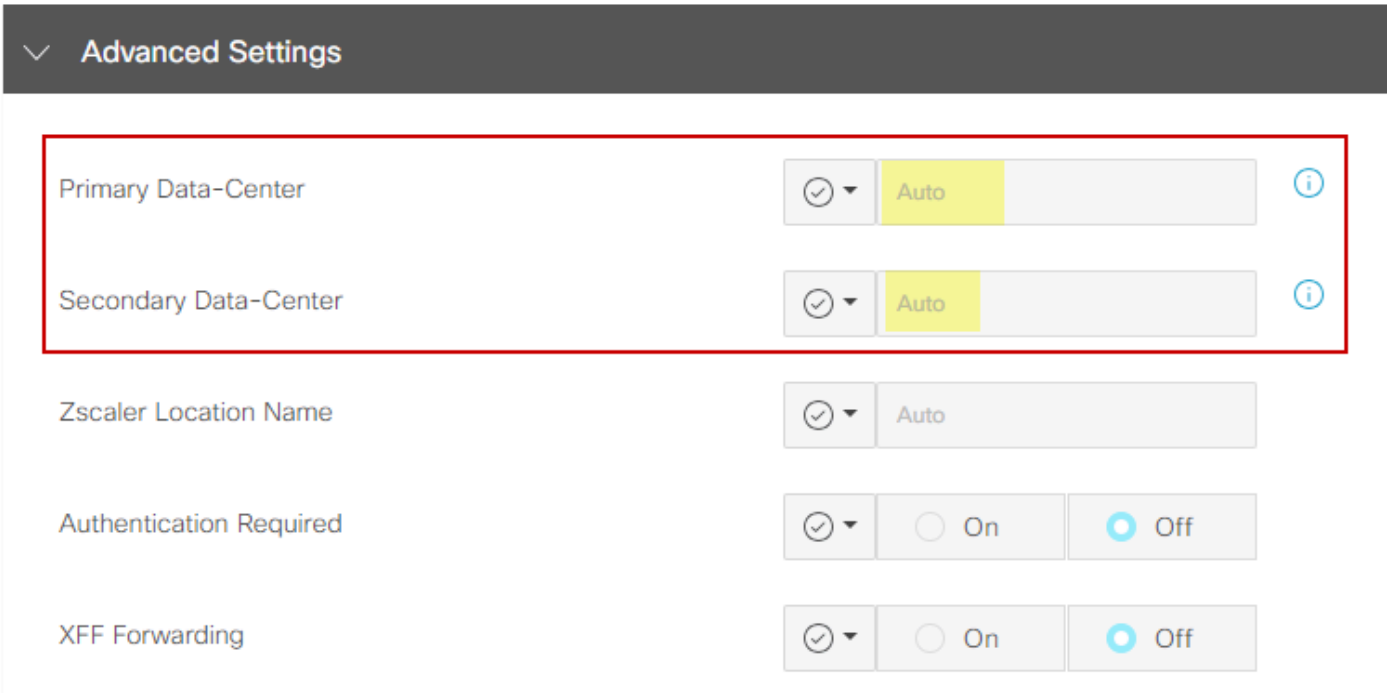
Aktiv/Standby-Design

Erweiterte Einstellungen

In diesem Abschnitt sind die wichtigsten Konfigurationen das primäre und das sekundäre Rechenzentrum.

Es wird empfohlen, beide als "automatisch" oder "manuell" zu konfigurieren. Es wird jedoch nicht empfohlen, sie als "gemischt" zu konfigurieren.

Wenn Sie diese manuell konfigurieren möchten, wählen Sie die richtige URL aus dem Zscaler-Portal aus, basierend auf Ihrer Partner Base URI.



Automatische oder manuelle Rechenzentren

Klicken Sie abschließend auf Speichern.

