Configure Service Side IPSec Tunnel with a C8000V on SD-WAN

Contents

Introduction

This document describes how to configure an IPSec tunnel between a SD-WAN Cisco Edge Router and a VPN Endpoint with service VRF.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-defined Wide Area Network (SD-WAN)
- Internet Protocol Security (IPSec)

Components

This document is based on these software and hardware versions:

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

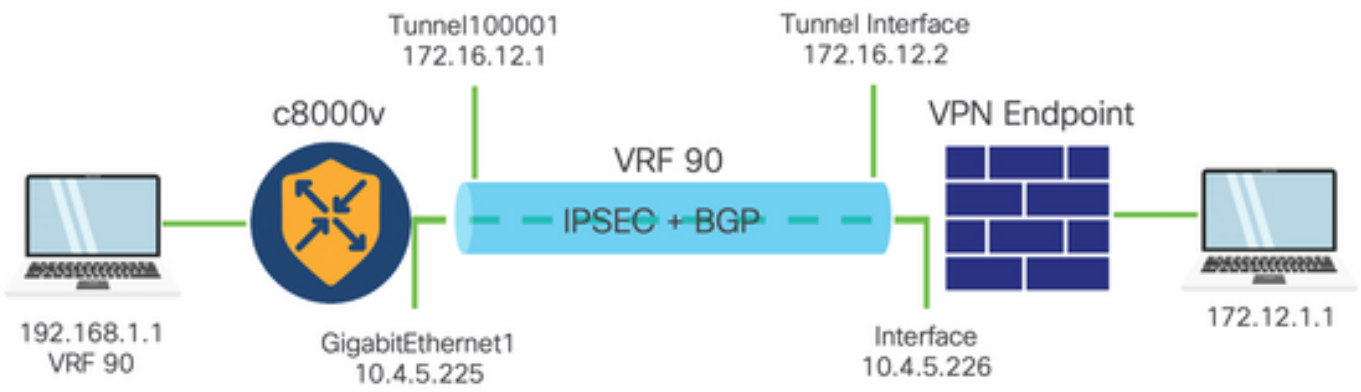
The information in this document was created from the devices in a specific lab environment. All the devices in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Background Information includes the scope of this document, the usability and the benefits of build a Service Side IPSec Tunnel with a C8000v on SD-WAN.

- To build an IPSec tunnel in a service Virtual Routing and Forwarding (VRF) between a Cisco IOS® XE router on controller-manage mode and a Virtual Private Network (VPN) Endpoint guarantees data confidentiality and integrity over the public Wide Area Network (WAN). It also facilitates the secure extension of the companies private networks and allow remote connections over the Internet while maintain a high level of security.
- The service VRF isolates traffic, which is particularly valuable in multi-client environments or for maintain segmentation between different parts of the network. In summary, this configuration enhances security and connectivity.
- This document considers that Border Gateway Protocol (BGP) is the routing protocol used to communicate the networks from the SD-WAN service VRF to the network behind the VPN Endpoint and vice versa.
- The BGP configuration is out of the scope of this document.
- This VPN Endpoint can be a Firewall, a router or any type of network device that has IPSec capabilities, the configuration of the VPN Endpoint is out of the scope of this document.
- This document assumes that the Router is already onboard with active control connections and service VRF.

Components of IPSEC Configuration



Phase 1 Internet Key Exchange (IKE)

Phase 1 of the IPSec configuration process involves negotiation of the security parameters and authentication between tunnel endpoints. These steps include:

IKE Configuration

- Define an encryption proposal (algorithm and key length).
- Configure an IKE policy that includes encryption proposal, time to live and authentication.

Configure remote end peers

- Define the IP address of the remote end.
- Configure shared key (pre-shared key) for authentication.

Phase 2 (IPSec) Configuration

Phase 2 involves negotiation of the security transformations and access rules for traffic flow through the tunnel. These steps include:

Configure IPSec Transformation Sets

- Define a proposed transform-set that includes the encryption algorithm and authentication.

Configure an IPSec policy

- Associate the transform-set with an IPSec policy.

Configure Tunnel Interfaces

Configure tunnel interfaces on both ends of the IPSec tunnel.

- Associate the tunnel interfaces with the IPSec policies.

Configure

Configuration on CLI

Step 1. Define an encryption proposal.

<#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
```

Step 2. Configure an IKE policy that includes proposal information.

<#root>

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

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

Step 3. Define the IP address of the remote end.

```
<#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
```

Step 4. Configure shared key (pre-shared key) for authentication.

