SD-WAN上のC8000Vを使用したサービス側IPSecトンネルの設定

内容

はじめに

前提条件

- 要件
- コンポーネント

背景説明

IPSEC設定のコンポーネント

設定

- CLIでの設定
- vManageのCLIアドオンテンプレートの設定

確認

トラブルシュート

便利なコマンド

関連情報

はじめに

このドキュメントでは、サービスVRFを使用してSD-WAN CiscoエッジルータとVPNエンドポイント間にIPSecトンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

コンポーネント

このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- Ciscoエッジルータバージョン17.6.1
- SD-WAN vManage 20.9.3.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントのすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください

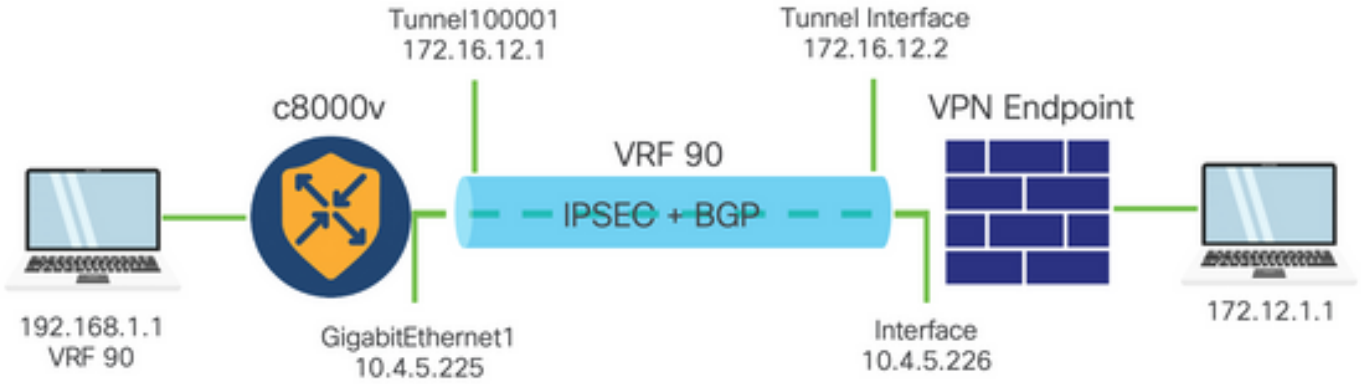
。

背景説明

背景説明には、このドキュメントの対象範囲、使いやすさ、およびSD-WAN上でC8000vを使用してサービス側のIPSecトンネルを構築する利点が含まれます。

- コントローラ管理モードのCisco IOS® XEルータとバーチャルプライベートネットワーク(VPN)エンドポイント間のサービス仮想ルーティングおよび転送(VRF)でIPSecトンネルを構築するには、パブリックワイドエリアネットワーク(WAN)上でデータの機密性と整合性を保証する必要があります。また、企業のプライベートネットワークの安全な拡張を促進し、高レベルのセキュリティを維持しながら、インターネット経由のリモート接続を可能にします。
- サービスVRFはトラフィックを分離します。これは、マルチクライアント環境で特に有用であり、ネットワークの異なる部分の間でセグメント化を維持する場合にも役立ちます。要約すると、この設定はセキュリティと接続を強化します。
- このドキュメントでは、ボーダーゲートウェイプロトコル(BGP)が、SD-WANサービスVRFからVPNエンドポイントの背後にあるネットワークへの通信（およびその逆）に使用されるルーティングプロトコルであると想定しています。
- BGP設定については、このドキュメントでは扱いません。
- このVPNエンドポイントには、ファイアウォール、ルータ、またはIPSec機能を備えたあらゆるタイプのネットワークデバイスを使用できます。VPNエンドポイントの設定については、このドキュメントでは扱いません。
- このドキュメントでは、ルータがすでにオンボードで、アクティブな制御接続とサービスVRFを備えていることを前提としています。

IPSEC設定のコンポーネント



フェーズ1インターネットキーエクスチェンジ(IKE)

IPSec設定プロセスのフェーズ1には、セキュリティパラメータのネゴシエーションとトンネルエンドポイント間の認証が含まれます。これらの手順を次に示します。

IKE の設定。

- 暗号化提案（アルゴリズムとキー長）を定義します。
- 暗号化提案、存続可能時間、および認証を含むIKEポリシーを設定します。

リモートエンドピアの設定

- リモートエンドのIPアドレスを定義します。
- 認証用の共有キー（事前共有キー）を設定します。

フェーズ2(IPSec)の設定

フェーズ2では、トンネルを通過するトラフィックフローに対するセキュリティトランスフォーメーションとアクセスルールのネゴシエーションが行われます。これらの手順を次に示します。

IPSecトランスフォーメーションセットの設定

- 暗号化アルゴリズムと認証を含む、提示されたトランスフォームセットを定義します。

IPSecポリシーの設定

- トランスフォームセットをIPSecポリシーに関連付けます。

トンネルインターフェイスの設定

IPSecトンネルの両端にトンネルインターフェイスを設定します。

- トンネルインターフェイスをIPSecポリシーに関連付けます。

設定

CLIでの設定

ステップ 1：暗号化提案を定義します。

```
<#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
```

