在SD-WAN上配置帶C8000V的服務端IPSec隧道

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [元件](#)

[背景資訊](#)

[IPSEC配置的元件](#)

[設定](#)

- [CLI上的配置](#)
- [在vManage上的CLI附加模板上進行配置](#)

[驗證](#)

[疑難排解](#)

[有用的命令](#)

[相關資訊](#)

簡介

本文檔介紹如何在SD-WAN Cisco Edge路由器和VPN端點之間配置使用服務VRF的IPSec隧道。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- 網際網路通訊協定安全(IPSec)

元件

本檔案根據這些軟體和硬體版本：

- 思科邊緣路由器版本17.6.1
- SD-WAN vManage 20.9.3.2

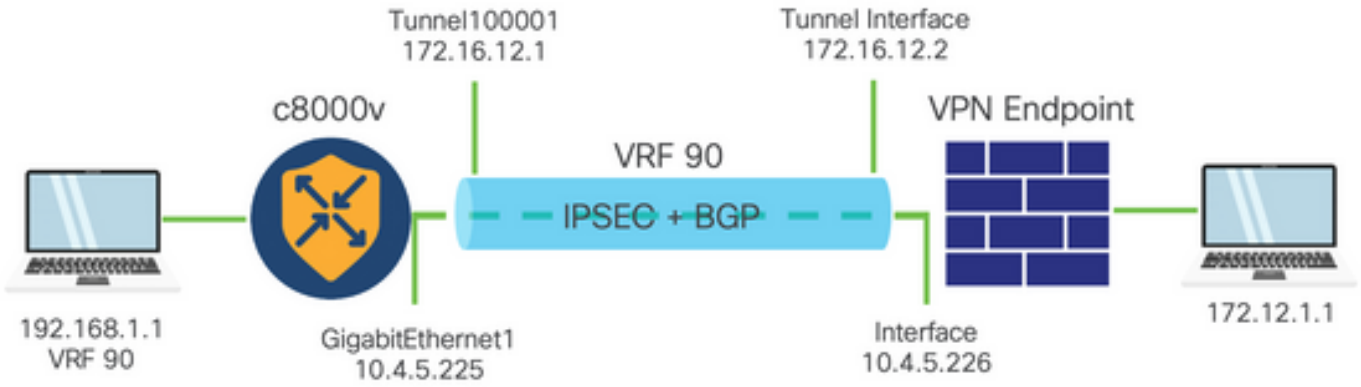
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

背景資訊包括本文檔的範圍、使用SD-WAN上的C8000v構建服務端IPSec隧道的可用性和優勢。

- 要在採用控制器管理模式的Cisco IOS® XE路由器與虛擬專用網路(VPN)端點之間的服務虛擬路由和轉發(VRF)中構建IPSec隧道，可保證公共廣域網(WAN)上的資料保密性和完整性。它還有助於公司專用網路的安全擴展，允許透過Internet進行遠端連線，同時保持高級別的安全性。
- 服務VRF可隔離流量，在多客戶端環境中或用於維護網路不同部分之間的分段時，流量尤其重要。總之，此配置增強了安全性和連通性。
- 本文認為邊界網關協定(BGP)是用於從SD-WAN服務VRF向VPN終端後面的網路傳輸網路的路由協定，反之亦然。
- BGP配置不在本文檔的討論範圍之內。
- 此VPN端點可以是防火牆、路由器或具有IPSec功能的任何型別的網路裝置，VPN端點的配置不在本文檔的討論範圍之內。
- 本文檔假定路由器已內建主動控制連線和服務VRF。

IPSEC配置的元件



第1階段網際網路金鑰交換(IKE)

IPSec配置過程的第1階段涉及安全引數的協商和隧道終端之間的身份驗證。這些步驟包括：

IKE配置

- 定義加密方案（演算法和金鑰長度）。
- 配置包括加密提議、生存時間和身份驗證的IKE策略。

配置遠端終端對等體

- 定義遠端的IP位址。
- 配置用於身份驗證的共用金鑰（預共用金鑰）。

第2階段(IPSec)配置

第2階段涉及隧道中流量的安全轉換和訪問規則的協商。這些步驟包括：

配置IPSec轉換集

- 定義提議的轉換集，包括加密演演算法與驗證。

配置IPSec策略

- 將轉換集與IPSec策略相關聯。

配置隧道介面

在IPSec隧道的兩端配置隧道介面。

- 將隧道介面與IPSec策略相關聯。

設定

CLI上的配置

步驟 1.定義加密方案。

<#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
```

步驟 2.配置包括建議資訊的IKE策略。

<#root>

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

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

步驟 3.定義遠端的IP位址。

<#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
```