```
<#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)#
```

Step 5. Define a proposed **transform-set** that includes the encryption algorithm and authentication.

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

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

Step 6. Associate the **transform-set** with an IPSec policy.

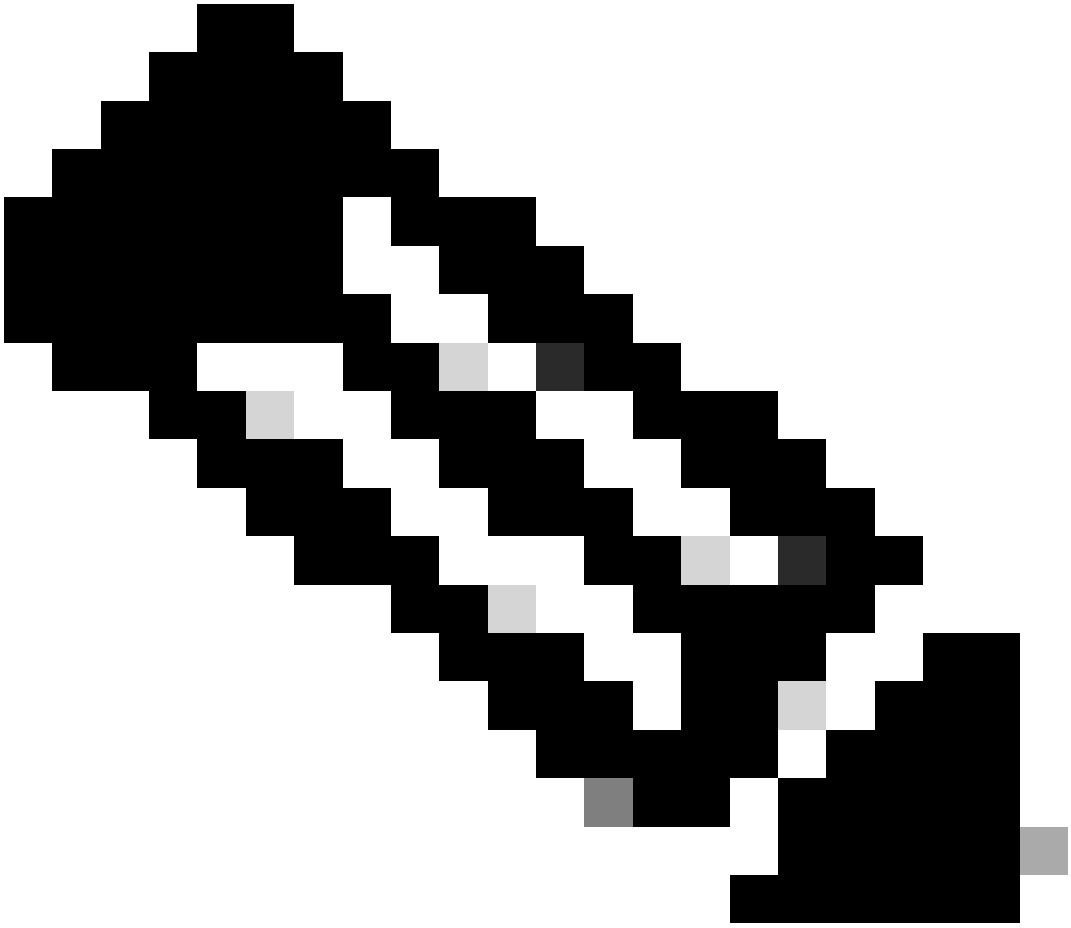
```
<#root>
cEdge(config)#
crypto ipsec profile if-ipsec1-ipsec-profile

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
```

Step 7. Create the interface tunnel and associate it with the IPSec policies.

<#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
```

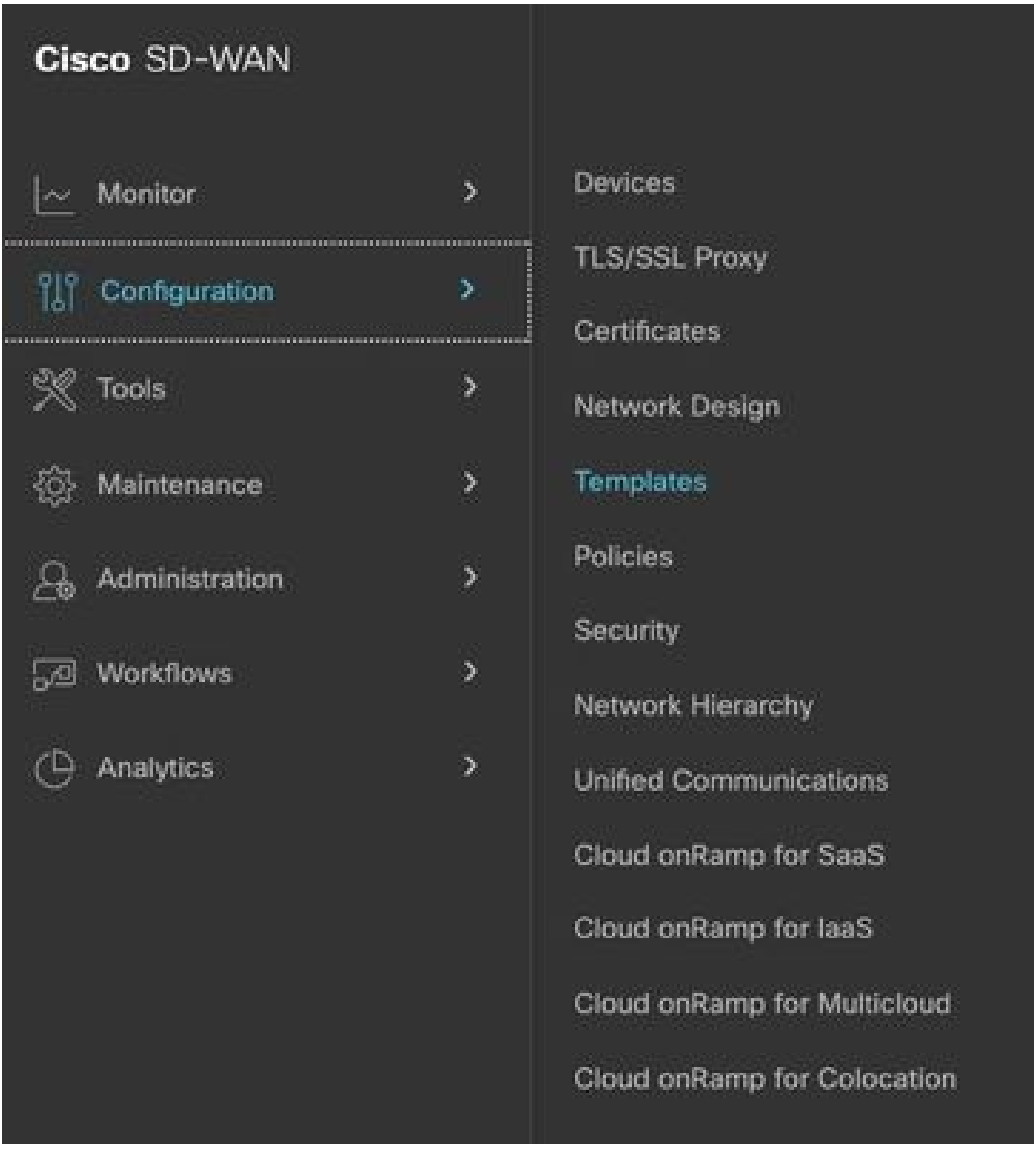
Configuration on a CLI Add-On Template on the vManage