ステップ 2：プロポーザル情報を含むIKEポリシーを設定します。

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

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

ステップ 3：リモートエンドのIPアドレスを定義します。

```
<#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
```

ステップ 4：認証用の共有キー（事前共有キー）を設定します。

```
<#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)#
```

ステップ 5：暗号化アルゴリズムと認証を含む、提示されたトランスフォームセットを定義します。

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

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

手順 6：トランスフォームセットをIPSecポリシーに関連付けます。

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

cEdge(ipsec-profile)#
```

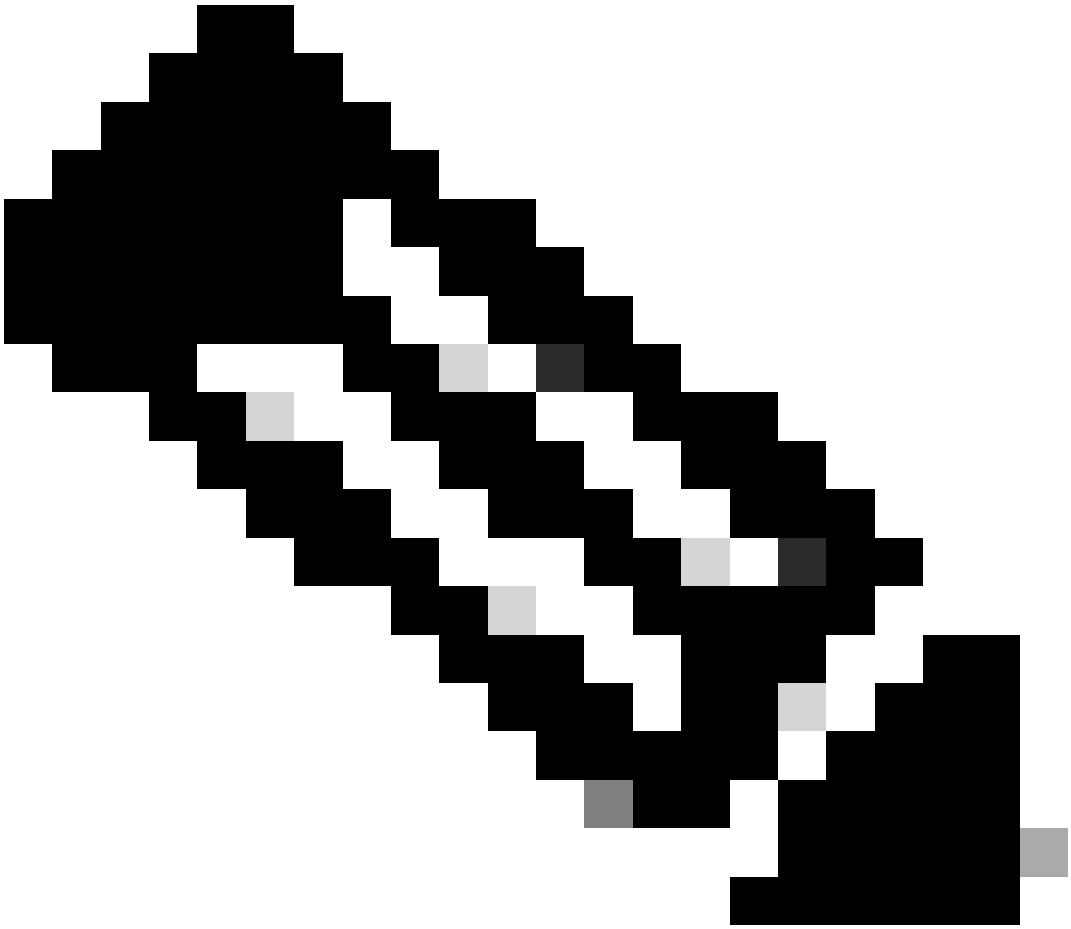
```
set security-association lifetime kilobytes disable

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
```

手順 7：インターフェイストンネルを作成し、IPSecポリシーに関連付けます。

