Configurazione del tunnel IPSec lato servizio con un C800V su SD-WAN

Sommario

Introduzione

In questo documento viene descritto come configurare un tunnel IPSec tra un router perimetrale Cisco SD-WAN e un endpoint VPN con VRF di servizio.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- IPSec (Internet Protocol Security)

Componenti

Questo documento si basa sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

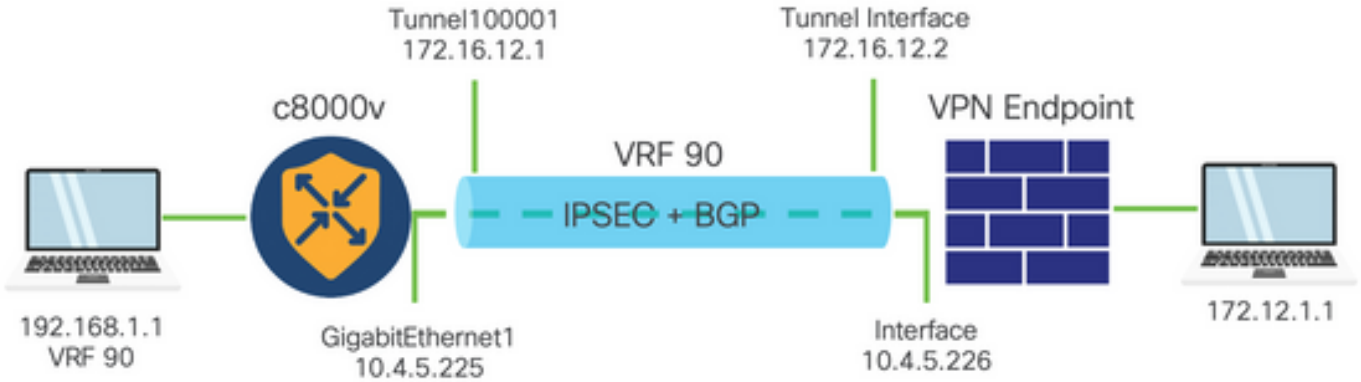
conseguenze derivanti dall'uso dei comandi.

Premesse

Le informazioni generali includono l'ambito di questo documento, la facilità di utilizzo e i vantaggi della creazione di un tunnel IPSec lato servizio con un C8000v su SD-WAN.

- Per creare un tunnel IPSec in un servizio VRF (Virtual Routing and Forwarding) tra un router Cisco IOS® XE in modalità di gestione dei controller e un endpoint VPN (Virtual Private Network), è necessario garantire la riservatezza e l'integrità dei dati sulla rete WAN pubblica. Facilita inoltre l'estensione sicura delle reti private aziendali e consente connessioni remote su Internet mantenendo un elevato livello di sicurezza.
- Il servizio VRF isola il traffico, un fattore particolarmente importante negli ambienti multi-client o per mantenere la segmentazione tra le diverse parti della rete. In breve, questa configurazione migliora la sicurezza e la connettività.
- In questo documento si considera che Border Gateway Protocol (BGP) sia il protocollo di routing usato per comunicare le reti dal servizio SD-WAN VRF alla rete dietro l'endpoint VPN e viceversa.
- La configurazione BGP non è compresa nell'ambito di questo documento.
- L'endpoint VPN può essere un firewall, un router o qualsiasi tipo di dispositivo di rete dotato di funzionalità IPSec. La configurazione dell'endpoint VPN non è inclusa nell'ambito di questo documento.
- In questo documento si presume che il router sia già integrato con connessioni di controllo attive e VRF di servizio.

Componenti della configurazione IPSEC



IKE (Internet Key Exchange) fase 1

La fase 1 del processo di configurazione di IPSec prevede la negoziazione dei parametri di protezione e l'autenticazione tra gli endpoint del tunnel. Ecco un riepilogo:

Configurazione IKE

- Definire una proposta di crittografia (algoritmo e lunghezza della chiave).

- Configurare un criterio IKE che includa la proposta di crittografia, la durata e l'autenticazione.

Configura peer remoti

- Definire l'indirizzo IP dell'estremità remota.
- Configurare la chiave condivisa (chiave già condivisa) per l'autenticazione.

Configurazione fase 2 (IPSec)

La fase 2 prevede la negoziazione delle trasformazioni della sicurezza e delle regole di accesso per il flusso del traffico attraverso il tunnel. Ecco un riepilogo:

Configurare i set di trasformazione IPSec

- Definire un set di trasformazioni proposto che includa l'algoritmo di crittografia e l'autenticazione.

Configurare un criterio IPSec

- Associare il set di trasformazioni a un criterio IPSec.

Configura interfacce tunnel

Configurare le interfacce tunnel su entrambe le estremità del tunnel IPSec.

- Associare le interfacce tunnel ai criteri IPSec.

Configurazione

Configurazione sulla CLI

Passaggio 1. Definire una proposta di crittografia.

<#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
```

Passaggio 2. Configurare un criterio IKE che includa informazioni sulle proposte.

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

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

Passaggio 3. Definire l'indirizzo IP dell'estremità 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
```

Passaggio 4. Configurare la chiave condivisa (chiave già condivisa) per l'autenticazione.

```
<#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)#
```

Passaggio 5. Definire un set di trasformazioni proposto che includa l'algoritmo di crittografia e l'autenticazione.

