Configurar e verificar o túnel SD-WAN IPsec SIG com Zscaler

Contents

Introdução

Este documento descreve as etapas de configuração e verificação de túneis SIG IPsec SD-WAN com Zscaler.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Security Internet Gateway (SIG) (Gateway de Internet de Segurança).
- Como os túneis IPsec funcionam, Fase1 e Fase2 no Cisco IOS®.

Requisitos adicionais

- O NAT precisa ser habilitado na interface de transporte que será voltada para a Internet.
- Um servidor DNS precisa ser criado na VPN 0 e a URL base Zscaler precisa ser resolvida com esse servidor DNS. Isso é importante porque, se isso não resolver, as chamadas de API falharão. As verificações de integridade da camada 7 também falharão, pois, por padrão, a URL é: http://gateway.<zscalercloud>.net/vpntest.

- O NTP (Network Time Protocol) deve garantir que o tempo do Cisco Edge Router seja preciso e que as chamadas à API não falhem.
- Uma rota de serviço que aponta para o SIG precisa ser configurada no Service-VPN Feature Template ou CLI:
  ip sdwan route vrf 1 0.0.0.0/0 service sig

Componentes Utilizados

Este documento é baseado nestas versões de software e hardware:

- Cisco Edge Router versão 17.6.6a
- vManage versão 20.9.4

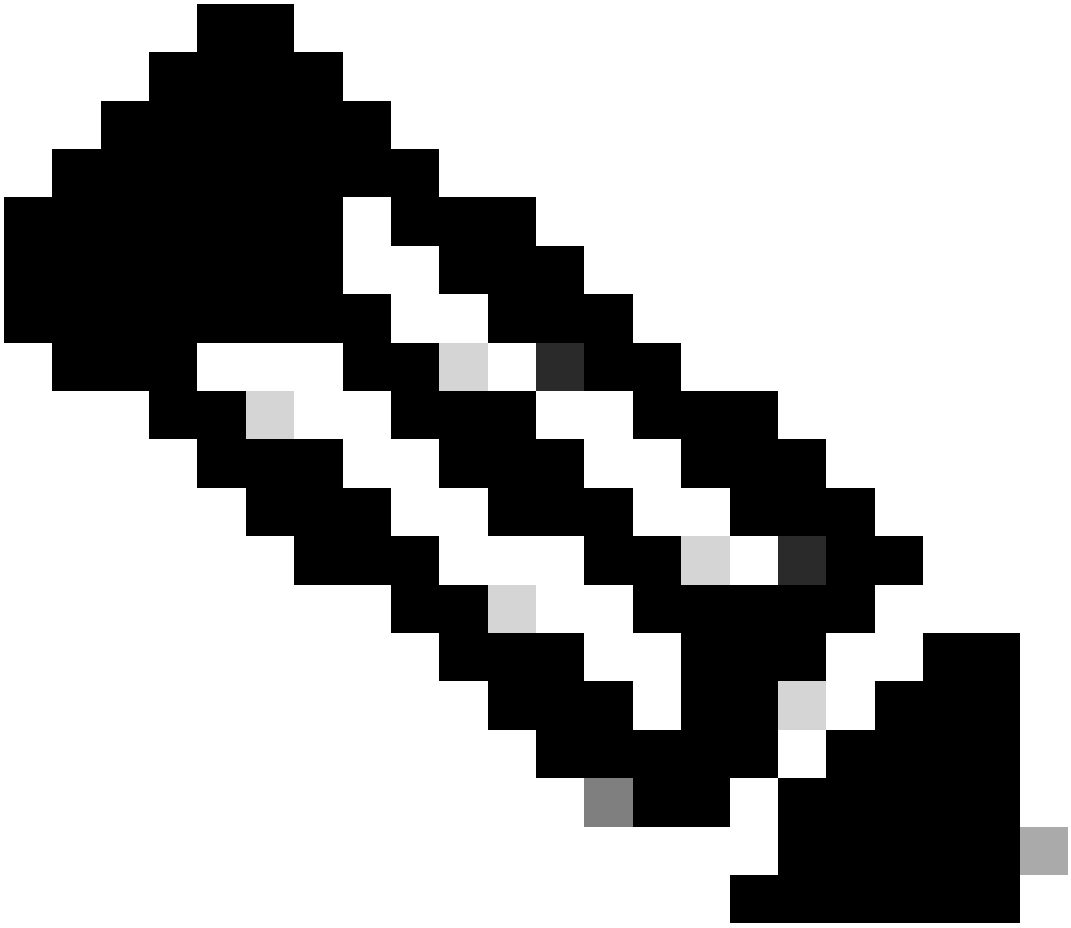
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Opções de projeto de rede

Aqui estão os vários tipos de implantações em uma configuração de combinação ativa/standby. O encapsulamento de túnel pode ser implantado em GRE ou IPsec.