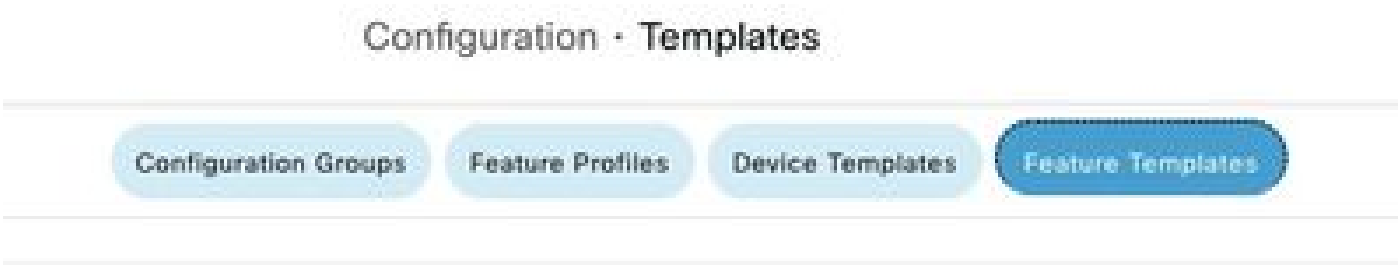
Note: This type of configuration can only be added via CLI Add-on template.

Step 1. Navigate to the **Cisco vManage** and log in.

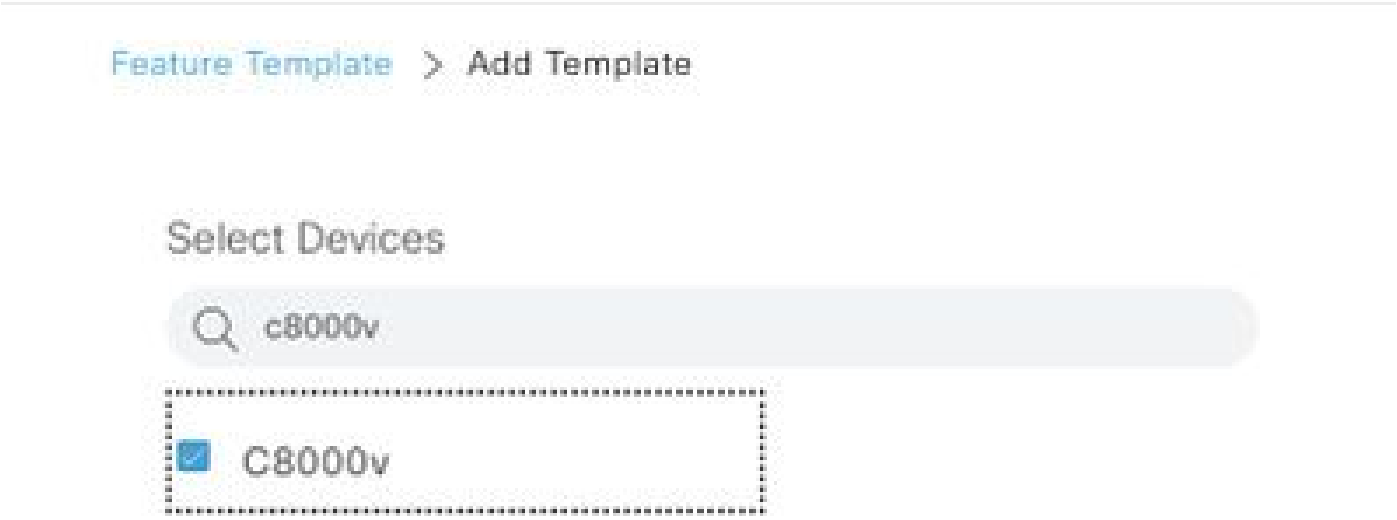
Step 2. Navigate to **Configuration > Templates.**



