Configuration du tunnel IPSec côté service avec un C8000V sur SD-WAN

Table des matières

Introduction

Ce document décrit comment configurer un tunnel IPSec entre un routeur de périphérie Cisco SD-WAN et un terminal VPN avec service VRF.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) de Cisco
- Sécurité du protocole Internet (IPSec)

Composants

Ce document est basé sur les versions logicielles et matérielles suivantes :

- Routeur de périphérie Cisco version 17.6.1
- SD-WAN vManage 20.9.3.2

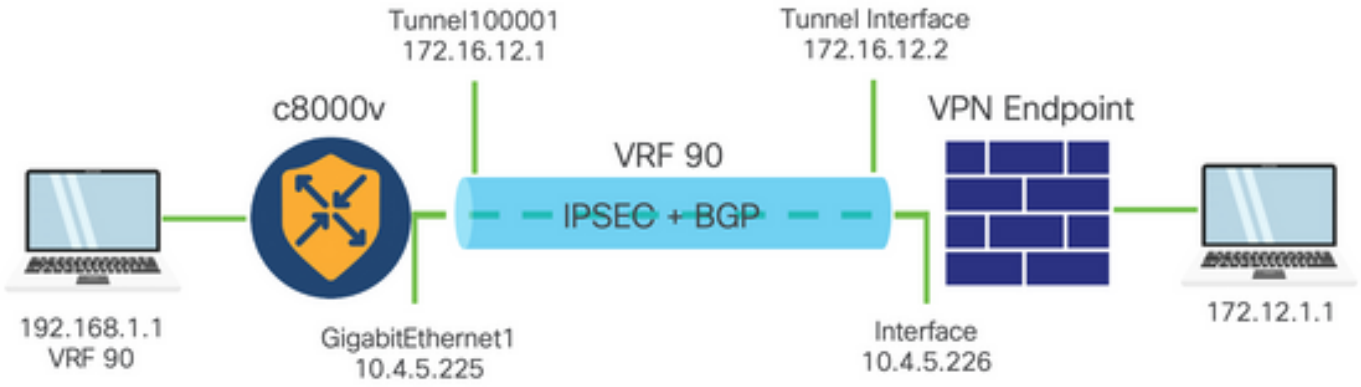
The information in this document was created from the devices in a specific lab environment. Tous les périphériques de ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les informations de base incluent la portée de ce document, la facilité d'utilisation et les avantages de construire un tunnel IPSec côté service avec un C8000v sur SD-WAN.

- Pour créer un tunnel IPSec dans un service de routage et de transfert virtuels (VRF) entre un routeur Cisco IOS® XE en mode de gestion de contrôleur et un terminal de réseau privé virtuel (VPN), vous devez garantir la confidentialité et l'intégrité des données sur le réseau étendu public (WAN). Il facilite également l'extension sécurisée des réseaux privés des entreprises et permet des connexions à distance sur Internet tout en maintenant un niveau de sécurité élevé.
- Le VRF de service isole le trafic, qui est particulièrement utile dans les environnements multi-clients ou pour maintenir la segmentation entre différentes parties du réseau. En résumé, cette configuration améliore la sécurité et la connectivité.
- Ce document considère que le protocole BGP (Border Gateway Protocol) est le protocole de routage utilisé pour communiquer les réseaux du VRF du service SD-WAN au réseau derrière le point d'extrémité VPN et vice versa.
- La configuration BGP sort du cadre de ce document.
- Ce terminal VPN peut être un pare-feu, un routeur ou tout type de périphérique réseau doté de fonctionnalités IPSec. La configuration du terminal VPN sort du cadre de ce document.
- Ce document suppose que le routeur est déjà intégré avec des connexions de contrôle actives et un VRF de service.

Composants de la configuration IPSEC



Phase 1 IKE (Internet Key Exchange)

La phase 1 du processus de configuration IPSec implique la négociation des paramètres de sécurité et l'authentification entre les points d'extrémité du tunnel. Ces étapes incluent les suivantes :

Configuration IKE

- Définissez une proposition de cryptage (algorithme et longueur de clé).
- Configurez une stratégie IKE qui inclut une proposition de cryptage, la durée de vie et

l'authentification.

Configurer des homologues distants

- Définissez l'adresse IP du terminal distant.
- Configurez la clé partagée (clé pré-partagée) pour l'authentification.