步驟 4.配置用於身份驗證的共用金鑰（預共用金鑰）。

<#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)#
```

步驟 5.定義一個包括加密演算法和驗證的建議轉換集。

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

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

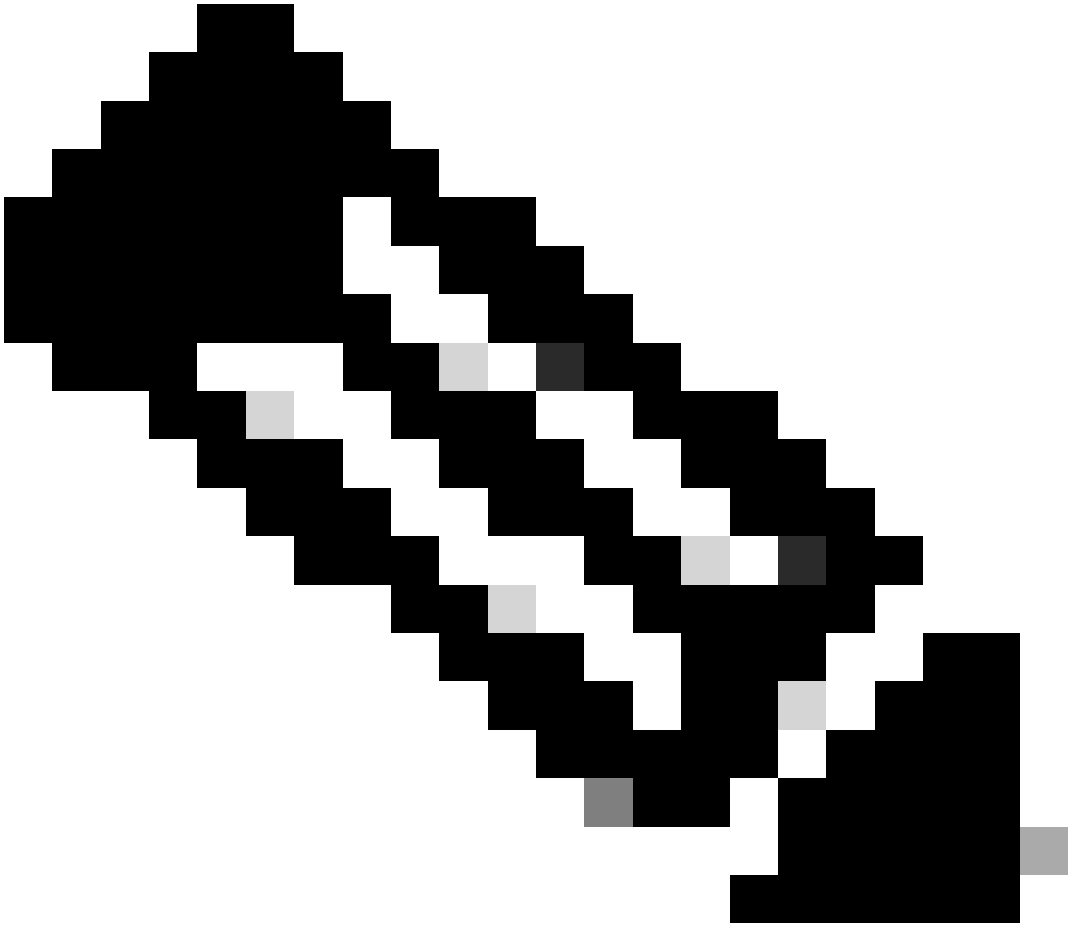
步驟 6.將轉換集與IPSec策略關聯。

```
<#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
```

步驟 7.建立介面隧道並將其與IPSec策略關聯。