Step 3. Navigate to **Feature Templates > Add Template.**

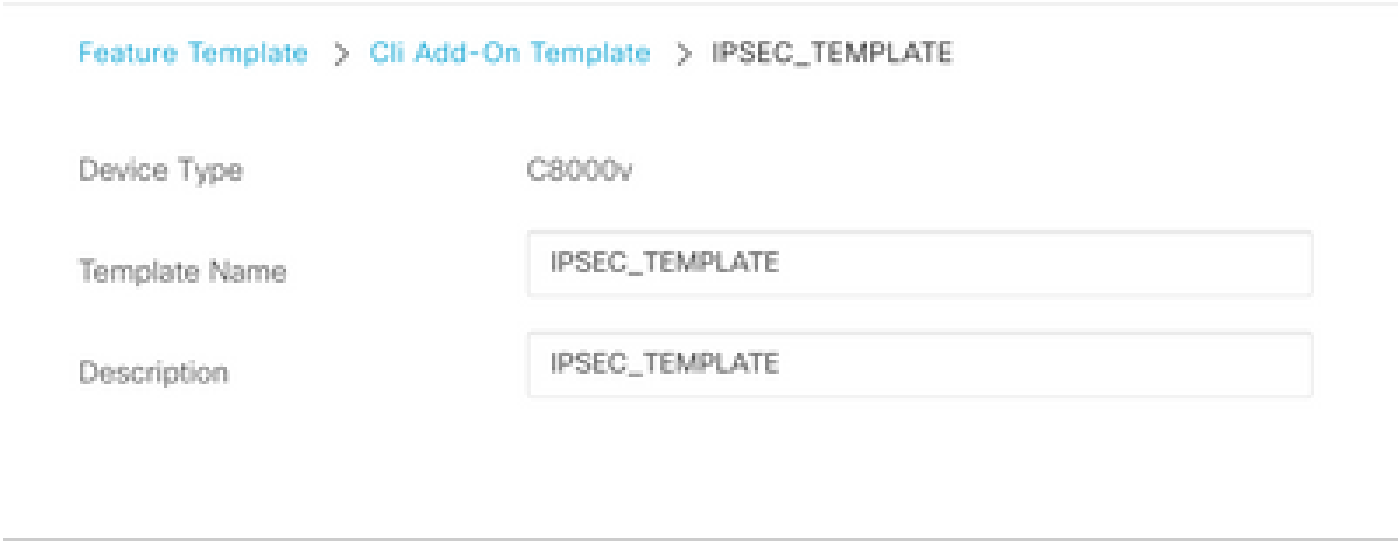


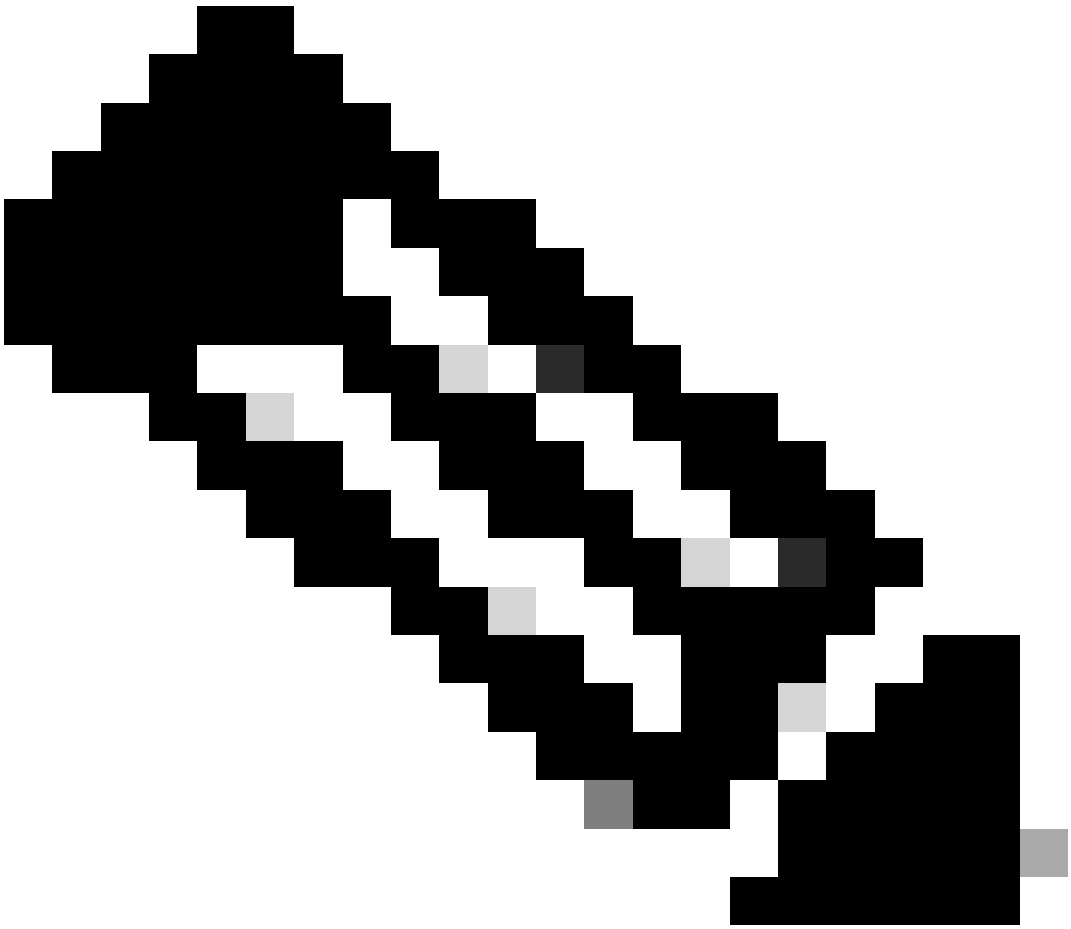
Step 4. Filter the model and choose the c8000v router.