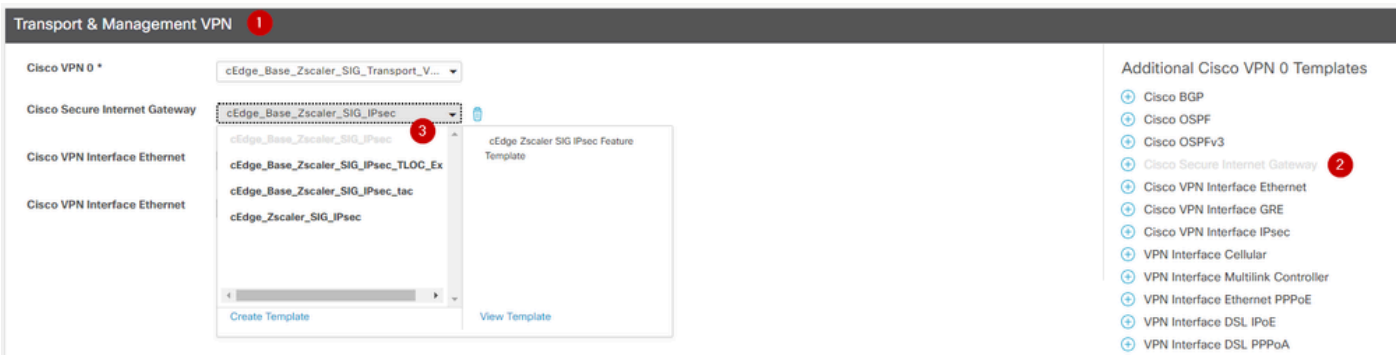
Wenn Sie die Konfiguration der SIG-Vorlagen abgeschlossen haben, müssen Sie diese unter der Gerätevorlage anwenden. Auf diese Weise wird die Konfiguration auf die Cisco Edge-Router übertragen.

Um diese Schritte auszuführen, navigieren Sie zu Configuration > Templates > Device Template (Konfiguration > Vorlagen > Gerätevorlage), und klicken Sie auf Edit (Bearbeiten).

1. Unter Transport & Management VPN

2. Fügen Sie eine Vorlage für ein sicheres Internet-Gateway hinzu.

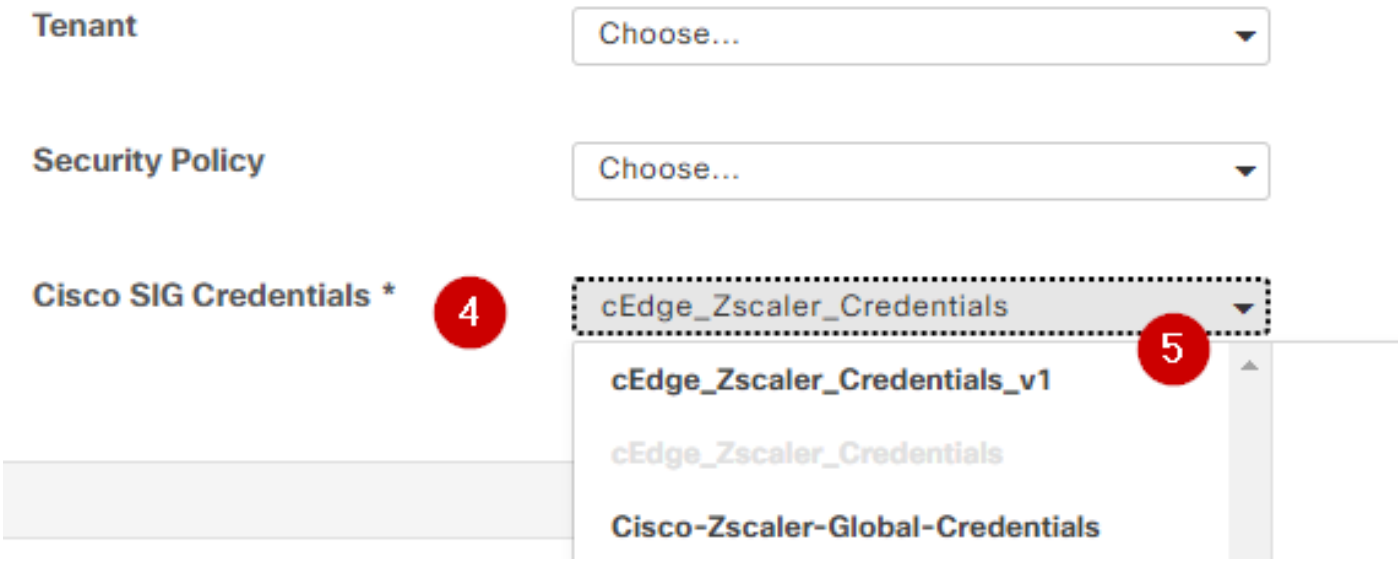
3. Wählen Sie auf Cisco Secure Internet Gateway die richtige SIG-Funktionsvorlage aus dem Dropdown-Menü aus.