Configuration de la phase 2 (IPSec)

La phase 2 implique la négociation des transformations de sécurité et des règles d'accès pour le flux de trafic à travers le tunnel. Ces étapes incluent les suivantes :

Configuration des jeux de transformation IPSec

- Définissez un jeu de transformation proposé qui inclut l'algorithme de chiffrement et l'authentification.

Configurer une stratégie IPSec

- Associez le jeu de transformation à une stratégie IPSec.

Configuration des interfaces de tunnel

Configurez les interfaces de tunnel aux deux extrémités du tunnel IPSec.

- Associez les interfaces de tunnel aux stratégies IPSec.

Configurer

Configuration sur CLI

Étape 1. Définissez une proposition de cryptage.

<#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
```

Étape 2. Configurez une stratégie IKE qui inclut des informations de proposition.

<#root>

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

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

Étape 3. Définissez l'adresse IP du terminal distant.

<#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
```

Étape 4. Configurez la clé partagée (clé pré-partagée) pour l'authentification.

<#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)#
```

Étape 5. Définissez un jeu de transformation proposé qui inclut l'algorithme de chiffrement et l'authentification.

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

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

Étape 6. Associez le transform-set à une stratégie IPSec.

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

cEdge(ipsec-profile)#
```

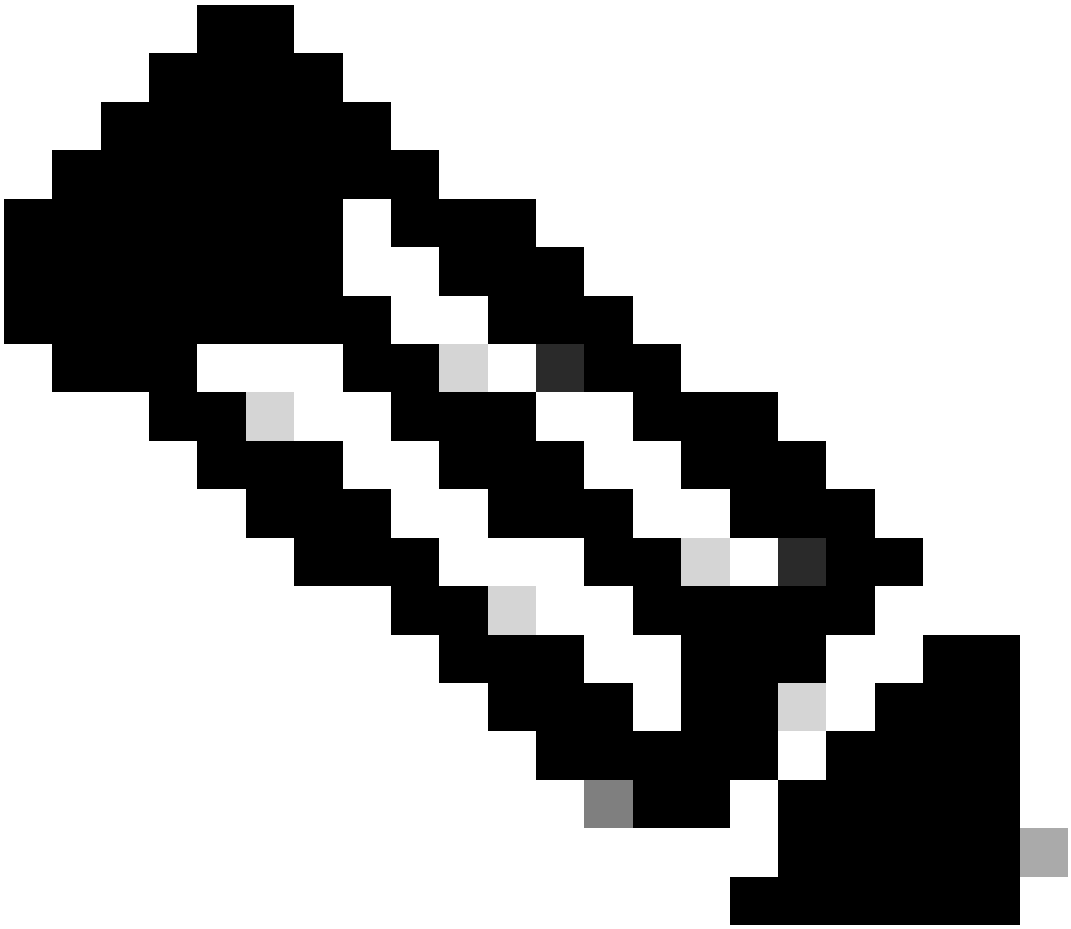
```
set security-association lifetime kilobytes disable

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
```