Step 5. Navigate to **Other Templates** and click on **Cli Add-On Template.**

Step 6. Add a **Template Name** and a **Description.**





Note: For more information about how to create variables on a CLI Add-On Template please refer to CLI Add-On Feature Templates.

Step 7. Add the commands.

CLI CONFIGURATION

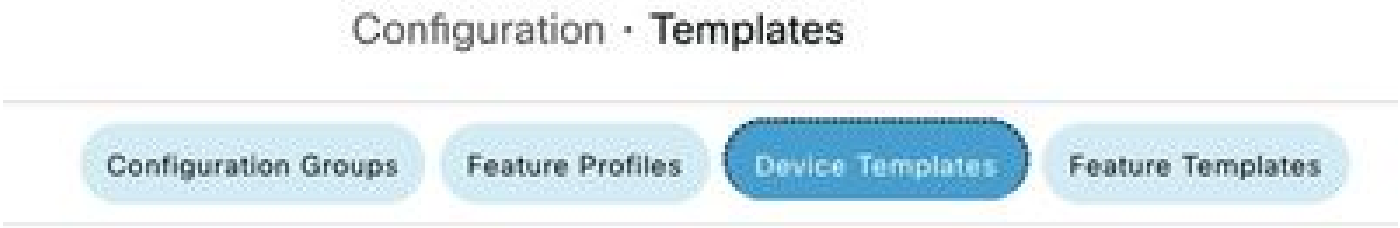
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key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

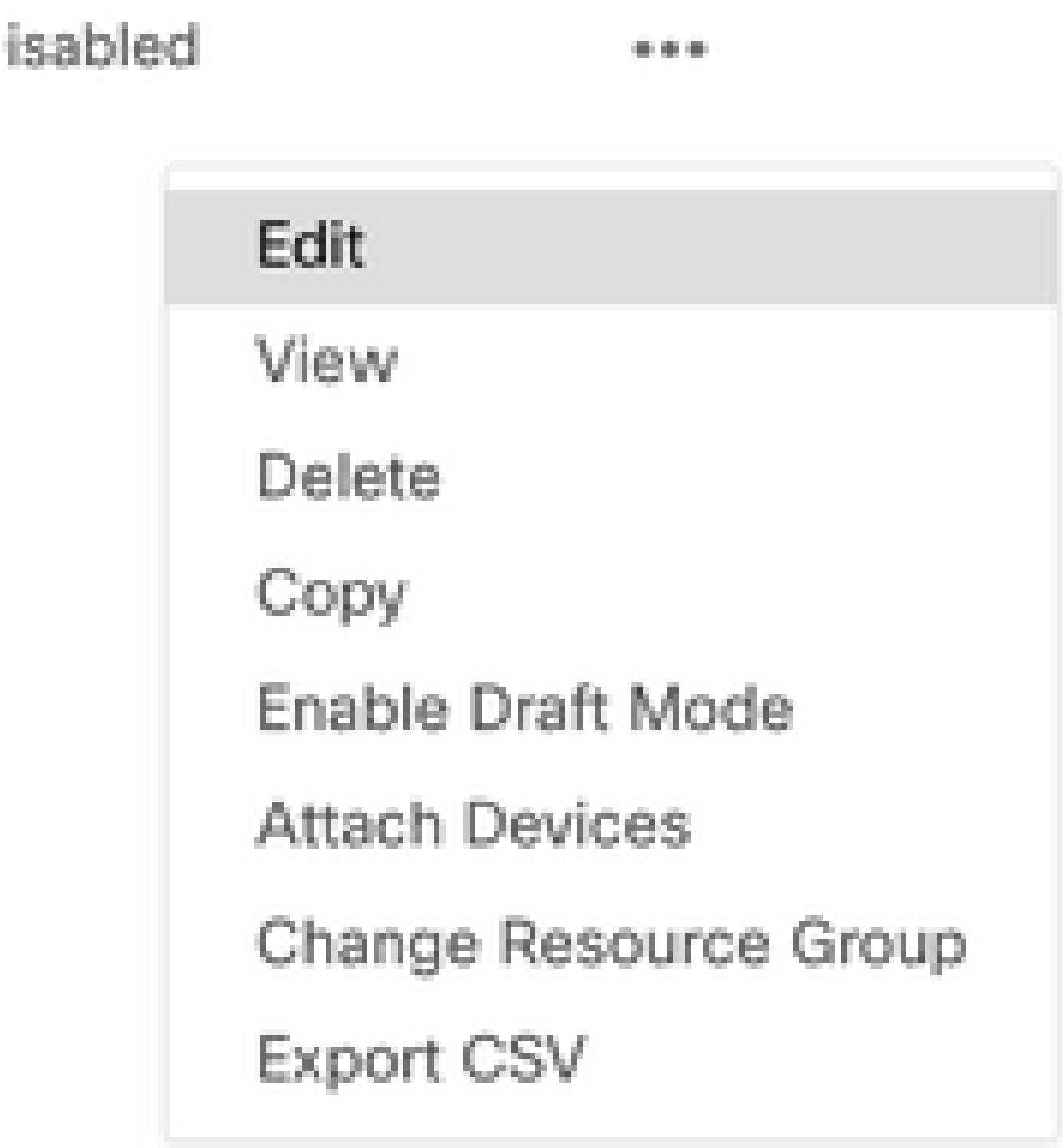
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