```
<#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
```

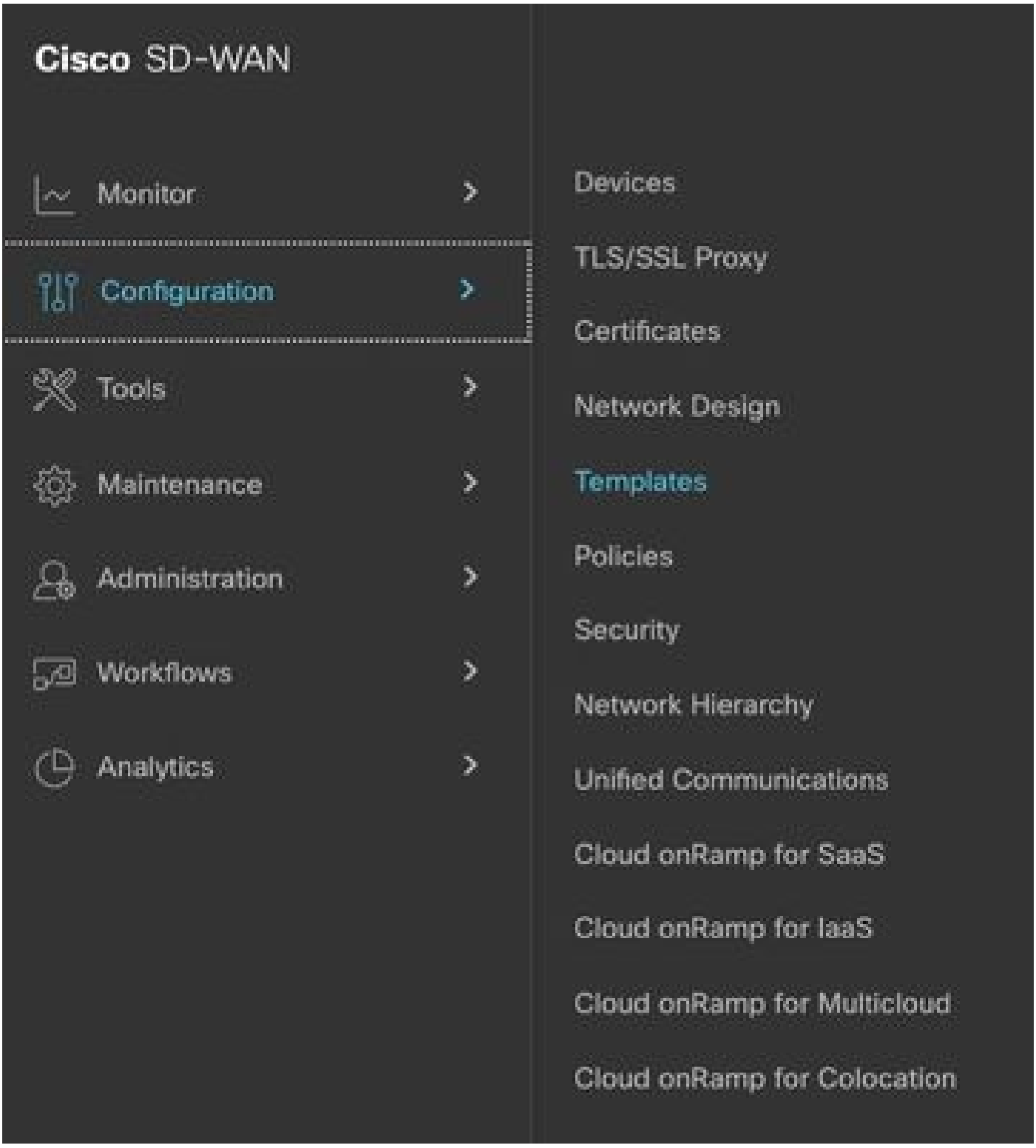
vManageのCLIアドオンテンプレートの設定



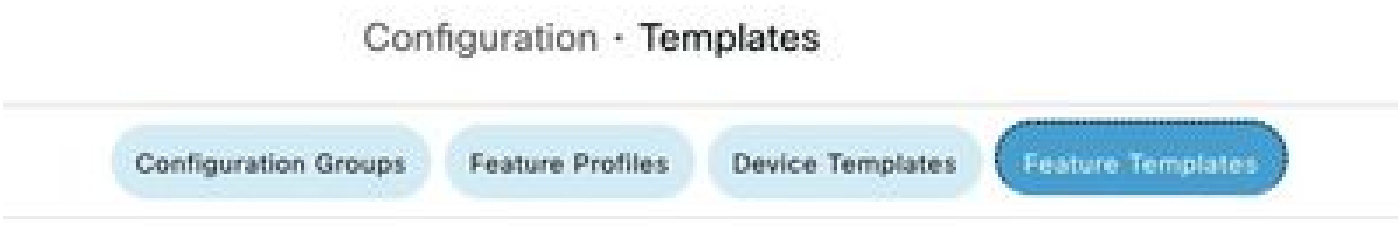
注：このタイプの設定は、CLIアドオンテンプレートを使用してのみ追加できます。

ステップ 1：Cisco vManageに移動してログインします。

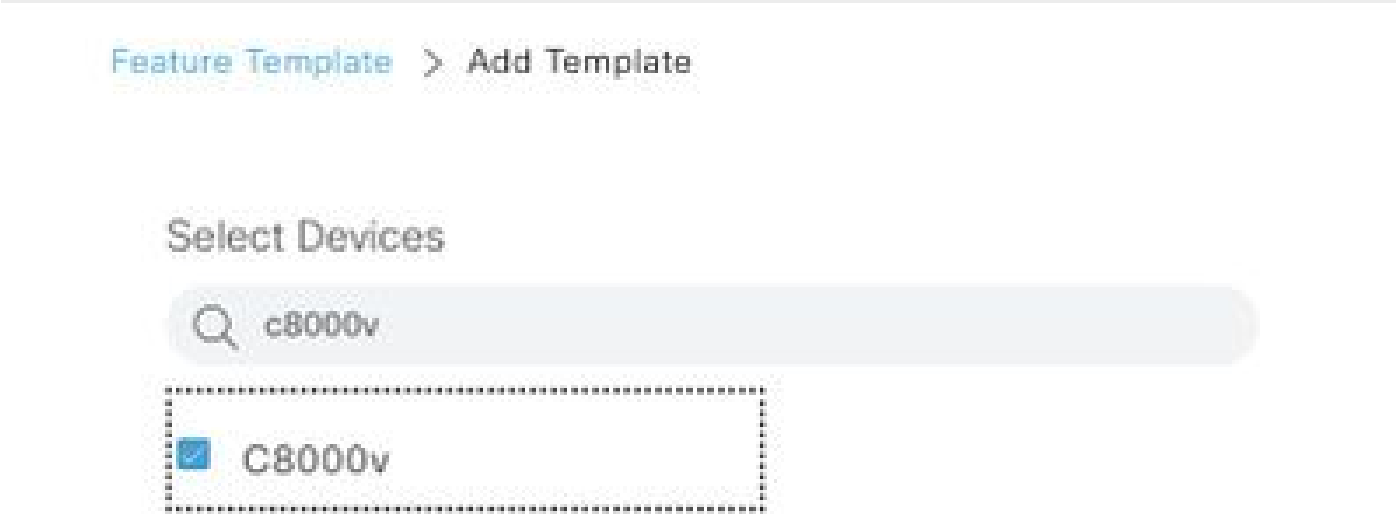
