Configurar o túnel IPSec do lado do serviço com um C8000V em SD-WAN

Contents

Introdução

Este documento descreve como configurar um túnel IPSec entre um Roteador Cisco Edge SD-WAN e um Endpoint VPN com VRF de serviço.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN)
- Segurança de Protocolo Internet (IPSec - Internet Protocol Security)

Componentes

Este documento é baseado nestas versões de software e hardware:

- Cisco Edge Router versão 17.6.1
- SD-WAN vManage 20.9.3.2

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

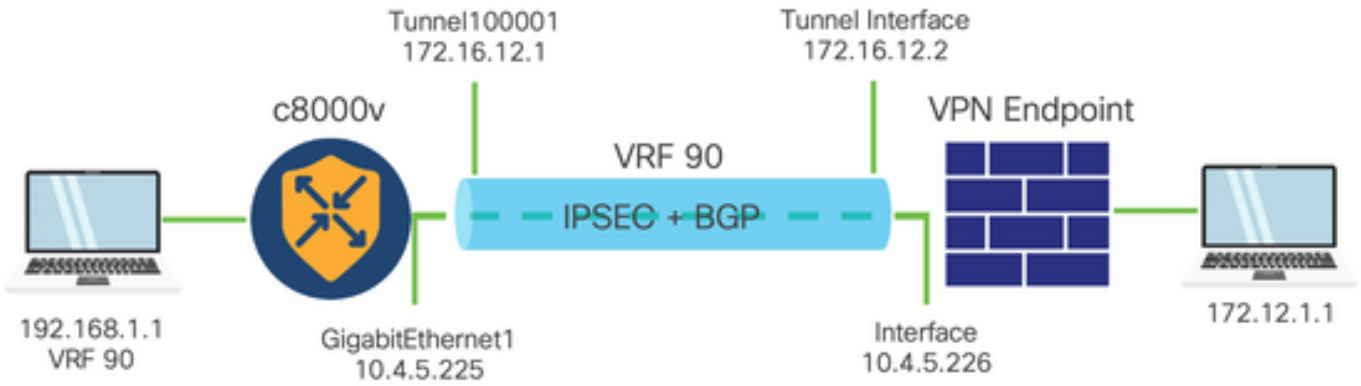
potencial de qualquer comando.

Informações de Apoio

Informações de apoio incluem o escopo deste documento, a usabilidade e os benefícios de construir um túnel IPSec do lado do serviço com um C8000v em SD-WAN.

- Para criar um túnel IPSec em um serviço Virtual Routing and Forwarding (VRF) entre um roteador Cisco IOS® XE no modo de gerenciamento de controlador e um ponto de extremidade de Rede Virtual Privada (VPN - Virtual Private Network) garante a confidencialidade e a integridade dos dados na Rede de Longa Distância (WAN - Wide Area Network) pública. Ele também facilita a extensão segura das redes privadas das empresas e permite conexões remotas pela Internet, mantendo um alto nível de segurança.
- O serviço VRF isola o tráfego, que é particularmente valioso em ambientes de vários clientes ou para manter a segmentação entre diferentes partes da rede. Em resumo, essa configuração melhora a segurança e a conectividade.
- Este documento considera que o Border Gateway Protocol (BGP) é o protocolo de roteamento usado para comunicar as redes do serviço SD-WAN VRF para a rede atrás do ponto final VPN e vice-versa.
- A configuração do BGP está fora do escopo deste documento.
- Este ponto final de VPN pode ser um firewall, um roteador ou qualquer tipo de dispositivo de rede que tenha recursos IPSec; a configuração do ponto final de VPN está fora do escopo deste documento.
- Este documento supõe que o Roteador já esteja integrado com conexões de controle ativo e serviço VRF.

Componentes da configuração do IPSEC



Fase 1 Internet Key Exchange (IKE)

A fase 1 do processo de configuração do IPSec envolve a negociação dos parâmetros de segurança e a autenticação entre os pontos finais do túnel. Essas etapas incluem:

Configuração de IKE

- Defina uma proposta de criptografia (algoritmo e comprimento da chave).
- Configure uma política IKE que inclua proposta de criptografia, tempo de vida e autenticação.

Configurar correspondentes finais remotos

- Defina o endereço IP da extremidade remota.
- Configure a chave compartilhada (chave pré-compartilhada) para autenticação.

Configuração da Fase 2 (IPSec)

A fase 2 envolve a negociação das transformações de segurança e das regras de acesso para o fluxo de tráfego pelo túnel. Essas etapas incluem:

Configurar conjuntos de transformação IPSec

- Defina um conjunto de transformações proposto que inclua o algoritmo de criptografia e a autenticação.

Configurar uma política de IPSec

- Associe o conjunto de transformação a uma política IPSec.

Configurar interfaces de túnel

Configure as interfaces de túnel em ambas as extremidades do túnel IPSec.

- Associe as interfaces de túnel às políticas de IPSec.

Configurar

Configuração na CLI

Etapa 1. Defina uma proposta de criptografia.

<#root>

```
cEdge(config)#
crypto ikev2 proposal p1-global

cEdge(config-ikev2-proposal)#
encryption aes-cbc-128 aes-cbc-256

cEdge(config-ikev2-proposal)#
integrity sha1 sha256 sha384 sha512

cEdge(config-ikev2-proposal)#
```

```
group 14 15 16
```

Etapa 2. Configure uma política IKE que inclua informações de proposta.

```
<#root>
cEdge(config)#
crypto ikev2 policy policy1-global

cEdge(config-ikev2-policy)#
proposal p1-global
```

Etapa 3. Defina o endereço IP da extremidade remota.

```
<#root>
cEdge(config)#
crypto ikev2 keyring if-ipsec1-ikev2-keyring

cEdge(config-ikev2-keyring)#
peer if-ipsec1-ikev2-keyring-peer

cEdge(config-ikev2-keyring-peer)#
address 10.4.5.226

cEdge(config-ikev2-keyring-peer)#
pre-shared-key Cisco
```

Etapa 4. Configure a chave compartilhada (chave pré-compartilhada) para autenticação.

```
<#root>
cEdge(config)#
crypto ikev2 profile if-ipsec1-ikev2-profile
```

```
cEdge(config-ikev2-profile)#
match identity remote address
10.4.5.226 255.255.255.0

cEdge(config-ikev2-profile)#
authentication remote

cEdge(config-ikev2-profile)#
authentication remote pre-share

cEdge(config-ikev2-profile)#
authentication local pre-share

cEdge(config-ikev2-profile)#
keyring local if-ipsec1-ikev2-keyring

cEdge(config-ikev2-profile)#
dpd 10 3 on-demand

cEdge(config-ikev2-profile)#
no config-exchange request

cEdge(config-ikev2-profile)#
```