Étape 7. Créez le tunnel d'interface et associez-le aux stratégies 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
```

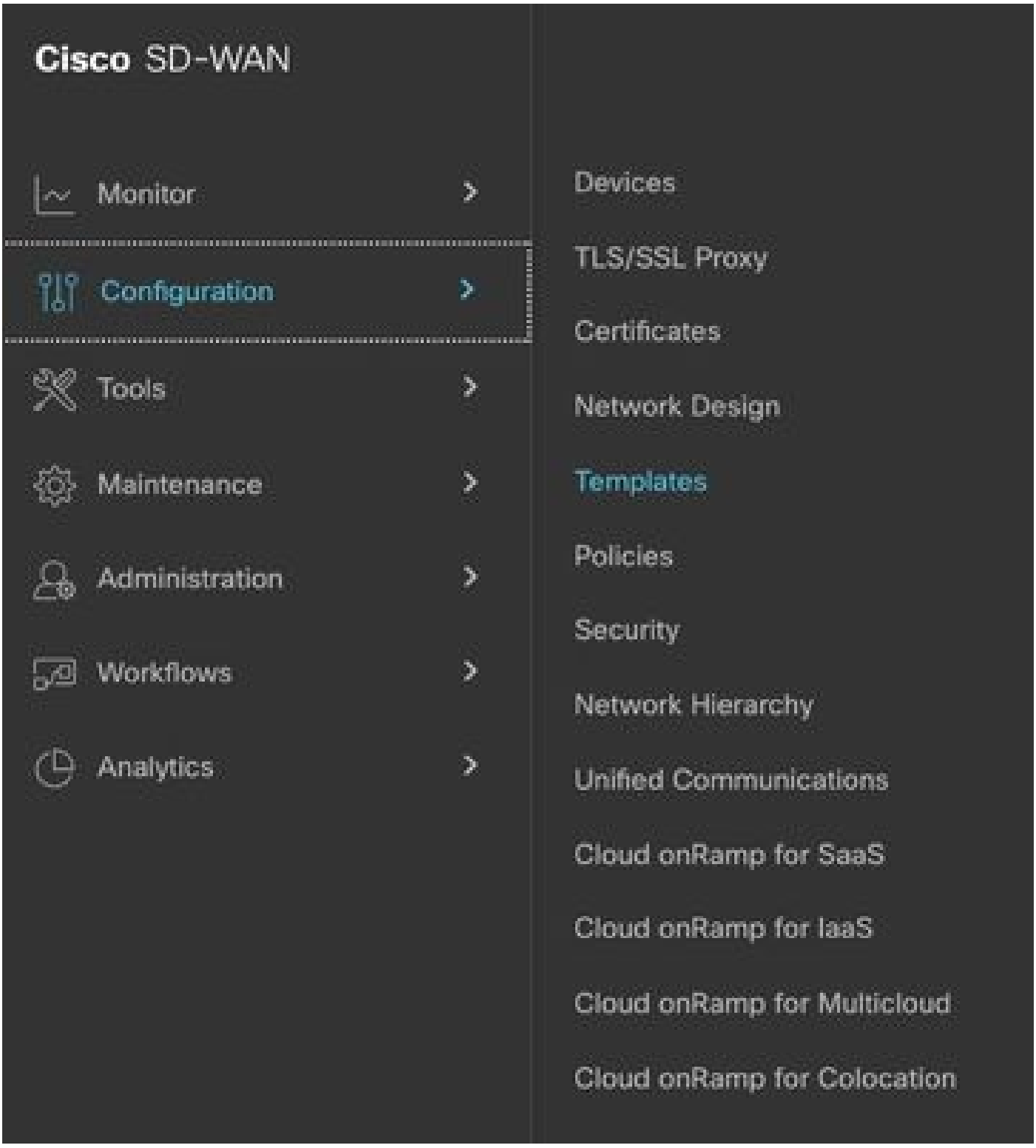
Configuration sur un modèle de module complémentaire CLI sur vManage



> Remarque : ce type de configuration ne peut être ajouté que via le modèle de module complémentaire CLI.

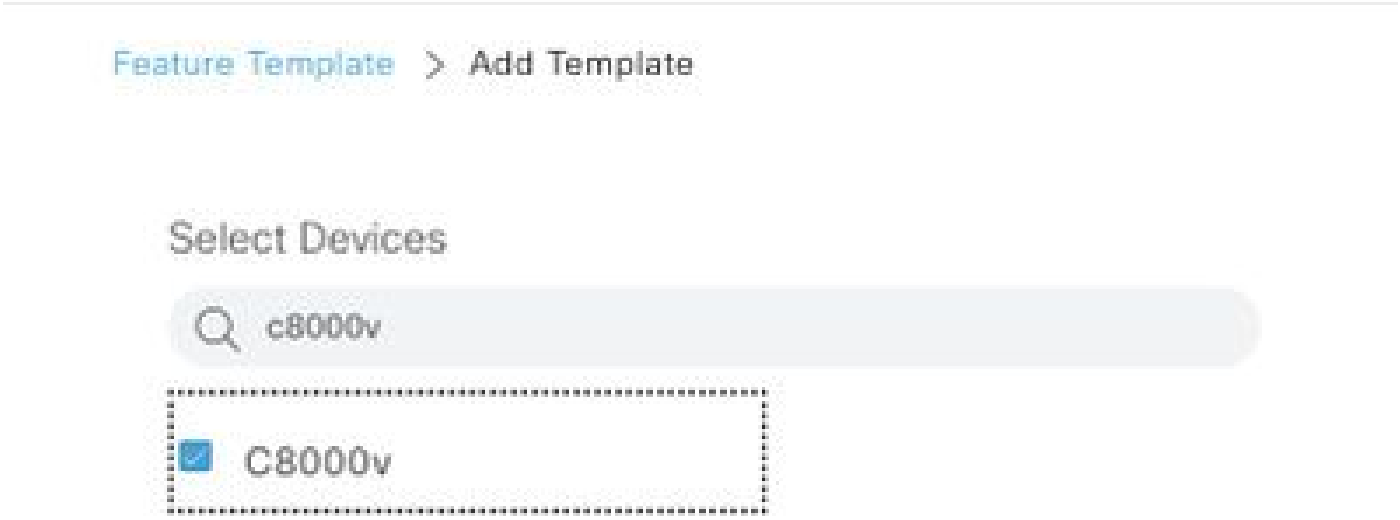
Étape 1. Accédez à Cisco vManage et connectez-vous.

Étape 2. Accédez à Configuration > Templates.



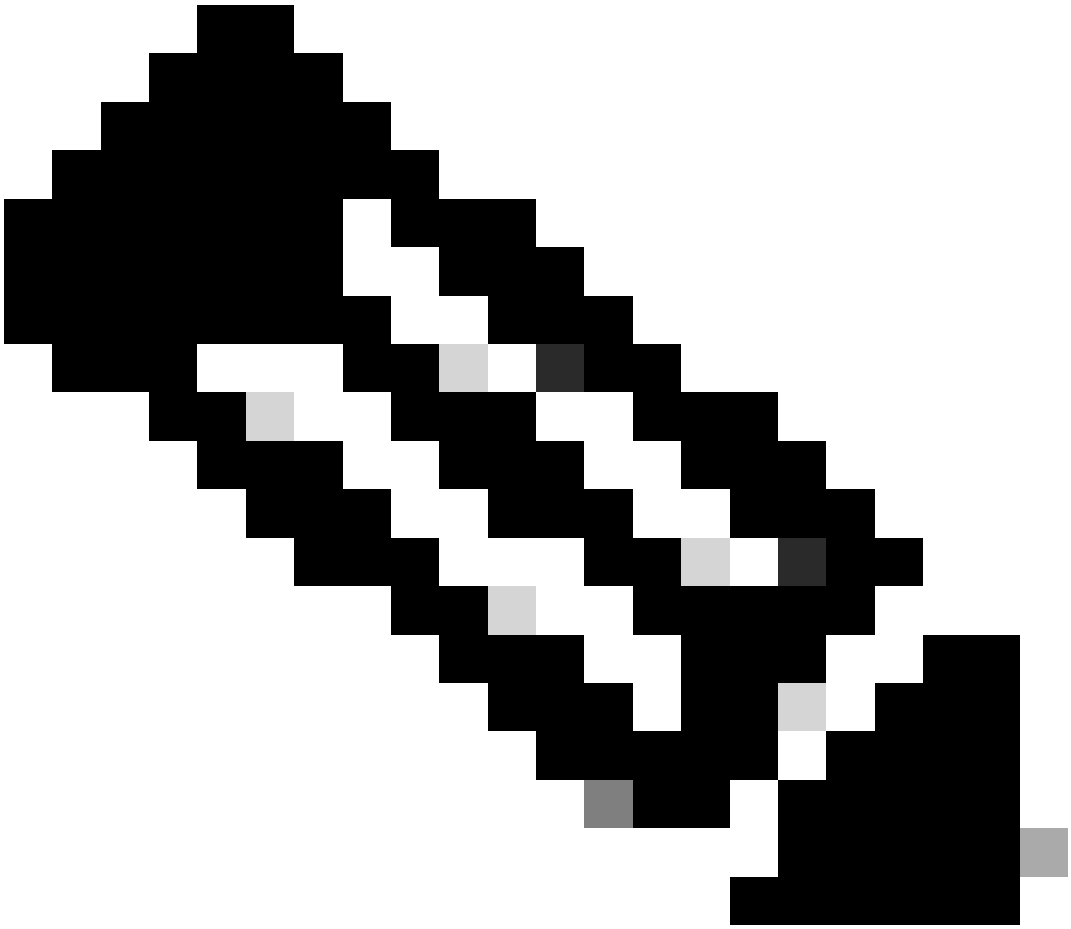
Étape 3. Accédez à Modèles de fonction > Ajouter un modèle.

Étape 4. Filtrez le modèle et choisissez le routeur c8000v.