ステップ 2：Configuration > Templatesの順に移動します。



ステップ 3：Feature Templates > Add Templateの順に移動します。

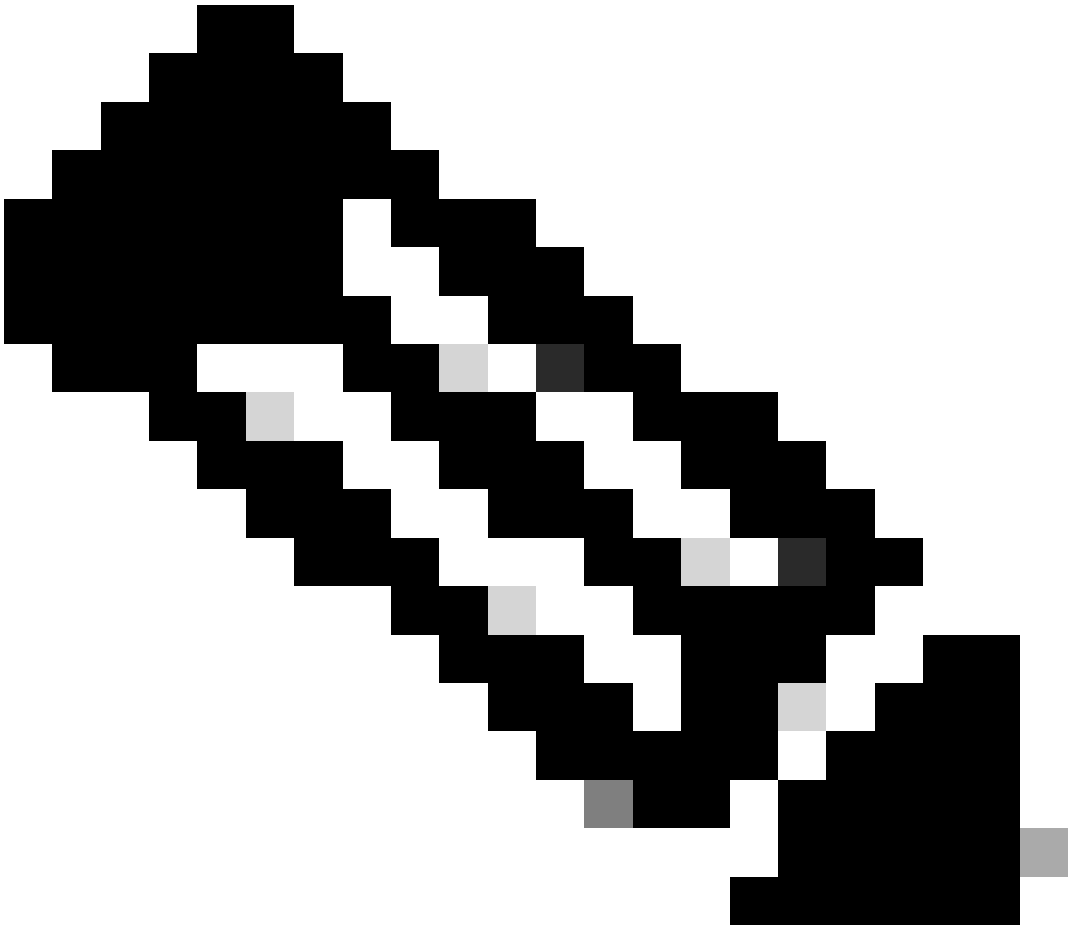


ステップ 4：モデルをフィルタリングし、c8000vルータを選択します。



ステップ 5：Other Templatesの順に移動し、Cli Add-On Templateをクリックします。

手順 6：テンプレート名と説明を追加します。