- Um par de túneis ativo/em espera.
- Um par de túneis ativo/ativo.
- Par de túneis ativo/em espera múltiplo.
- Par de túneis ativo/ativo múltiplo.



Observação: nos Cisco Edge Routers SD-WAN, você pode utilizar uma ou mais interfaces de transporte conectadas à Internet para que essas configurações funcionem de forma eficaz.

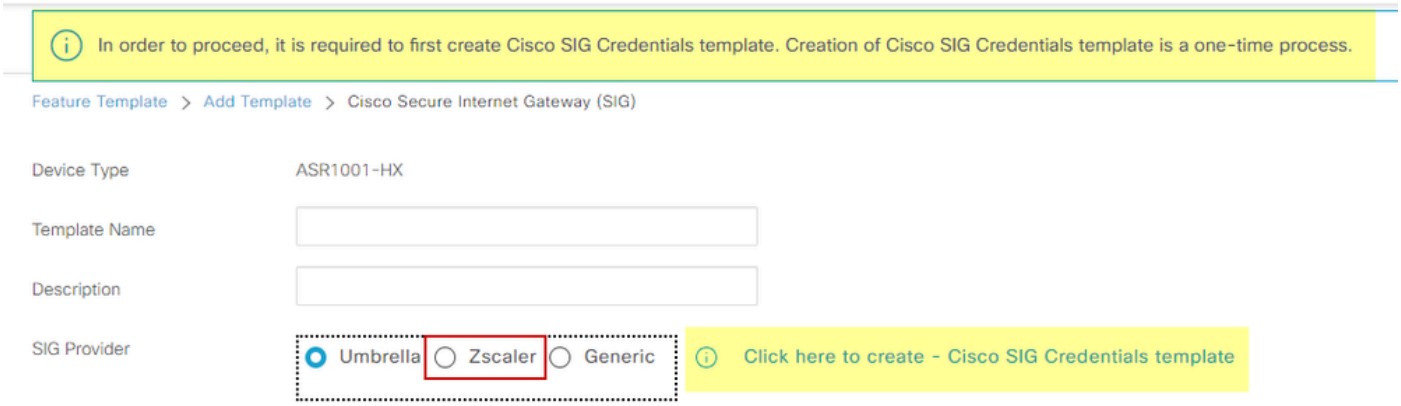
Configurações

Continue com a configuração destes modelos:

- Modelo de recurso de credencial SIG (Security Internet Gateway):
  - Você precisa de um para todos os Cisco Edge Routers. As informações para preencher os campos necessários do modelo precisam ser criadas no portal Zscaler.
- Modelo do recurso Security Internet Gateway (SIG):
  - Neste modelo de recurso, você configura túneis IPsec, garante a implantação de alta disponibilidade (HA) no modo ativo/ativo ou ativo/standby e seleciona o Zscaler Datacenter automaticamente ou manualmente.

Para criar um modelo de Credenciais do Zscaler, navegue para Configuration > Template > Feature Template > Add Template.

Selecione o modelo de dispositivo que você usará para essa finalidade e procure SIG. Quando você o cria pela primeira vez, o sistema mostra que as Credenciais do Zscaler precisam ser criadas primeiro, como neste exemplo:
Você precisa selecionar Zscaler como um provedor SIG e clicar no modelo Clique aqui para criar - Credenciais Cisco SIG.



Modelo de credencial de assinatura

"

Você é redirecionado para o modelo Credenciais. Neste modelo, você deve inserir os valores para todos os campos:

- Nome do modelo
- Descrição
- Provedor SIG (selecionado automaticamente na etapa anterior)
- Organização
- URI da Base de Parceiros
- Nome de usuário
- Senha
- Chave API do parceiro

Click Save.

Você é redirecionado para o modelo Secure Internet Gateway (SIG). Este modelo permite que você configure tudo o que for necessário para SIG IPsec SD-WAN com Zscaler.

