在SD-WAN上配置带C8000V的服务端IPSec隧道

目录

简介

本文档介绍如何使用service VRF在SD-WAN Cisco Edge路由器和VPN终端之间配置IPSec隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科软件定义的广域网(SD-WAN)
- 互联网协议安全(IPSec)

组件

本文档基于以下软件和硬件版本：

- Cisco Edge路由器版本17.6.1
- SD-WAN vManage 20.9.3.2

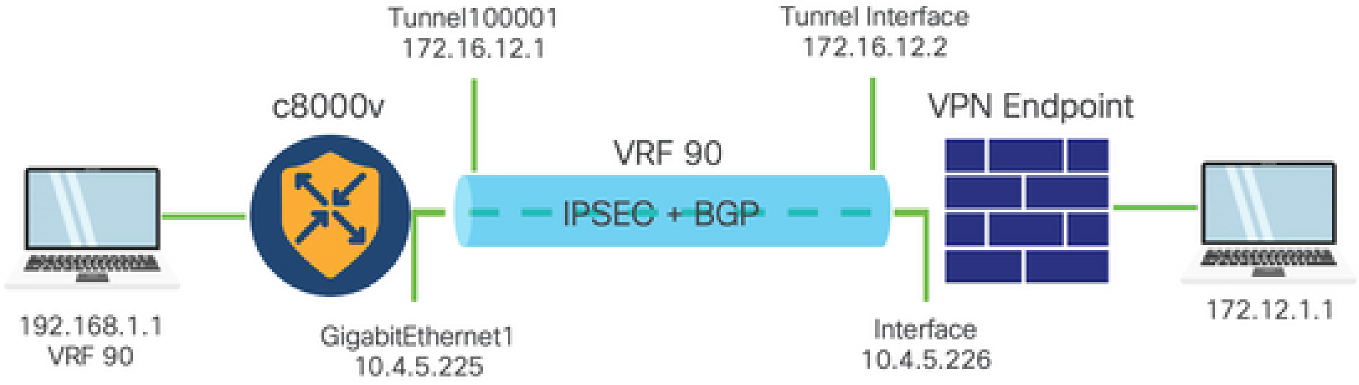
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中的所有设备均以清除（默认）配置开头。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

背景信息包括本文档的范围、在SD-WAN上使用C8000v构建服务端IPSec隧道的可用性和优点。

- 要在控制器管理模式的Cisco IOS® XE路由器与虚拟专用网络(VPN)终端之间构建服务虚拟路由和转发(VRF)中的IPSec隧道，可以确保公共广域网(WAN)上的数据保密性和完整性。它还有助于企业专用网络的安全扩展，允许通过Internet进行远程连接，同时保持高级别的安全性。
- 服务VRF可隔离流量，这对于多客户端环境或维护网络不同部分之间的分段尤为重要。总之，此配置增强了安全性和连接性。
- 本文档认为边界网关协议(BGP)是用于将网络从SD-WAN服务VRF通信到VPN终端后面的网络的路由协议，反之亦然。
- BGP配置不在本文档的讨论范围之内。
- 此VPN端点可以是防火墙、路由器或具有IPSec功能的任何类型的网络设备，VPN端点的配置不在本文档的讨论范围之内。
- 本文档假设路由器已随附主动控制连接和服务VRF。

IPSEC配置的组件



第1阶段互联网密钥交换(IKE)

IPSec配置过程的第1阶段涉及安全参数的协商和隧道端点之间的身份验证。这些步骤包括：

IKE 配置

- 定义加密方案（算法和密钥长度）。
- 配置包括加密提议、生存时间和身份验证的IKE策略。

配置远程终端对等体

- 定义远程端的IP地址。
- 配置身份验证的共享密钥（预共享密钥）。

第2阶段(IPSec)配置

第2阶段涉及通过隧道的数据流的安全转换和访问规则的协商。这些步骤包括：

配置IPSec转换集

- 定义建议的转换集，包括加密算法和身份验证。

配置IPSec策略

- 将转换集与IPSec策略相关联。

配置隧道接口

在IPSec隧道的两端配置隧道接口。

- 将隧道接口与IPSec策略相关联。

配置

CLI上的配置

步骤1:定义加密方案。

```
<#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
```

第二步：配置包含建议信息的IKE策略。

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

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

第三步：定义远程端的IP地址。

```
<#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
```

第四步：配置身份验证的共享密钥（预共享密钥）。

```
<#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)#
```

第五步：定义包含加密算法和身份验证的建议转换集。

```
<#root>

cEdge(config)#

crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256

cEdge(cfg-crypto-trans)#

mode tunnel
```

第六步：将转换集与IPSec策略相关联。

```
<#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
```