```
<#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
```

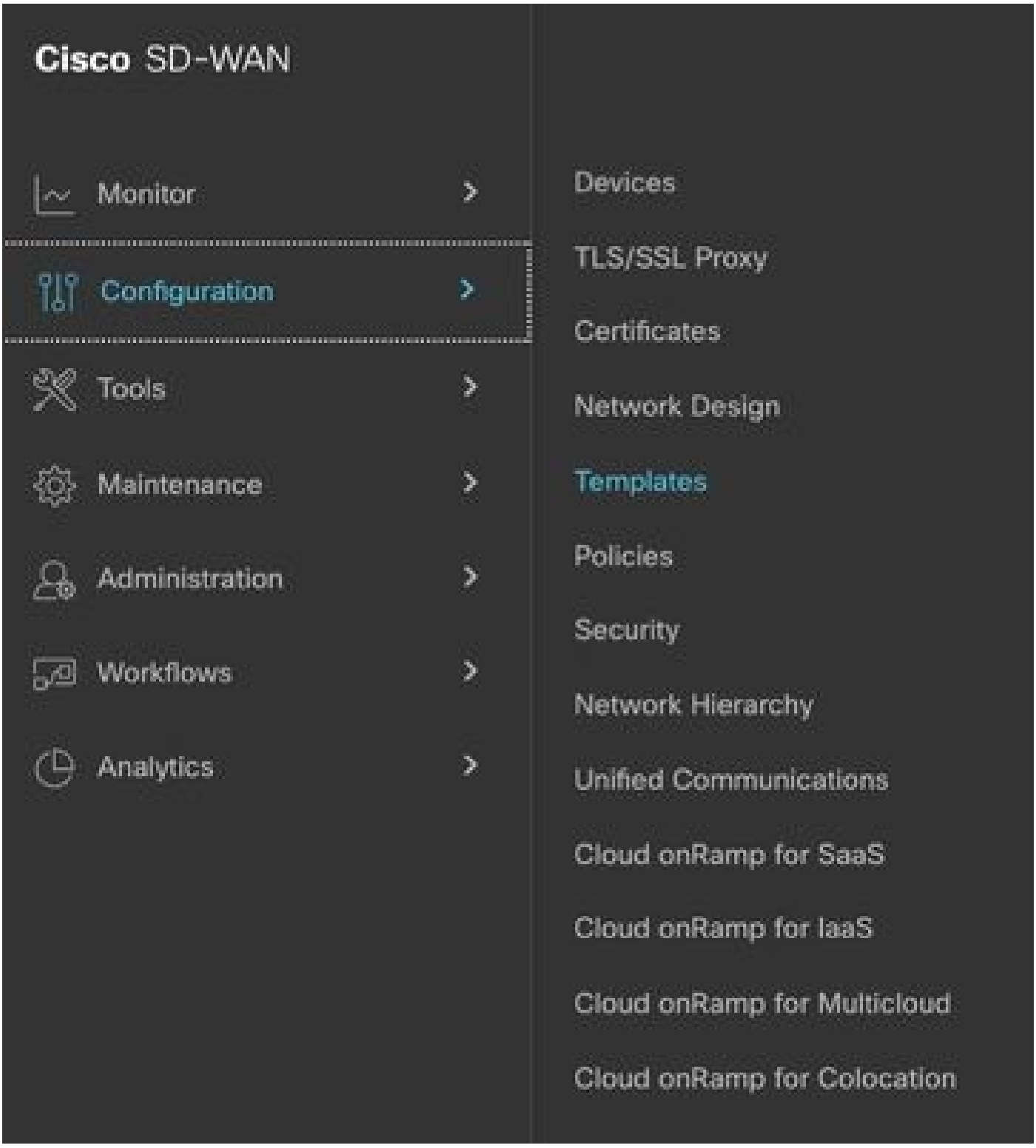
在vManage上的CLI附加模板上進行配置



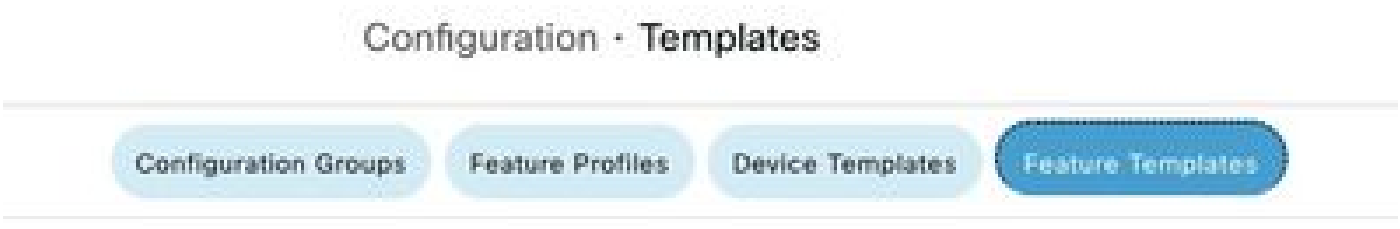
注意：此型別的配置只能透過CLI載入項模板增加。

步驟 1.導航到Cisco vManage並登入。