注:CLIアドオンテンプレートで変数を作成する方法の詳細については、「CLIアドオン機能テンプレート」を参照してください。

手順 7：コマンドを追加します。

CLI CONFIGURATION

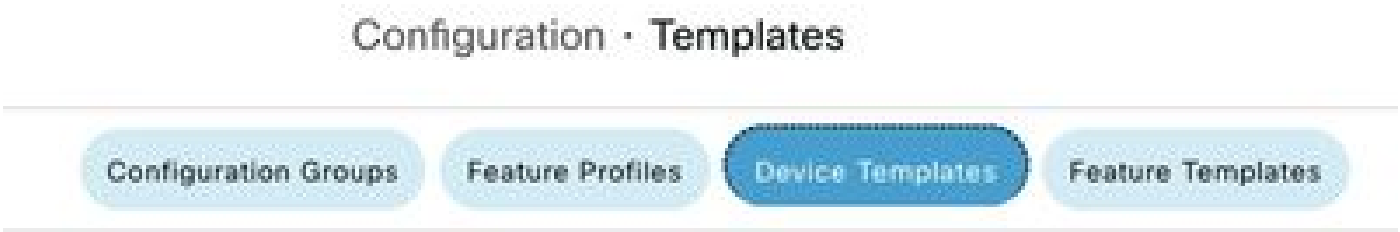
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key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

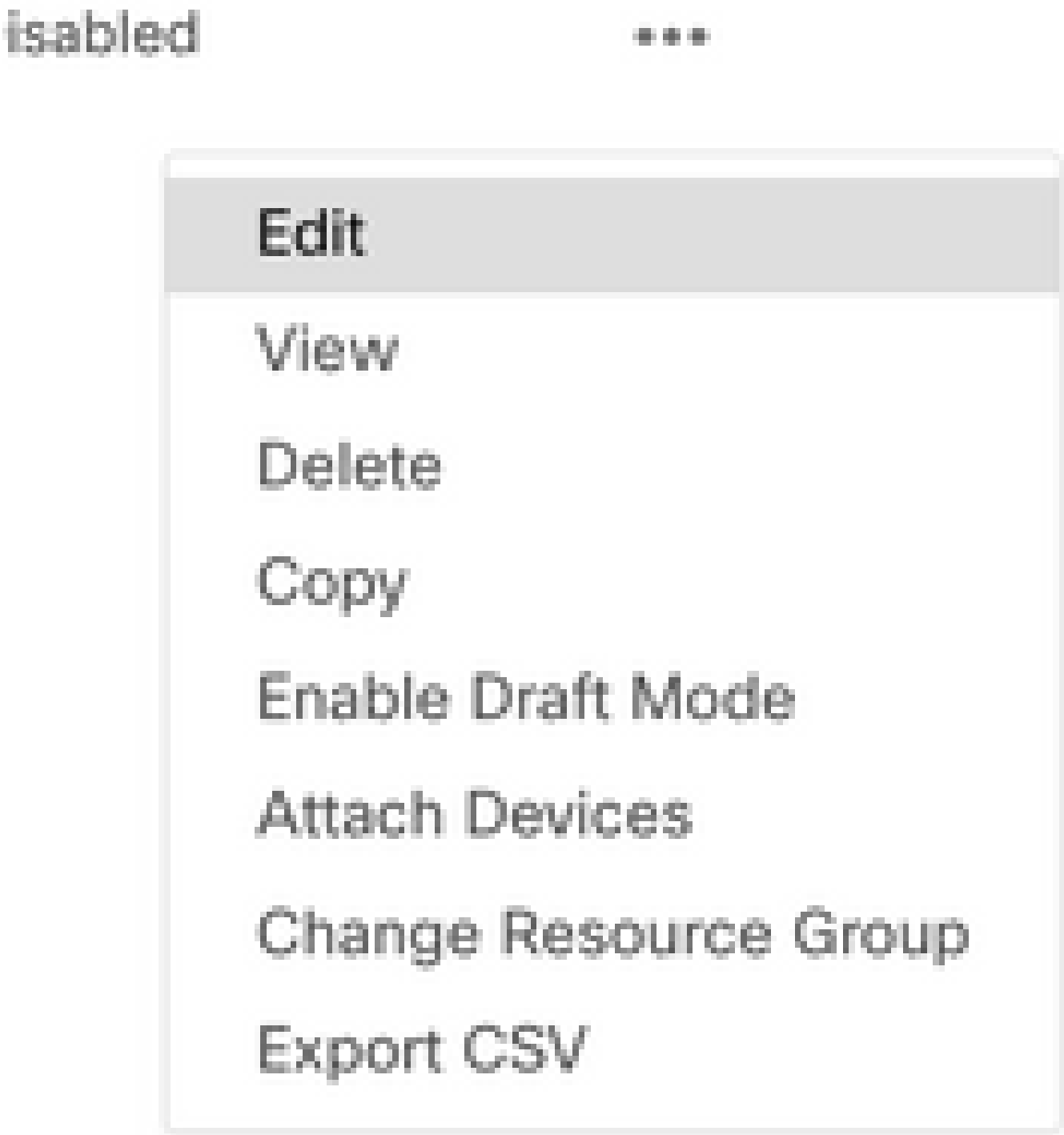