步骤 7.创建接口隧道并将其与IPSec策略相关联。

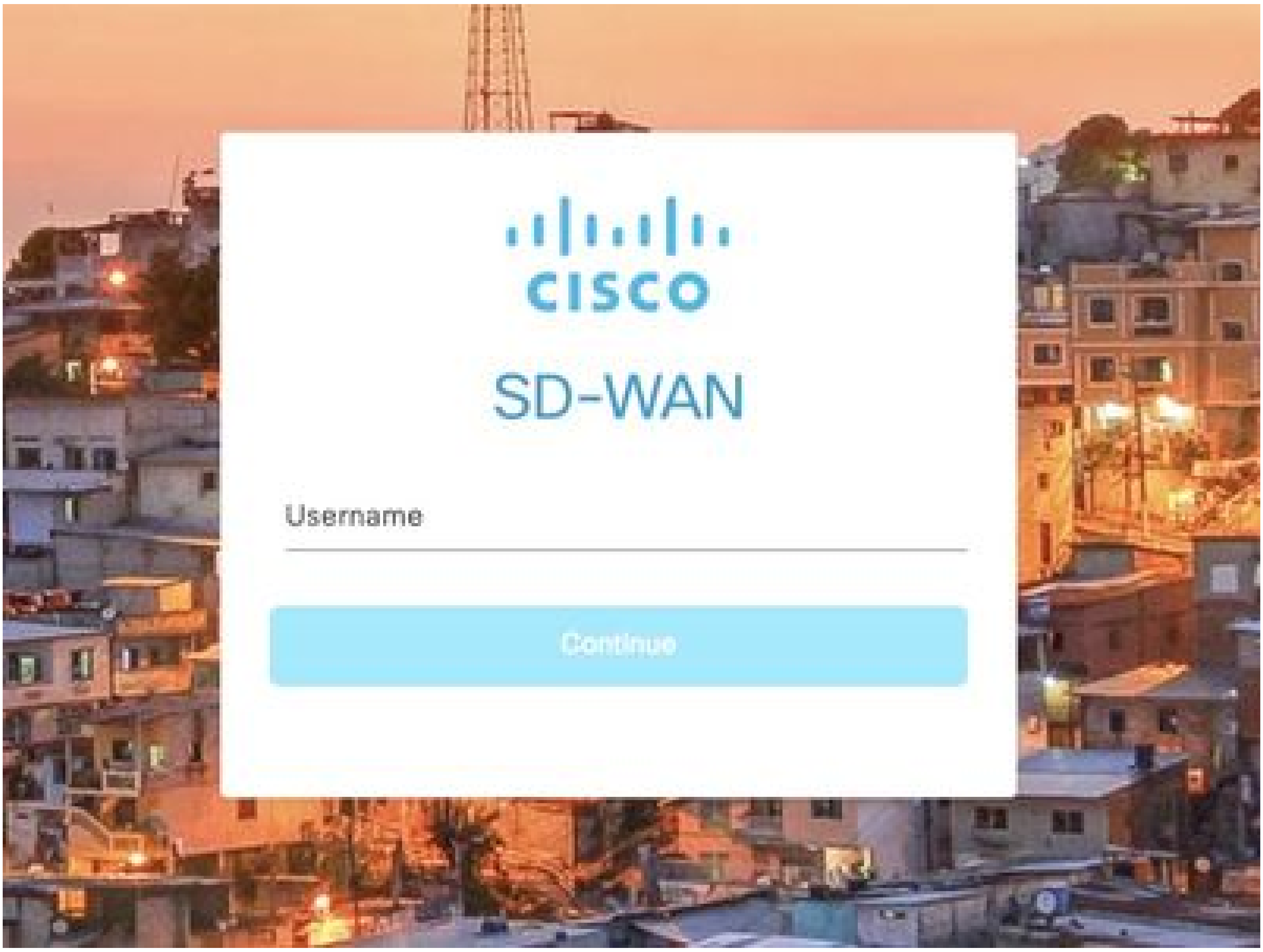
<#root>

```
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
```