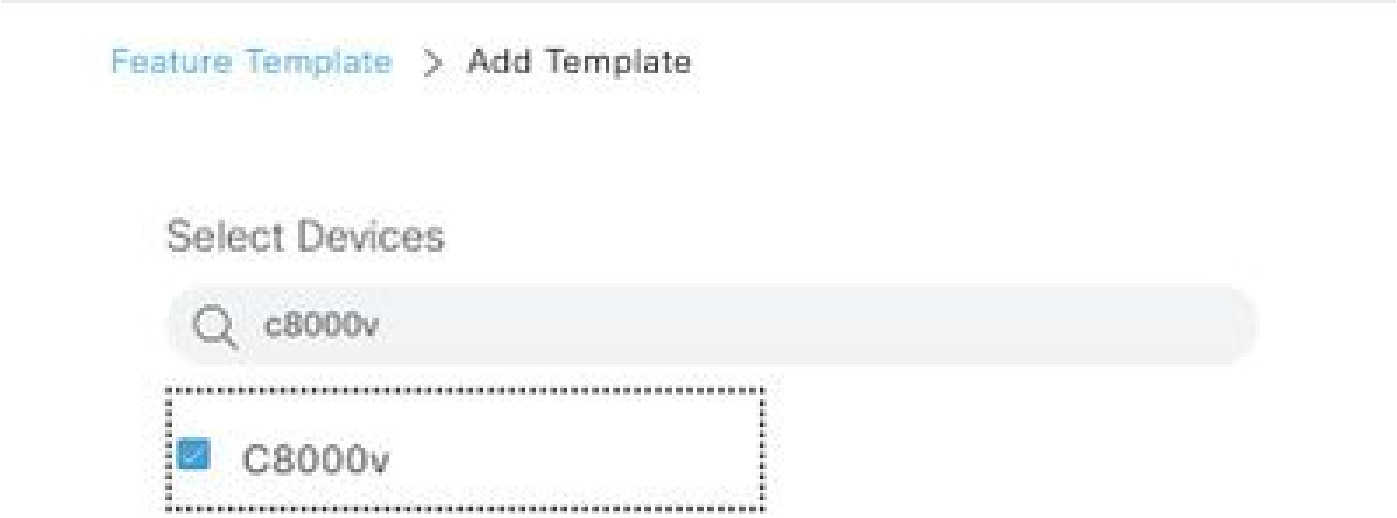
步驟 2.導航到配置>模板。



步驟 3.導航到功能模板>增加模板。

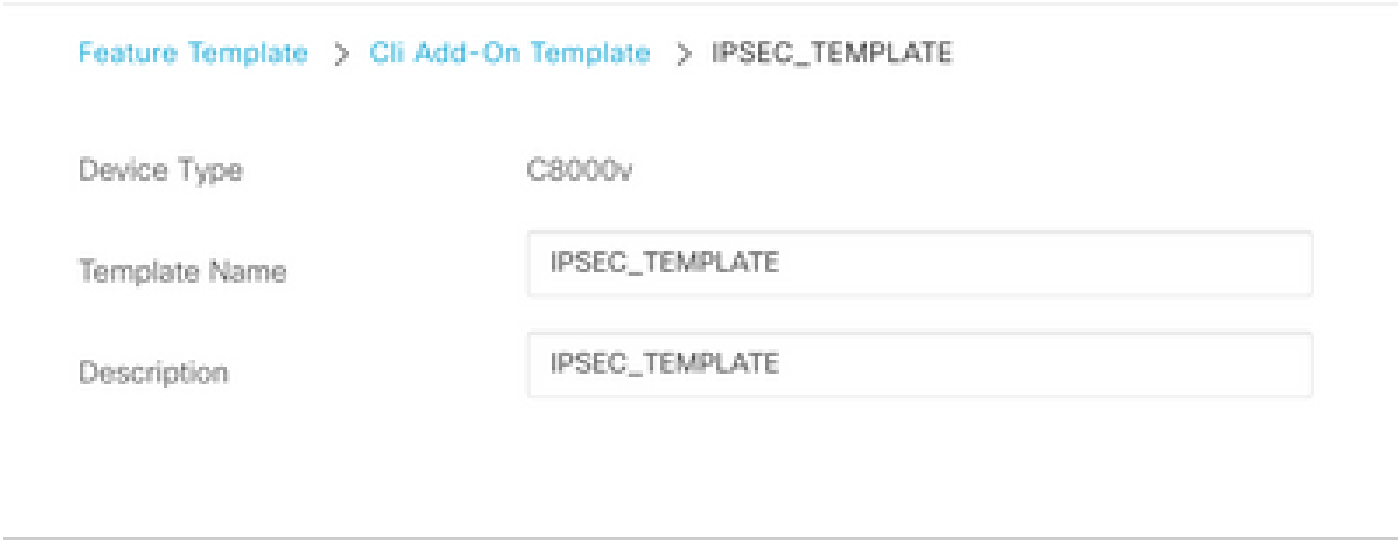


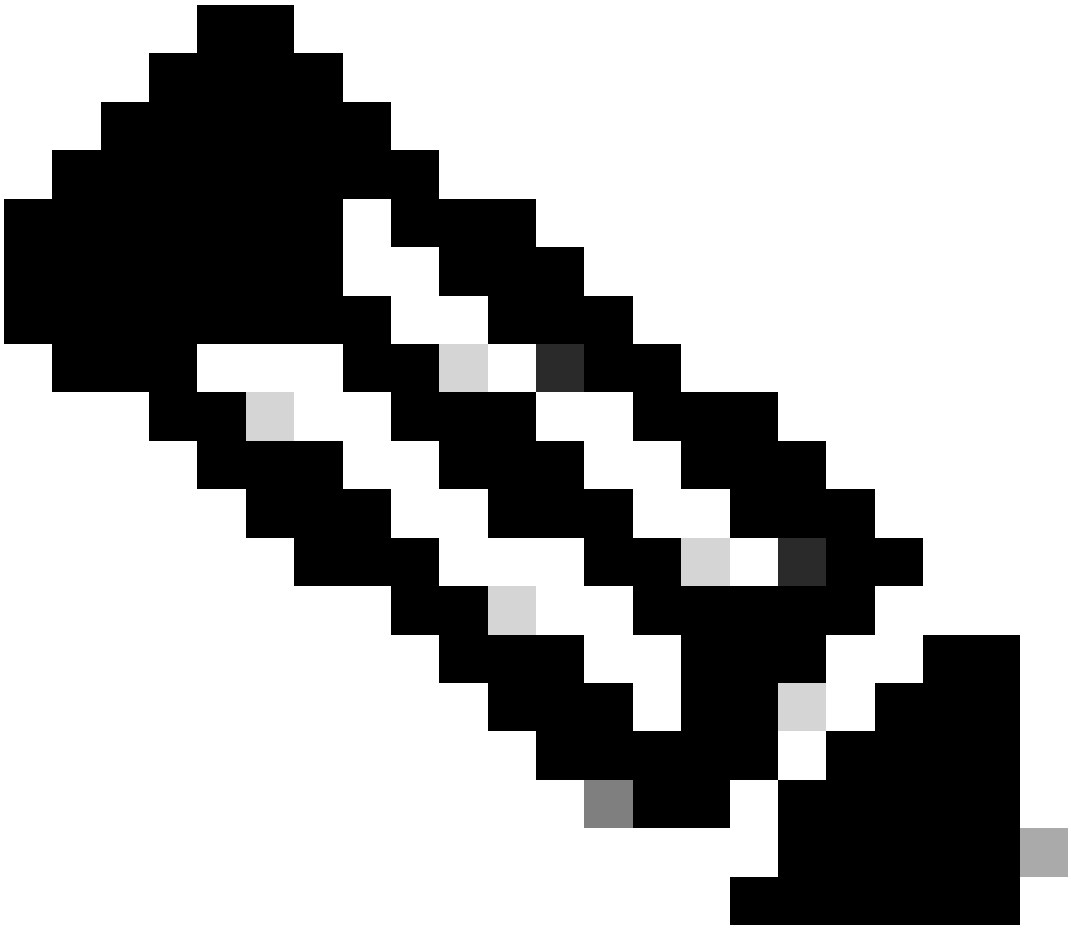
步驟 4.過濾型號並選擇c8000v路由器。



步驟 5.導航到其他模板，然後按一下Cli外掛模板。

步驟 6.增加模板名稱和說明。





注意：有關如何在CLI附加模組模板上建立變數的詳細資訊，請參閱CLI附加模組功能模板。

