Configuración del túnel IPSec del lado de servicio con un C8000V en SD-WAN

Contenido

Introducción

Este documento describe cómo configurar un túnel IPSec entre un router periférico de Cisco SD-WAN y un terminal VPN con servicio VRF.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software de Cisco (SD-WAN)
- Seguridad de protocolo de Internet (IPSec)

Componentes

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

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos de este documento se iniciaron con una configuración desactivada (predeterminada). Si tiene una red en vivo, asegúrese de entender el

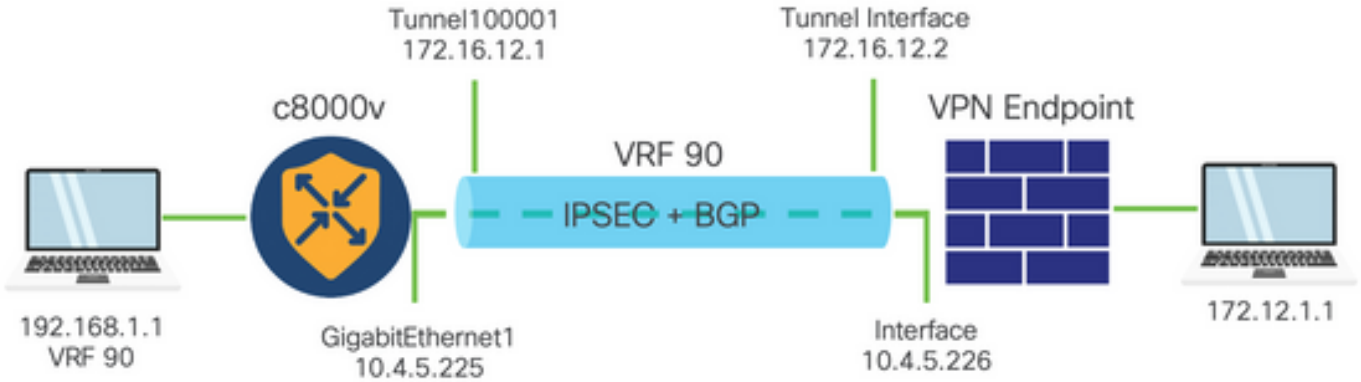
posible impacto de cualquier comando.

Antecedentes

La información general incluye el alcance de este documento, la facilidad de uso y las ventajas de construir un túnel IPSec del lado de servicio con un C8000v en SD-WAN.

- Para crear un túnel IPSec en un servicio de reenvío y routing virtuales (VRF) entre un router Cisco IOS® XE en modo de gestión de controladores y un terminal de red privada virtual (VPN), se garantiza la confidencialidad y la integridad de los datos en la red de área extensa (WAN) pública. También facilita la extensión segura de las redes privadas de las empresas y permite conexiones remotas a través de Internet manteniendo un alto nivel de seguridad.
- El servicio VRF aísla el tráfico, lo que resulta especialmente valioso en entornos de varios clientes o para mantener la segmentación entre las diferentes partes de la red. En resumen, esta configuración mejora la seguridad y la conectividad.
- Este documento considera que el Protocolo de gateway fronterizo (BGP) es el protocolo de ruteo utilizado para comunicar las redes del servicio VRF SD-WAN a la red detrás del punto final VPN y viceversa.
- La configuración BGP está fuera del alcance de este documento.
- Este extremo VPN puede ser un firewall, un router o cualquier tipo de dispositivo de red que tenga capacidades IPSec; la configuración del extremo VPN está fuera del alcance de este documento.
- Este documento asume que el router ya está incorporado con conexiones de control activas y VRF de servicio.

Componentes de la configuración IPSEC



Fase 1 Intercambio de claves de Internet (IKE)

La fase 1 del proceso de configuración IPSec implica la negociación de los parámetros de seguridad y la autenticación entre los extremos del túnel. Estos pasos incluyen:

Configuración IKE

- Defina una propuesta de cifrado (algoritmo y longitud de clave).

- Configure una política IKE que incluya la propuesta de cifrado, el tiempo de vida y la autenticación.

Configurar pares extremos remotos

- Defina la dirección IP del extremo remoto.
- Configure la clave compartida (clave previamente compartida) para la autenticación.

Configuración de fase 2 (IPSec)

La fase 2 implica la negociación de las transformaciones de seguridad y las reglas de acceso para el flujo de tráfico a través del túnel. Estos pasos incluyen:

Configurar conjuntos de transformación IPSec

- Defina un conjunto de transformación propuesto que incluya el algoritmo de cifrado y la autenticación.

Configurar una directiva IPSec

- Asocie el conjunto de transformación a una directiva IPSec.

Configurar interfaces de túnel

Configure las interfaces de túnel en ambos extremos del túnel IPSec.

- Asocie las interfaces de túnel con las directivas IPSec.

Configurar

Configuración en CLI

Paso 1. Defina una propuesta de cifrado.

<#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
```

Paso 2. Configure una política IKE que incluya información de la propuesta.

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

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

Paso 3. Defina la dirección IP del extremo remoto.

```
<#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
```

Paso 4. Configure la clave compartida (clave previamente compartida) para la autenticación.

```
<#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)#
```

Paso 5. Defina un conjunto de transformación propuesto que incluya el algoritmo de cifrado y la autenticación.