Etapa 5. Defina um conjunto de transformação proposto que inclua o algoritmo de criptografia e a autenticação.

```
<#root>
cEdge(config)#
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256

cEdge(cfg-crypto-trans)#
mode tunnel
```

Etapa 6. Associe o conjunto de transformação a uma política IPSec.

```
<#root>
cEdge(config)#
```

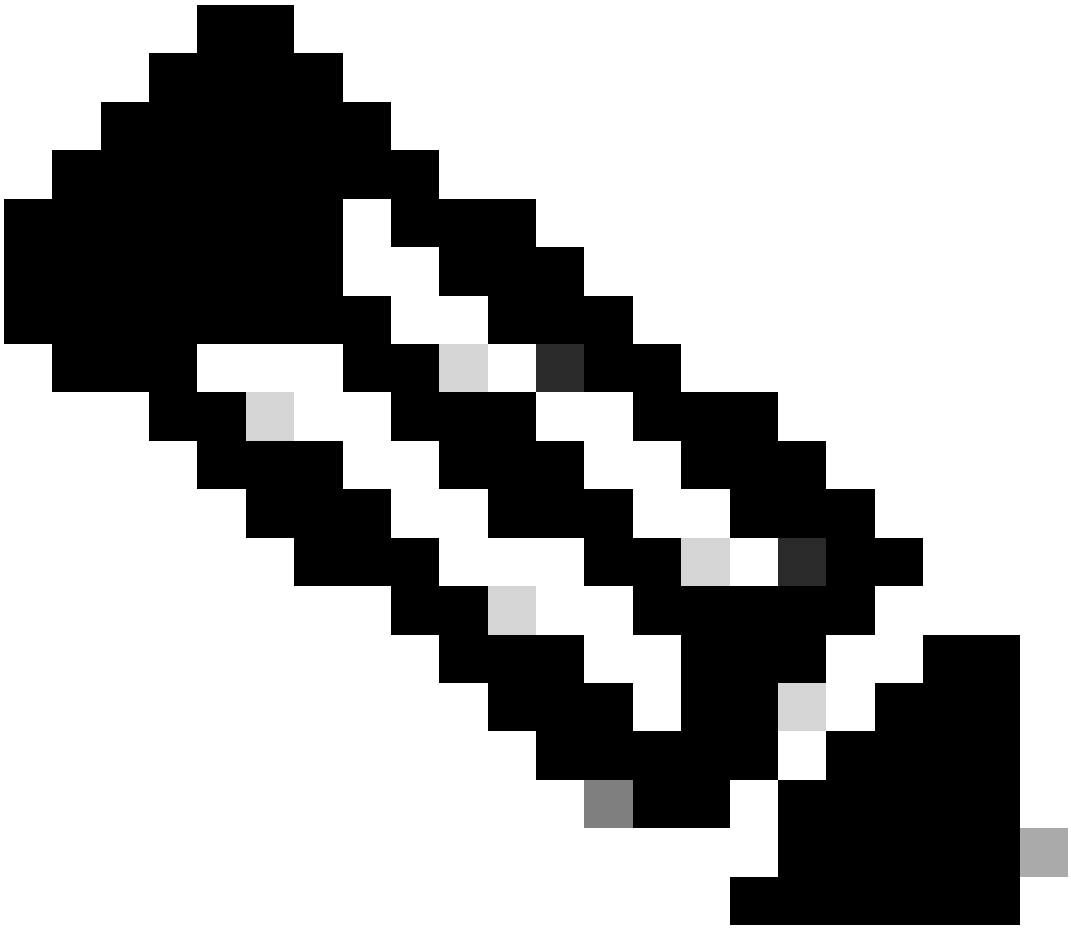
```
crypto ipsec profile if-ipsec1-ipsec-profile

cEdge(ipsec-profile)#
set security-association lifetime kilobytes disable

cEdge(ipsec-profile)#
set security-association replay window-size 512

cEdge(ipsec-profile)#
set transform-set if-ipsec1-ikev2-transform

cEdge(ipsec-profile)#
set ikev2-profile if-ipsec1-ikev2-profile
```

Passo 7. Crie o túnel de interface e associe-o às políticas de IPSec.

```
<#root>
cEdge(config)#
interface Tunnel100001

cEdge(config-if)#
vrf forwarding 90

cEdge(config-if)#
ip address 172.16.12.1 255.255.255.252

cEdge(config-if)#
ip mtu 1500

cEdge(config-if)#
tunnel source GigabitEthernet1

cEdge(config-if)#
tunnel mode ipsec ipv4

cEdge(config-if)#
tunnel destination 10.4.5.226
```

```
cEdge(config-if)#
tunnel path-mtu-discovery

cEdge(config-if)#
tunnel protection ipsec profile if-ipsec1-ipsec-profile
```