步驟 7.增加命令。

CLI CONFIGURATION

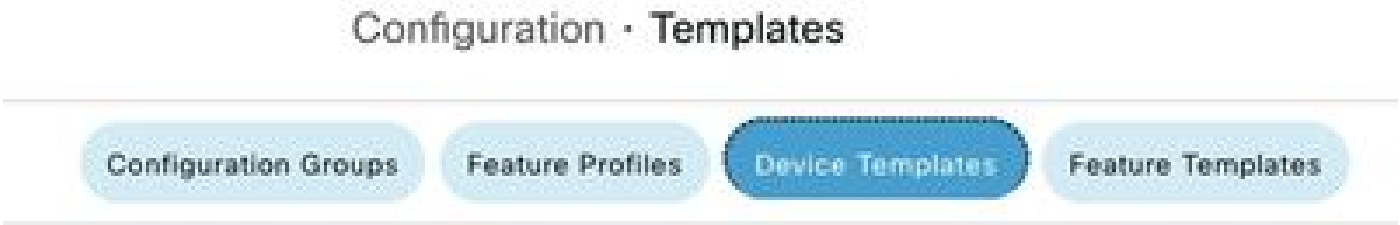
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key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

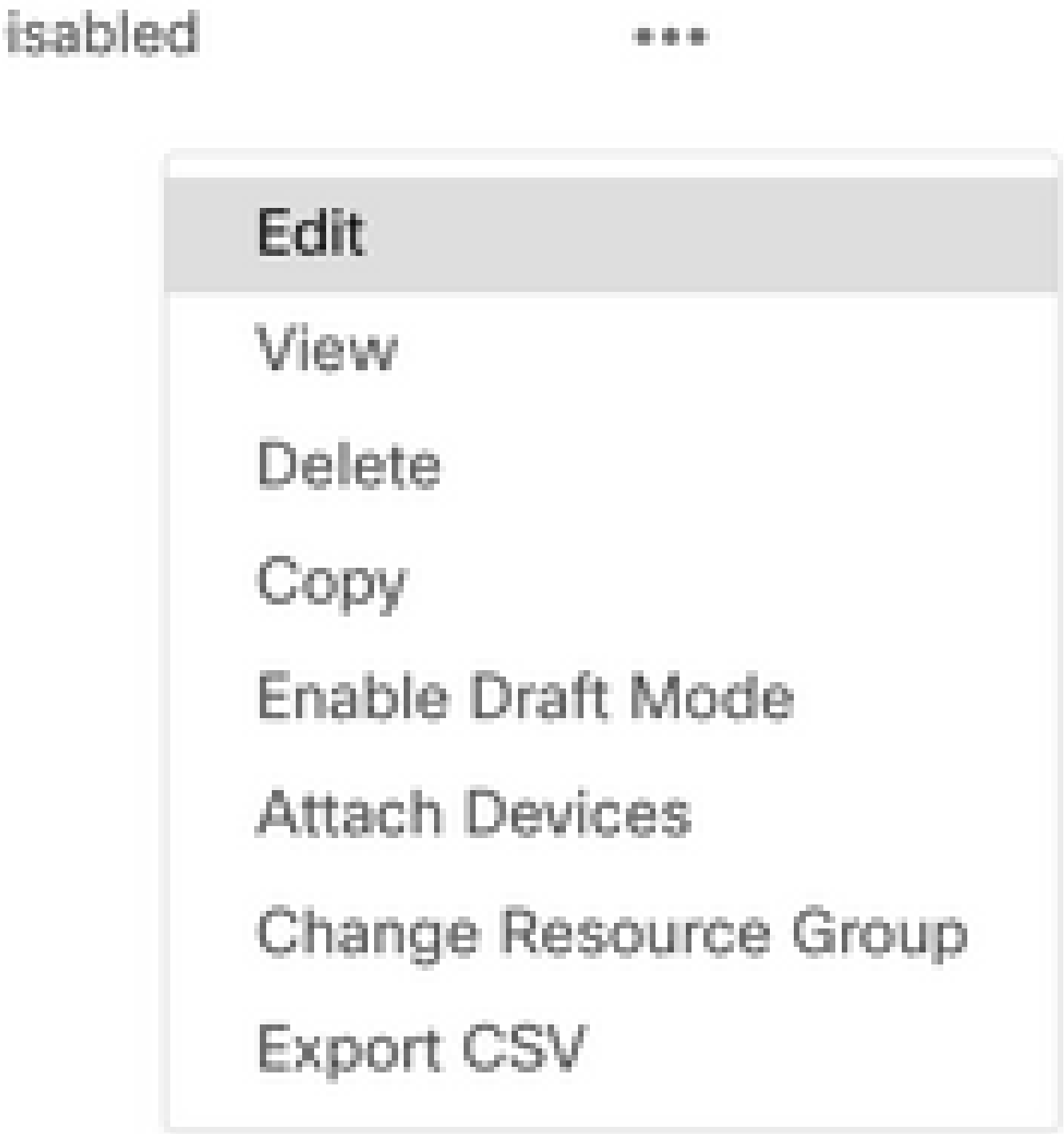