Étape 5. Accédez à Other Templates et cliquez sur Cli Add-On Template.

Étape 6. Ajoutez un nom de modèle et une description.



Remarque : pour plus d'informations sur la création de variables sur un modèle de module complémentaire CLI, reportez-vous à la section Modèles de fonctions complémentaires CLI.

Étape 7. Ajoutez les commandes.

CLI CONFIGURATION

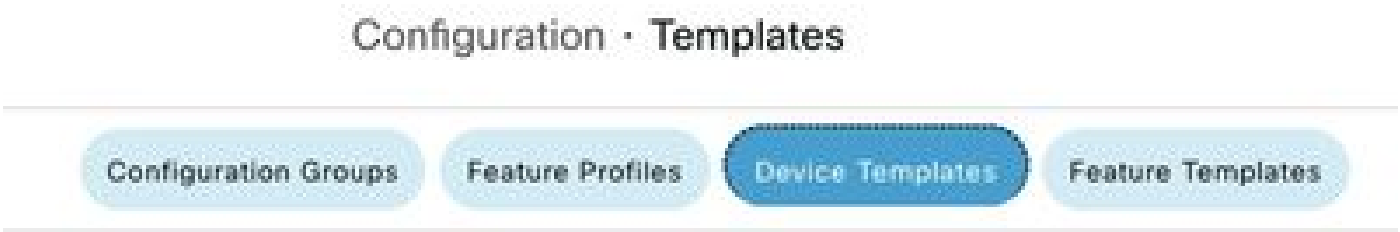
```
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 integrity sha1 sha256 sha384 sha512
 group 14 15 16
!
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 keyring if-ipsec1-ikev2-keyring
 peer if-ipsec1-ikev2-keyring-peer
  address 10.4.5.226
  pre-shared-key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