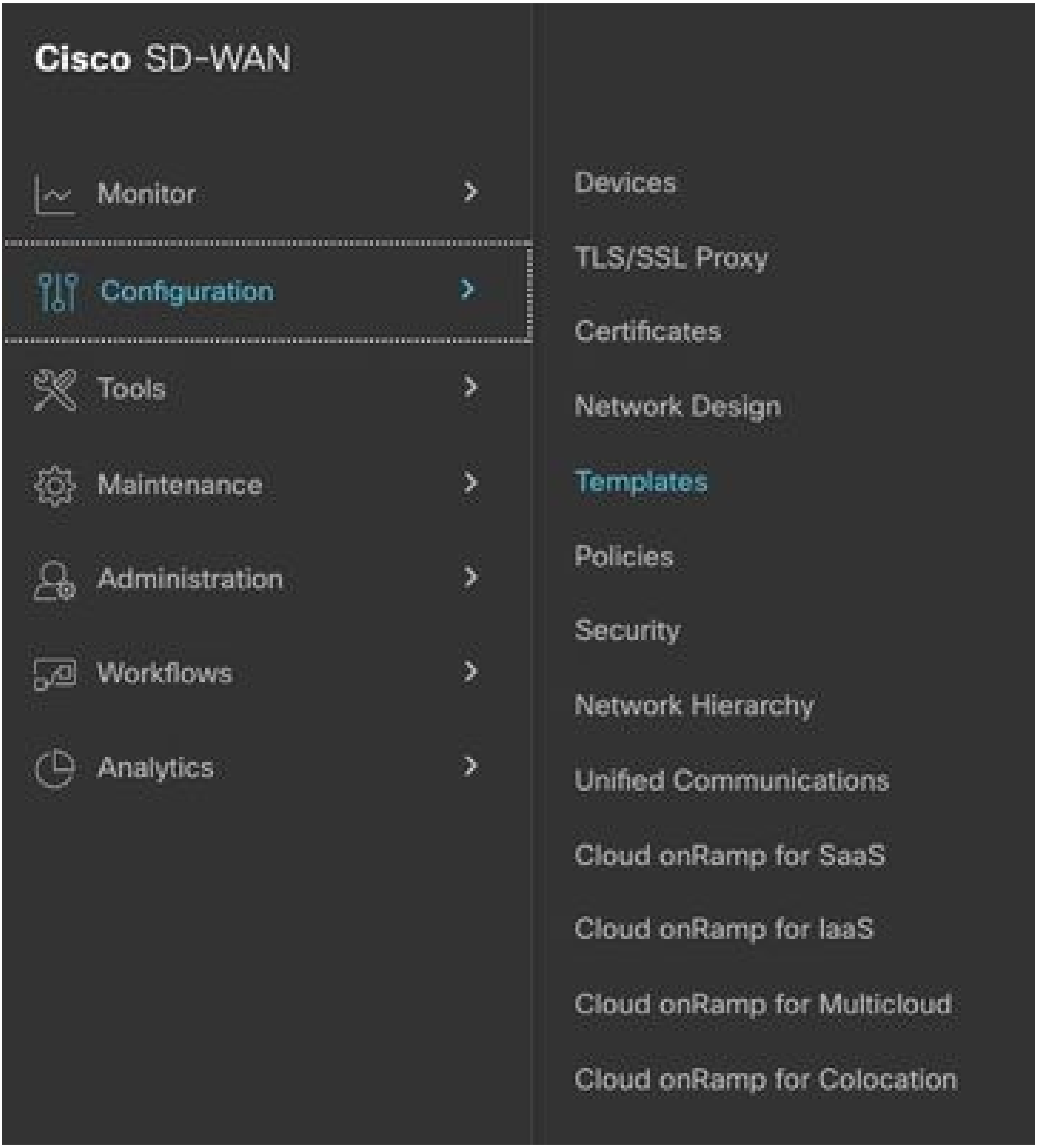
在vManage的CLI加载项模板上进行配置

注意：此类配置只能通过CLI加载项模板添加。

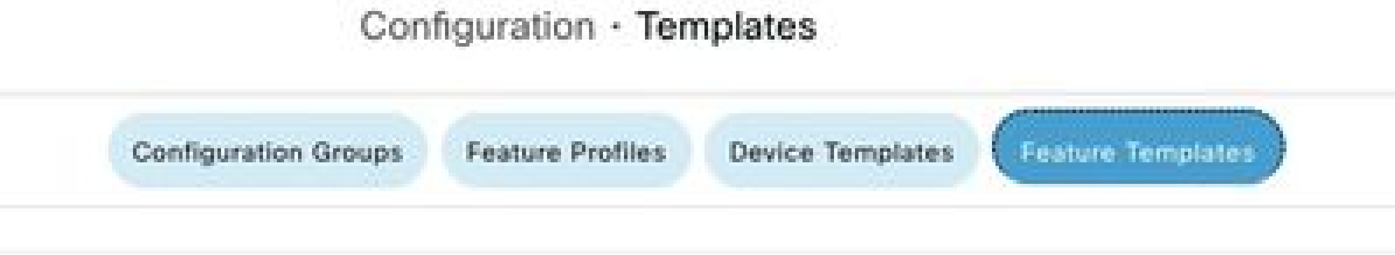
步骤1:导航到Cisco vManage并登录。



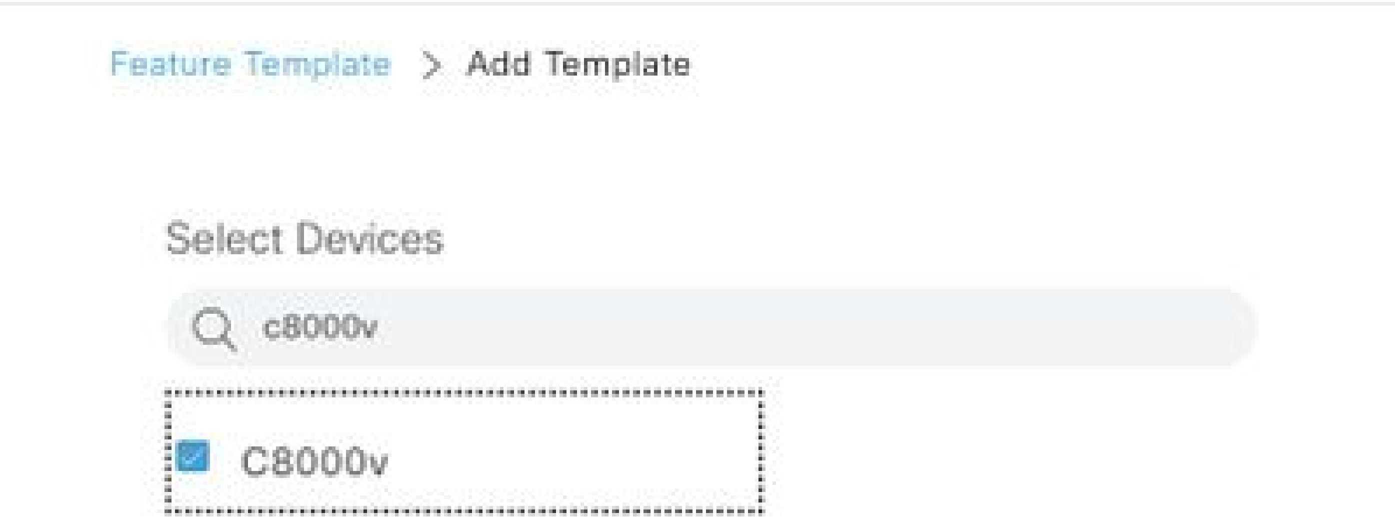
第二步：导航至配置>模板。



第三步：导航到功能模板>添加模板。