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

步驟 8.點選儲存。

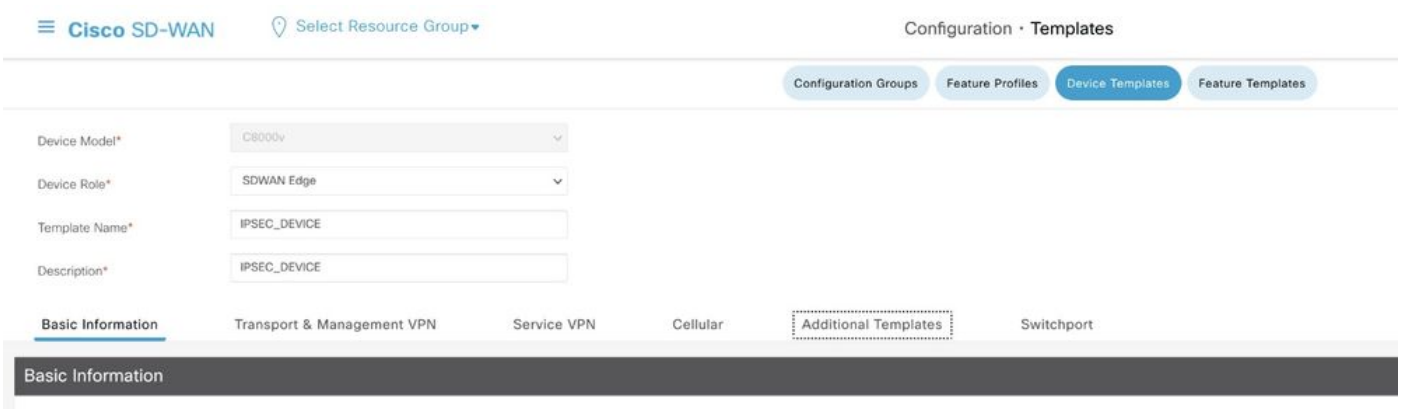
步驟 9.導航至裝置模板。



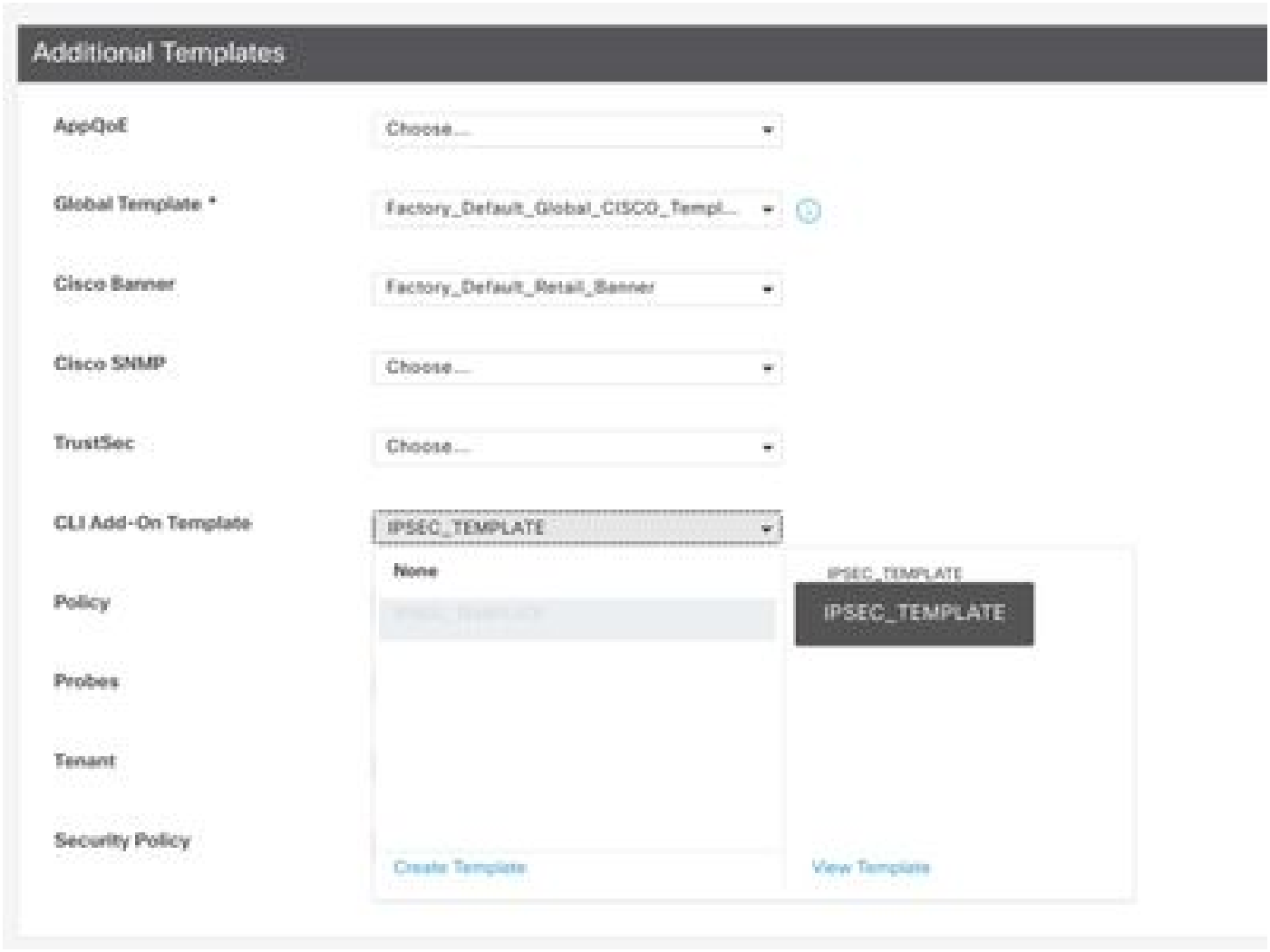
步驟 10.選擇正確的裝置模板並在3點上編輯。



步驟 11.切換作業選項至其他樣版。

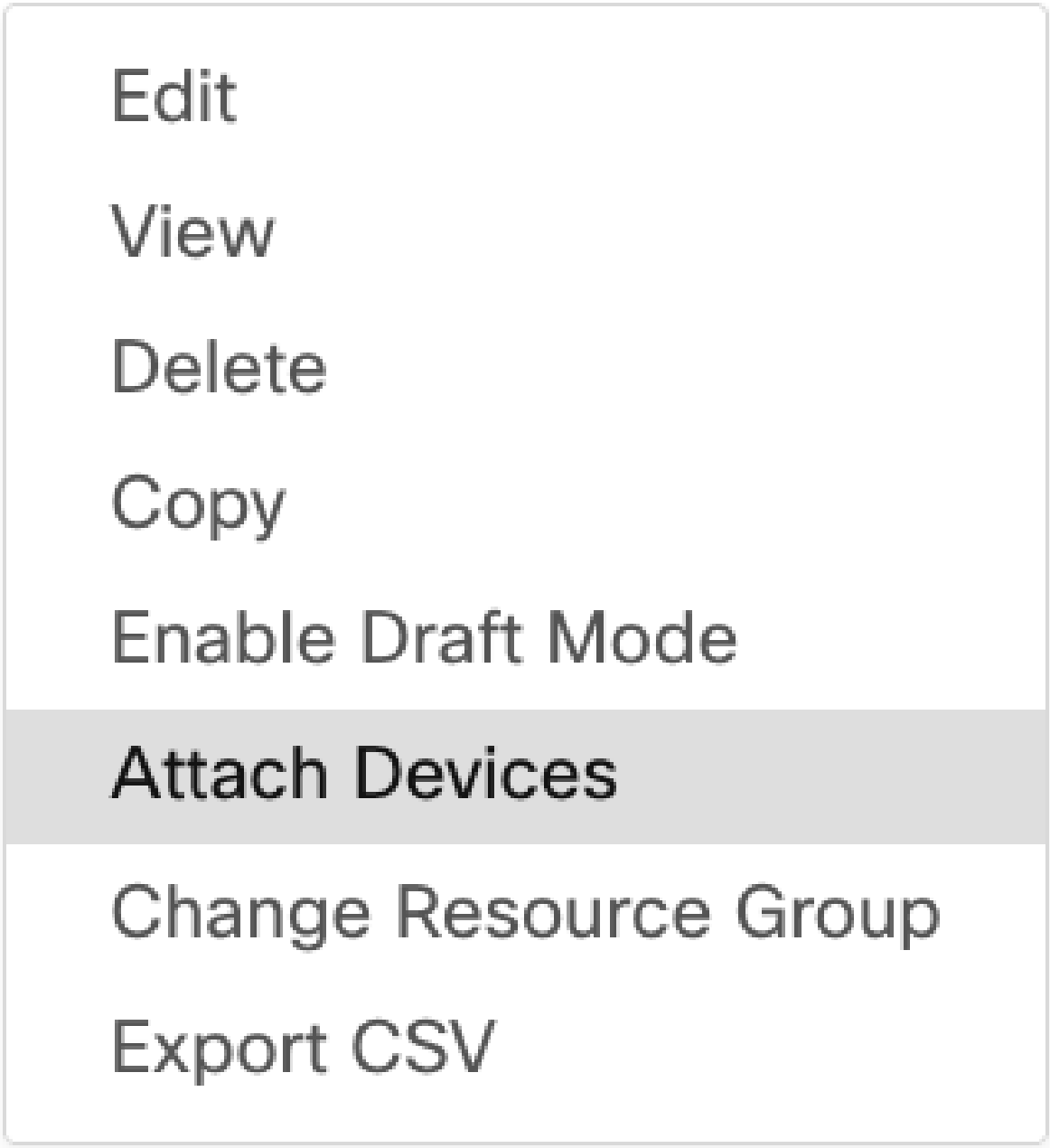


步驟 12.在CLI Add-On Template上，選擇先前建立的功能模板。



步驟 13.按一下Update。

步驟 14.點選3個點中的Attach Devices，然後選擇正確的路由器以推送模板。



驗證

使用本節內容，確認您的組態是否正常運作。

運行show ip interface brief命令以驗證IPSec隧道的狀態。

<#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#
```

