Configuración y verificación del túnel SIG IPsec SD-WAN con Zscaler

Contenido

Introducción

Este documento describe los pasos de configuración y verificación de los túneles SIG IPsec SD-WAN con Zscaler.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Gateway de Internet de seguridad (SIG).
- Cómo funcionan los túneles IPsec, Phase1 y Phase2 en Cisco IOS®.

Requisitos adicionales

- La NAT debe estar habilitada en la interfaz de transporte que se va a conectar a Internet.
- Es necesario crear un servidor DNS en VPN 0 y resolver la URL base de Zscaler con este servidor DNS. Esto es importante porque si no se resuelve, las llamadas a la API fallarán. Las comprobaciones de estado de la capa 7 también fallarán, ya que, de forma predeterminada, la URL es: http://gateway.<zscalercloud>.net/vpntest.

- El NTP (protocolo de tiempo de red) debe garantizar que la hora del router de borde de Cisco sea precisa y que las llamadas a la API no fallen.
- Una ruta de servicio que apunta a SIG debe configurarse en la plantilla de la función Service-VPN o CLI:
  ip sdwan route vrf 1 0.0.0.0/0 service sig

Componentes Utilizados

Este documento se basa en las siguientes versiones de software y hardware:

- Router de extremo de Cisco versión 17.6.6a
- vManage versión 20.9.4

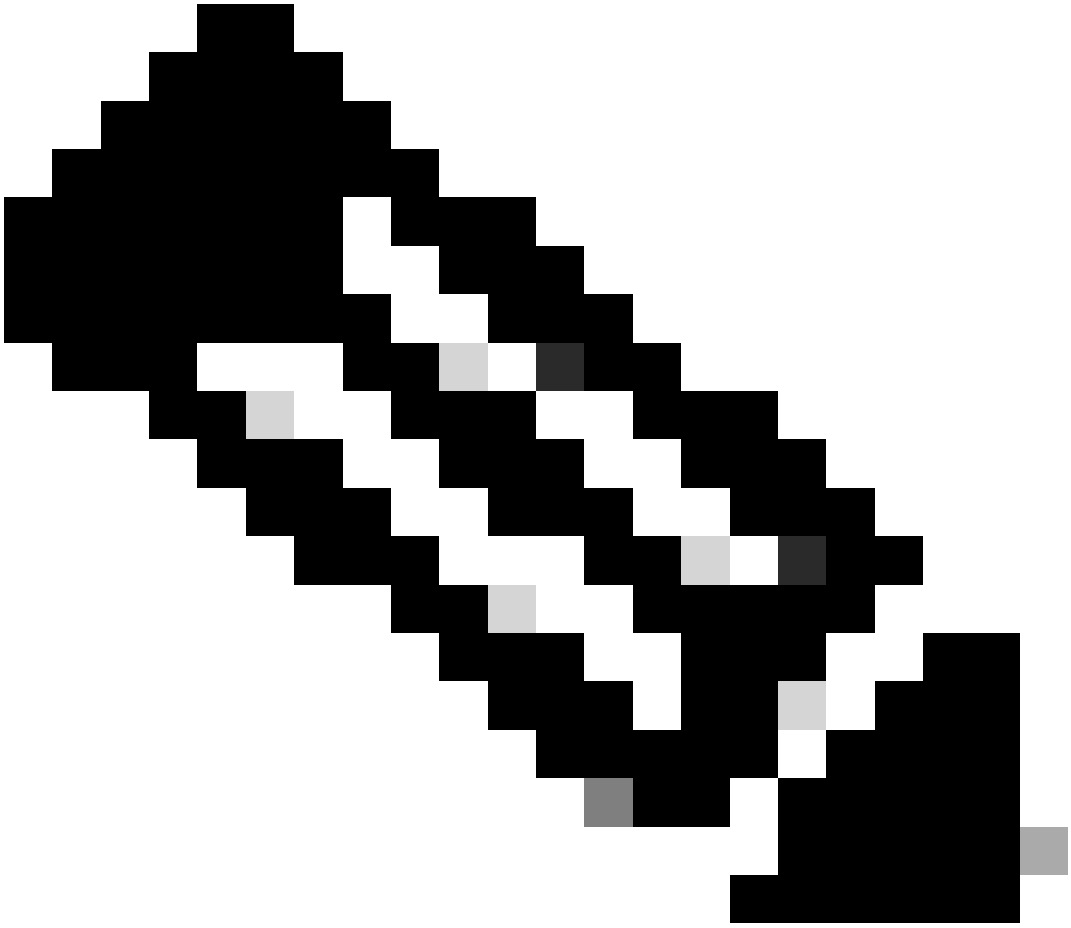
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Opciones de diseño de red