```
<#root>

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

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

Paso 6. Asocie el conjunto de transformación a una política IPSec.

```
<#root>

cEdge(config)#
crypto ipsec profile if-ipsec1-ipsec-profile
```

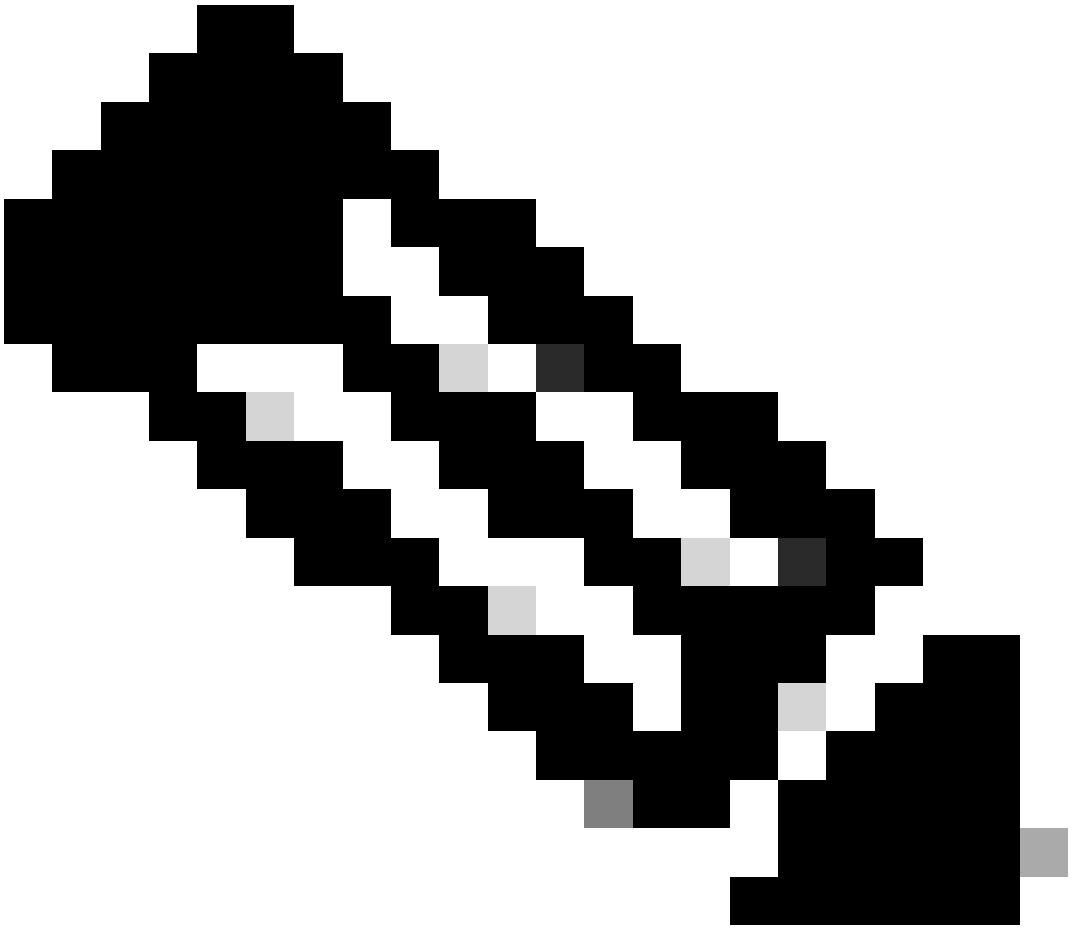
```
cEdge(ipsec-profile)#
set security-association lifetime kilobytes disable

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
```