Step 8. Click on **Save.**

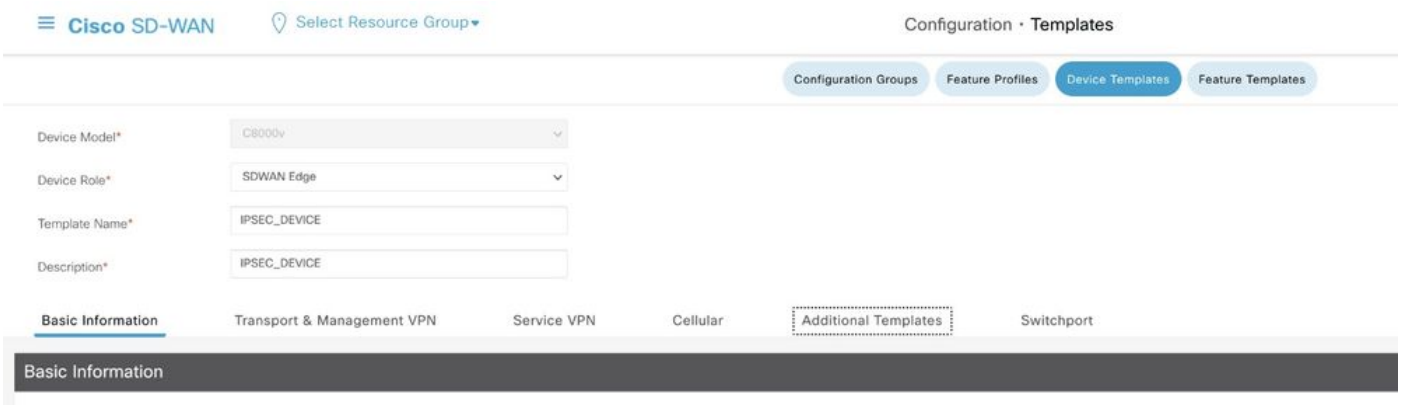
Step 9. Navigate to **Device Templates.**



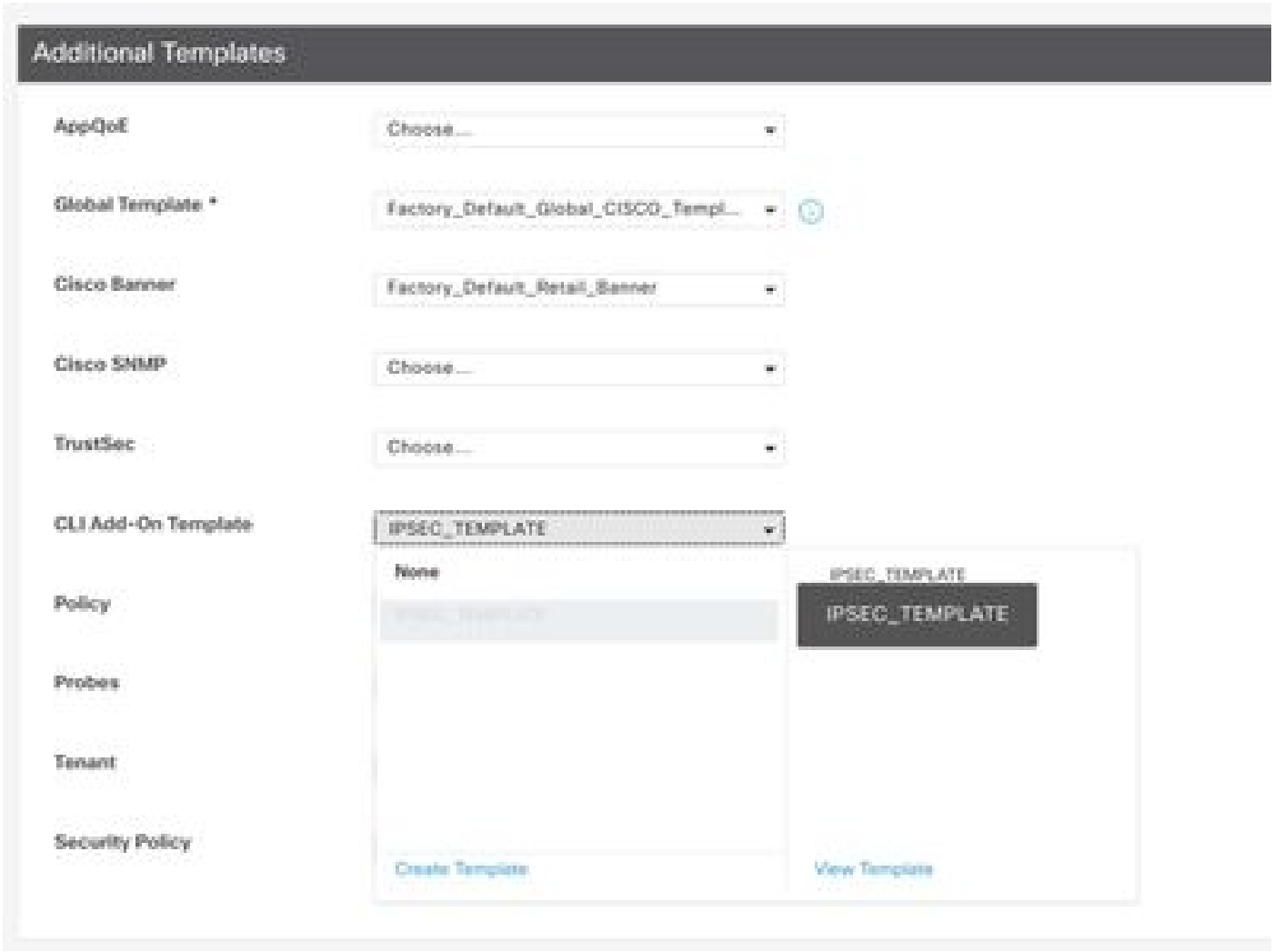
Step 10. Choose the correct Device Template and **Edit** it on the 3 dots.