SIG-Vorlage zur Gerätevorlage hinzufügen

Unter Zusätzliche Vorlagen

4. Cisco SIG-Anmeldedaten
5. Wählen Sie die richtige Vorlage für Cisco SIG-Anmeldeinformationen aus dem Dropdown-Menü:



SIG-Vorlage für Anmeldeinformationen

Klicken Sie auf Aktualisieren. Beachten Sie, dass Sie bei einer aktiven Vorlage für Ihr Gerät die Standardschritte verwenden müssen, um Konfigurationen für eine aktive Vorlage zu übernehmen.

Überprüfung

Die Überprüfung kann in der Konfigurationsvorschau durchgeführt werden, während Sie die Änderungen übertragen. Beachten Sie dabei Folgendes:

```
secure-internet-gateway
     zscaler organization <removed>
     zscaler partner-base-uri <removed>
     zscaler partner-key <removed>
     zscaler username <removed>
     zscaler password <removed>
    !
```

In diesem Beispiel sehen Sie, dass das Design aktiv/Standby ist.

<#root>

```
ha-pairs
  interface-pair

Tunnel100001 active

-interface-weight 1
```

```
Tunnel100002 backup

-interface-weight 1
  interface-pair

Tunnel100011 active

-interface-weight 1

Tunnel100012 backup

-interface-weight 1
```

Sie werden feststellen, dass weitere Konfigurationen hinzugefügt werden, wie crypto ikev2-Profile und -Richtlinien, mehrere Schnittstellen, die mit Tunnel1xxxxx beginnen, vrf definition 65530, ip sdwan route vrf 1 0.0.0.0/0 service sig.

Alle diese Änderungen sind Teil der IPsec-SIG-Tunnel mit Zscaler.

Dieses Beispiel zeigt, wie die Konfiguration für die Tunnelschnittstelle aussieht:

```
interface Tunnel100001
     no shutdown
     ip unnumbered       GigabitEthernet1
     no ip clear-dont-fragment
     ip mtu              1400
     tunnel source GigabitEthernet1
     tunnel destination dynamic
     tunnel mode ipsec ipv4
     tunnel protection ipsec profile if-ipsec1-ipsec-profile
     tunnel vrf multiplexing
```

Nachdem die Konfigurationen erfolgreich auf die Cisco Edge-Router übertragen wurden, können Sie mithilfe von Befehlen überprüfen, ob die Tunnel hochgefahren werden.

<#root>

```
Router#show sdwan secure-internet-gateway zscaler tunnels

HTTP

TUNNEL IF                                              TUNNEL

RESP

NAME          TUNNEL NAME                              ID        FQDN           TUNNEL FSM STATE

CODE

-------------------------------------------------------------------------------------------------------
Tunnel100001  site<removed>Tunnel100001            <removed>   <removed>     add-vpn-credential-info
```

```
200

Tunnel100002  site<removed>Tunnel100002              <removed>  <removed>     add-vpn-credential-info
200
```

Wenn http bzw. Code 200 nicht angezeigt wird, bedeutet dies, dass Sie mit einem Problem im Zusammenhang mit dem Kennwort oder dem Partnerschlüssel konfrontiert sind.

Verwenden Sie den Befehl, um den Schnittstellenstatus zu überprüfen.

<#root>

```
Router#
show ip interface brief

Interface              IP-Address      OK? Method Status    Protocol
GigabitEthernet1       10.2.234.146    YES DHCP   up            up
GigabitEthernet2       10.2.58.221     YES other  up            up
GigabitEthernet3       10.2.20.77      YES other  up            up
GigabitEthernet4       10.2.248.43     YES other  up            up
Sdwan-system-intf      10.10.10.221    YES unset  up            up
Loopback65528          192.168.1.1     YES other  up            up
Loopback65530          192.168.0.2     YES other  up            up   <<< This is the IP that you used or

NVI0                   unassigned      YES unset  up            up
Tunnel2                10.2.58.221     YES TFTP   up            up
Tunnel3                10.2.20.77      YES TFTP   up            up
Tunnel100001           10.2.58.221     YES TFTP   up            up


Tunnel100002           10.2.58.221     YES TFTP   up            up
```