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

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

Passaggio 6. Associare il set di trasformazioni a un criterio IPSec.

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

cEdge(ipsec-profile)#
```

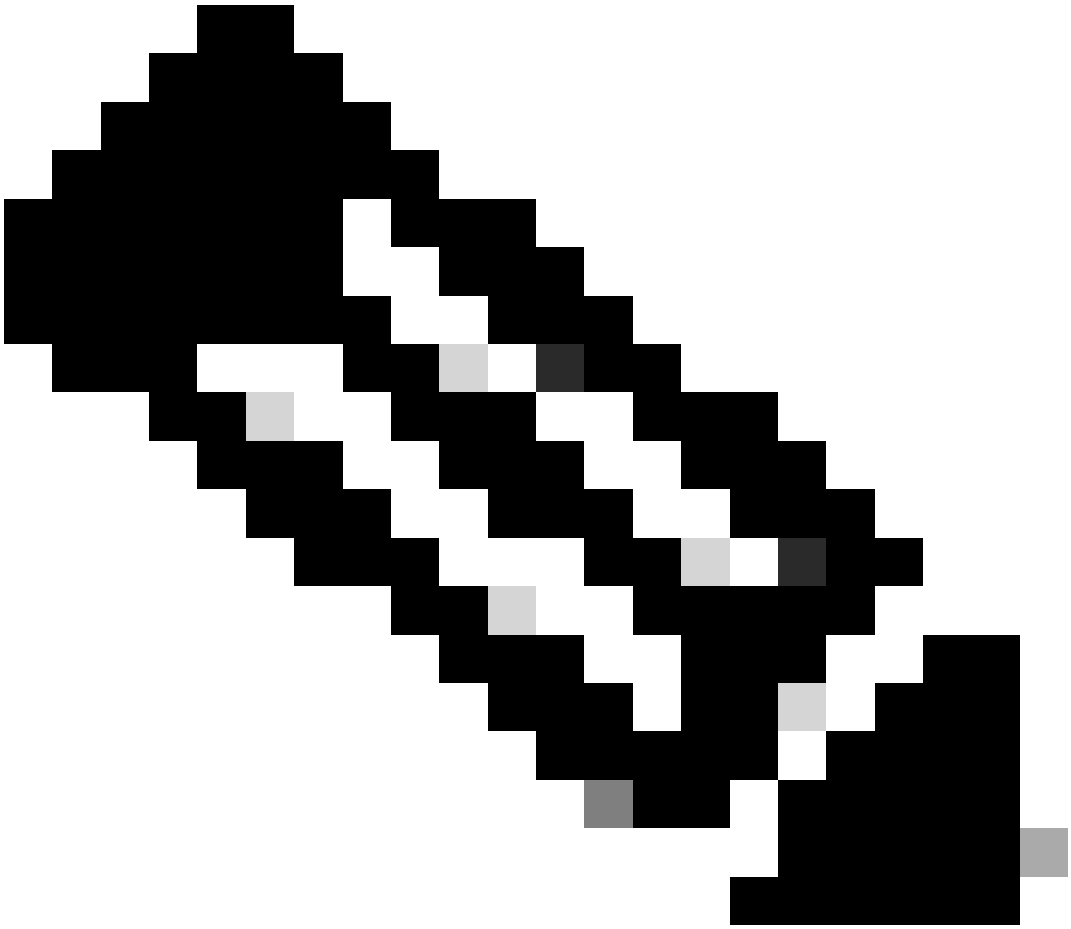
```
set security-association lifetime kilobytes disable

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
```

Passaggio 7. Creare il tunnel di interfaccia e associarlo ai criteri 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
```