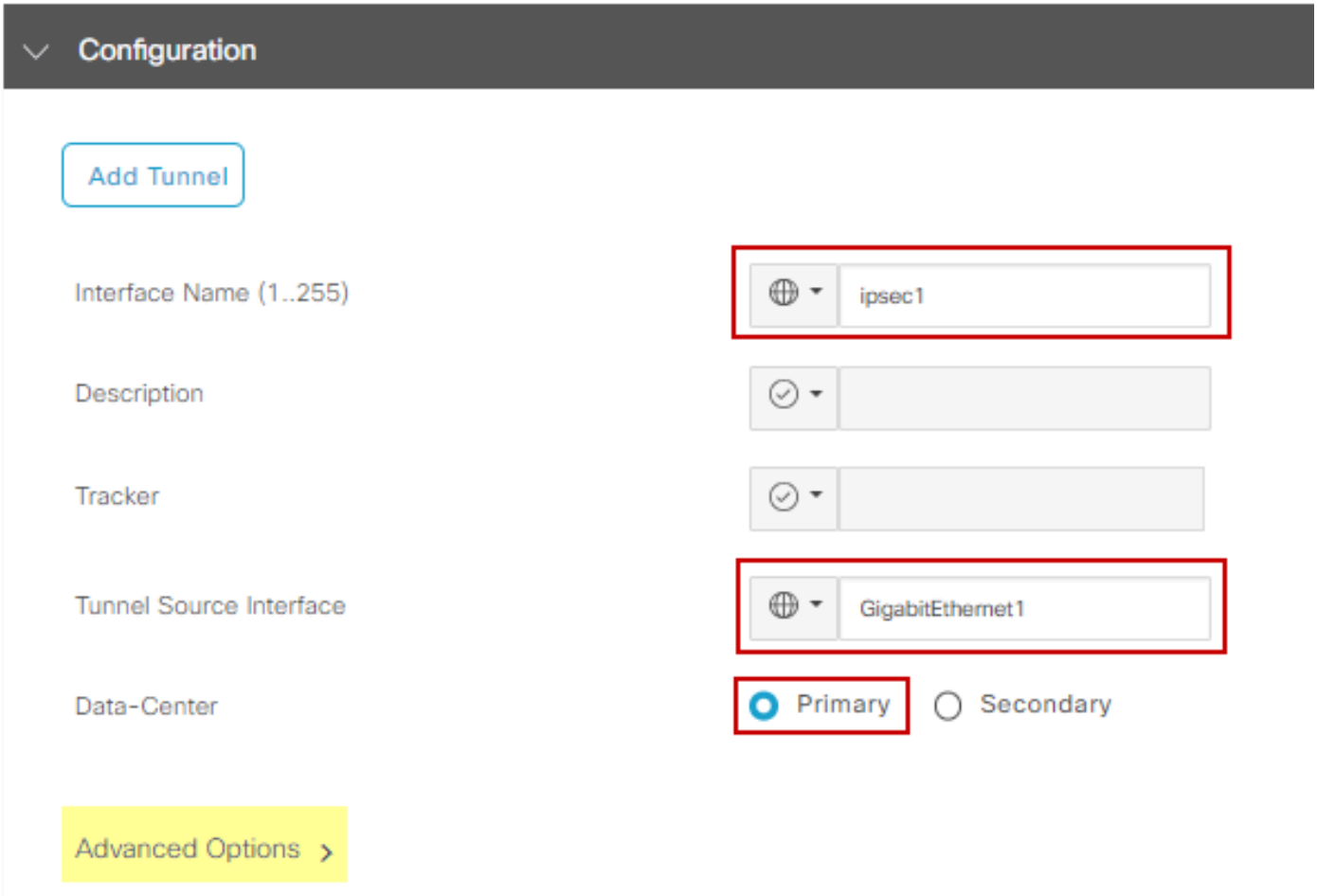
Na primeira seção do modelo, forneça um nome e uma descrição. O rastreador padrão é ativado automaticamente. A URL da API usada para a verificação de integridade da camada 7 do Zscaler é: zscaler_L7_health_check) ishttp://gateway<zscalercloud>net/vpntest.

No Cisco IOS XE, você precisa definir um endereço IP para o rastreador. Qualquer IP privado dentro do intervalo /32 é aceitável. O endereço IP definido pode ser utilizado pela interface Loopback 6530, que é criada automaticamente para executar inspeções de integridade do

Zscaler.