Estos son los distintos tipos de implementaciones en una configuración de combinación de activo y en espera. La encapsulación de túnel se puede implementar en GRE o IPsec.

- Un par de túneles activo/en espera.
- Un Par de Túnel Activo/Activo.
- Par de túnel activo/en espera múltiple.
- Par de túnel activo/activo múltiple.



Nota: En los routers periféricos de Cisco SD-WAN, puede utilizar una o más interfaces de transporte conectadas a Internet para que estas configuraciones funcionen eficazmente.

Configuraciones

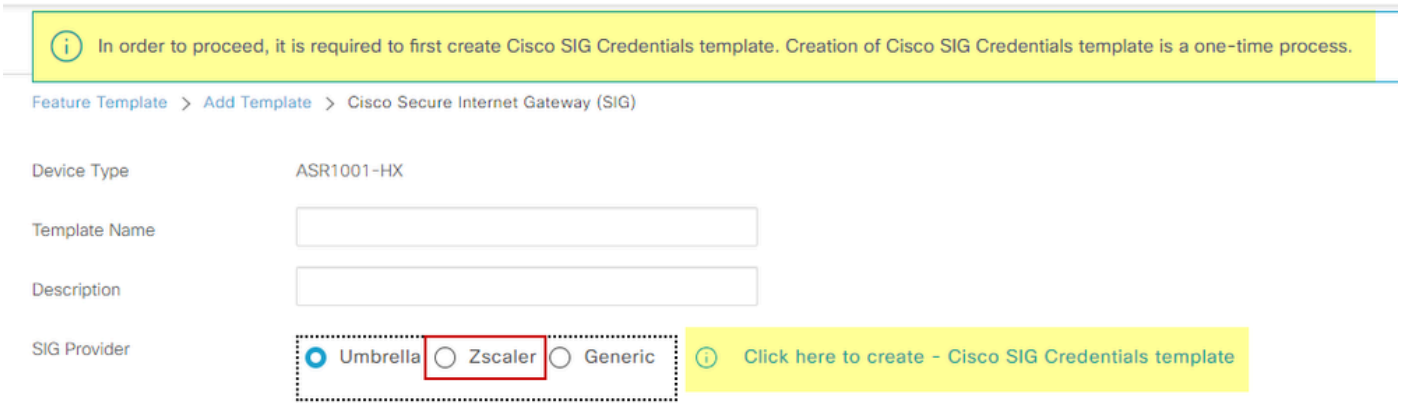
Continúe con la configuración de estas plantillas:

- Plantilla de la función de credenciales de gateway de Internet de seguridad (SIG):
  - Necesita uno para todos los routers periféricos de Cisco. La información para rellenar los campos necesarios de la plantilla debe crearse en el portal de Zscaler.
- Plantilla de la función Security Internet Gateway (SIG):
  - En esta plantilla de función, se configuran los túneles IPsec, se garantiza la alta disponibilidad de implementación (HA) en modo activo/activo o activo/en espera y se selecciona Zscaler Datacenter de forma automática o manual.

Para crear una plantilla de credenciales de Zscaler, navegue hasta Configuration > Template >

Feature Template > Add Template.