疑難排解

運行show crypto ikev2 session命令以顯示有關在裝置上建立的IKEv2會話的詳細資訊。

<#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#
```

運行命令show crypto ipsec sa interface Tunnel100001以顯示有關IPSec安全關聯(SA)的資訊。

<#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#
```

運行命令show crypto ikev2 statistics以顯示與IKEv2會話有關的統計資訊和計數器。

<#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#
```

運行命令show crypto session顯示有關裝置上的活動安全會話的資訊。

<#root>

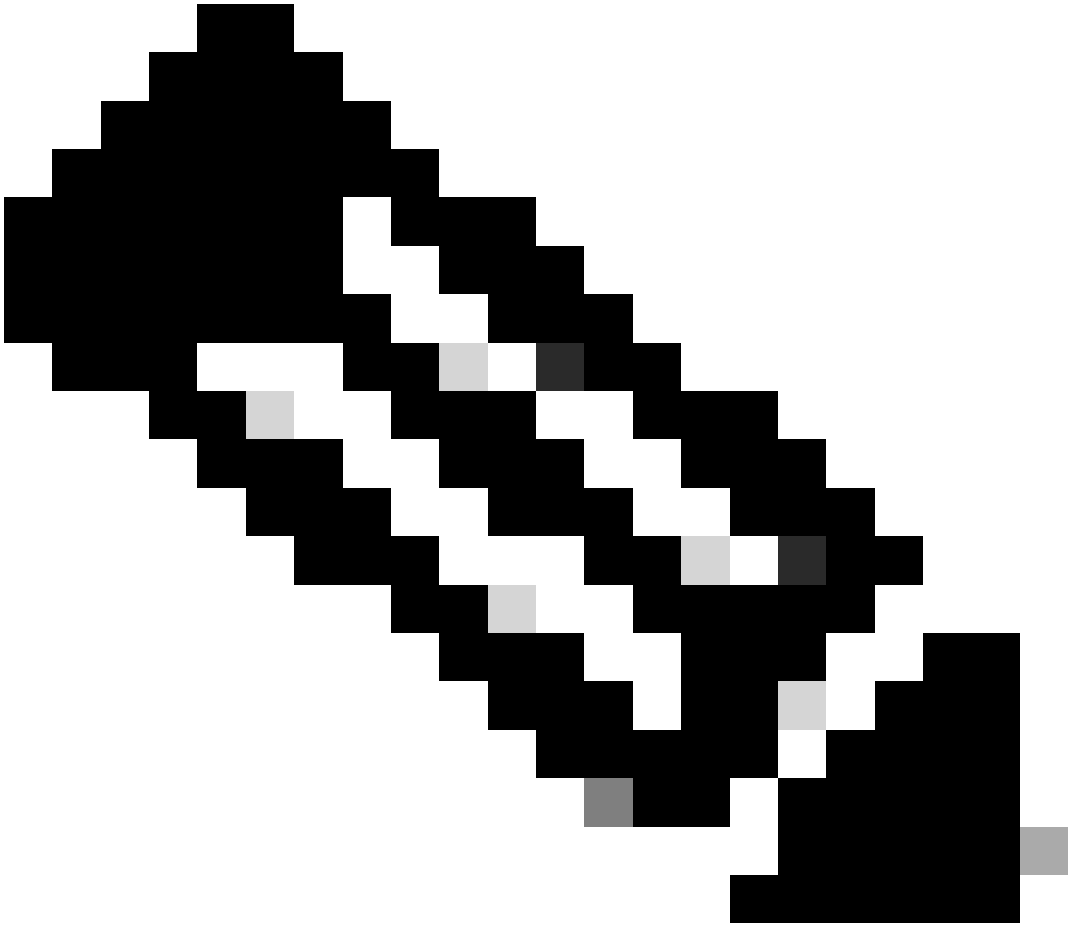
```
cEdge#

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
```

要獲取有關裝置資料包處理器中IPSec相關資料包丟棄的資訊，您可以運行：

show platform hardware qfp active feature ipsec datapath drops clear

show platform hardware qfp active statistics drop clear

這些命令需要在關閉之前執行，而no shut則透過隧道介面清除計數器和統計資訊，這有助於獲取有關裝置資料包處理器資料路徑中IPsec相關資料包丟棄的資訊。



注意：這些指令可以在不清除選項的情況下執行。請務必強調丟棄計數器是歷史計數器。

<#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#
```

在shut and no shut the Tunnel Interface後，您可以運行以下命令以檢視是否有新統計資訊或計數器註冊：

show ip interface brief | 包括隧道100001

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#

有用的命令

<#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

相關資訊

IPsec成對金鑰

Cisco Catalyst SD-WAN安全配置指南，Cisco IOS® XE Catalyst SD-WAN版本17.x

Cisco IPsec技術簡介

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。