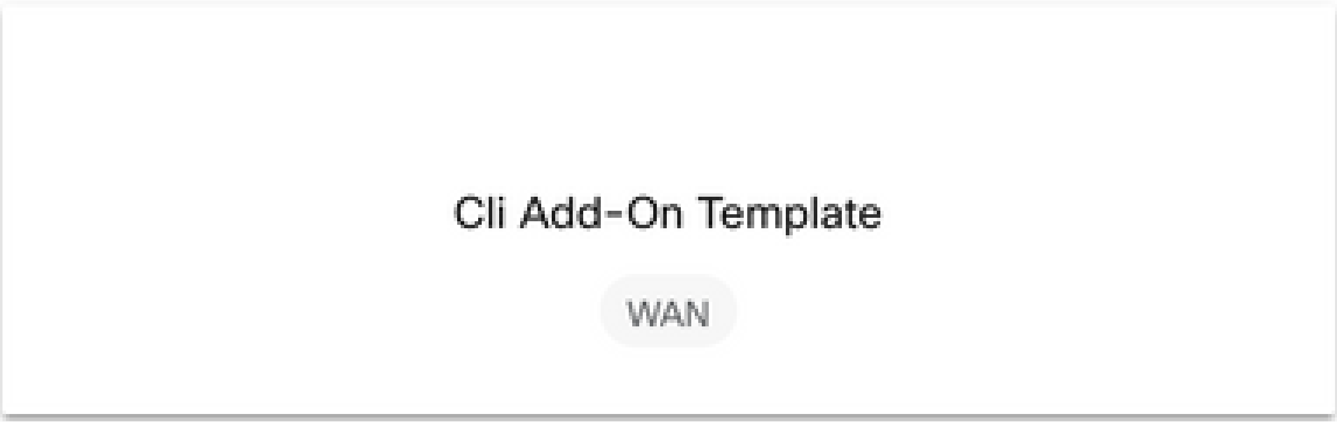
第四步：过滤型号并选择c8000v路由器。



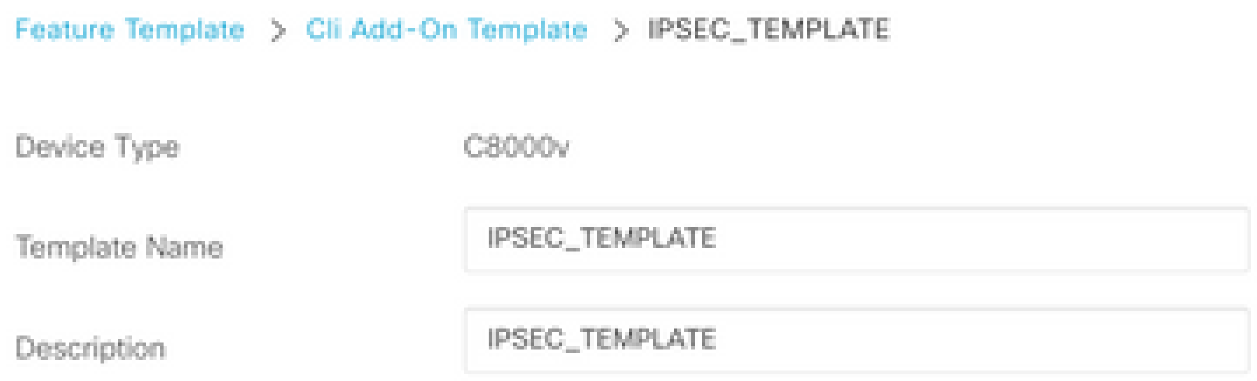
c8000v

☑ C8000v

第五步：导航到其他模板，然后单击Cli加载项模板。



第六步：添加模板名称和说明。



Feature Template > Cli Add-On Template > IPSEC_TEMPLATE