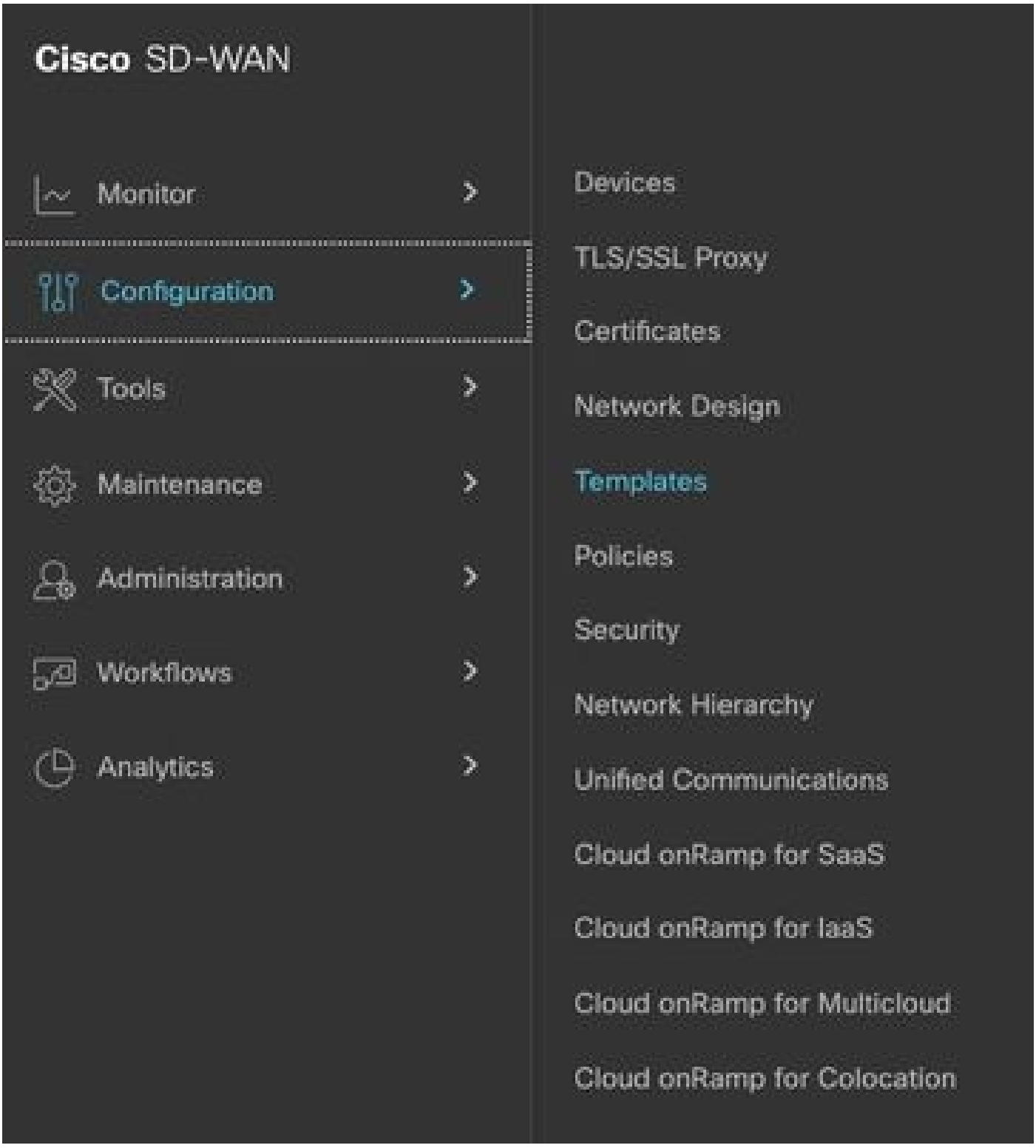
Configuração em um modelo de complemento CLI no vManage



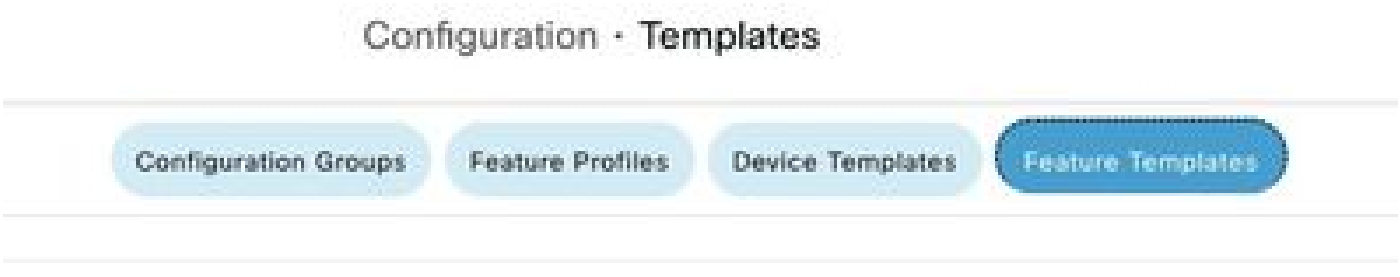
> Observação: esse tipo de configuração só pode ser adicionado por meio do modelo Complemento CLI.

Etapa 1. Navegue até o Cisco vManage e faça login.

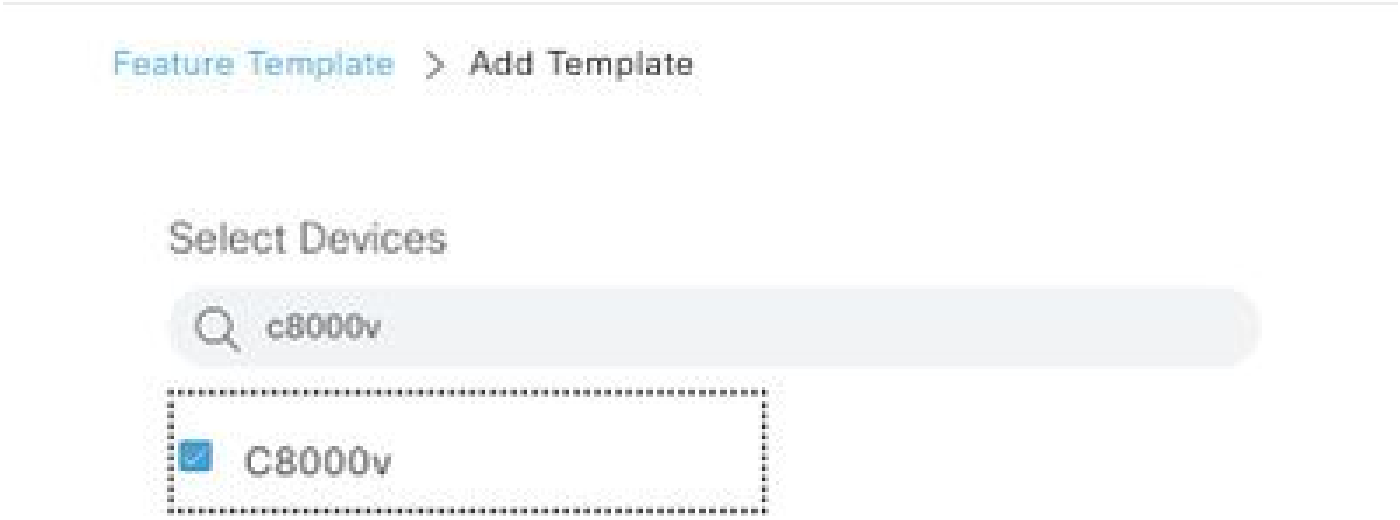
Etapa 2. Navegue até Configuração > Modelos.



Etapa 3. Navegue até Modelos de recurso > Adicionar modelo.