Na seção Configuration (Configuração), você pode criar os túneis IPsec clicando em Add Tunnel. Na nova janela pop-up, faça seleções com base em seus requisitos.

Neste exemplo, a interface IPsec1 foi criada, usando a interface WAN GigabitEthernet1 como origem do túnel. Em seguida, ele pode formar conectividade com o data center principal Zcaler. É recomendável manter os valores de Opções avançadas como padrão.

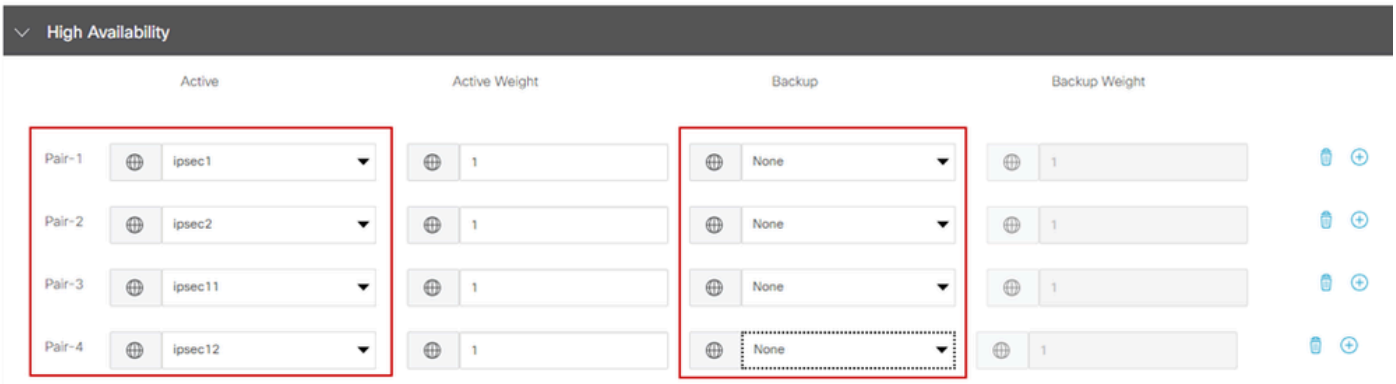


Configuração de interface IPsec

Alta Disponibilidade

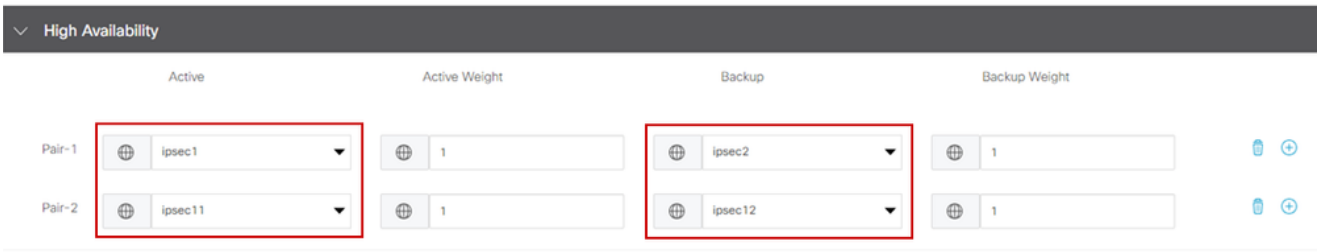
Nesta seção, você escolhe se o design será Ativo/Ativo ou Ativo/Em espera e determina qual interface IPsec será ativa.

Este é um exemplo de um design Ativo/Ativo. Todas as interfaces são selecionadas em Ative, deixando Backup com none.



Design ativo/ativo

Este exemplo mostra um design Ativo/Em espera. IPsec1 e IPsec11 são selecionados para serem interfaces ativas, enquanto IPsec2 e IPsec12 são designados como interfaces em espera.