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

ステップ 8：[Save] をクリックします。

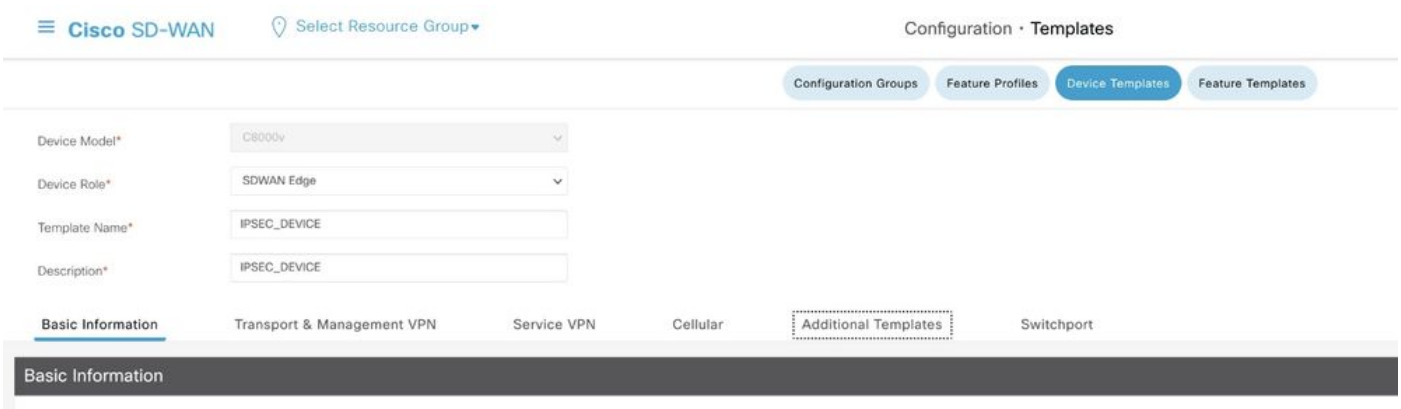
ステップ 9：Device Templatesに移動します。



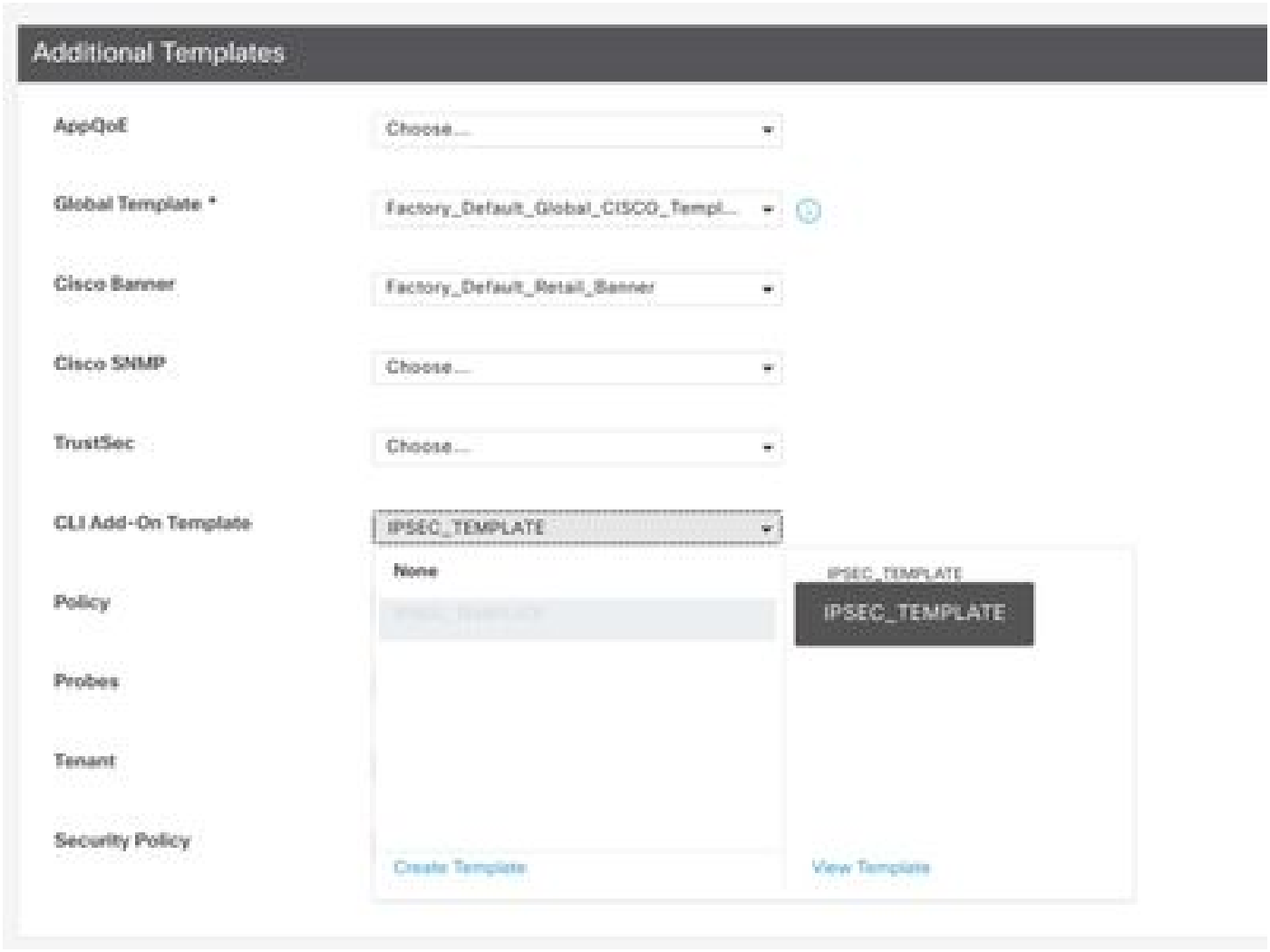
ステップ 10：正しいデバイステンプレートを選択し、3つのドットで編集します。



ステップ 11追加テンプレートに移動します。

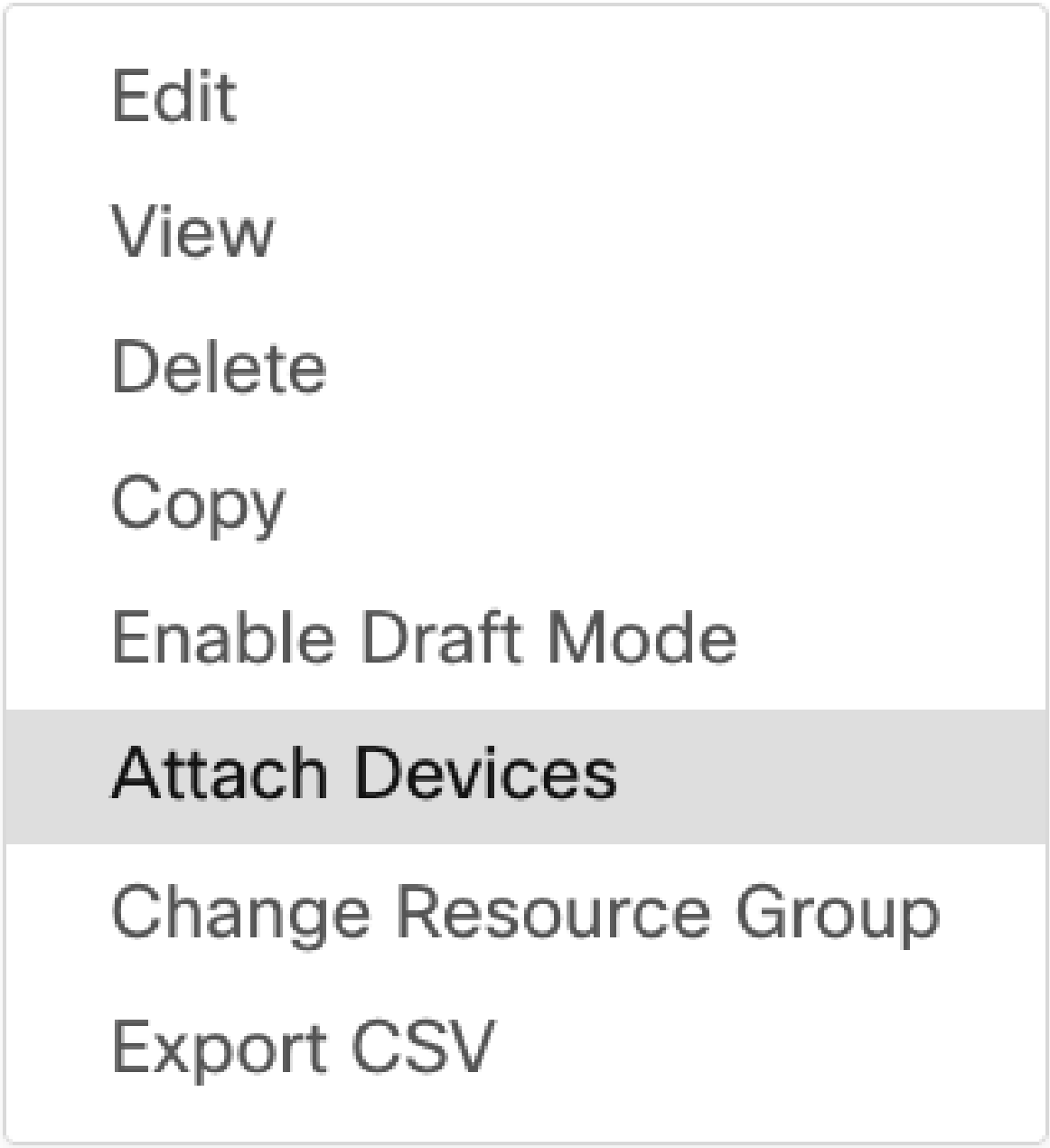


ステップ 12CLIアドオンテンプレートで、以前に作成した機能テンプレートを選択します。



ステップ 13Updateをクリックします。

ステップ 14：3つのドットからAttach Devicesをクリックし、テンプレートをプッシュする正しいルータを選択します。



確認

このセクションでは、設定が正常に動作していることを確認します。

show ip interface briefコマンドを実行して、IPSecトンネルのステータスを確認します。

<#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#
```