Seleccione el modelo de dispositivo que va a utilizar para este fin y busque SIG. Cuando se crea por primera vez, el sistema muestra que las credenciales de Zscaler deben crearse en primer lugar, como en este ejemplo:
Debe seleccionar Zscaler como proveedor SIG y hacer clic en la plantilla Click here to create - Cisco SIG Credentials.



Plantilla de credenciales de firma

"

Se le redirigirá a la plantilla de credenciales. En esta plantilla, debe introducir los valores de todos los campos:

- Nombre de plantilla
- Descripción
- Proveedor SIG (seleccionado automáticamente del paso anterior)
- Organización
- URI base del partner
- Nombre de usuario
- Contraseña
- Clave de API del partner

Click Save.

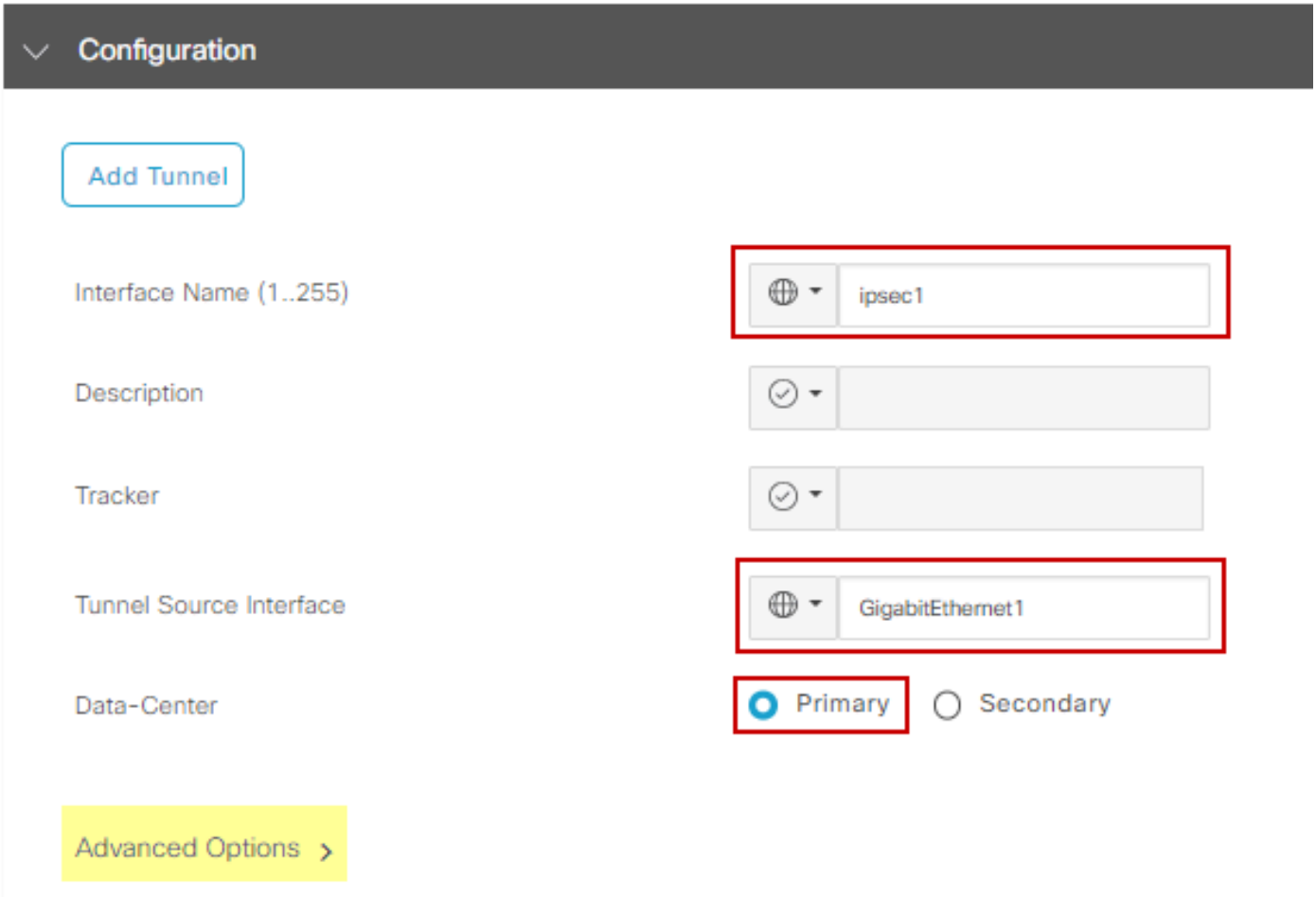
Se le redirigirá a la plantilla Secure Internet Gateway (SIG). Esta plantilla le permite configurar todo lo necesario para SD-WAN IPsec SIG con Zscaler.