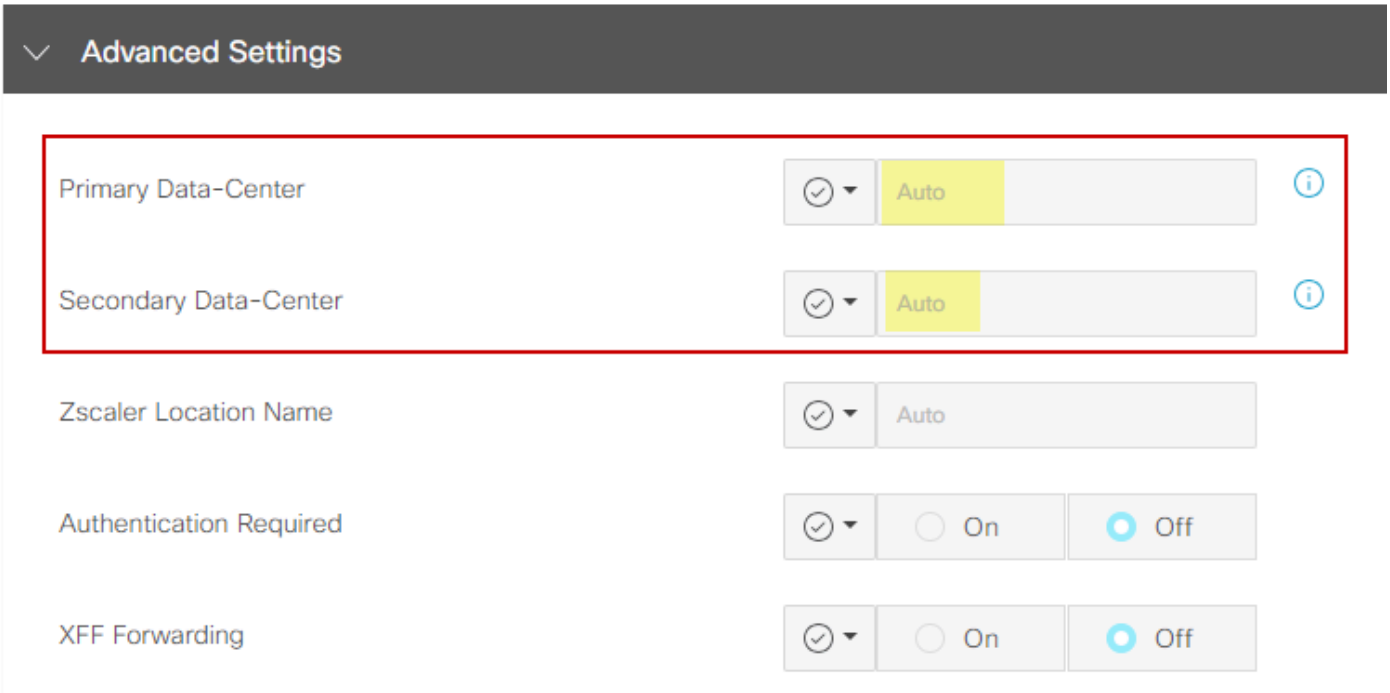
Design ativo/em espera

Configurações avançadas

Nesta seção, as configurações mais importantes são o data center principal e o data center secundário.

É recomendável configurar ambos como automáticos ou manuais, mas não é recomendável configurá-los como mistos.

Se você optar por configurá-los manualmente, selecione o URL correto no portal Zscaler, com base no URI da base de parceiros



Data centers automáticos ou manuais

Clique em Salvar quando terminar.

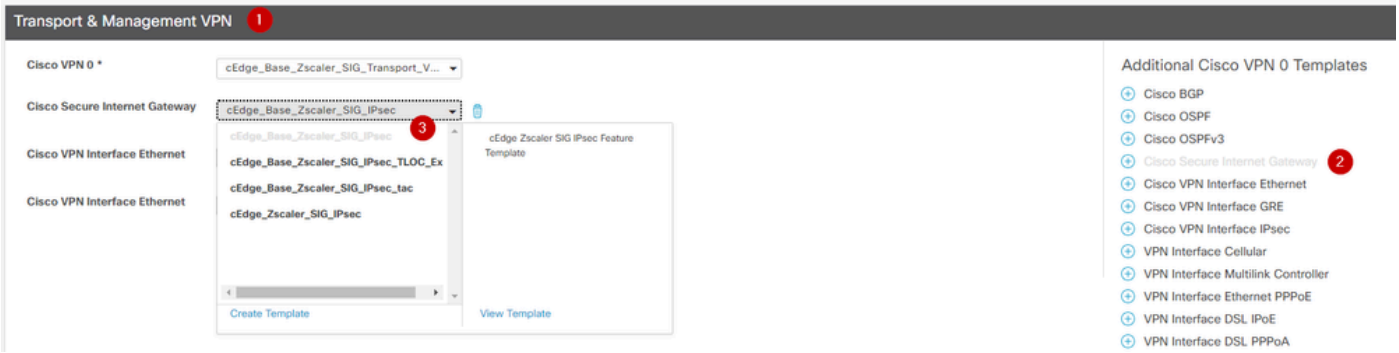
Depois de concluir a configuração dos modelos SIG, você deve aplicá-los no modelo do dispositivo. Dessa forma, a configuração é inserida nos Cisco Edge Routers.