トラブルシュート

show crypto ikev2 sessionコマンドを実行して、デバイスで確立されたIKEv2セッションに関する詳細情報を表示します。

```
<#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#
```

IPSecセキュリティアソシエーション(SA)に関する情報を表示するには、show crypto ipsec sa interface Tunnel100001コマンドを実行します。

```
<#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#
```

IKEv2セッションに関連する統計情報とカウンタを表示するには、コマンドshow crypto ikev2 statisticsを実行します。

<#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#
```

デバイス上のアクティブなセキュリティセッションに関する情報を表示するには、show crypto sessionコマンドを実行します。

<#root>

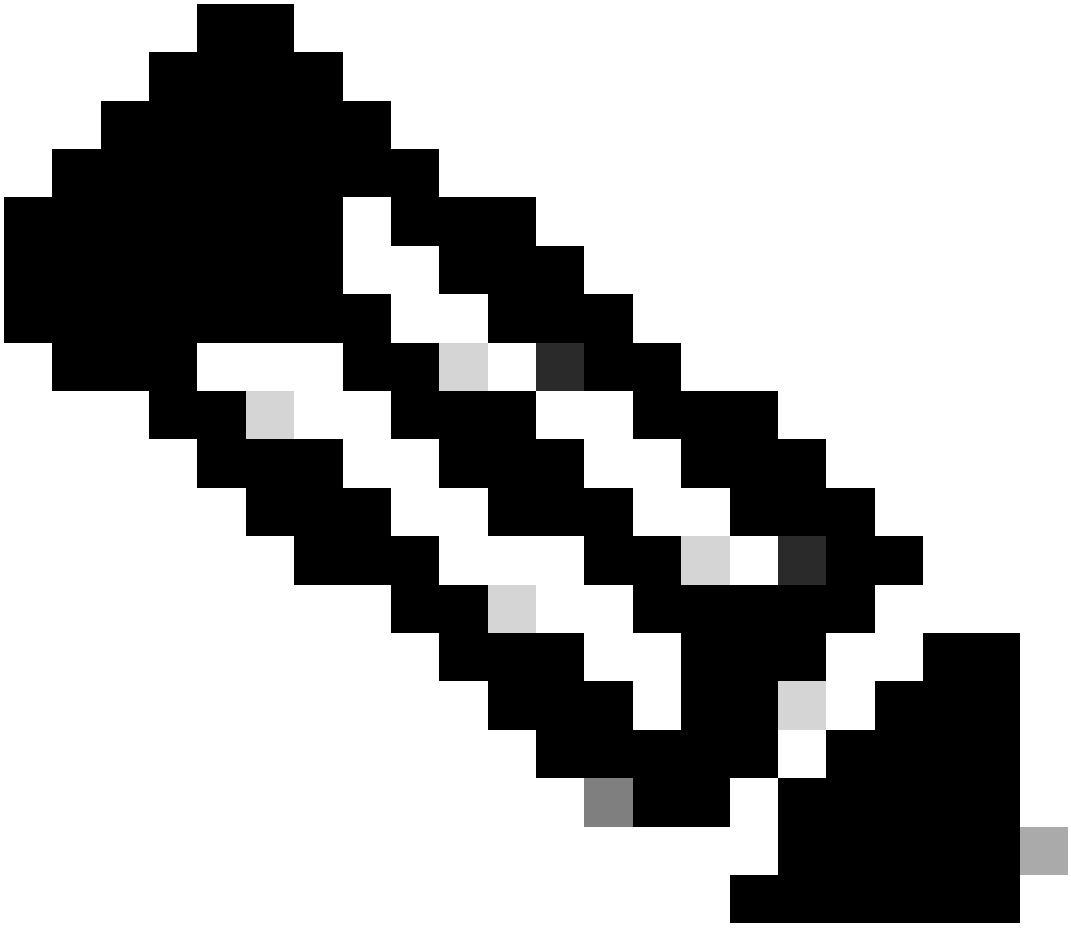
```
cEdge#

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
```

デバイスパケットプロセッサでのIPSec関連のパケットドロップに関する情報を取得するには、次のコマンドを実行します。

show platform hardware qfp active feature ipsec datapath drops clear

show platform hardware qfp active statistics drop clear

これらのコマンドは、Tunnelインターフェイスのshutおよびno shutの前に実行して、カウンタと統計情報をクリアする必要があります。これにより、デバイスパケットプロセッサデータパスでのIPSec関連のパケットドロップに関する情報を取得できます。



注：これらのコマンドは、オプションclearを指定せずに実行できます。ドロップカウンタが履歴であることを強調することが重要です。

<#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#

トンネルインターフェイスのshutおよびno shutの後に、次のコマンドを実行して、新しい統計情報またはカウンタが登録されたかどうかを確認できます。

show ip interface brief | Tunnel100001の追加

show platform hardware qfp active statistics drop（プラットフォームのハードウェアqfpアクティブ統計ドロップ）

show platform hardware qfp active feature ipsecデータパスドロップ

<#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#
```

便利なコマンド

<#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
```

関連情報

IPsecペアワイズキー

Cisco Catalyst SD-WANセキュリティコンフィギュレーションガイド、Cisco IOS® XE Catalyst SD-WANリリース17.x

Cisco IPsecテクノロジーの概要

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。