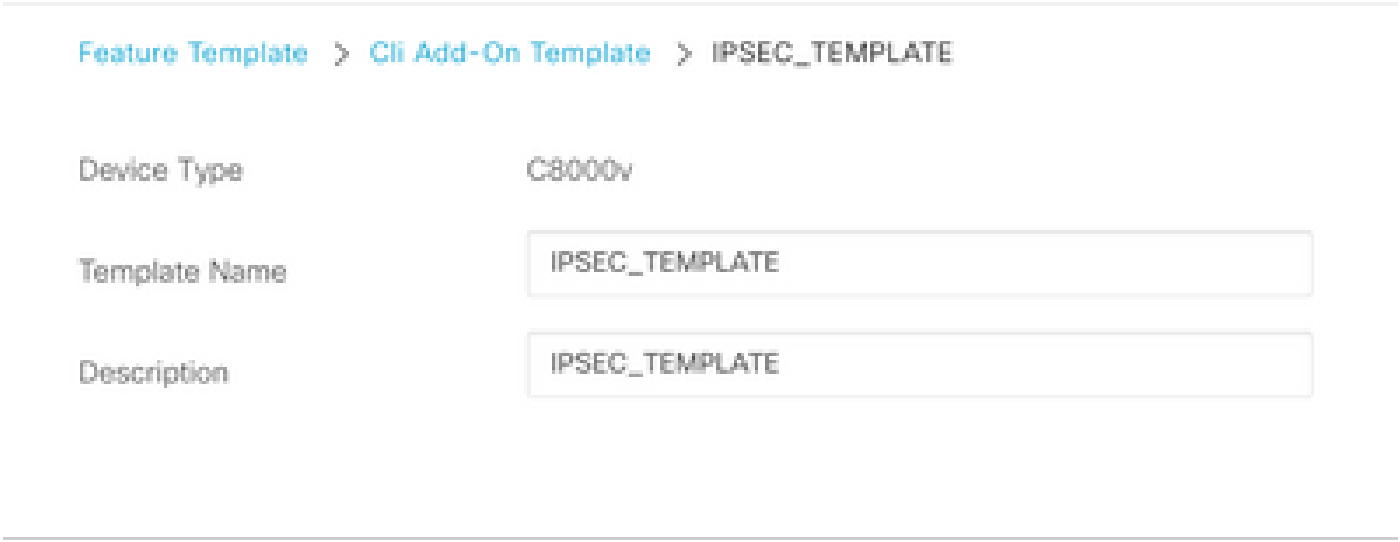


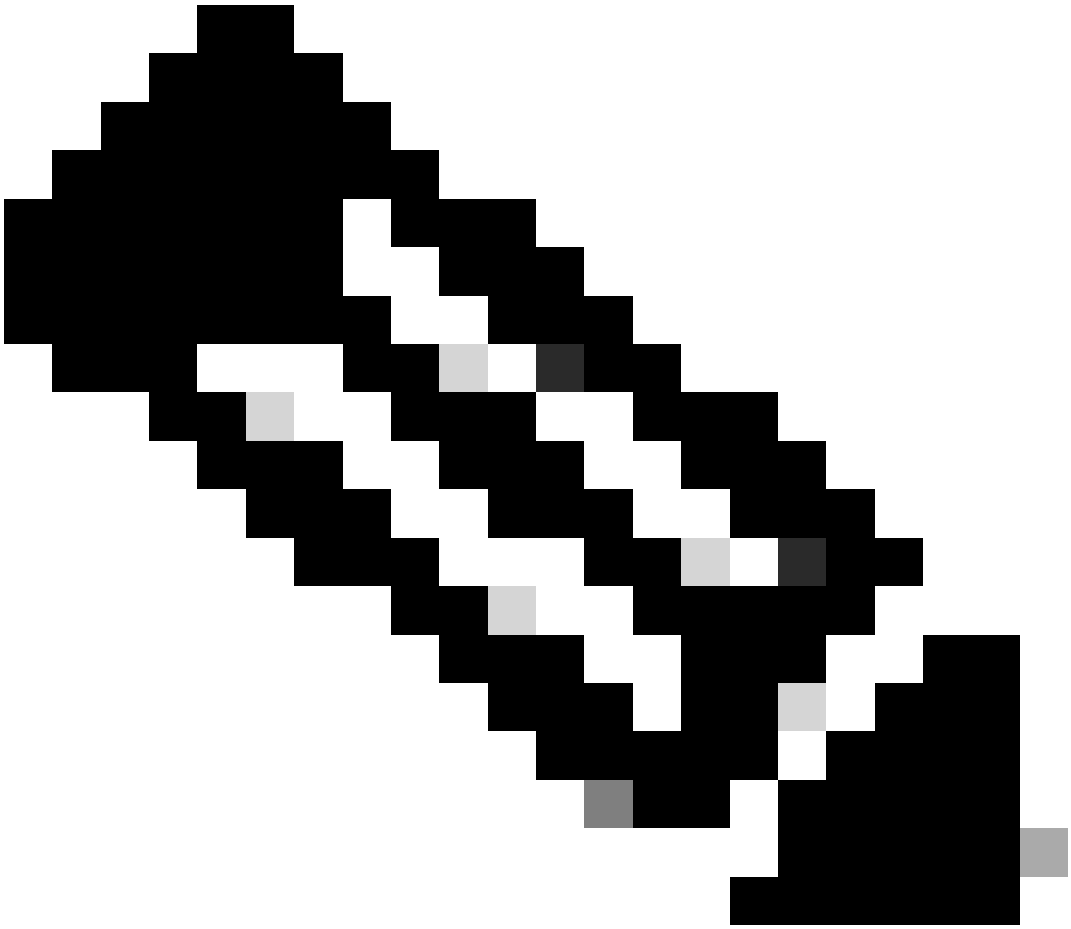
Etapa 4. Filtre o modelo e escolha o roteador c8000v.



Etapa 5. Navegue até Outros modelos e clique em Modelo de complemento Cli.

Etapa 6. Adicione um Nome do modelo e uma Descrição.





Observação: para obter mais informações sobre como criar variáveis em um modelo de complemento CLI, consulte Modelos de recurso de complemento CLI.

Passo 7. Adicione os comandos.