En la primera sección de la plantilla, proporcione un nombre y una descripción. El rastreador predeterminado se habilita automáticamente. La URL de la API utilizada para la comprobación de estado de Zscaler Layer 7 es: zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest.

En Cisco IOS XE, debe establecer una dirección IP para el rastreador. Cualquier IP privada dentro del rango /32 es aceptable. La dirección IP que configure puede ser utilizada por la interfaz Loopback 6530, que se crea automáticamente para realizar inspecciones de estado de Zscaler.

En la sección Configuración, puede crear los túneles IPsec haciendo clic en Agregar túnel. En la nueva ventana emergente, seleccione las opciones que desee en función de sus requisitos.

En este ejemplo, se ha creado la interfaz IPsec1, que utiliza la interfaz WAN GigabitEthernet1 como origen del túnel. A continuación, puede formar conectividad con el Data Center principal de Zcaler.
Se recomienda mantener los valores de Opciones avanzadas como valores predeterminados.

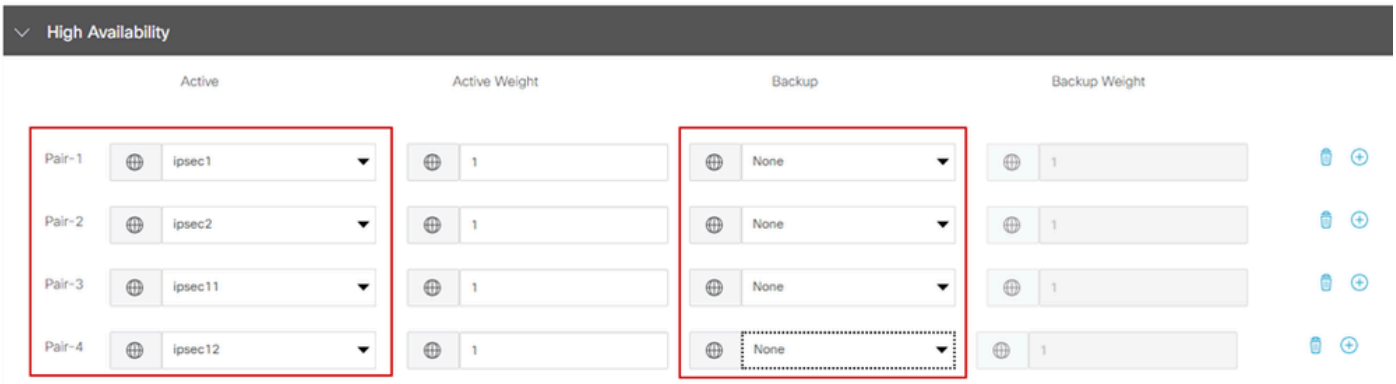


Configuración de interfaz IPsec

Alta disponibilidad

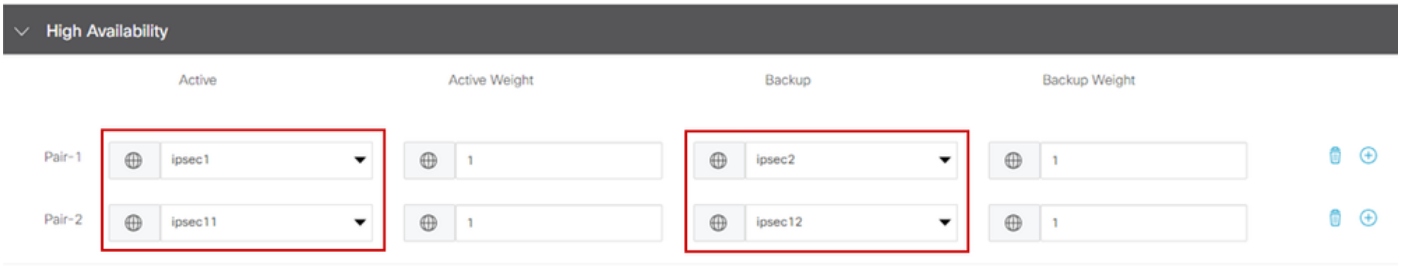
En esta sección, usted elige si el diseño va a ser Activo/Activo o Activo/En espera, y determina qué interfaz IPSec va a estar activa.

Este es un ejemplo de un diseño Activo/Activo. Todas las interfaces se seleccionan en Activo, dejando Copia de seguridad sin ninguna.



Diseño activo/activo

En este ejemplo se muestra un diseño Activo/En espera. IPsec1 e IPsec1 se seleccionan para ser interfaces activas, mientras que IPsec2 e IPsec12 se designan como interfaces en espera.