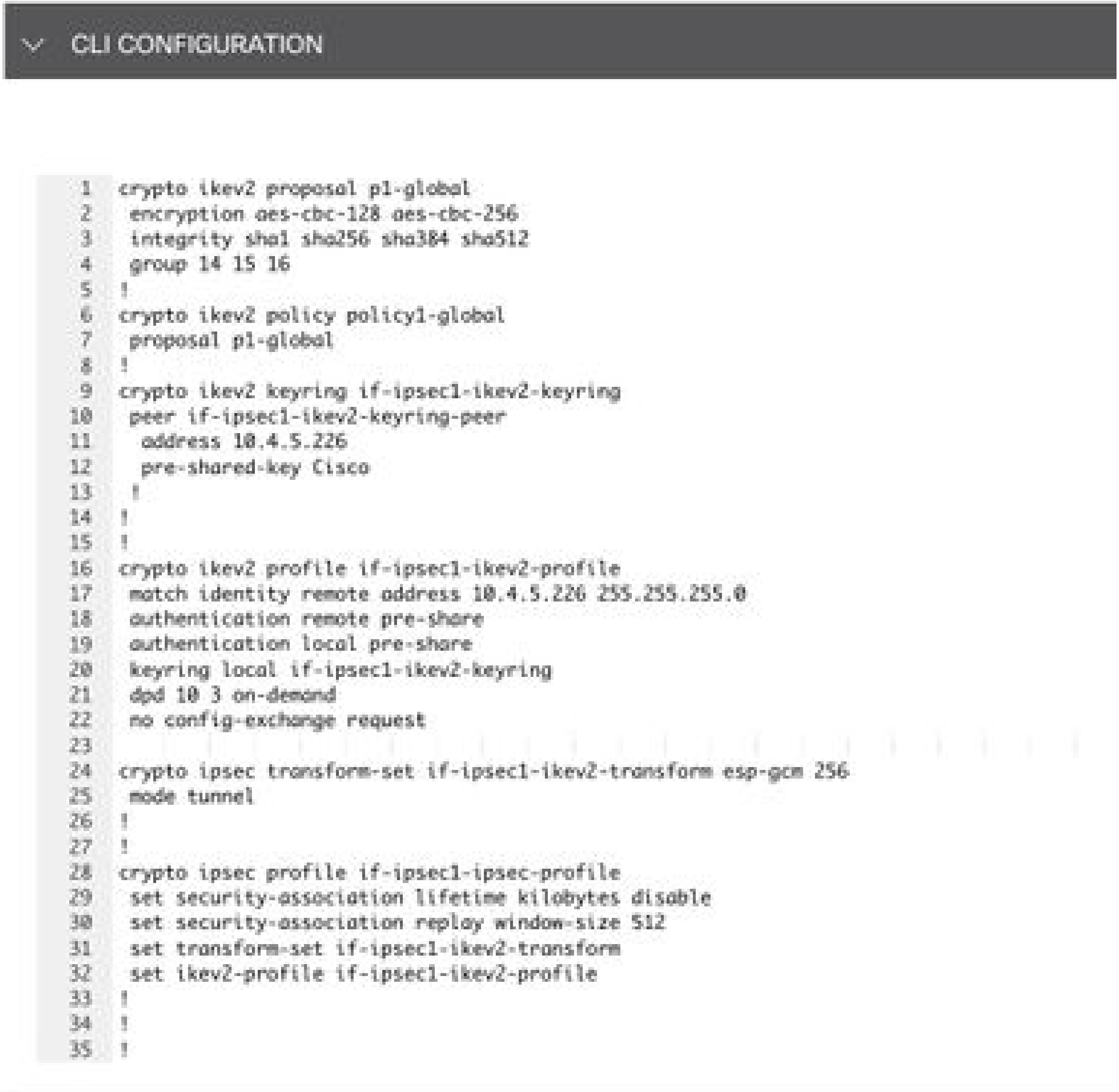
Device Type C8000v

Template Name IPSEC_TEMPLATE

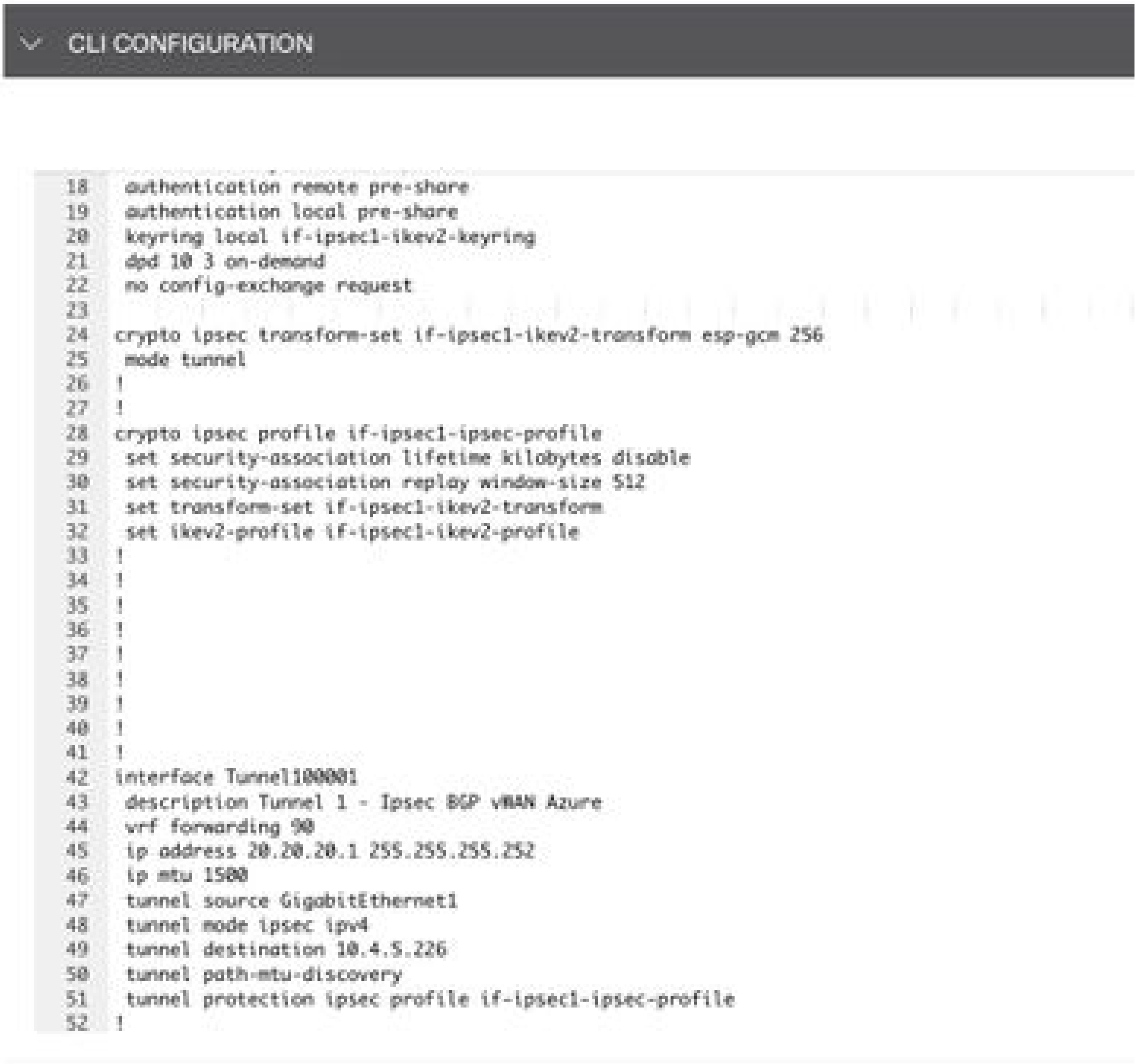
Description IPSEC_TEMPLATE

注：有关如何在CLI加载项模板上创建变量的详细信息，请参阅CLI加载项功能模板。

步骤 7.添加命令。