CLI CONFIGURATION

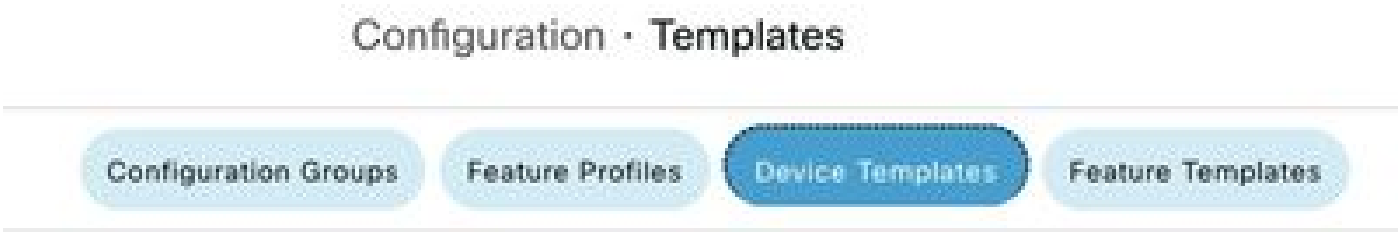
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key Cisco
 !
!
!
crypto ikev2 profile if-ipsec1-ikev2-profile
 match identity remote address 10.4.5.226 255.255.255.0
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
 set transform-set if-ipsec1-ikev2-transform
 set ikev2-profile if-ipsec1-ikev2-profile
!
!
!
```

CLI CONFIGURATION

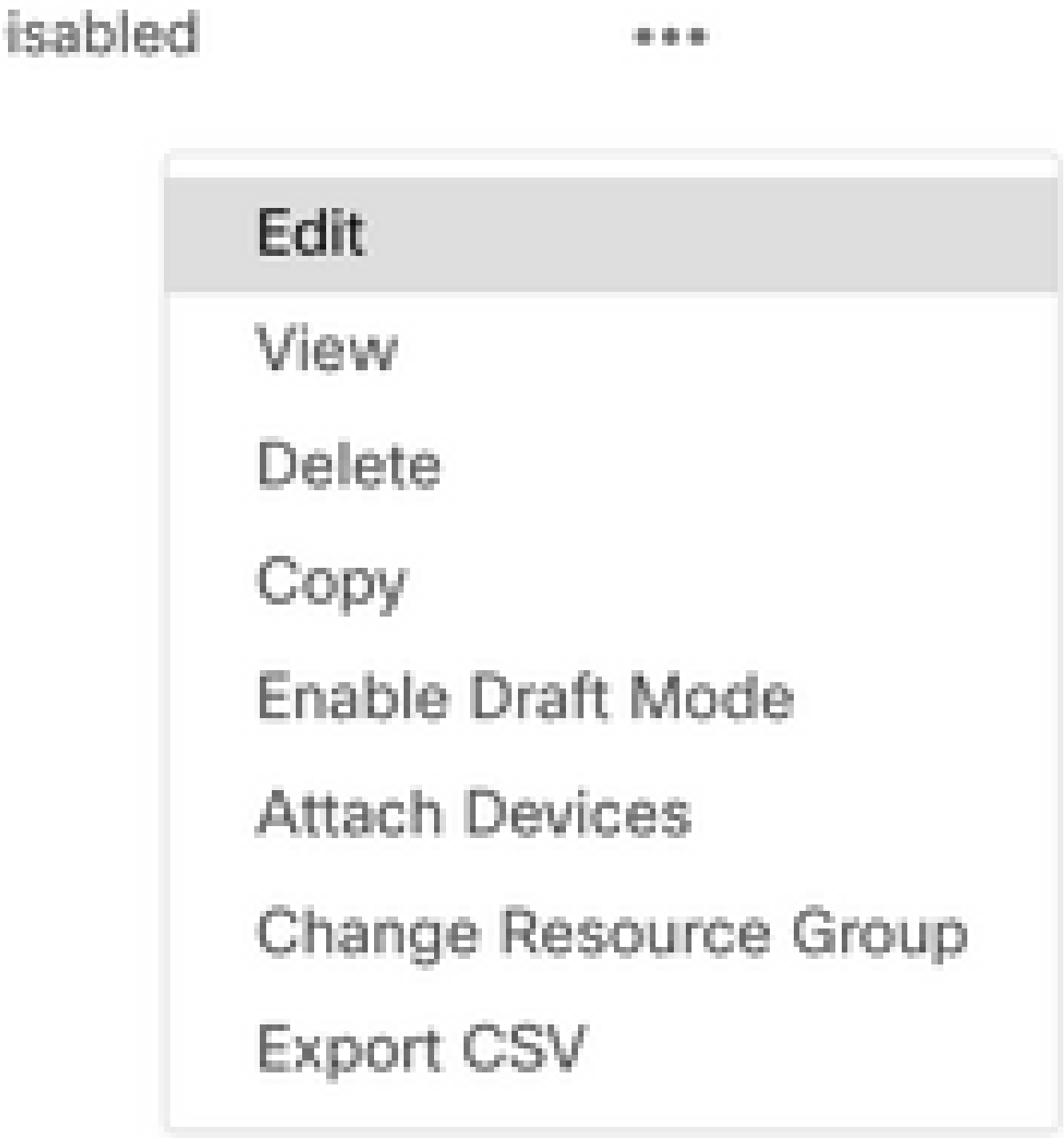
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set security-association lifetime kilobytes disable
 set security-association replay window-size 512
 set transform-set if-ipsec1-ikev2-transform
 set ikev2-profile if-ipsec1-ikev2-profile
!
!
!
!
!
!
!
!
interface Tunnel100001
 description Tunnel 1 - Ipsec BGP vWAN Azure
 vrf forwarding 90
 ip address 20.20.20.1 255.255.255.252
 ip mtu 1500
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 10.4.5.226
 tunnel path-mtu-discovery
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
!
```

Etapa 8. Clique em Salvar.