Paso 7. Cree el túnel de interfaz y asócielo a las políticas 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
```

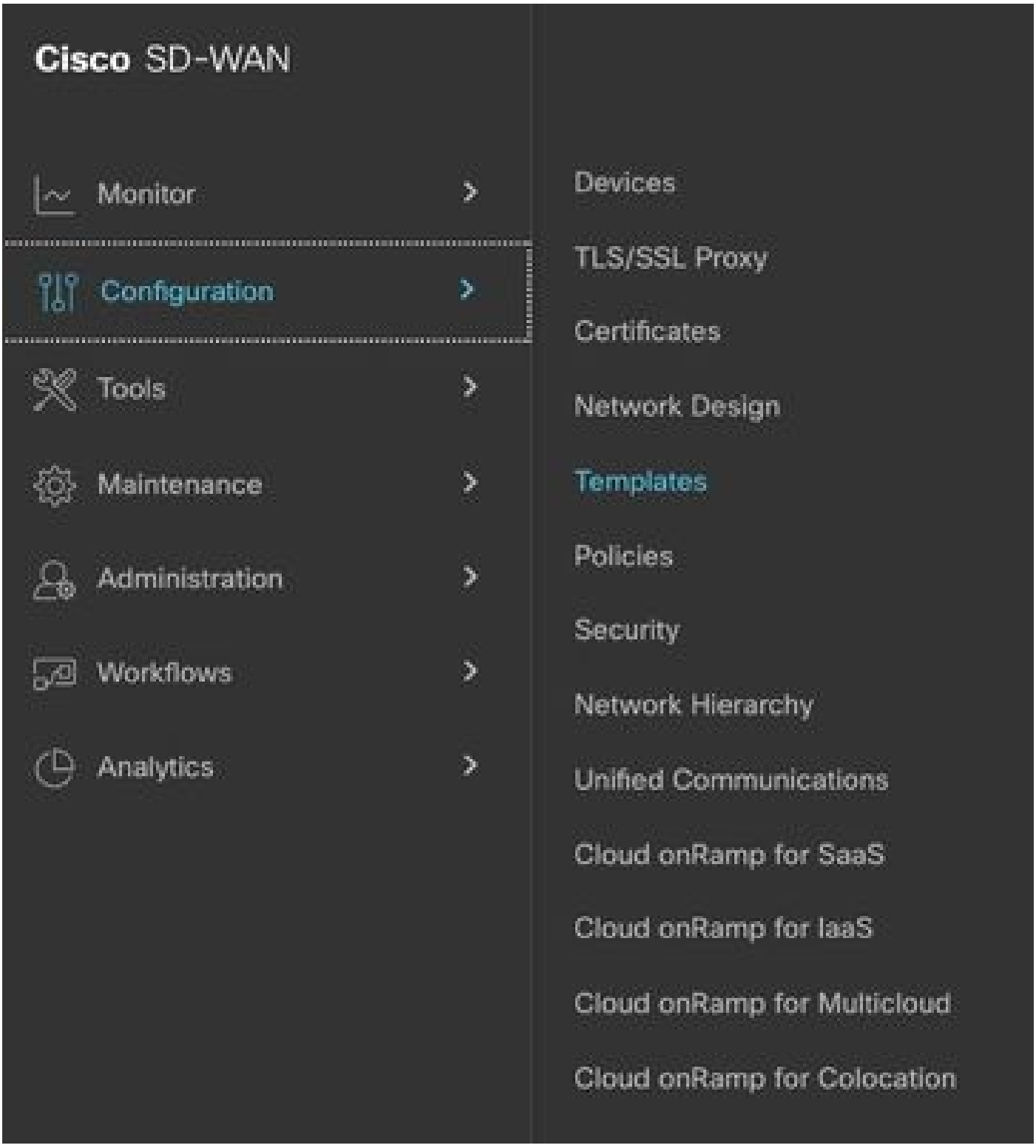
Configuración en una plantilla de complementos de CLI en vManage



> Nota: este tipo de configuración solo se puede agregar mediante la plantilla de complementos de CLI.

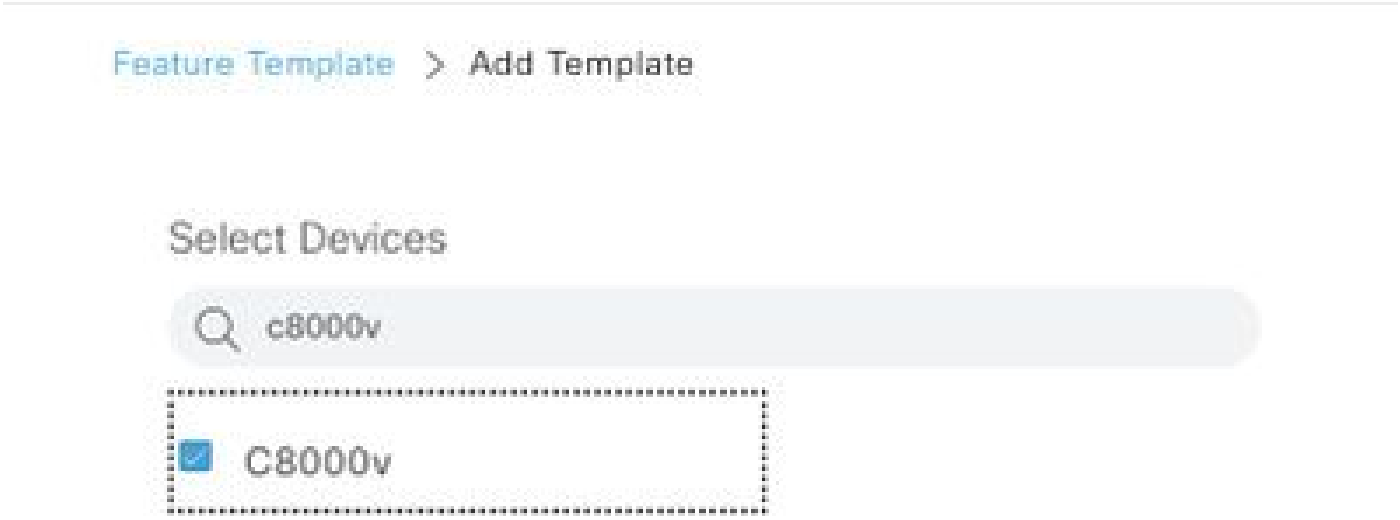
Paso 1. Navegue hasta Cisco vManage e inicie sesión.