Step 11. Navigate to **Additional Templates.**

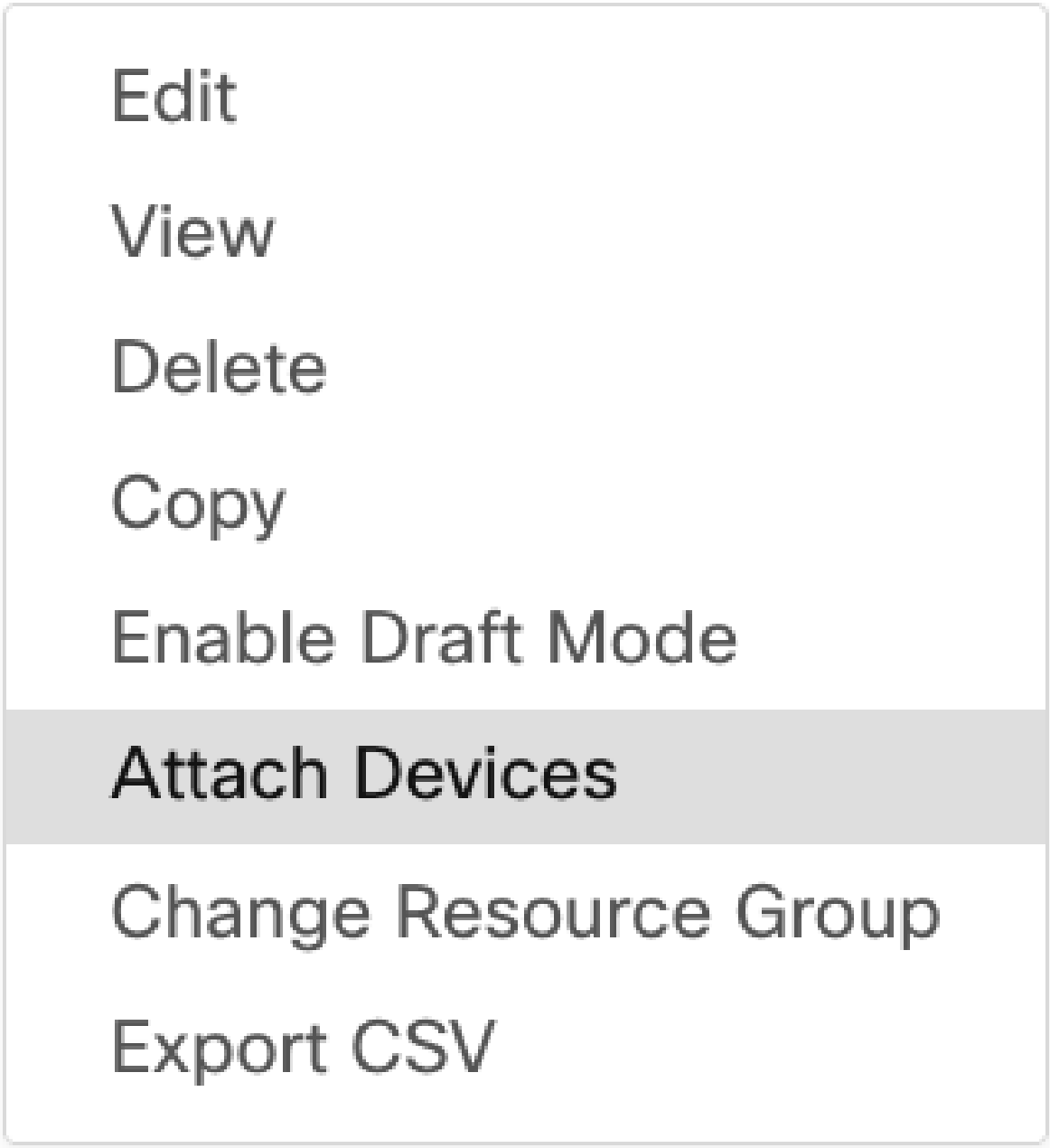


Step 12. On **CLI Add-On Template** choose the previously created Feature Template.