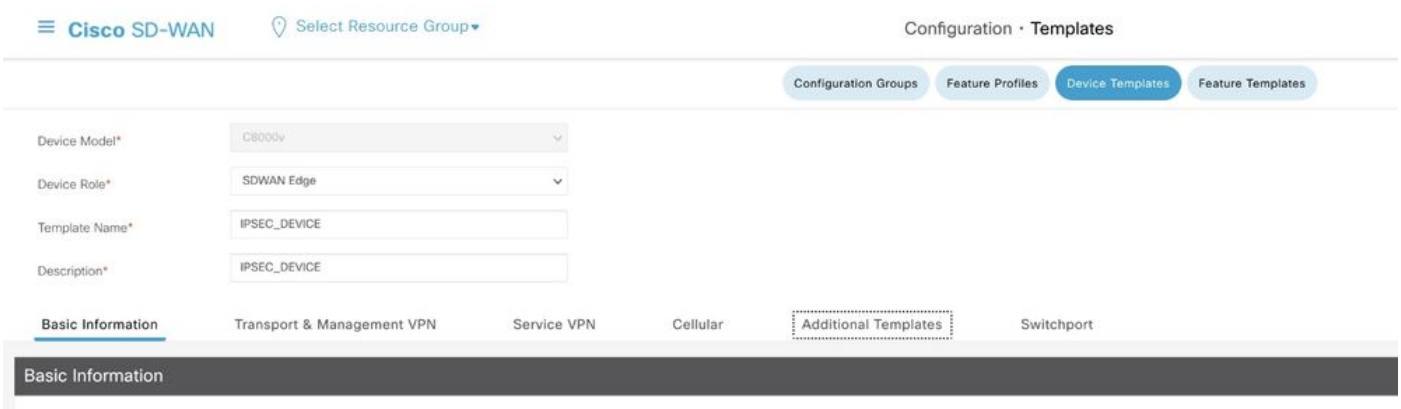
Etapa 9. Navegue até Modelos de dispositivo.



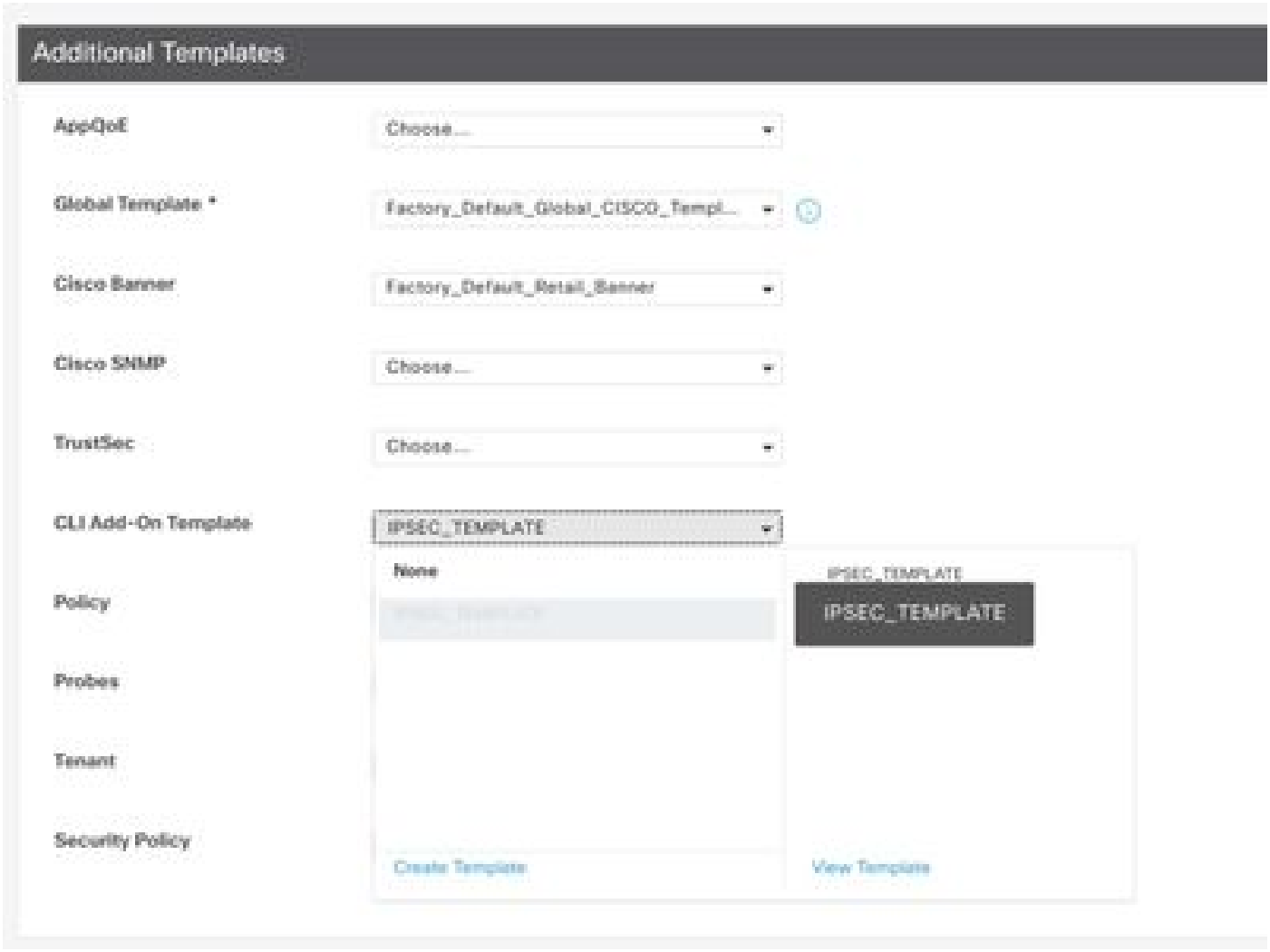
Etapa 10. Escolha o Modelo de dispositivo correto e Edite-o nos 3 pontos.



Etapa 11. Navegue até Modelos Adicionais.