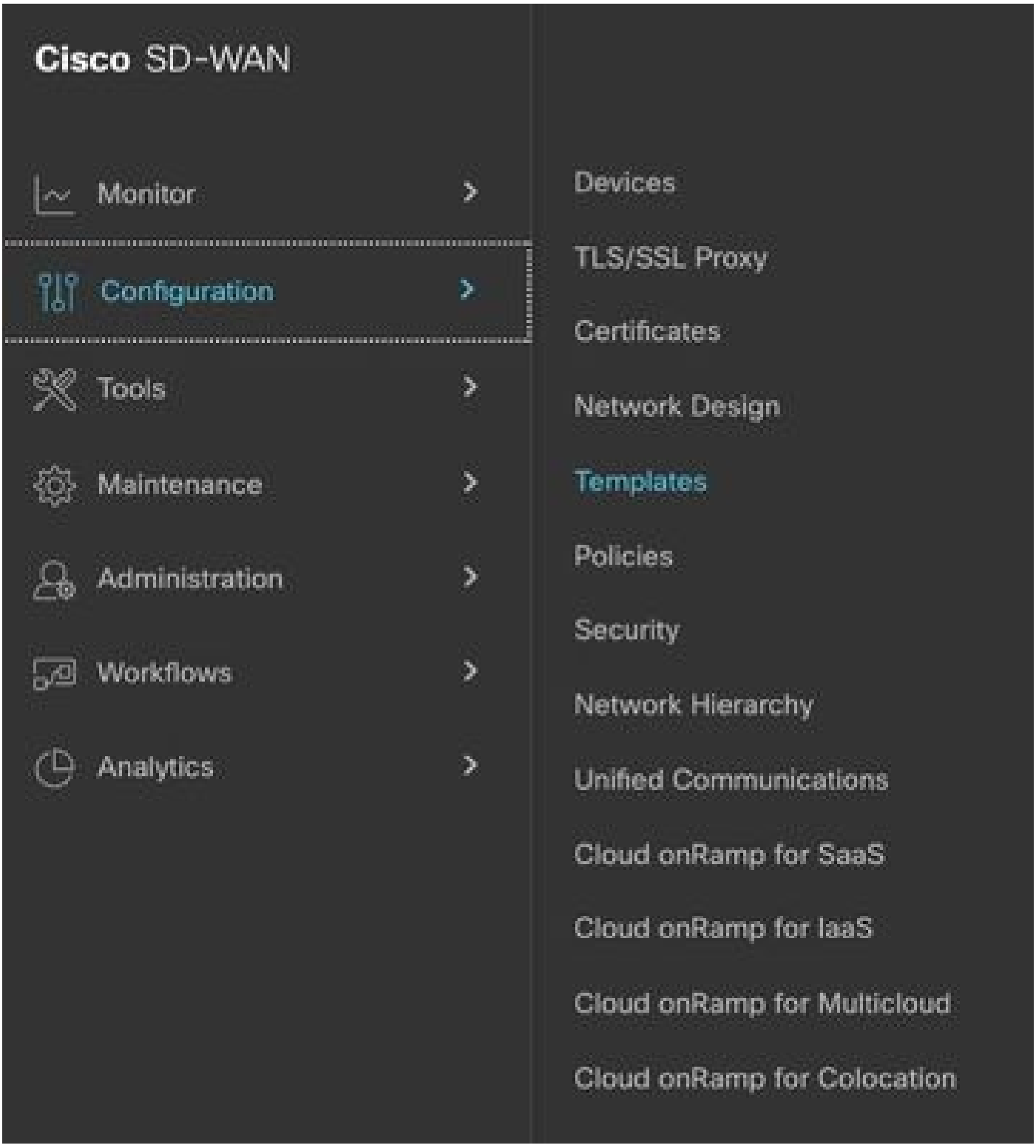
Configurazione su un modello aggiuntivo CLI su vManage



> Nota: questo tipo di configurazione può essere aggiunto solo tramite il modello aggiuntivo CLI.

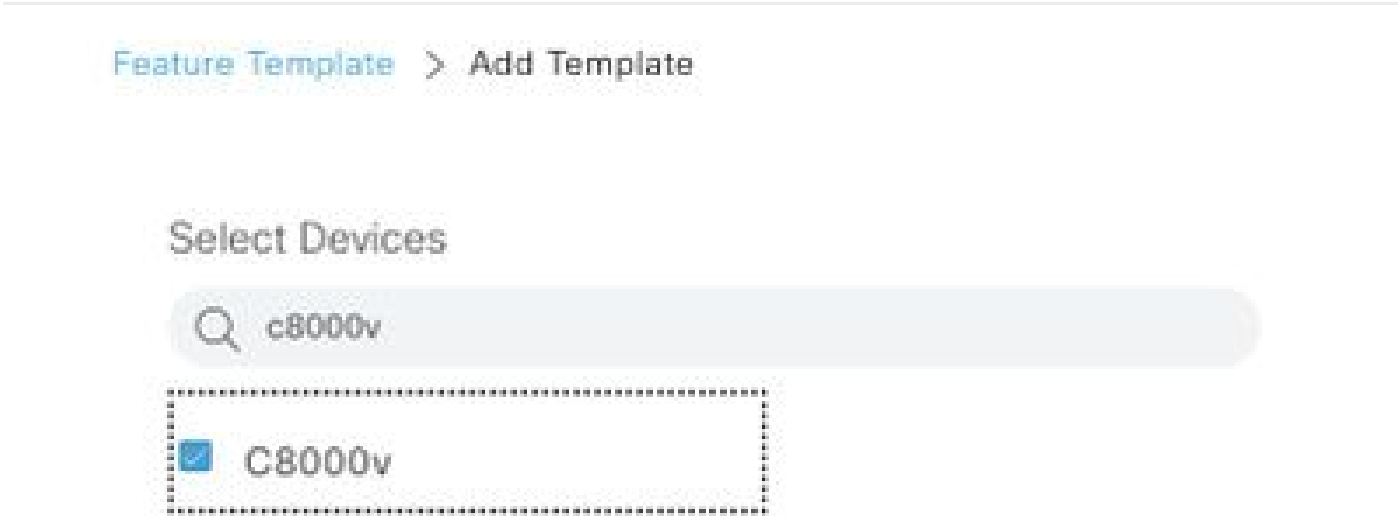
Passaggio 1. Passare a Cisco vManage ed eseguire l'accesso.

Passaggio 2. Selezionare Configurazione > Modelli.