Um den Status des Trackers zu überprüfen, führen Sie die Befehle show endpoint-tracker und show endpoint-tracker records aus. So können Sie die URL bestätigen, die der Tracker verwendet

```
Router#show endpoint-tracker
Interface              Record Name            Status          RTT in msecs    Probe ID        Next Hop
Tunnel100001           #SIGL7#AUTO#TRACKER    Up              194             44              None
Tunnel100002           #SIGL7#AUTO#TRACKER    Up              80              48              None



Router#show endpoint-tracker records
```

```
Record Name            Endpoint                              EndPoint Type   Threshold(ms)    Multiplier
#SIGL7#AUTO#TRACKER    http://gateway.<removed>.net/vpnt API_URL         1000             2
```

Weitere Validierungen, die Sie durchführen können:
Führen Sie den folgenden Befehl aus, um sicherzustellen, dass Routen der VRF-Instanz auf IPsec-Tunnel verweisen:

show ip route vrf 1

Gateway der letzten Instanz ist 0.0.0.0 zu Netzwerk 0.0.0.0

S* 0.0.0.0/0 [2/65535], Tunnel100002
[2/65535], Tunnel100001
10.0.0.0/8 ist variabel subnettiert, 4 Subnetze, 2 Masken

Um die Validierung noch weiter auszubauen, können Sie einen Ping in Richtung Internet senden und eine Traceroute durchführen, um die Hops zu überprüfen, die der Datenverkehr belegt:

<#root>

```
Router#
```

ping vrf 1 cisco.com

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to <removed>, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 406/411/417 ms
```

<#root>

```
Router1#
```

traceroute vrf 1 cisco.com

```
Type escape sequence to abort.
Tracing the route to redirect-ns.cisco.com (<removed>)
VRF info: (vrf in name/id, vrf out name/id)
1 * * *
2
```

<The IP here need to be Zcaler IP>

```
 195 msec 193 msec 199 msec
3
```

<The IP here need to be Zcaler IP>

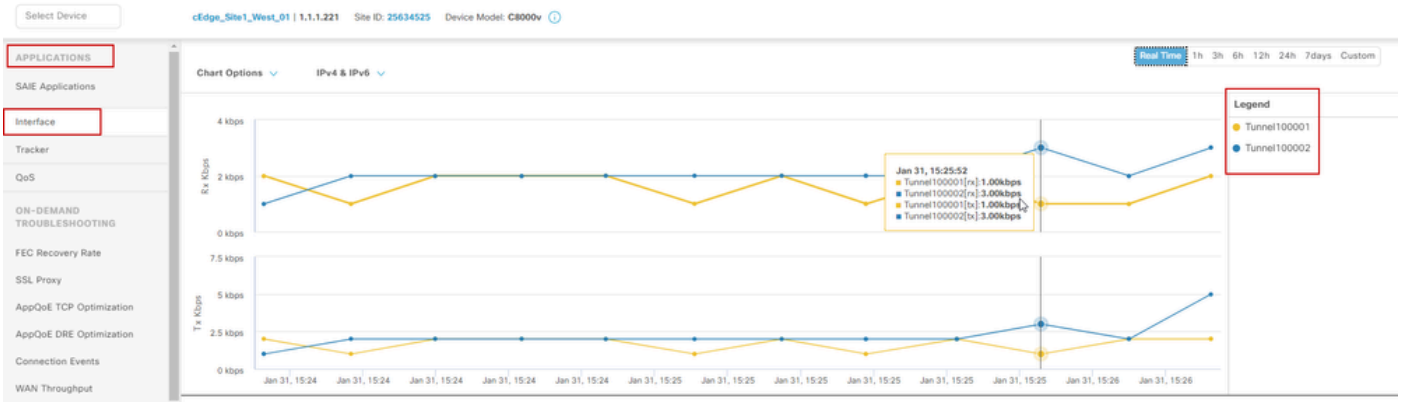
```
 200 msec
```

<The IP here need to be Zcaler IP>