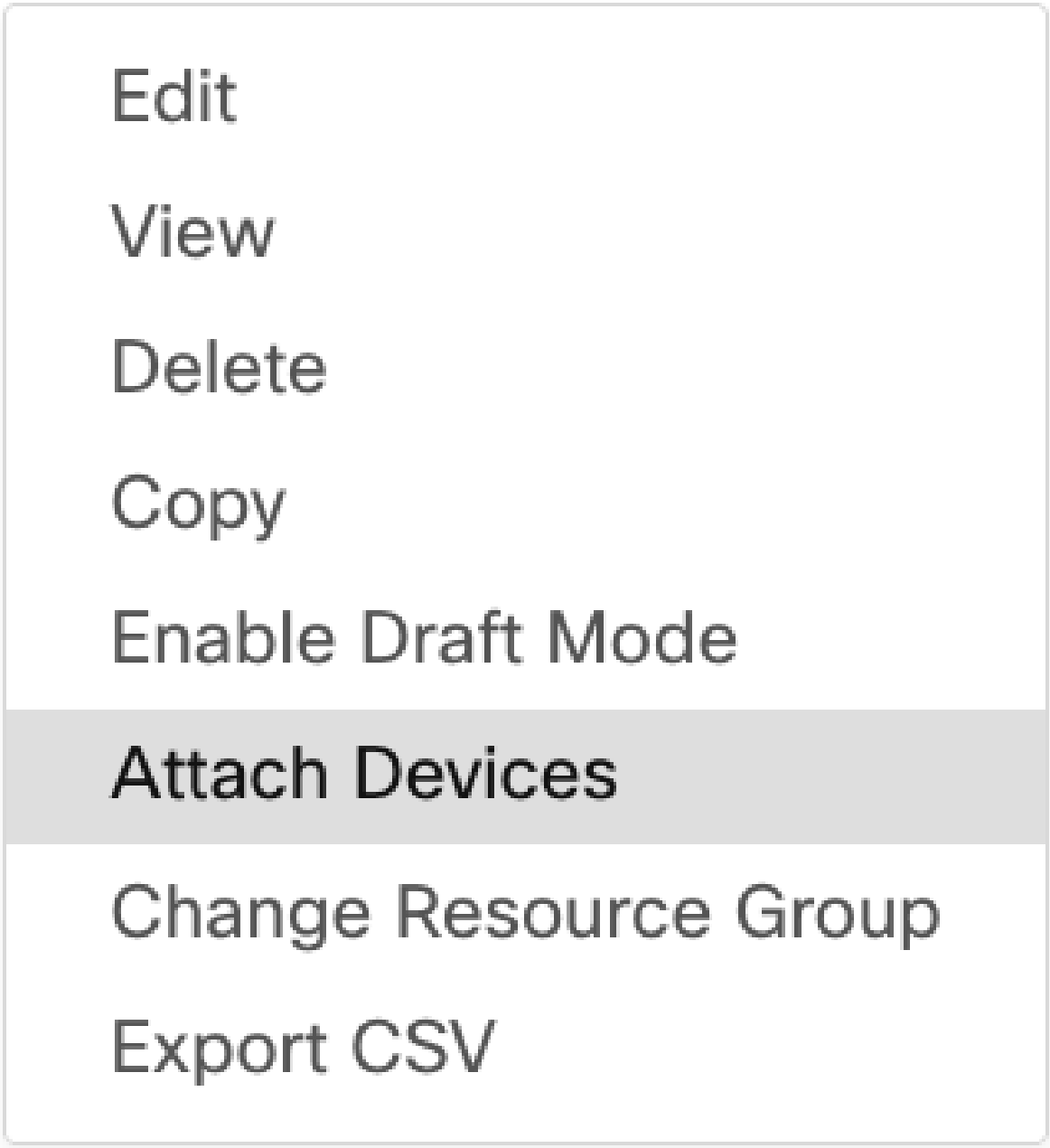


Etapa 12. Em Modelo de complemento CLI, escolha o Modelo de recurso criado anteriormente.



Etapa 13. Clique em Update.

Etapa 14. Clique em Attach Devices de 3 pontos e selecione o roteador correto para o qual enviar o modelo.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Execute o comando show ip interface brief para verificar o status do túnel IPSec.

<#root>

cEdge#

show ip interface brief

```
Interface IP-Address OK? Method Status Protocol
GigabitEthernet1 10.4.5.224 YES other up up
```

--- output omitted ---

Tunnel100001 172.16.12.1 YES other up up

```
cEdge#
```

Troubleshooting

Execute o comando show crypto ikev2 session para exibir informações detalhadas sobre as sessões IKEv2 estabelecidas no dispositivo.

<#root>

```
cEdge#
```

show crypto ikev2 session

```
IPv4 Crypto IKEv2 Session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote fvrf/ivrf Status
1 10.4.5.224/500 10.4.5.225/500 none/90 READY
Encr: AES-CBC, keysize: 128, PRF: SHA1, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/207 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xFC13A6B7/0x1A2AC4A0

IPv6 Crypto IKEv2 Session

cEdge#
```

Execute o comando show crypto ipsec sa interface Tunnel10001 para exibir informações sobre Associações de Segurança (SAs) IPSec.

<#root>

```
cEdge#
```

show crypto ipsec sa interface Tunnel100001

```
interface: Tunnel100001
Crypto map tag: Tunnel100001-head-0, local addr 10.4.5.224
```

```
protected vrf: 90
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 10.4.5.225 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 38, #pkts encrypt: 38, #pkts digest: 38
#pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.4.5.224, remote crypto endpt.: 10.4.5.225
plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x1A2AC4A0(439010464)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xFC13A6B7(4229146295)
transform: esp-gcm 256 ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: CSR:1, sibling_flags FFFFFFFF80000048, crypto map: Tunnel100001-head-0
sa timing: remaining key lifetime (sec): 2745
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 512
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x1A2AC4A0(439010464)
transform: esp-gcm 256 ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: CSR:2, sibling_flags FFFFFFFF80000048, crypto map: Tunnel100001-head-0
sa timing: remaining key lifetime (sec): 2745
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 512
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
cEdge#
```

Execute o comando show crypto ikev2 statistics para exibir estatísticas e contadores relacionados a sessões IKEv2.

```
<#root>

cEdge#

show crypto ikev2 statistics


--------------------------------------------------------------------------------
```

```
Crypto IKEv2 SA Statistics
--------------------------------------------------------------------------------
System Resource Limit: 0 Max IKEv2 SAs: 0 Max in nego(in/out): 40/400
Total incoming IKEv2 SA Count: 0 active: 0 negotiating: 0
Total outgoing IKEv2 SA Count: 1 active: 1 negotiating: 0
Incoming IKEv2 Requests: 0 accepted: 0 rejected: 0
Outgoing IKEv2 Requests: 1 accepted: 1 rejected: 0
Rejected IKEv2 Requests: 0 rsrc low: 0 SA limit: 0
IKEv2 packets dropped at dispatch: 0
Incoming Requests dropped as LOW Q limit reached : 0
Incoming IKEV2 Cookie Challenged Requests: 0
accepted: 0 rejected: 0 rejected no cookie: 0
Total Deleted sessions of Cert Revoked Peers: 0

cEdge#
```

Execute o comando show crypto session para exibir informações sobre sessões de segurança ativas no dispositivo.