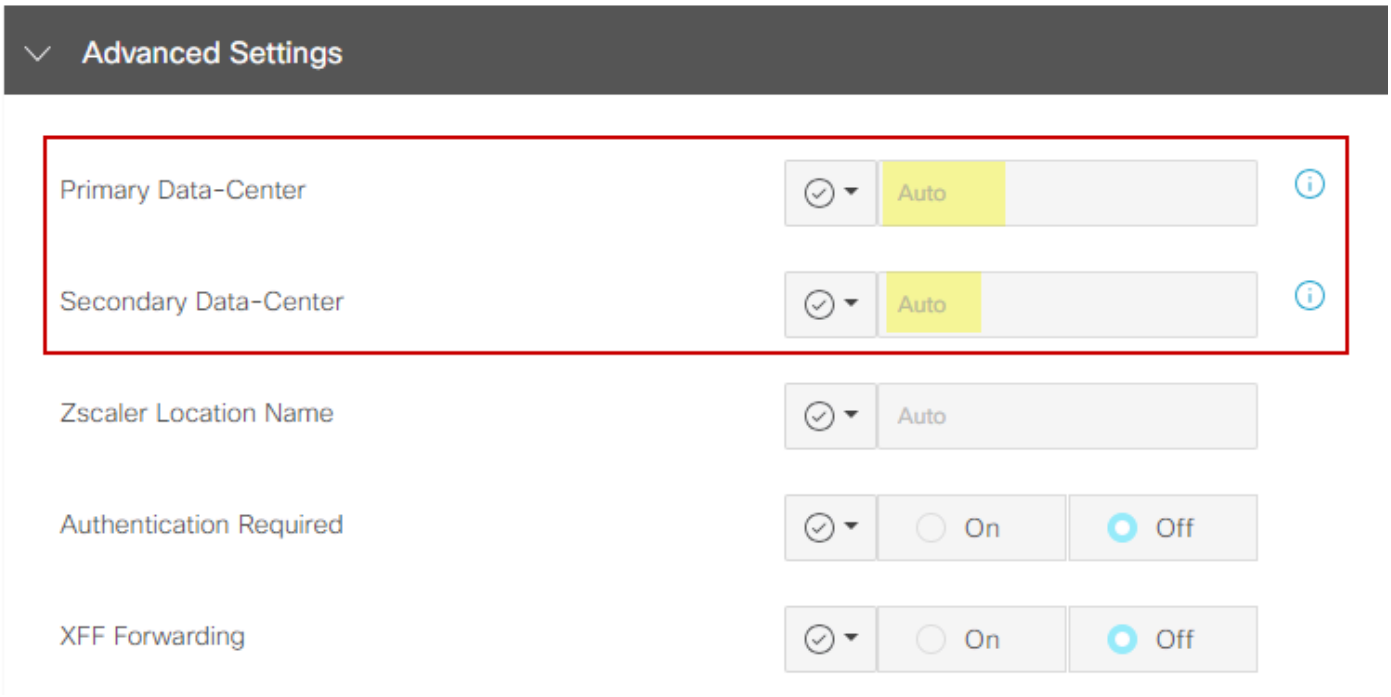
Diseño activo/en espera

Configuración avanzada

En esta sección, las configuraciones más importantes son el Data Center principal y el Data Center secundario.

Se recomienda configurar ambos como automáticos o manuales, pero no se recomienda configurarlos como mixtos.

Si decide configurarlos manualmente, seleccione la URL correcta del portal Zscaler, en función de su URI de base de partners