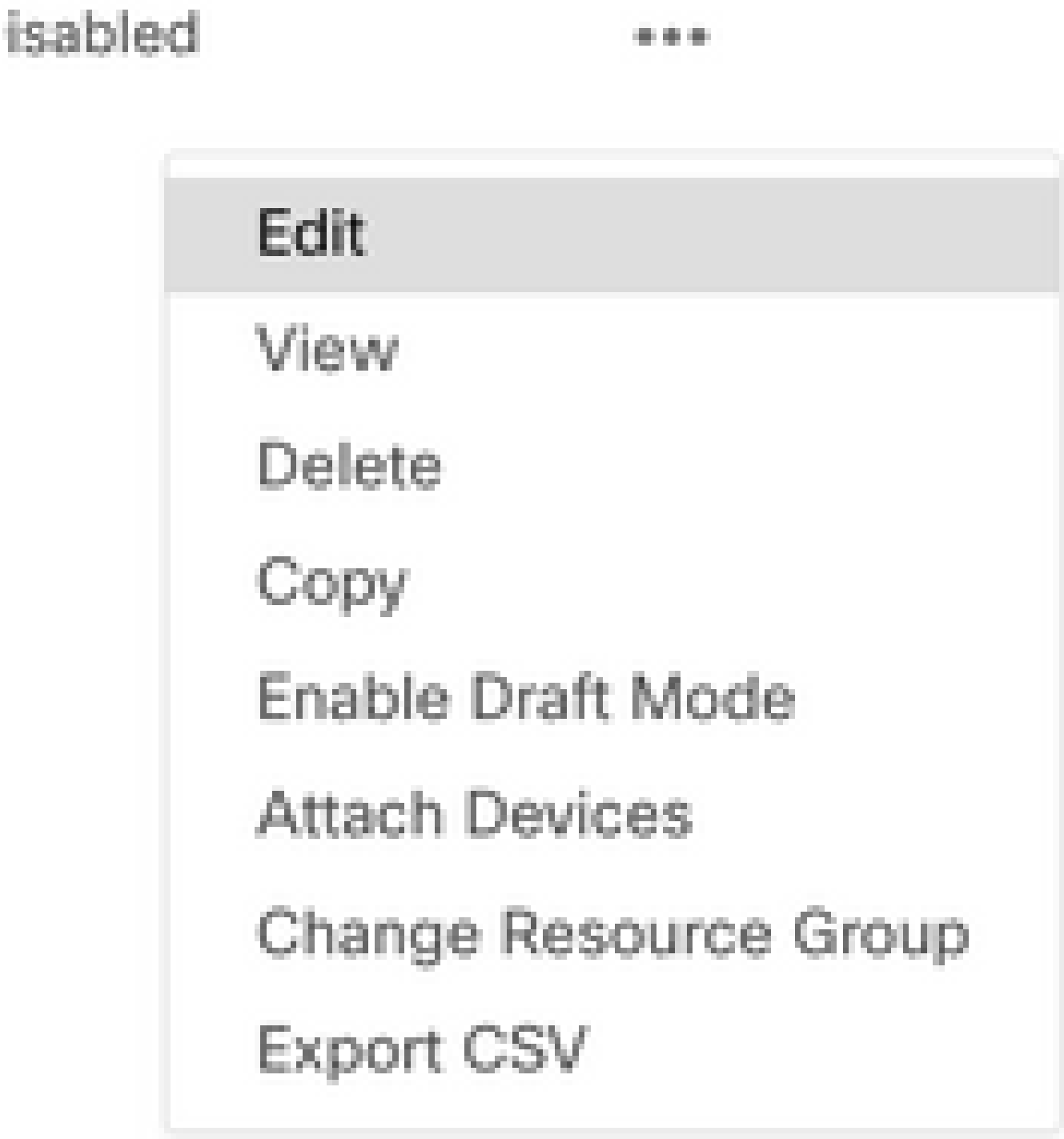
```
 authentication remote pre-share
 authentication local pre-share
 keyring local if-ipsec1-ikev2-keyring
 dpd 10 3 on-demand
 no config-exchange request

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
!
```