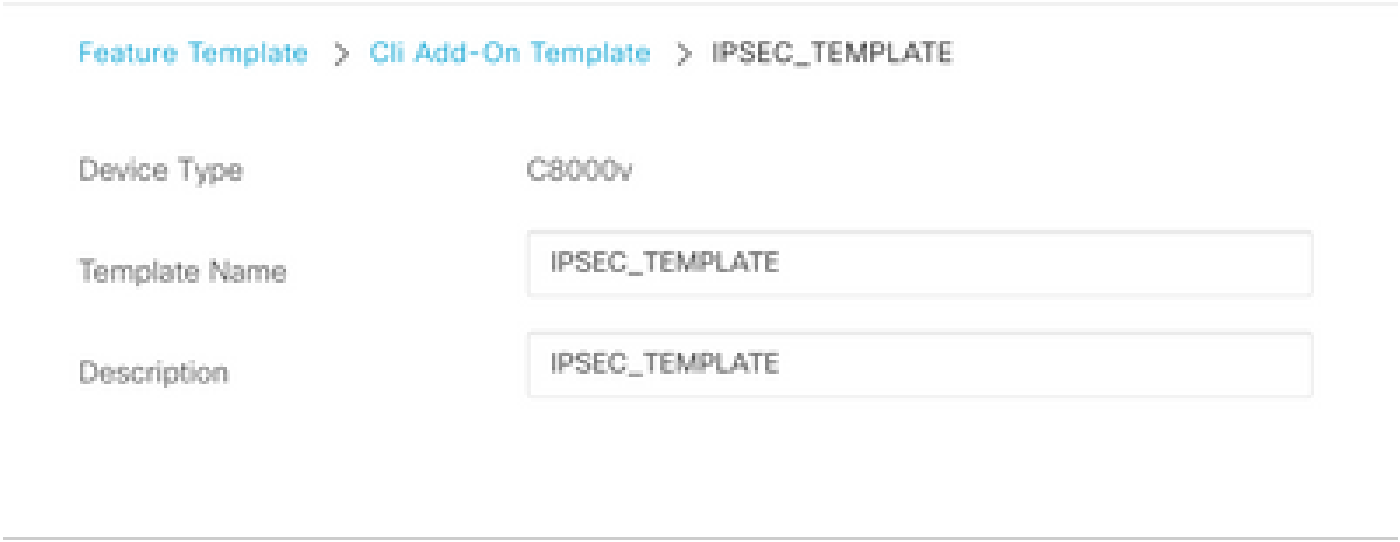
Passaggio 3. Selezionare Modelli funzionalità > Aggiungi modello.

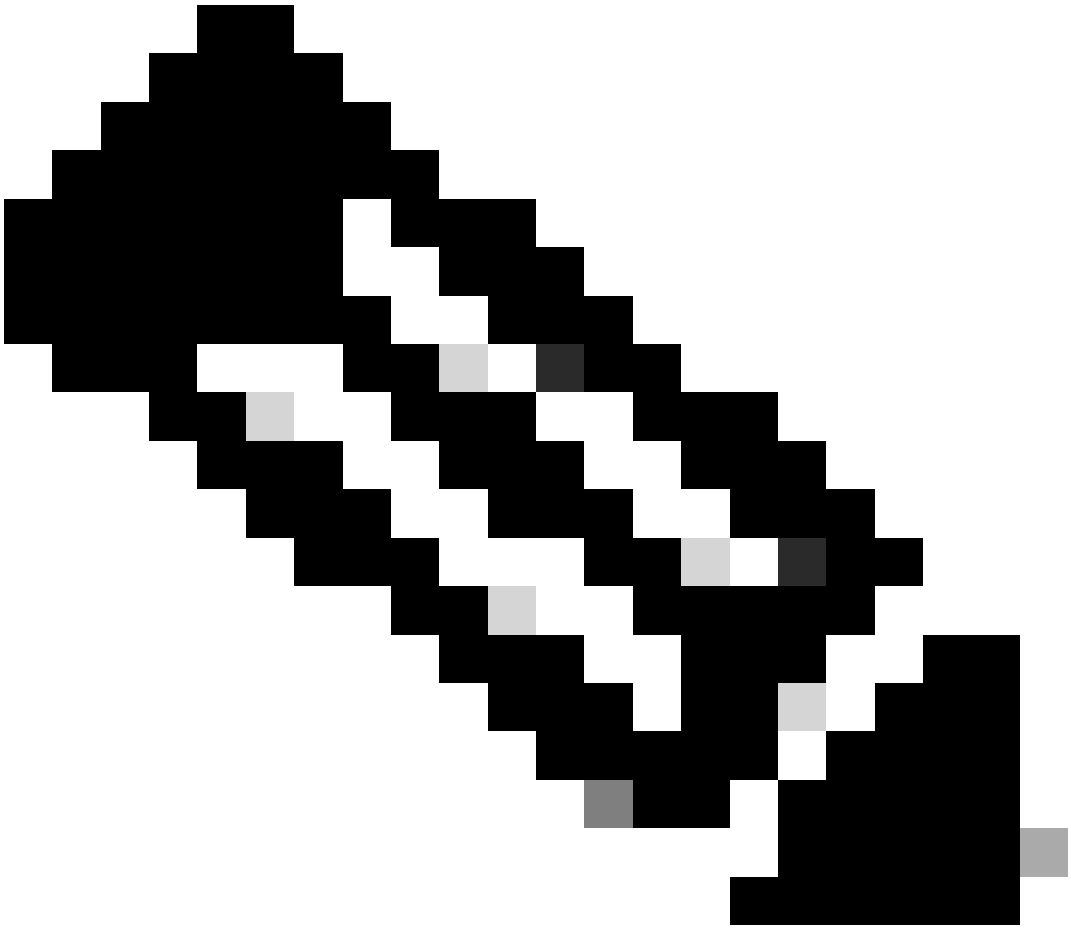
Passaggio 4. Filtrare il modello e scegliere il router c8000v.