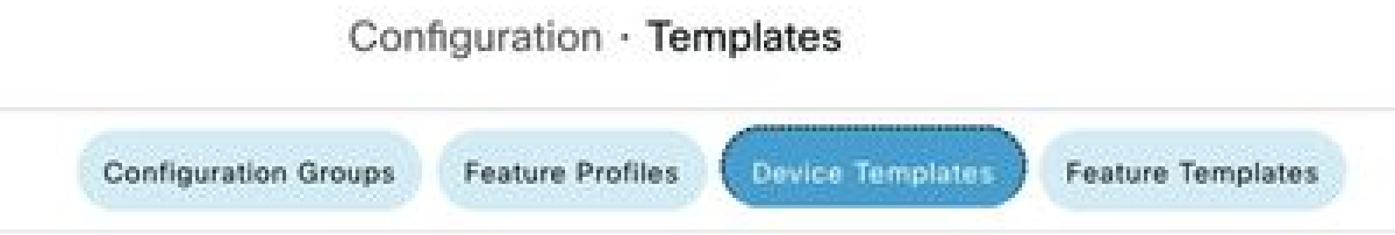
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key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



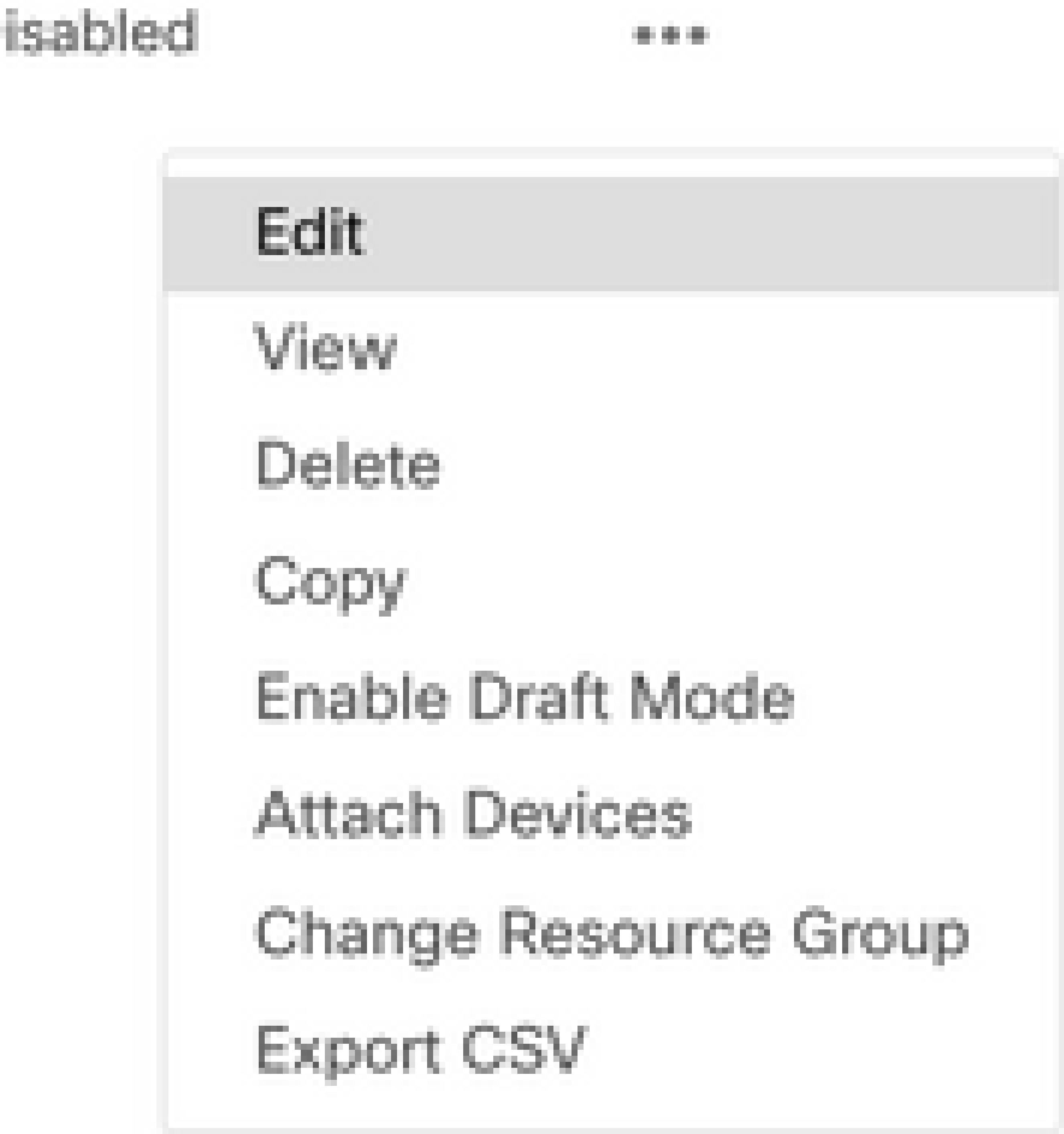
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