<#root>

```
cEdge#
```

show crypto session

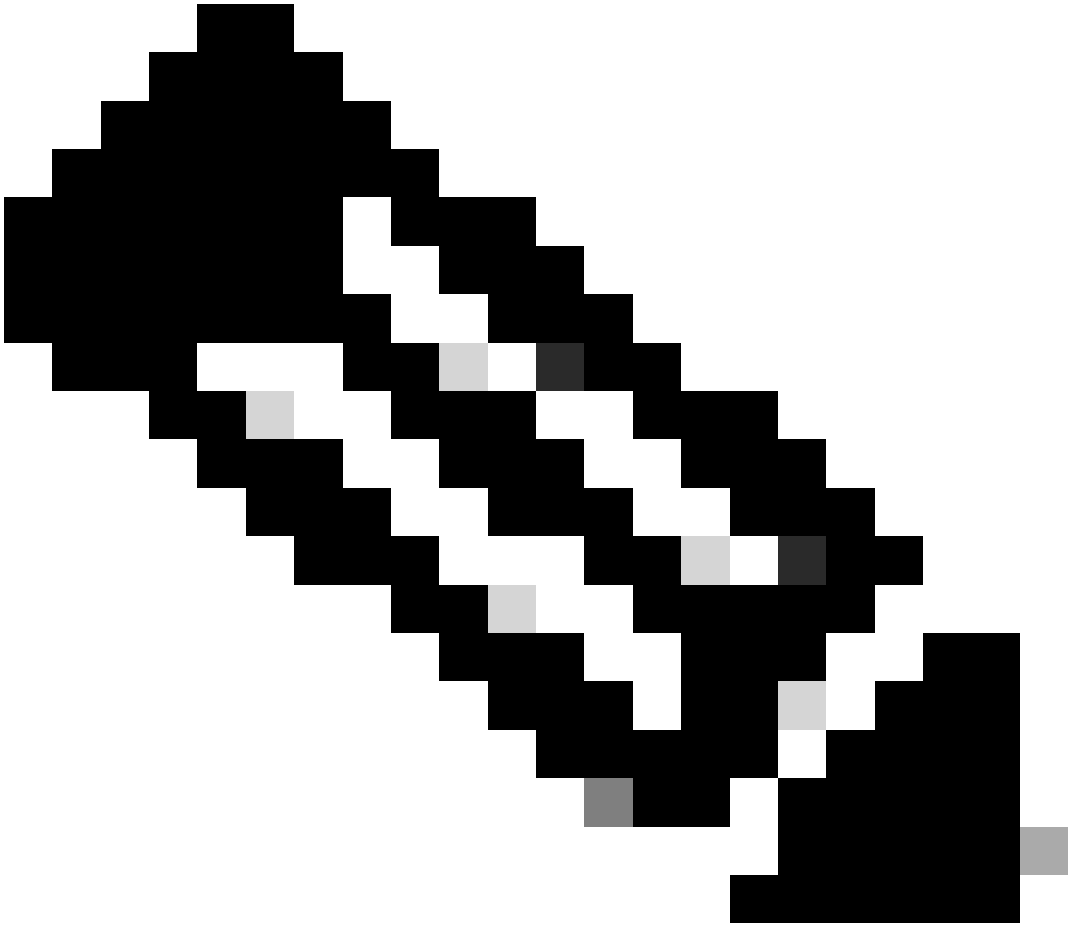
```
Crypto session current status

Interface: Tunnel100001
Profile: if-ipsec1-ikev2-profile
Session status: UP-ACTIVE
Peer: 10.4.5.225 port 500
Session ID: 1
IKEv2 SA: local 10.4.5.224/500 remote 10.4.5.225/500 Active
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
Active SAs: 2, origin: crypto map
```

Para obter informações sobre descartes de pacotes relacionados ao IPSec no processador de pacotes de dispositivos, você pode executar:

show platform hardware qfp ative feature ipsec datapath drops clear

show platform hardware qfp ative statistics drop clear

Esses comandos precisam ser colocados antes de serem fechados e não devem ser desligados na interface de túnel para limpar os contadores e as estatísticas. Isso pode ajudar a obter informações sobre descartes de pacotes relacionados ao IPsec em um caminho de dados do processador de pacotes do dispositivo.



Observação: esses comandos podem ser executados sem a opção clear. É importante destacar que os contadores de queda são históricos.

<#root>

```
cEdge#

show platform hardware qfp active feature ipsec datapath drops clear


----------------------------------------------------------------------
Drop Type Name Packets
----------------------------------------------------------------------



IPSEC detailed dp drop counters cleared after display.

cEdge#
```

<#root>

cEdge#

show platform hardware qfp active statistics drop clear

Last clearing of QFP drops statistics : Thu Sep 28 01:35:11 2023

Global Drop Stats Packets Octets

Ipv4NoRoute 17 3213
UnconfiguredIpv6Fia 18 2016

cEdge#

Após shut e no shut the Tunnel Interface, você poderá executar estes comandos para ver se houve um registro de novas estatísticas ou contadores:

show ip interface brief | Incluir túnel100001

show platform hardware qfp ative statistics drop

show platform hardware qfp ative feature ipsec datapath drops

<#root>

cEdge#

show ip interface brief | include Tunnel100001

Tunnel100001 169.254.21.1 YES other up up
cEdge#
cEdge#sh pl hard qfp act feature ipsec datapath drops

Drop Type Name Packets

<#root>

cEdge#

show platform hardware qfp active statistics drop

Last clearing of QFP drops statistics : Thu Sep 28 01:35:11 2023
(5m 23s ago)

Global Drop Stats Packets Octets

Ipv4NoRoute 321 60669
UnconfiguredIpv6Fia 390 42552

```
cEdge#
```

<#root>

```
cEdge#
```

show platform hardware qfp active feature ipsec datapath drops

```
----------------------------------------------------------------------
Drop Type Name Packets
----------------------------------------------------------------------

cEdge#
```

Comandos úteis

<#root>

show crypto ipsec sa peer <peer_address> detail

show crypto ipsec sa peer <peer_address> platform

show crypto ikev2 session

show crypto ikev2 profile

show crypto isakmp policy

show crypto map

show ip static route vrf NUMBER

show crypto isakmp sa

debug crypto isakmp

debug crypto ipsec

Informações Relacionadas

Teclas Pairwise IPsec

Guia de configuração de segurança do Cisco Catalyst SD-WAN, Cisco IOS® XE Catalyst SD-WAN versão 17.x

Introdução à tecnologia Cisco IPsec

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.