Étape 8. Cliquez sur Enregistrer.

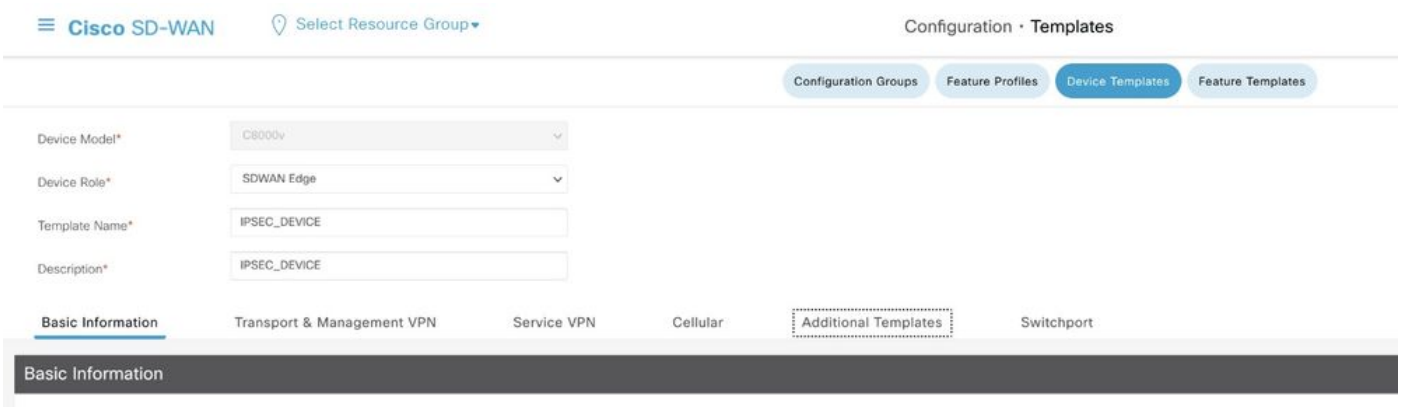
Étape 9. Accédez à Modèles de périphérique.