Step 13. Click on **Update.**

Step 14. Click on **Attach Devices** from 3 dots and select the correct router to push the template to.



Verify

Use this section to confirm that your configuration works properly.

Run the **show ip interface brief** command to verify the status of the IPSec tunnel.

```
<#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

Run the **show crypto ikev2 session** command to display detailed information about the IKEv2 sessions established on the device.

```
<#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#
```

Run the command **show crypto ipsec sa interface Tunnel100001** to display information about IPSec Security Associations (SAs).

```
<#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#
```

Run the command **show crypto ikev2 statistics** to display statistics and counters related to IKEv2 sessions.

```
<#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#
```

Run the command **show crypto session** to display information about active security sessions on the device.

<#root>

```
cEdge#
```

show crypto session

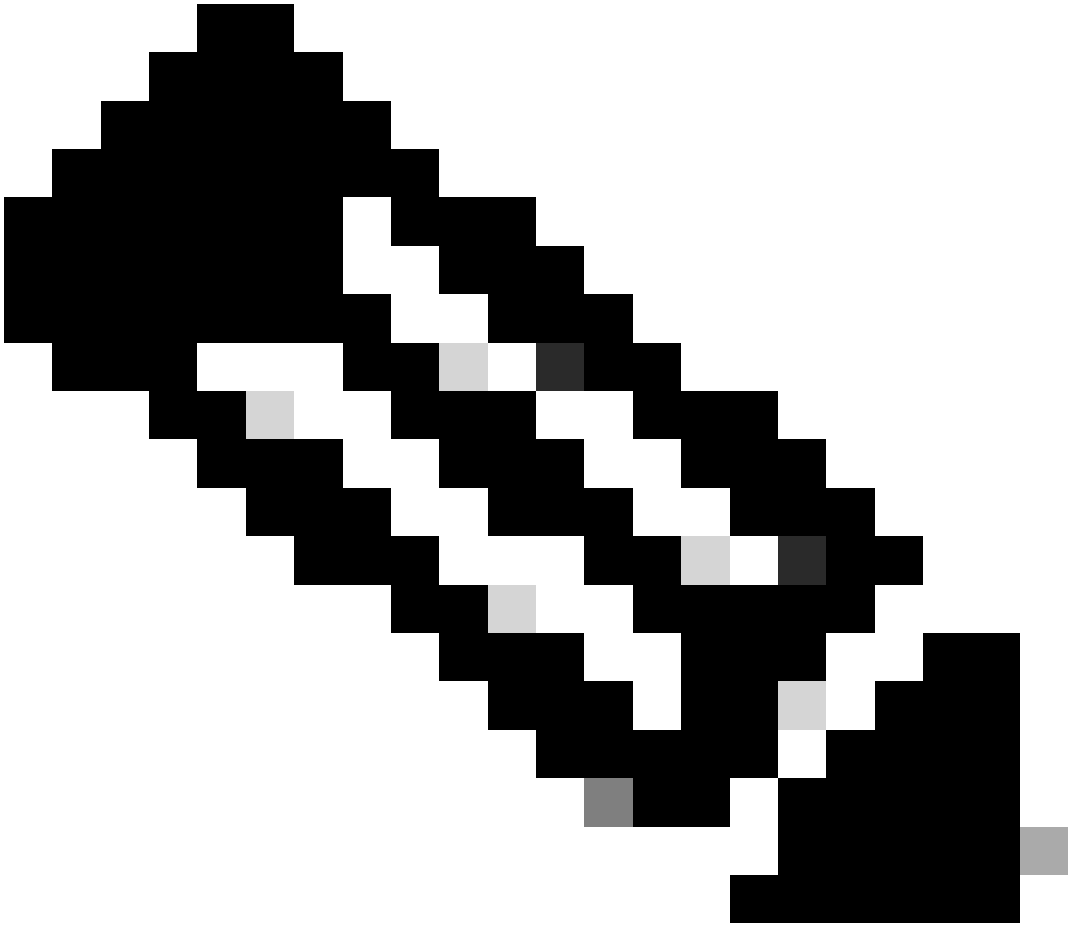
```
Crypto session current status

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
```

In order to obtain information about IPSec-related packet drops in the device packet processor you can run:

show platform hardware qfp active feature ipsec datapath drops clear

show platform hardware qfp active statistics drop clear

These commands needs to be put before to shut and no shut the Tunnel interface to clear the counters and statistics, this can help to obtain information about IPsec-related packet drops in a device packet processor datapath.



Note: These commands can be run without the option clear. It is important to highlight that the drop counters are historical.

<#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#
```

After shut and no shut the **Tunnel Interface** you can run these commands to see if there was a registration of new statistics or counters:

show ip interface brief | include 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#

Useful Commands

<#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

Related Information

IPsec Pairwise Keys

Cisco Catalyst SD-WAN Security Configuration Guide, Cisco IOS® XE Catalyst SD-WAN Release 17.x

Introduction to Cisco IPsec Technology