Passaggio 5. Passare ad Altri modelli e fare clic su Modello aggiuntivo Cli.

Passaggio 6. Aggiungere un nome di modello e una descrizione.





Nota: per ulteriori informazioni su come creare variabili su un modello di componente aggiuntivo CLI, fare riferimento ai modelli di funzionalità dei componenti aggiuntivi CLI.

Passaggio 7. Aggiungere i comandi.

CLI CONFIGURATION

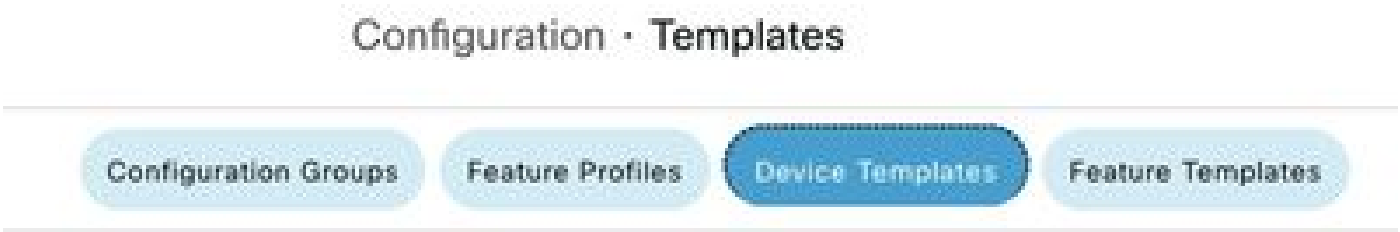
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key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

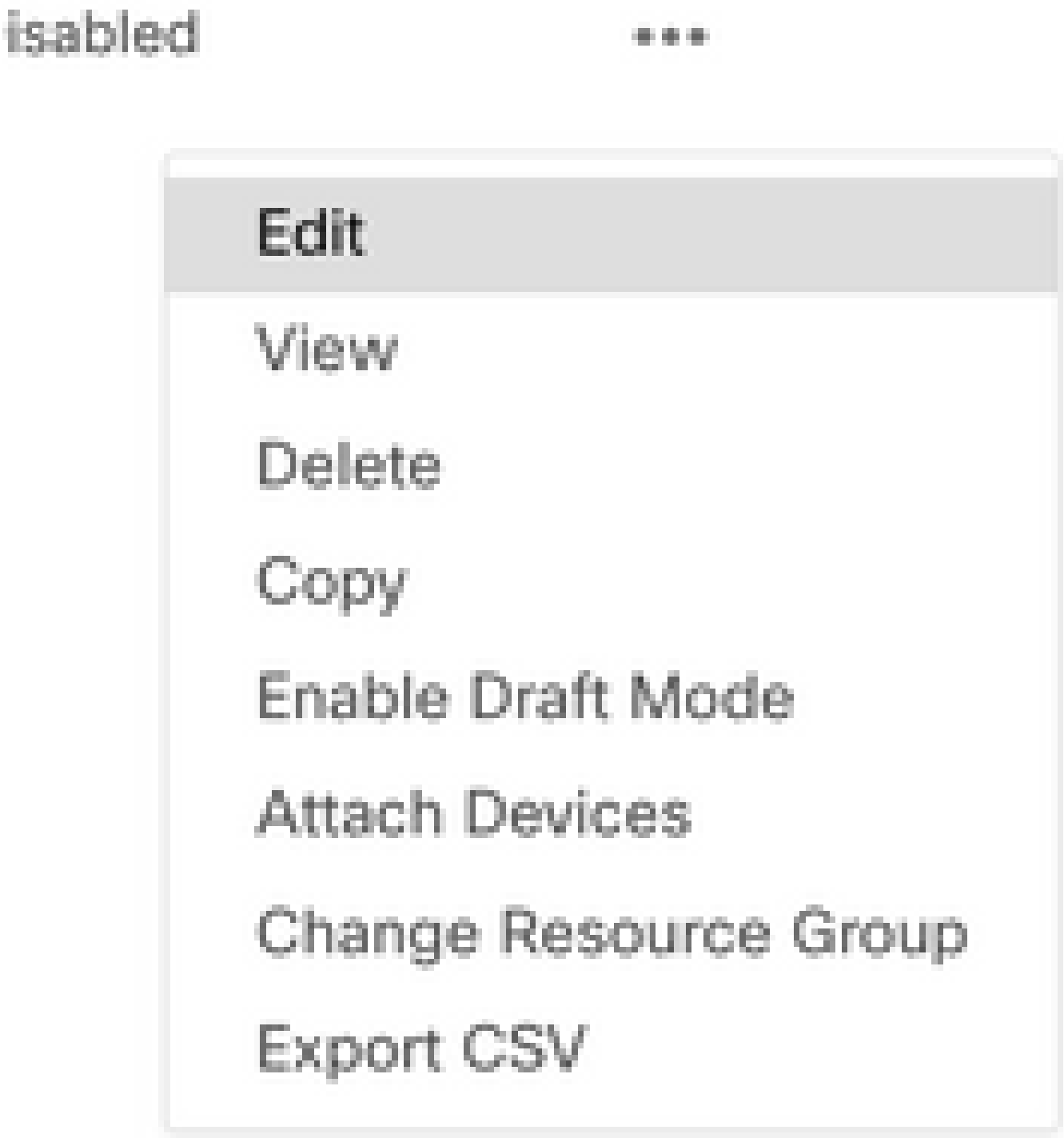
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

Passaggio 8. Fare clic su Save (Salva).