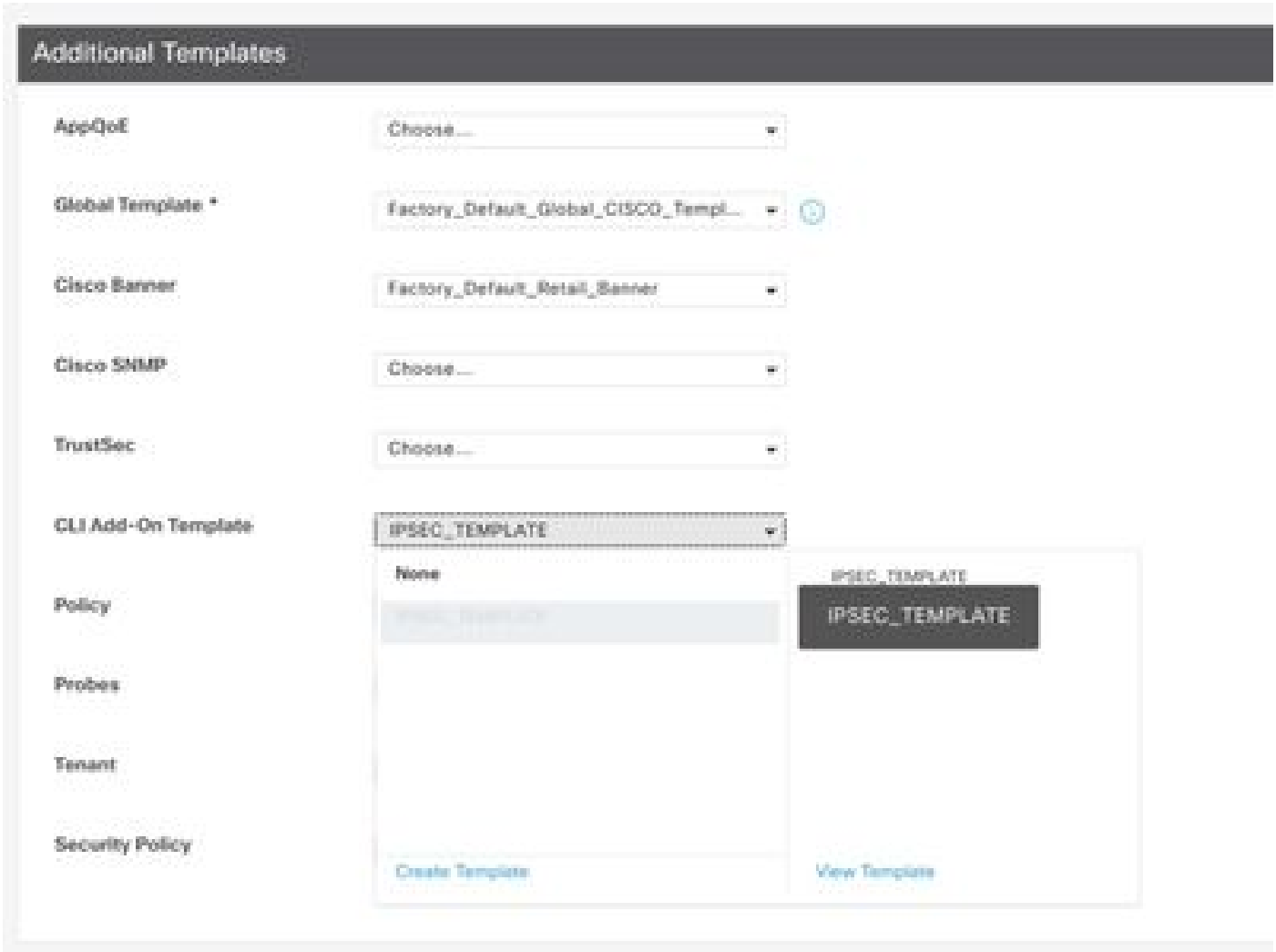
Étape 10. Choisissez le modèle de périphérique approprié et modifiez-le sur les 3 points.



Étape 11. Accédez à Modèles supplémentaires.