Paso 2. Vaya a Configuration > Templates .



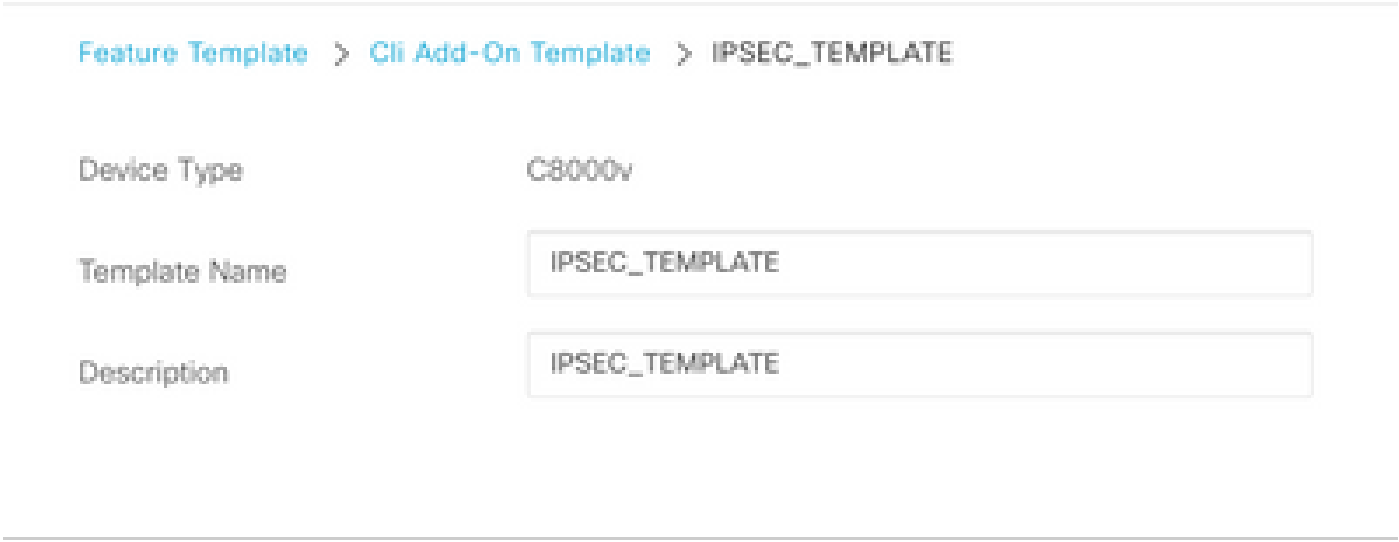
Paso 3. Navegue hasta Plantillas de funciones > Agregar plantilla.

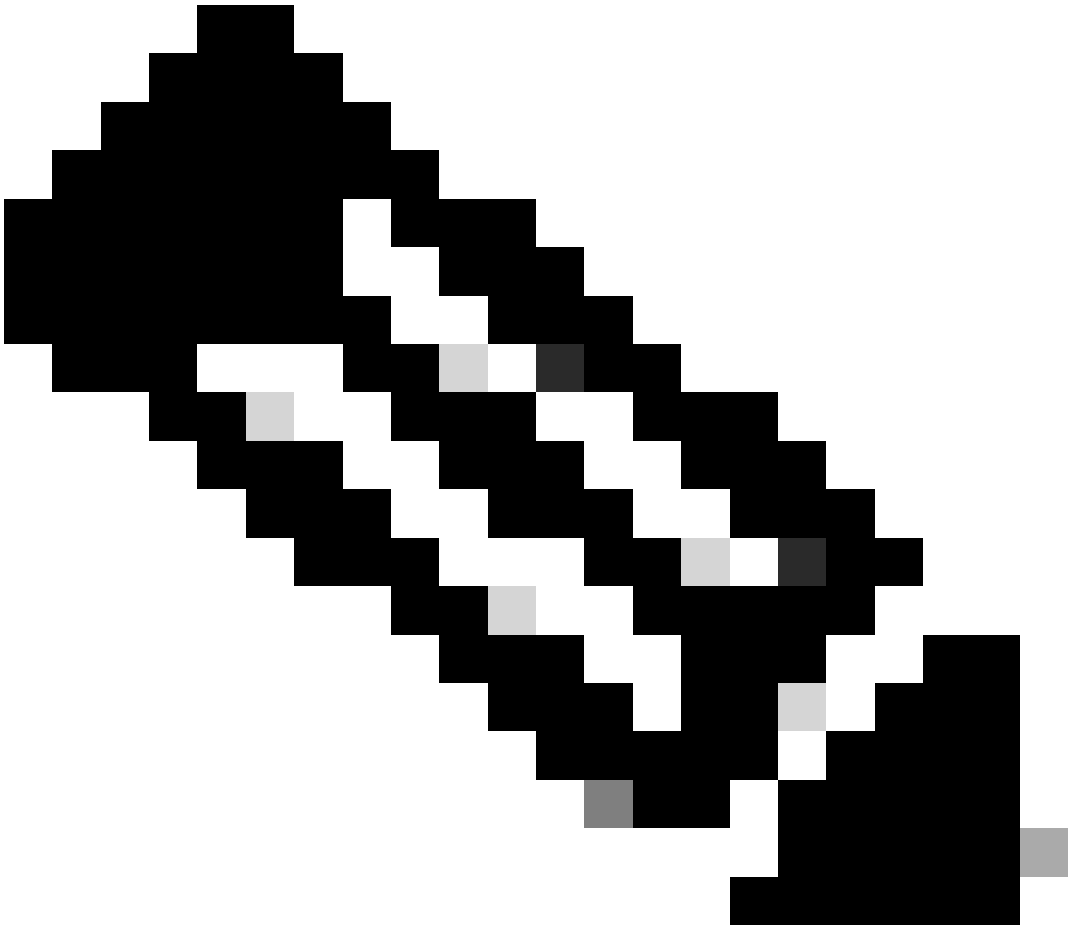
Paso 4. Filtre el modelo y elija el router c8000v.



Paso 5. Navegue hasta Otras plantillas y haga clic en Plantilla de complementos de Cli.

Paso 6. Agregue un nombre de plantilla y una descripción.