Para concluir essas etapas, navegue até Configuration > Templates > Device Template, em três pontos, clique em Edit.

1. Em VPN de Transporte e Gerenciamento

2. Adicione o modelo Secure Internet Gateway.

3. No Cisco Secure Internet Gateway selecione o modelo de recurso SIG correto no menu suspenso.

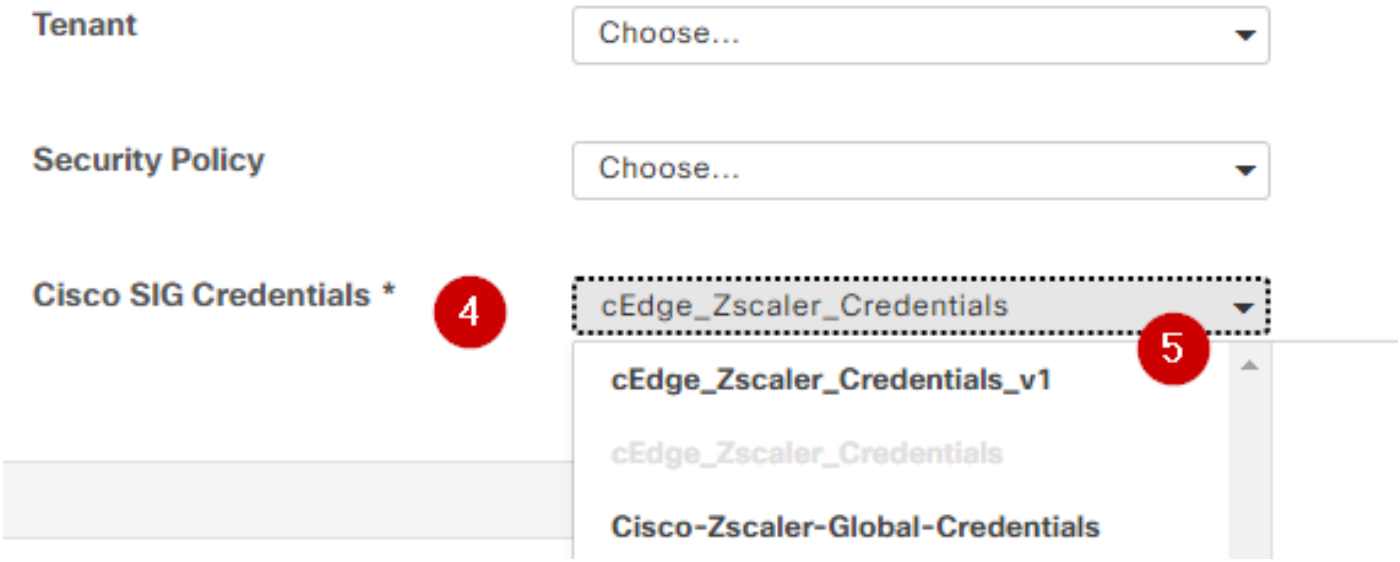


Adicionar modelo SIG ao modelo do dispositivo

Em Modelos Adicionais

4. Em Credenciais Cisco SIG

5. Selecione o modelo correto de Credenciais Cisco SIG no menu suspenso:



Modelo SIG de credencial

Clique em Atualizar. Observe que se o modelo do seu dispositivo for um modelo ativo, use as etapas padrão para enviar configurações em um modelo ativo.

Verificar

A verificação pode ser feita durante a visualização da configuração enquanto você estiver enviando as alterações, o que você deve observar é:

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

Neste exemplo, você pode ver que o design está ativo/em 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
```

Você observará que mais configurações são adicionadas, como os perfis e políticas de criptografia ikev2, várias interfaces iniciando com Tunnel1xxxxx, 65530 de definição vrf, ip sdwan route vrf 1 0.0.0.0/0 service sig.

Todas essas alterações fazem parte dos túneis IPsec SIG com Zscaler.

Este exemplo mostra como é a configuração da interface Tunnel:

```
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
```

Depois que as configurações forem enviadas com êxito para os Cisco Edge Routers, você poderá usar comandos para verificar se os túneis estão sendo ativados ou não.

<#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
```

Se você não vir o http resp code 200, isso significa que você está enfrentando um problema relacionado à senha ou à chave do parceiro.