Data Centers automáticos o manuales

Haga clic en Guardar cuando haya terminado.

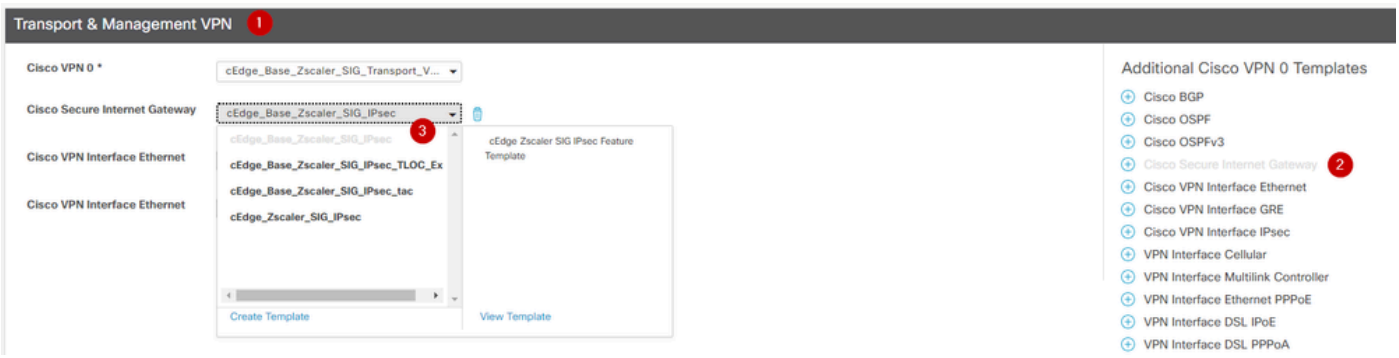
Una vez que haya terminado con la configuración de las plantillas SIG, debe aplicarlas en la plantilla del dispositivo. De esta manera, la configuración se envía a los routers periféricos de Cisco.

Para completar estos pasos, navegue hasta Configuration > Templates > Device Template, en tres puntos haga clic en Edit.