步骤 8点击保存。

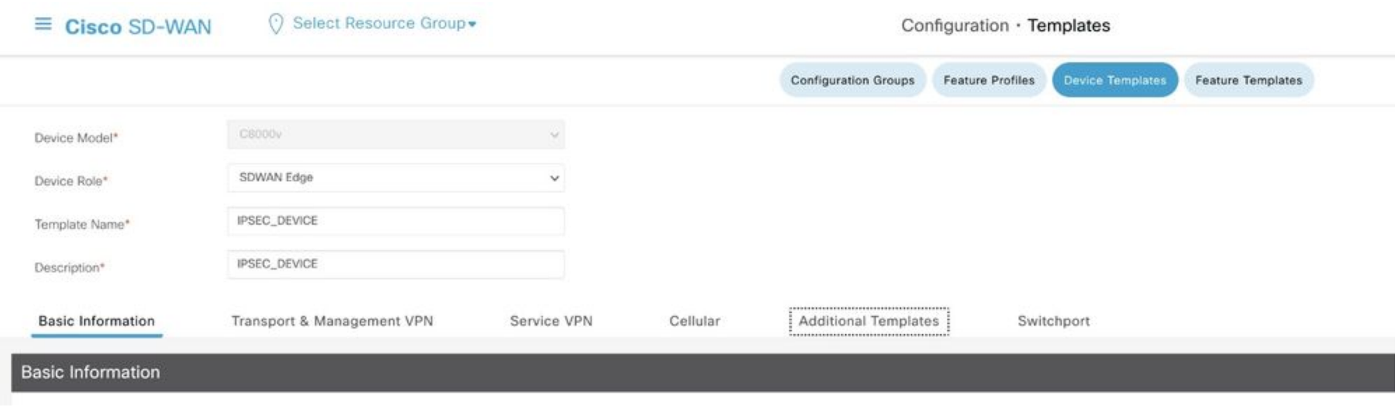
步骤 9导航到设备模板。



步骤 10选择正确的设备模板并在3个点上编辑。



步骤 11导航至其他模板。



Configuration · Templates

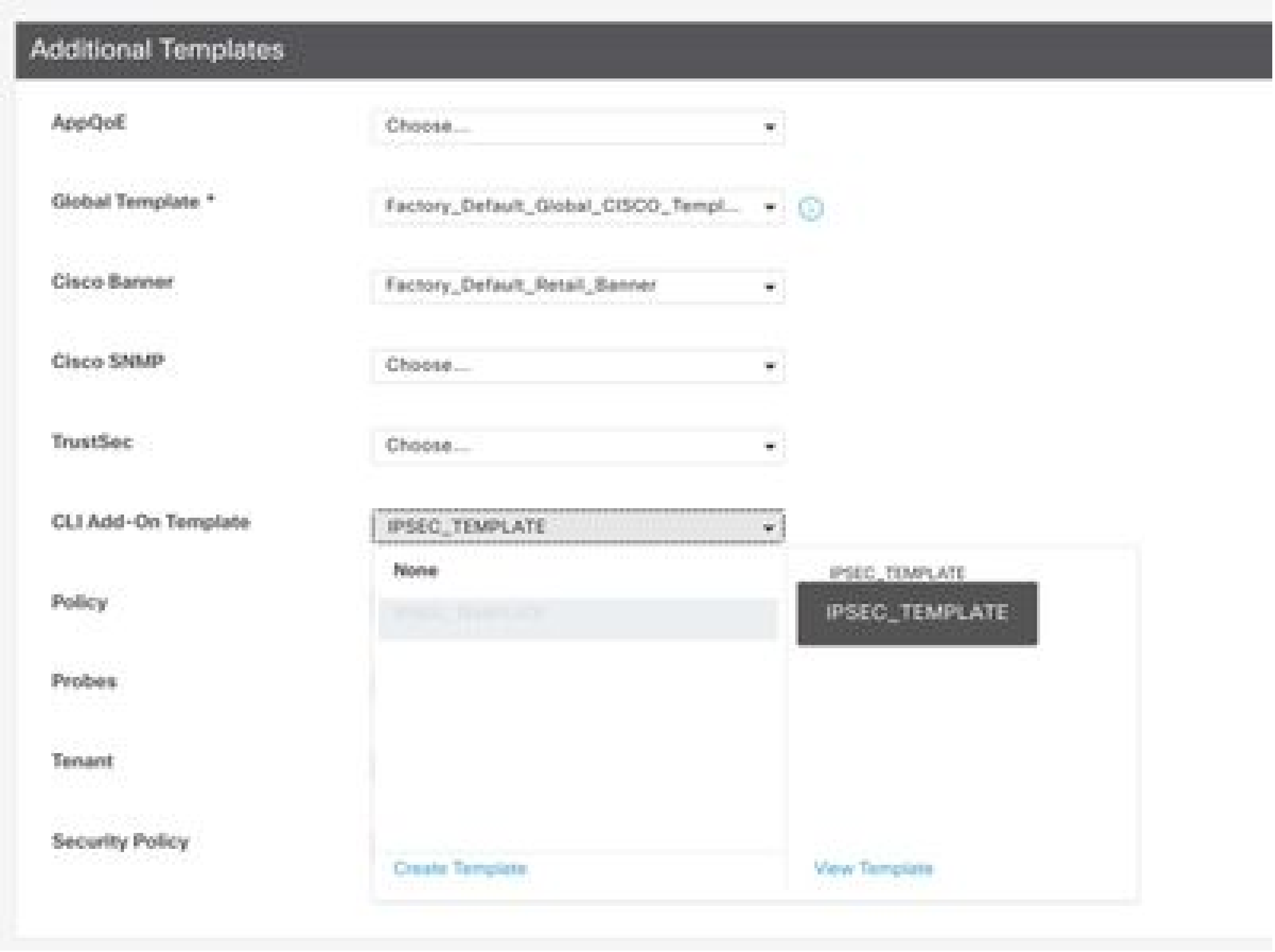
Device Model*: C8000v

Device Role*: SDWAN Edge

Template Name*: IPSEC_DEVICE

Description*: IPSEC_DEVICE

步骤 12在CLI Add-On Template上，选择先前创建的功能模板。



Additional Templates

AppQoE: Choose...