Nota: Para obtener más información sobre cómo crear variables en una plantilla de complementos de CLI, consulte Plantillas de funciones de complementos de CLI.

Paso 7. Agregue los comandos.

CLI CONFIGURATION

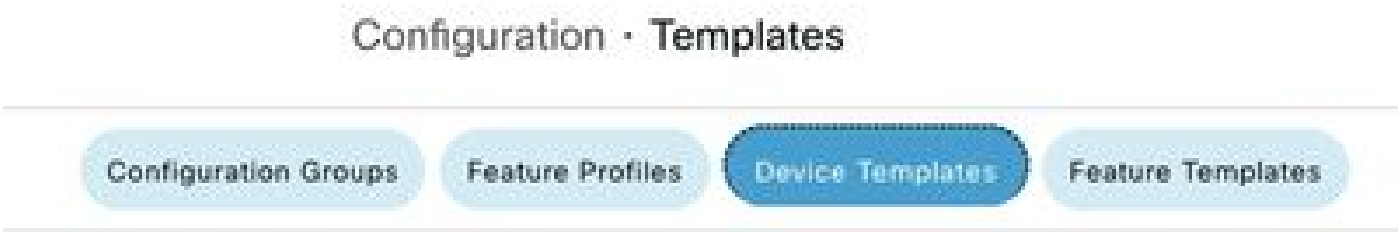
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key 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

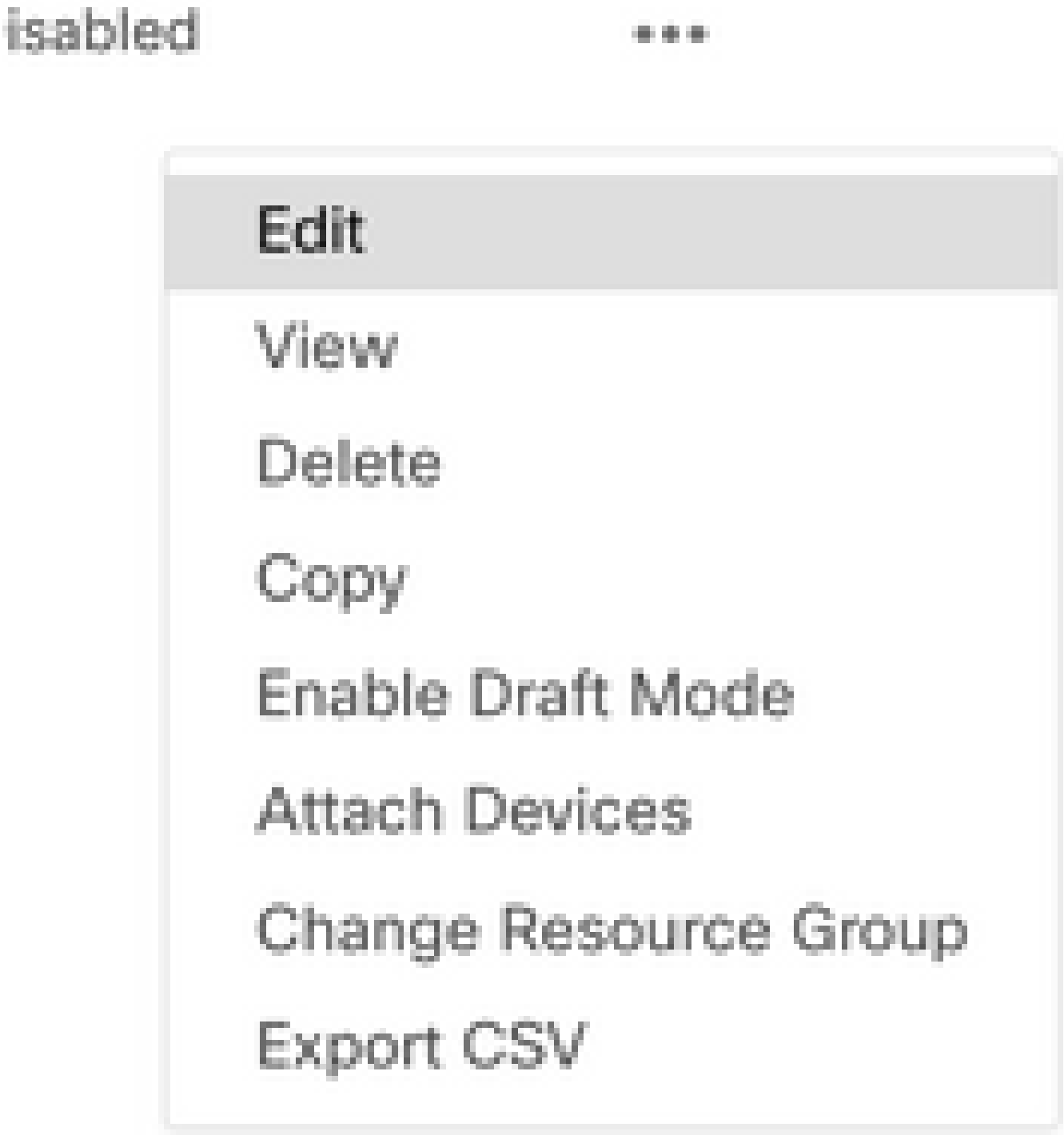