```
 199 msec *
.....
```

Sie können IPsec-Schnittstellen über die vManage-GUI validieren, indem Sie auf Monitor > Device (Monitor > Gerät) oder Monitor > Network (für Codes 20.6 und frühere Versionen) navigieren.

- Wählen Sie Ihren Router aus, und navigieren Sie zu Anwendungen > Schnittstellen.
- Wählen Sie Tunnel10001 und Tunnel100002 aus, um den Echtzeitdatenverkehr anzuzeigen oder die Einstellungen je nach erforderlichem Zeitrahmen anzupassen:



Überwachen von IPsec-Tunneln

Fehlerbehebung

Wenn der SIG-Tunnel nicht ausgeführt wird, gehen Sie wie folgt vor, um das Problem zu beheben.

Schritt 1: Überprüfen Sie die Fehler mit dem Befehl show sdwan secure-internet-gateway zscaler tunnels. Wenn Sie den HTTP-RESP-Code 401 bemerken, weist die Ausgabe darauf hin, dass ein Authentifizierungsproblem vorliegt.

Sie können die Werte in der Vorlage für die SIG-Anmeldeinformationen überprüfen, um festzustellen, ob das Kennwort oder der Partnerschlüssel richtig ist.

<#root>

Router#

show sdwan secure-internet-gateway zscaler tunnels

HTTP

TUNNEL IF TUNNEL LOCATION

RESP

```
NAME TUNNEL             NAME                ID        FQDN   TUNNEL FSM STATE      ID        LOCATION FS
LAST HTTP REQ

CODE

-------------------------------------------------------------------------------------------------------------
Tunnel100001   site<removed>Tunnel100001   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401

Tunnel100002   site<removed>Tunnel100002   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401

Tunnel100011   site<removed>Tunnel100011   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401

Tunnel100012   site<removed>Tunnel100012   0                tunnel-st-invalid  <removed>  location-init
req-auth-session      401
```

Aktivieren Sie zum weiteren Debuggen diese Befehle, und suchen Sie nach Protokollmeldungen zu SIG, HTTP oder Tracker:

- debug plattform software sdwan ftm sig
- debug plattform software sdwan sig
- debug plattform software sdwan tracker
- debug plattform software sdwan ftm rtm-events

Dies ist ein Beispiel für die Ausgabe von Debugbefehlen:

```
<#root>

Router#

show logging | inc SIG


Jan 31 19:39:38.666: ENDPOINT TRACKER: endpoint tracker SLA already unconfigured: #SIGL7#AUTO#TRACKER
Jan 31 19:39:38.669: ENDPOINT TRACKER: endpoint tracker SLA already unconfigured: #SIGL7#AUTO#TRACKER
Jan 31 19:59:18.240: SDWAN INFO:

 Tracker entry Tunnel100001/#SIGL7#AUTO#TRACKER state => DOWN


Jan 31 19:59:18.263: SDWAN INFO: Tracker entry Tunnel100002/#SIGL7#AUTO#TRACKER state => DOWN
Jan 31 19:59:18.274: SDWAN INFO: Tracker entry Tunnel100011/#SIGL7#AUTO#TRACKER state => DOWN
Jan 31 19:59:18.291: SDWAN INFO: Tracker entry Tunnel100012/#SIGL7#AUTO#TRACKER state => DOWN
```

Führen Sie den Befehl show ip interface brief aus, und überprüfen Sie das Tunnels Interface Protocol, ob ein Bild angezeigt wird oder nicht.

<#root>

```
Router#
```

show ip interface brief

```
Interface              IP-Address      OK? Method Status    Protocol
GigabitEthernet1       10.2.234.146    YES DHCP   up            up
GigabitEthernet2       10.2.58.221     YES other  up            up
```

Tunnel100001 10.2.58.221 YES TFTP up down

Tunnel100002 10.2.58.221 YES TFTP up down

Nachdem Sie sichergestellt haben, dass keine Probleme mit den Zscaler-Anmeldeinformationen auftreten, können Sie die SIG-Schnittstelle aus der Gerätevorlage entfernen und an den Router weiterleiten.

Wenden Sie nach Abschluss der Übertragung die SIG-Vorlage an, und schieben Sie sie zurück auf den Router. Bei dieser Methode müssen die Tunnel von Grund auf neu erstellt werden.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

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.