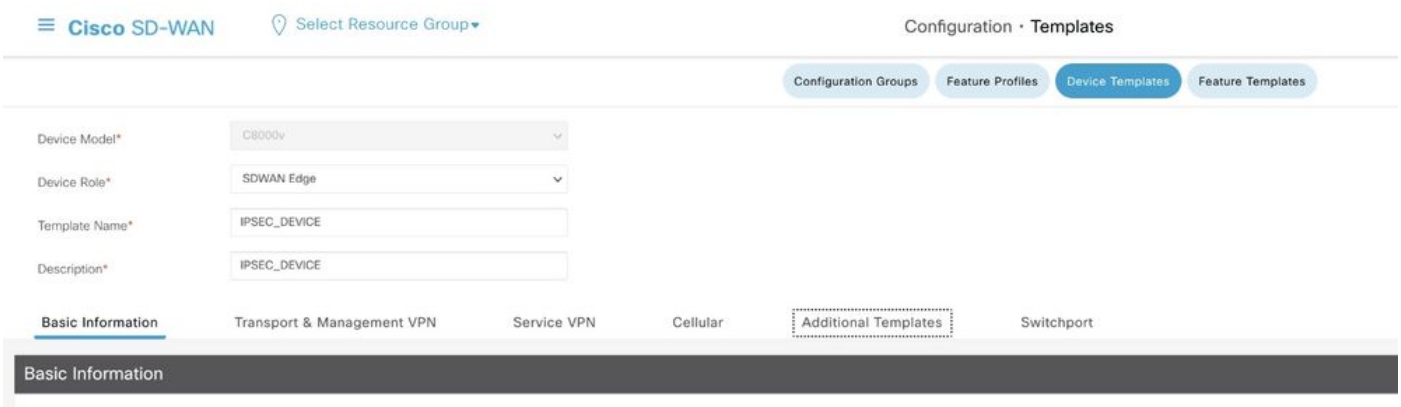
Passaggio 9. Passare a Modelli di dispositivo.



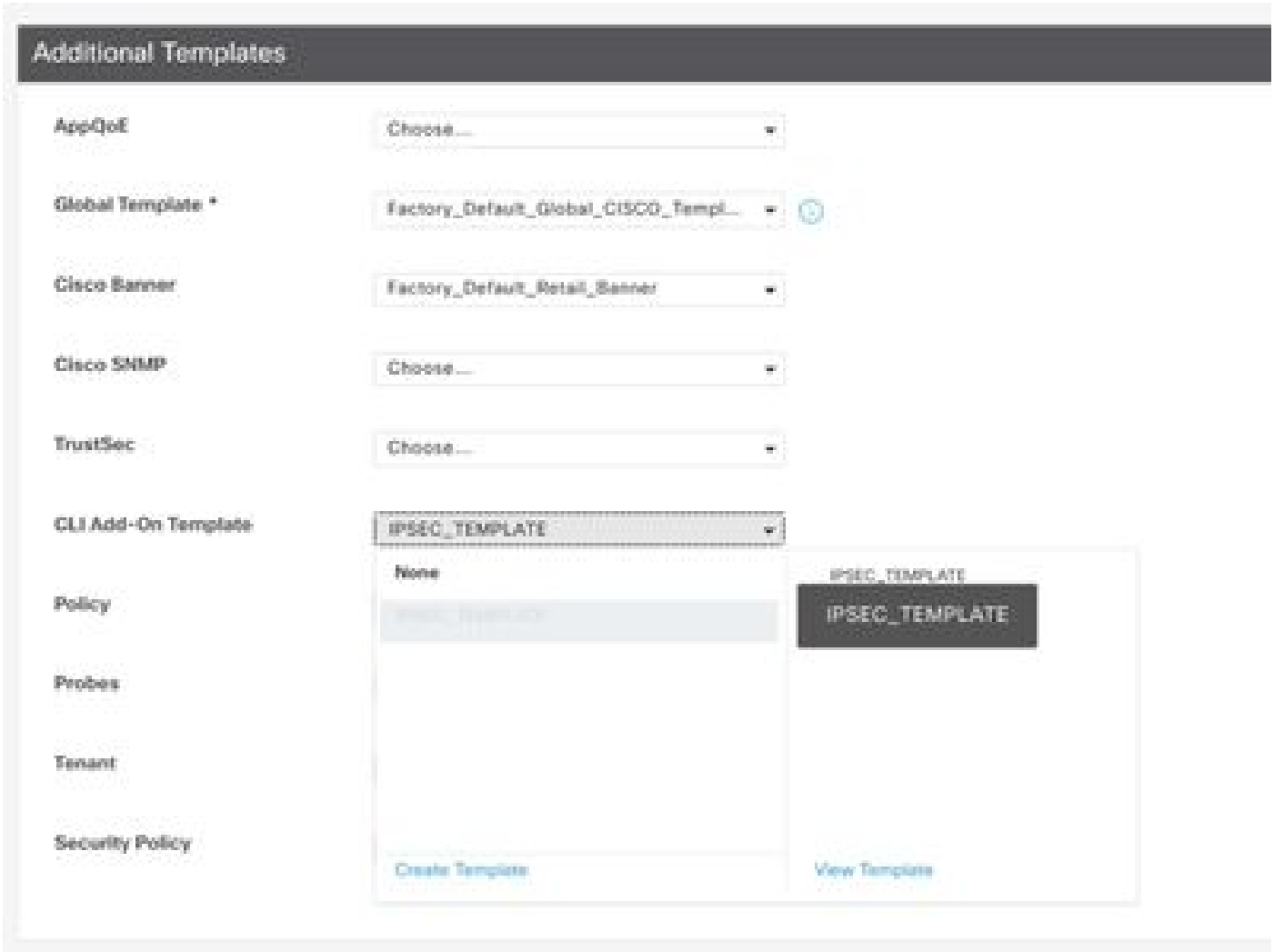
Passaggio 10. Scegliere il modello di dispositivo corretto e modificarlo nei 3 punti.