Global Template *: Factory_Default_Global_CISCO_Templ...

Cisco Banner: Factory_Default_Retail_Banner

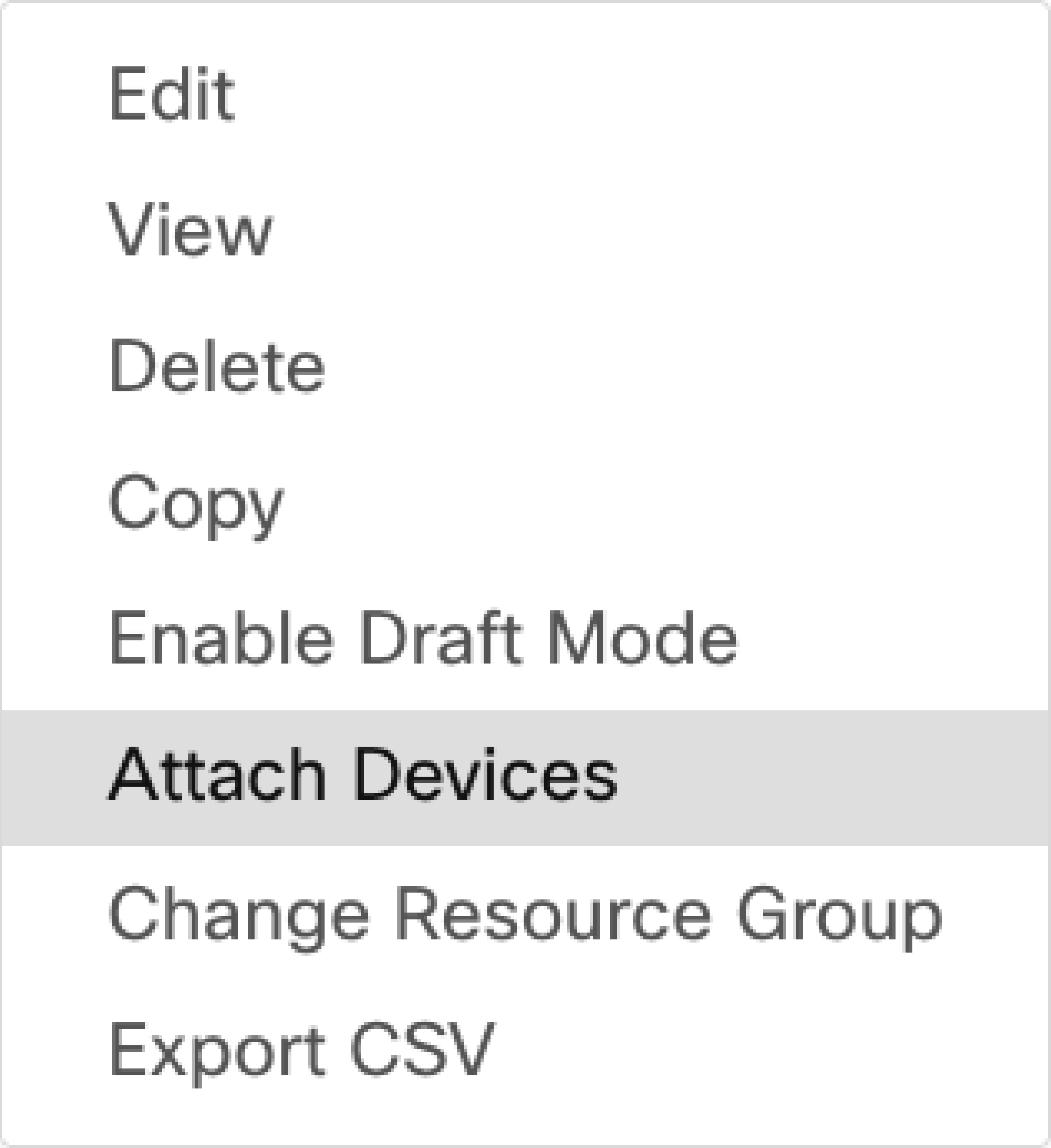
Cisco SNMP: Choose...

TrustSec: Choose...

CLI Add-On Template: IPSEC_TEMPLATE

步骤 13单击Update。

步骤 14点击三个点中的连接设备，选择要将模板推到的正确路由器。



验证

使用本部分可确认配置能否正常运行。

运行show ip interface brief 命令以验证IPSec隧道的状态。

<#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#
```

故障排除

运行show crypto ikev2 session命令以显示有关在设备上建立的IKEv2会话的详细信息。

<#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#
```

运行命令show crypto ipsec sa interface Tunnel100001以显示有关IPSec安全关联(SA)的信息。

<#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#
```

运行命令show crypto ikev2 statistics以显示与IKEv2会话相关的统计信息和计数器。

<#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#
```

运行show crypto session命令显示有关设备上的活动安全会话的信息。

<#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
```

要获取有关设备数据包处理器中IPSec相关丢包的信息，您可以运行：

show platform hardware qfp active feature ipsec datapath drops clear

show platform hardware qfp active statistics drop clear

这些命令需要在shut和no shut隧道接口之前执行，以清除计数器和统计信息，这有助于获取有关设备数据包处理器数据路径中IPsec相关数据包丢弃的信息。

注意：这些命令可以在没有清除选项的情况下运行。必须强调丢弃计数器是历史计数器。

<#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和no shut Tunnel Interface后，您可以运行以下命令以查看是否有新统计信息或计数器的注册：

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#
```

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
```

相关信息

IPsec配对密钥

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

Cisco IPsec技术简介

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。