1. En VPN de transporte y administración

2. Agregue la plantilla Gateway de Internet segura.

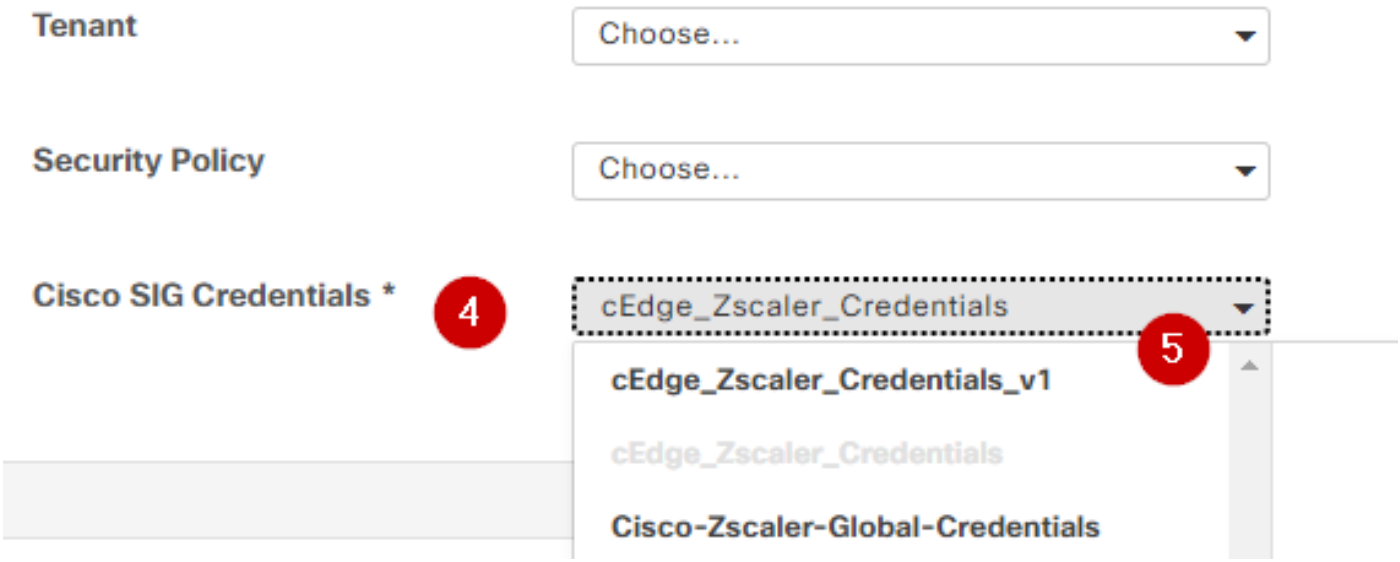
3. En Cisco Secure Internet Gateway, seleccione la plantilla de función SIG correcta en el menú desplegable.



Agregar plantilla SIG en plantilla de dispositivo

En Plantillas adicionales

4. En Credenciales de Cisco SIG
5. Seleccione la plantilla de credenciales de Cisco SIG correcta en el menú desplegable:



Plantilla SIG de credenciales

Haga clic en Update; por favor, tenga en cuenta que si su plantilla de dispositivo es una plantilla activa, utilice los pasos estándar para insertar configuraciones en una plantilla activa.

Verificación

La verificación se puede hacer durante la previsualización de la configuración mientras usted está empujando los cambios, lo que debe notar son:

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

En este ejemplo puede ver que el diseño está activo/en espera

<#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
```

Verá que se agregan más configuraciones como perfiles y políticas crypto ikev2, interfaz múltiple que comienza con Tunnel1xxxxx, definición vrf 65530, ip sdwan route vrf 1 0.0.0.0/0 service sig.

Todos estos cambios son parte de los túneles IPsec SIG con Zscaler.

Este ejemplo muestra el aspecto de la configuración de la interfaz de túnel:

```
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
```

Una vez que las configuraciones se hayan insertado correctamente en los routers periféricos de Cisco, puede utilizar comandos para verificar si los túneles se están activando o no.

<#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
```

Si no ve http resp code 200, significa que se enfrenta a un problema relacionado con la contraseña o la clave de partner.

Para verificar el estado de las interfaces, utilice el comando.