Passaggio 11. Passare a Modelli aggiuntivi.

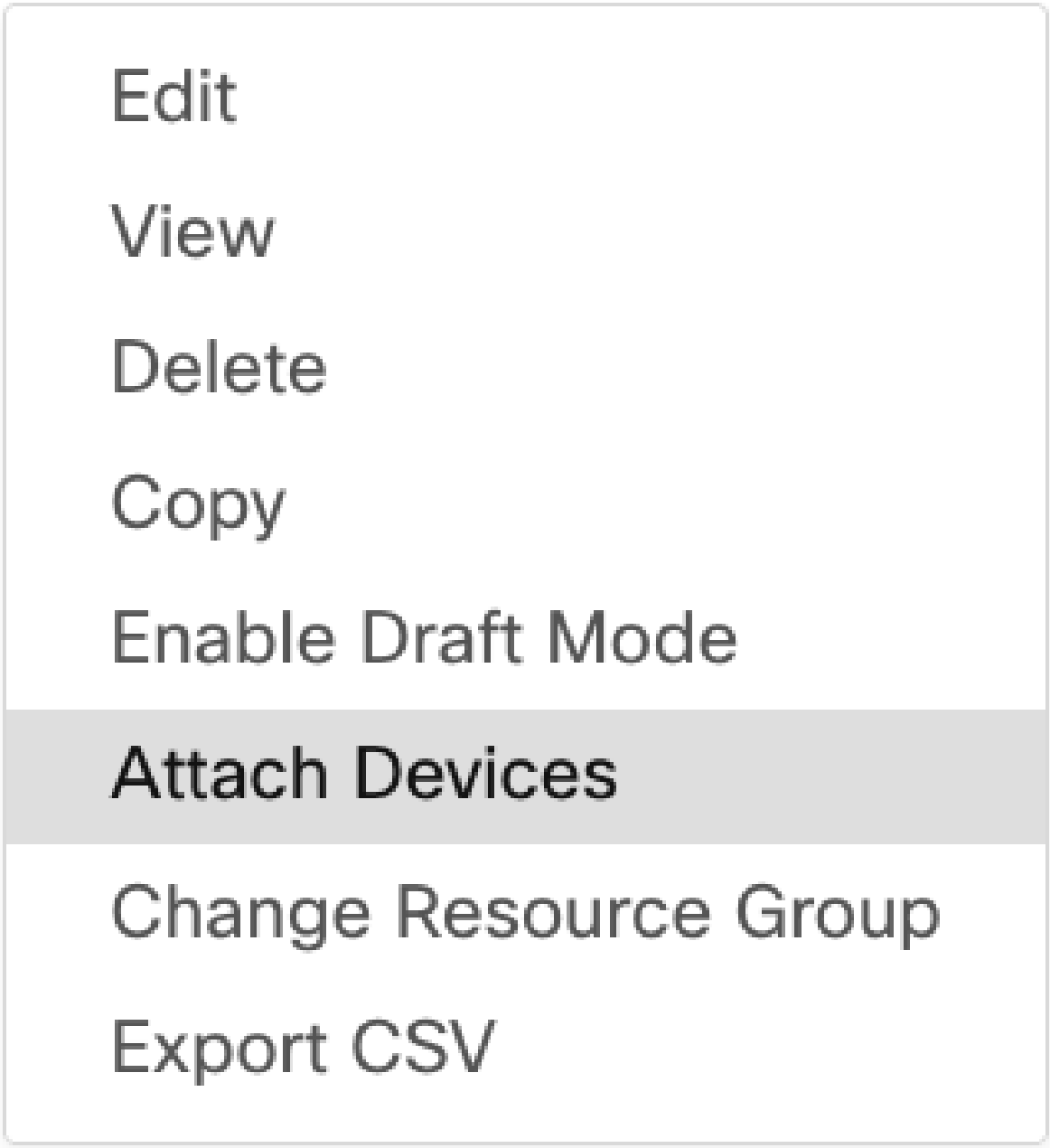


Passaggio 12. In CLI Add-On Template (Modello aggiuntivo CLI) scegliere il modello di funzionalità creato in precedenza.



Passaggio 13. Fare clic su Aggiorna.