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

Paso 8. Haga clic en Guardar.

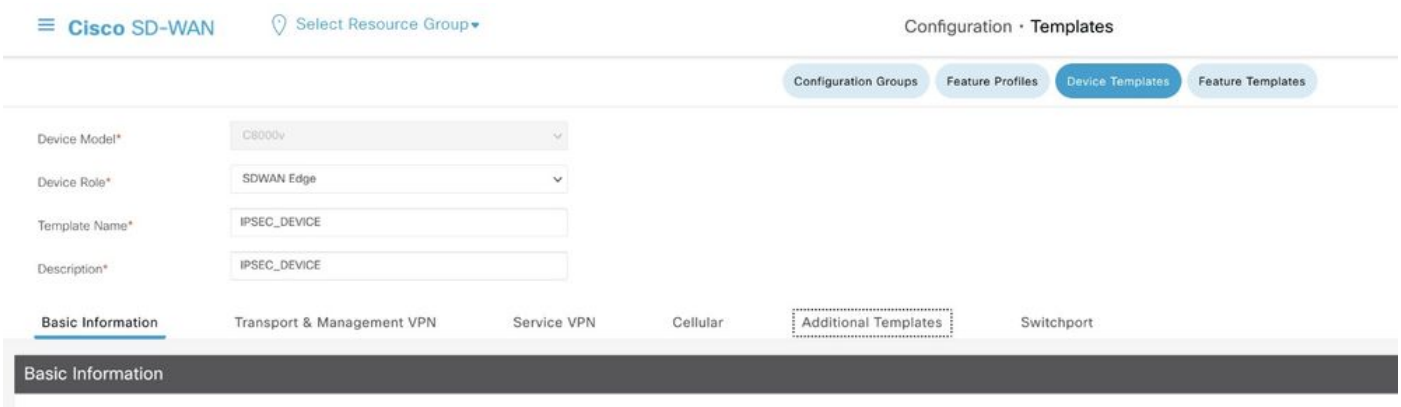
Paso 9. Vaya a Plantillas de dispositivo.



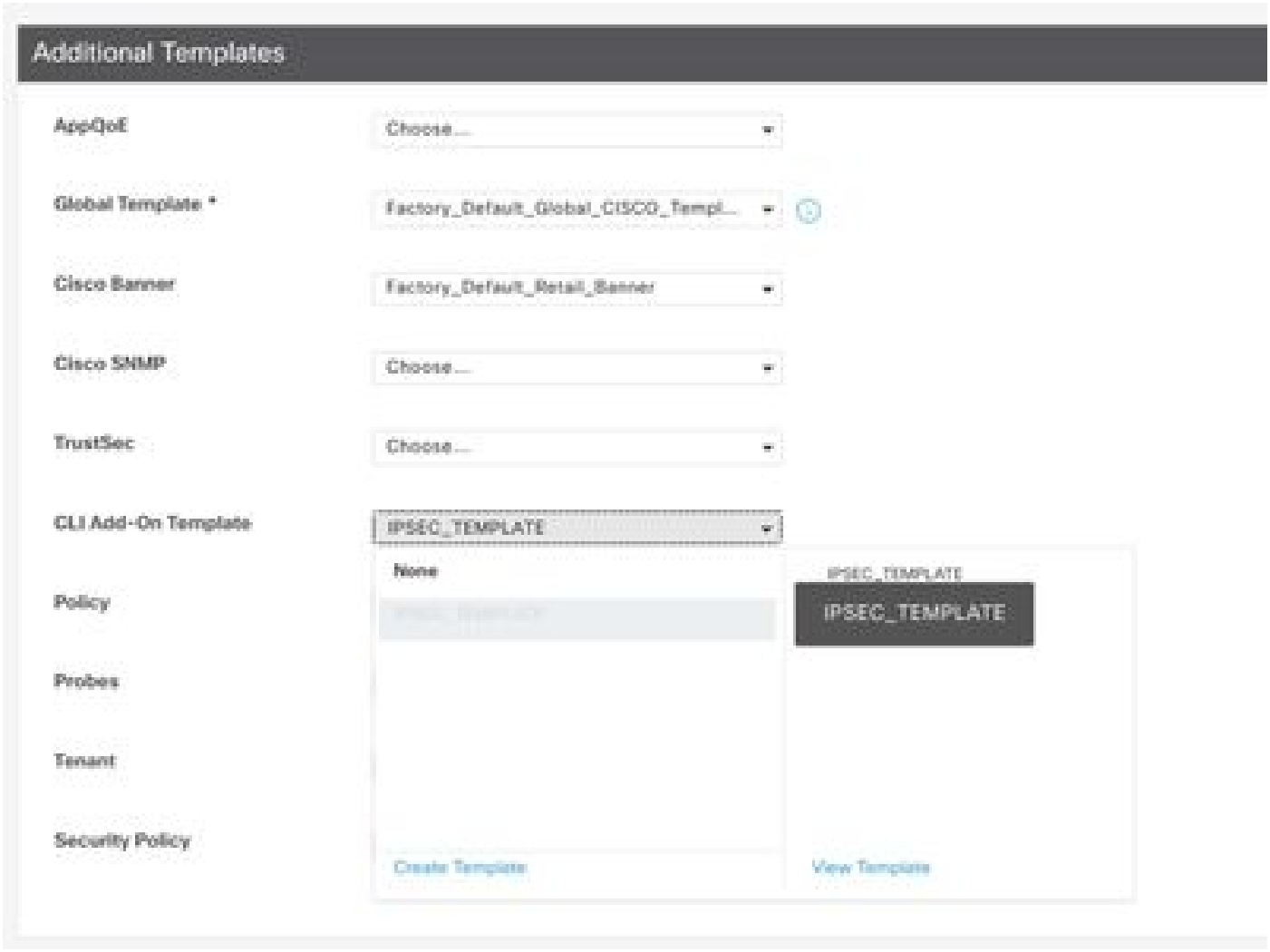
Paso 10. Elija la plantilla de dispositivo correcta y edítela en los 3 puntos.



Paso 11. Vaya a Plantillas adicionales.

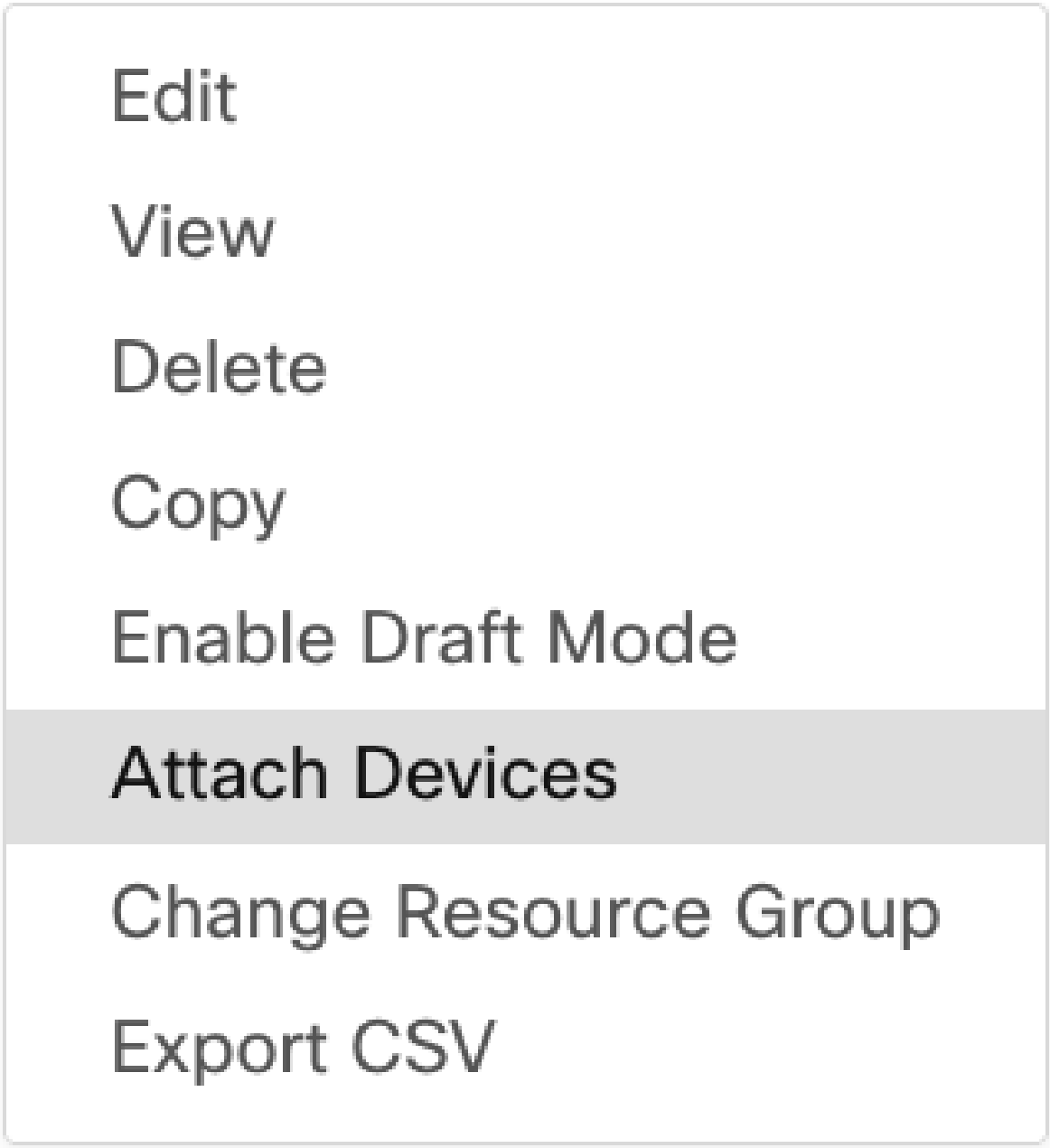


Paso 12. En CLI Add-On Template elija la plantilla de funciones creada anteriormente.



Paso 13. Haga clic en Update (Actualizar).

Paso 14. Haga clic en Attach Devices de 3 puntos y seleccione el router correcto al que enviar la plantilla.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Ejecute el comando show ip interface brief para verificar el estado del 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#
```