Para verificar o status das interfaces, use o 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 o status do rastreador, execute os comandos show endpoint-tracker e show endpoint-tracker records. Isso ajuda a confirmar o URL que o rastreador está utilizando

```
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
```

Outras validações que você pode fazer são:
Para garantir que as rotas no VRF estejam apontando para túneis IPsec, execute este comando:

show ip route vrf 1

O gateway de último recurso é 0.0.0.0 para a rede 0.0.0.0

S* 0.0.0.0/0 [2/65535], Túnel100002
[2/65535], túnel100001
10.0.0.0/8 tem sub-redes variáveis, 4 sub-redes, 2 máscaras

Para validar ainda mais, você pode fazer ping em direção à Internet e fazer uma rota de rastreamento para verificar os saltos que o tráfego está fazendo:

<#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>

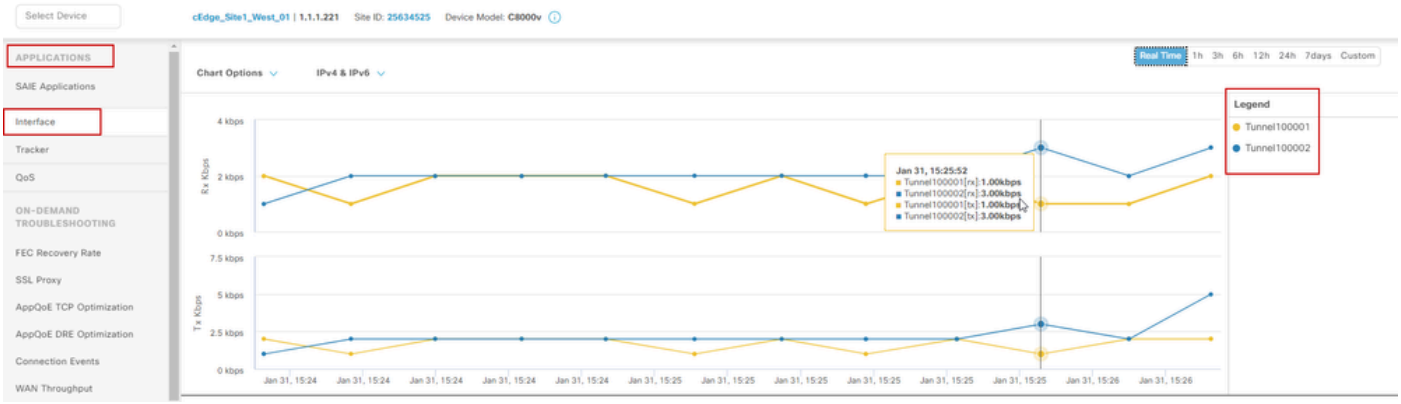
```
 200 msec
```

<The IP here need to be Zcaler IP>

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

Você pode validar interfaces IPsec da GUI do vManage navegando em Monitor > Device ou Monitor > Network (para códigos 20.6 e anteriores).

- Selecione o roteador e navegue Applications > Interfaces.
- Selecione Tunnel100001 e Tunnel100002 para ver o tráfego em tempo real ou personalizar de acordo com o intervalo de tempo necessário:



Monitorando túneis IPsec

Troubleshooting

Se o túnel SIG não estiver em execução, estas são as etapas para solucionar o problema.

Etapa 1: verifique os erros usando o comando show sdwan secure-internet-gateway zscaler tunnels. Na saída, se você observar o HTTP RESP Code 401, indica que há um problema com a autenticação.

Você pode verificar os valores no modelo de Credenciais SIG para ver se a senha, ou a Chave do parceiro, está correta.

```
<#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 depuração adicional, ative esses comandos e procure mensagens de log relacionadas a SIG, HTTP ou rastreador:

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

Este é um exemplo de saída dos 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
```

Execute o comando show ip interface brief e verifique o protocolo da interface de túneis se houver

exibição para cima ou para baixo.

<#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

Depois de confirmar que não há problemas com as credenciais do Zscaler, você pode remover a interface SIG do modelo do dispositivo e enviá-la ao roteador.

Quando o envio estiver concluído, aplique o modelo SIG e envie-o de volta ao roteador. Este método força os túneis a serem recriados do zero.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.