Passaggio 14. Fare clic su Attach Devices (Allega dispositivi) da 3 punti e selezionare il router corretto su cui inviare il modello.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Eseguire il comando show ip interface brief per verificare lo stato del tunnel 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#
```

Risoluzione dei problemi

Eseguire il comando show crypto ikev2 session per visualizzare informazioni dettagliate sulle sessioni IKEv2 stabilite sul 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#
```

Eseguire il comando show crypto ipsec sa interface Tunnel100001 per visualizzare informazioni sulle associazioni di sicurezza 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#
```

Eseguire il comando show crypto ikev2 statistics per visualizzare le statistiche e i contatori relativi alle sessioni 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#
```

Eseguire il comando show crypto session per visualizzare le informazioni sulle sessioni di sicurezza attive sul dispositivo.

<#root>

```
cEdge#
```

show crypto session

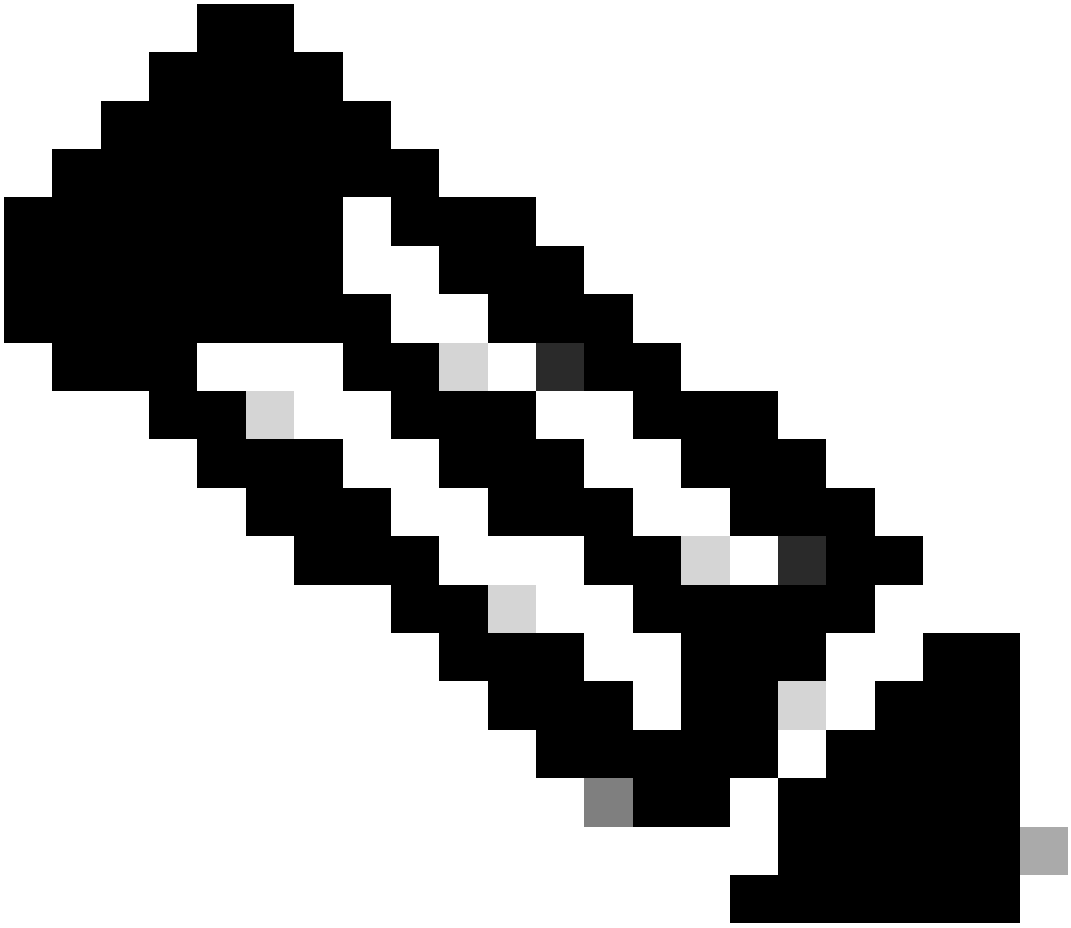
```
Crypto session current status

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
```

Per ottenere informazioni sulle perdite di pacchetti relative a IPSec nel processore pacchetti del dispositivo, è possibile eseguire:

show platform hardware qfp active feature ipsec datapath drops clear

mostra eliminazione statistiche attive qfp hardware della piattaforma

Per cancellare i contatori e le statistiche, è necessario anteporre questi comandi all'interfaccia del tunnel in modo da ottenere informazioni sulle perdite di pacchetti relative a IPsec in un percorso dati del processore pacchetti del dispositivo.



Nota: questi comandi possono essere eseguiti senza l'opzione clear. È importante sottolineare che i contatori di caduta sono storici.

<#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#

Dopo aver chiuso e non aver chiuso l'interfaccia del tunnel è possibile eseguire questi comandi per verificare se è stata eseguita una registrazione di nuove statistiche o contatori:

show ip interface brief | includere Tunnel100001

show platform hardware qfp active statistics drop

show platform hardware qfp active feature ipsec datapath drop

<#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#
```

Comandi utili

<#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

Informazioni correlate

Chiavi Pairwise IPsec

Guida alla configurazione della sicurezza di Cisco Catalyst SD-WAN, Cisco IOS® XE Catalyst SD-WAN release 17.x

Introduzione alla tecnologia Cisco IPsec

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).