Troubleshoot

Ejecute el comando show crypto ikev2 session para mostrar información detallada sobre las sesiones IKEv2 establecidas en el 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#
```

Ejecute el comando show crypto ipsec sa interface Tunnel10001 para mostrar información sobre las asociaciones de seguridad (SA) 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#
```

Ejecute el comando show crypto ikev2 statistics para mostrar estadísticas y contadores relacionados con las sesiones 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#
```

Ejecute el comando show crypto session para mostrar información sobre las sesiones de seguridad activas en el dispositivo.

<#root>

```
cEdge#
```

show crypto session

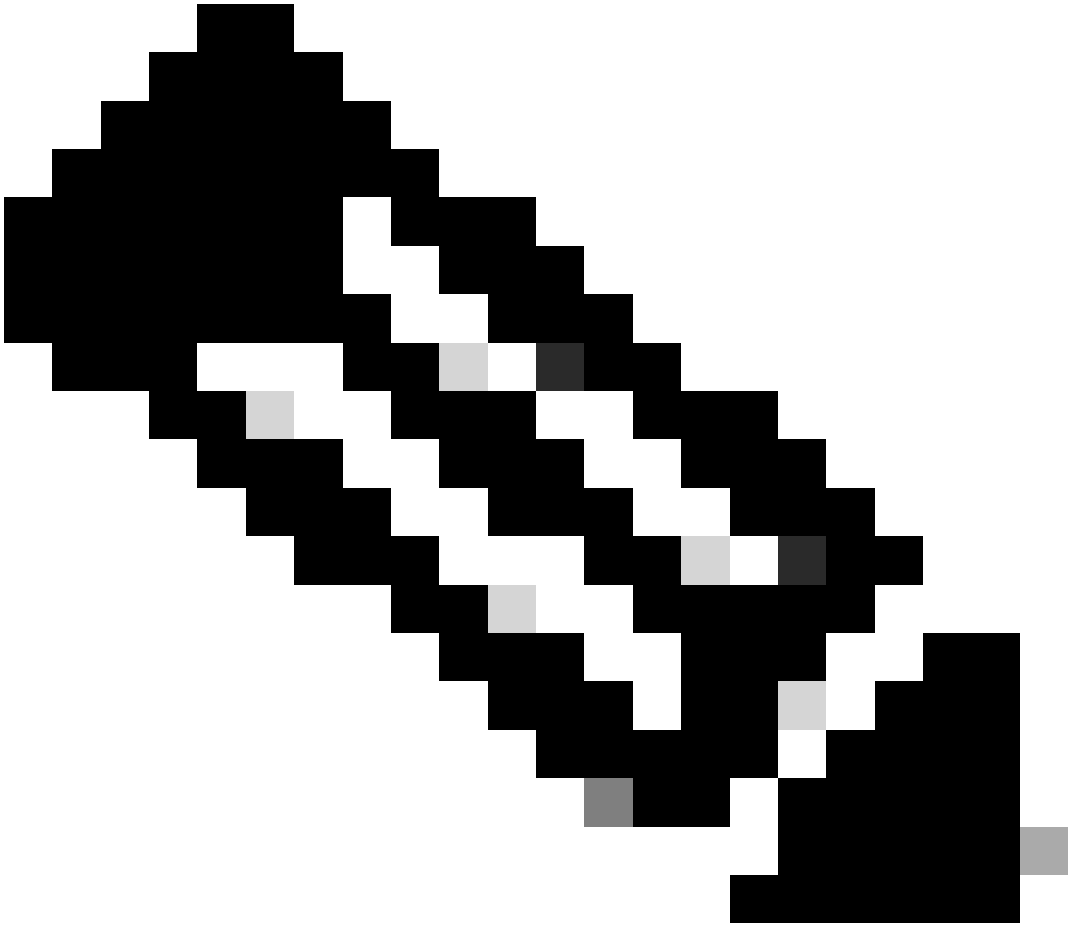
```
Crypto session current status

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 obtener información sobre las caídas de paquetes relacionadas con IPSec en el procesador de paquetes de dispositivos, puede ejecutar:

show platform hardware qfp active feature ipsec datapath drops clear

show platform hardware qfp active statistics drop clear

Estos comandos se deben poner antes de cerrar y no cerrar la interfaz de túnel para borrar los contadores y las estadísticas, esto puede ayudar a obtener información sobre las caídas de paquetes relacionadas con IPsec en una ruta de datos del procesador de paquetes de dispositivos.



Nota: Estos comandos se pueden ejecutar sin que la opción esté desactivada. Es importante destacar que los contadores de caídas son 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#

Después de cerrar y no cerrar la Interfaz de Túnel puede ejecutar estos comandos para ver si hubo un registro de nuevas estadísticas o contadores:

show ip interface brief | incluir Tunnel100001

show platform hardware qfp active statistics drop

show platform hardware qfp active 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 útiles

<#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

Información Relacionada

Claves IPsec en pares

Guía de Configuración de Seguridad de Cisco Catalyst SD-WAN, Cisco IOS® XE Catalyst SD-WAN Release 17.x

Introducción a la tecnología Cisco IPsec

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).