<#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
```

Para verificar el estado del rastreador, ejecute los comandos show endpoint-tracker y show endpoint-tracker records. Esto le ayuda a confirmar la URL que está utilizando el rastreador

```
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
```

Otras validaciones que puede realizar son:
Para asegurarse de que las rutas en VRF apunten a túneles IPsec, ejecute este comando:

show ip route vrf 1

El gateway de último recurso es 0.0.0.0 a la red 0.0.0.0

S* 0.0.0.0/0 [2/65535], Túnel100002
[2/65535], túnel100001
10.0.0.0/8 está dividido en subredes de forma variable, 4 subredes, 2 máscaras

Para validarlo aún más, puede hacer ping hacia Internet y hacer una ruta de seguimiento para verificar los saltos que está tomando el tráfico:

<#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>

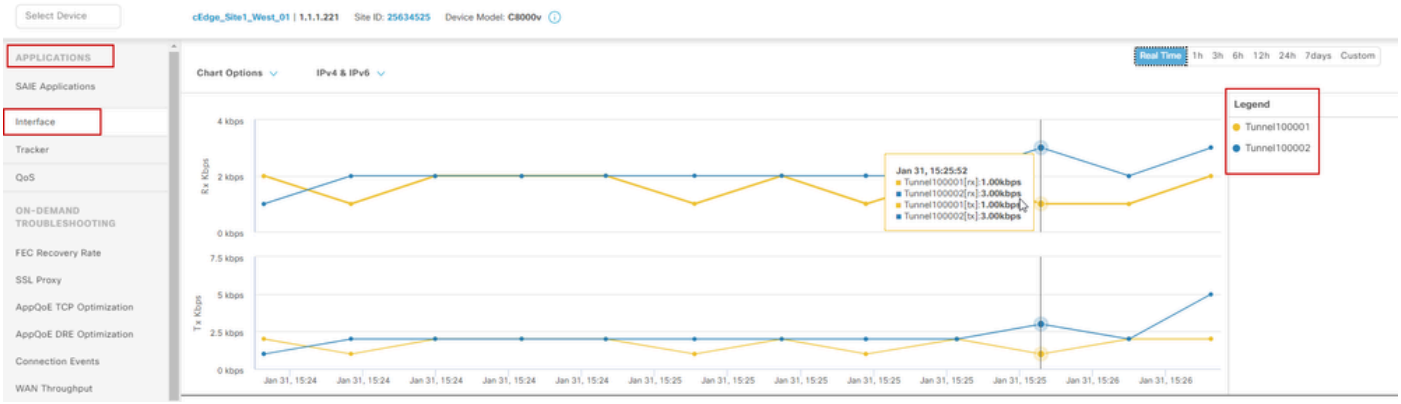
```
 200 msec
```

<The IP here need to be Zcaler IP>

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

Puede validar las interfaces IPsec desde la GUI de vManage en Monitor > Device o Monitor > Network (para los códigos 20.6 y anteriores).

- Seleccione el router y navegue Aplicaciones > Interfaces.
- Seleccione Tunnel10001 y Tunnel100002 para ver el tráfico en tiempo real o personalícelo por intervalo de tiempo requerido:



Supervisión de túneles IPsec

Troubleshoot

Si el túnel SIG no se está ejecutando, estos son los pocos pasos para resolver el problema.

Paso 1: Verifique los errores utilizando el comando show sdwan secure-internet-gateway zscaler tunnels. En el resultado, si observa HTTP RESP Code 401, indica que hay un problema con la autenticación.

Puede comprobar los valores de la plantilla de credenciales de SIG para ver si la contraseña, o clave de partner, es correcta.

```
<#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 F

LAST HTTP REQ
```

CODE

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

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

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

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

Para una depuración adicional, habilite estos comandos y busque mensajes de registro relacionados con SIG, HTTP o tracker:

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

Este es un ejemplo del resultado de los comandos debug:

<#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
```

Ejecute el comando show ip interface brief y verifique el protocolo de interfaz de túneles Protocol

si se muestran arriba o abajo.

<#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

Después de confirmar que no hay problemas con las credenciales de Zscaler, puede quitar la interfaz SIG de la plantilla del dispositivo y enviarla al router.

Una vez completada la inserción, aplique la plantilla SIG y vuelva a insertarla en el router. Este método obliga a que los túneles se vuelvan a crear desde el principio.

Información Relacionada

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).