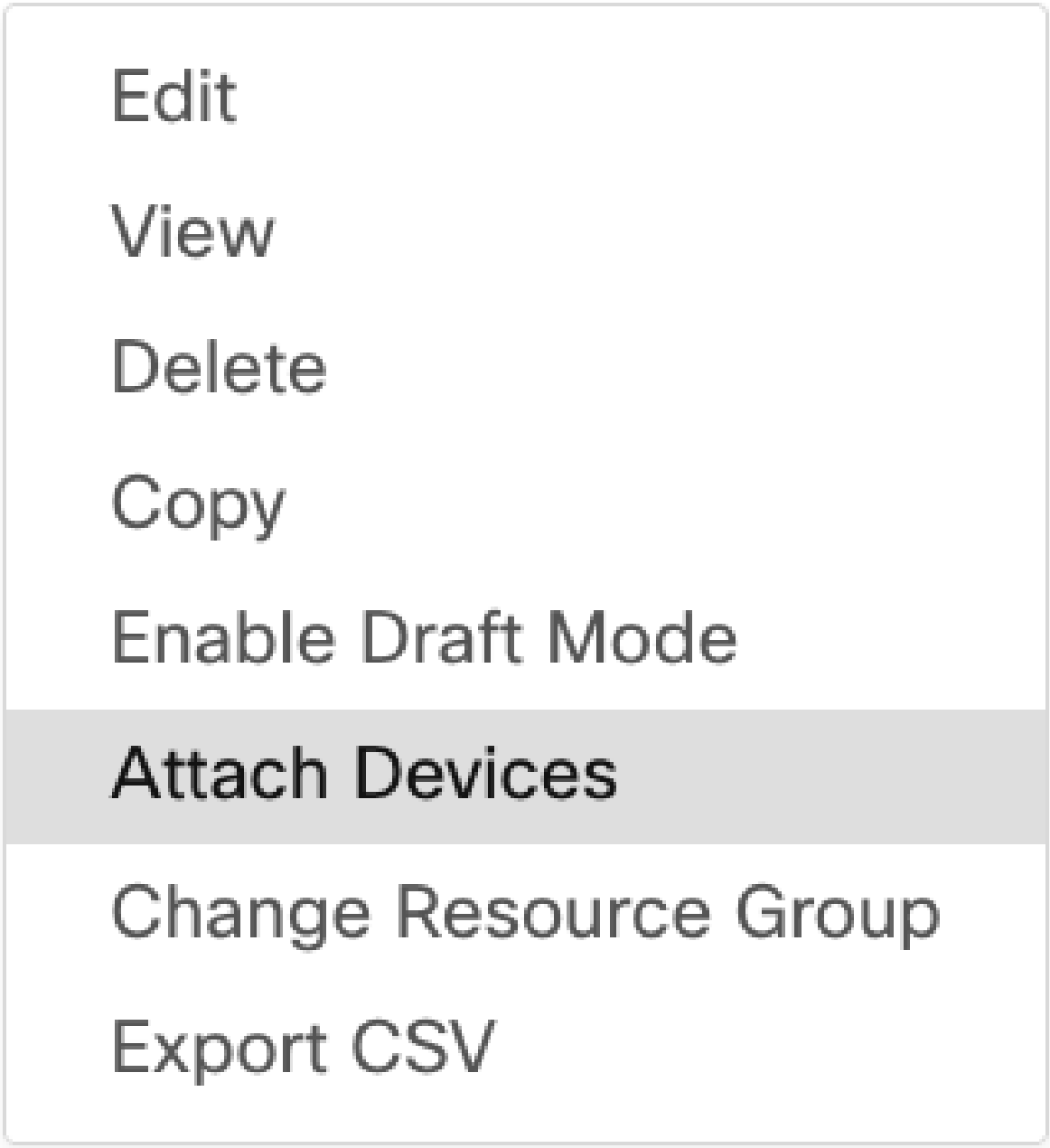


Étape 12. Dans Modèle de module complémentaire CLI, sélectionnez le modèle de fonction créé précédemment.



Étape 13. Cliquez sur Update.

Étape 14. Cliquez sur Attach Devices à partir de 3 points et sélectionnez le routeur correct vers lequel pousser le modèle.



Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Exécutez la commande show ip interface brief pour vérifier l'état du 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#
```

Dépannage

Exécutez la commande show crypto ikev2 session pour afficher des informations détaillées sur les sessions IKEv2 établies sur le périphérique.

<#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#
```

Exécutez la commande show crypto ipsec sa interface Tunnel100001 pour afficher des informations sur les associations de sécurité 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#
```

Exécutez la commande show crypto ikev2 statistics pour afficher les statistiques et les compteurs liés aux sessions 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#
```

Exécutez la commande show crypto session pour afficher des informations sur les sessions de sécurité actives sur le périphérique.

<#root>

```
cEdge#
```

show crypto session

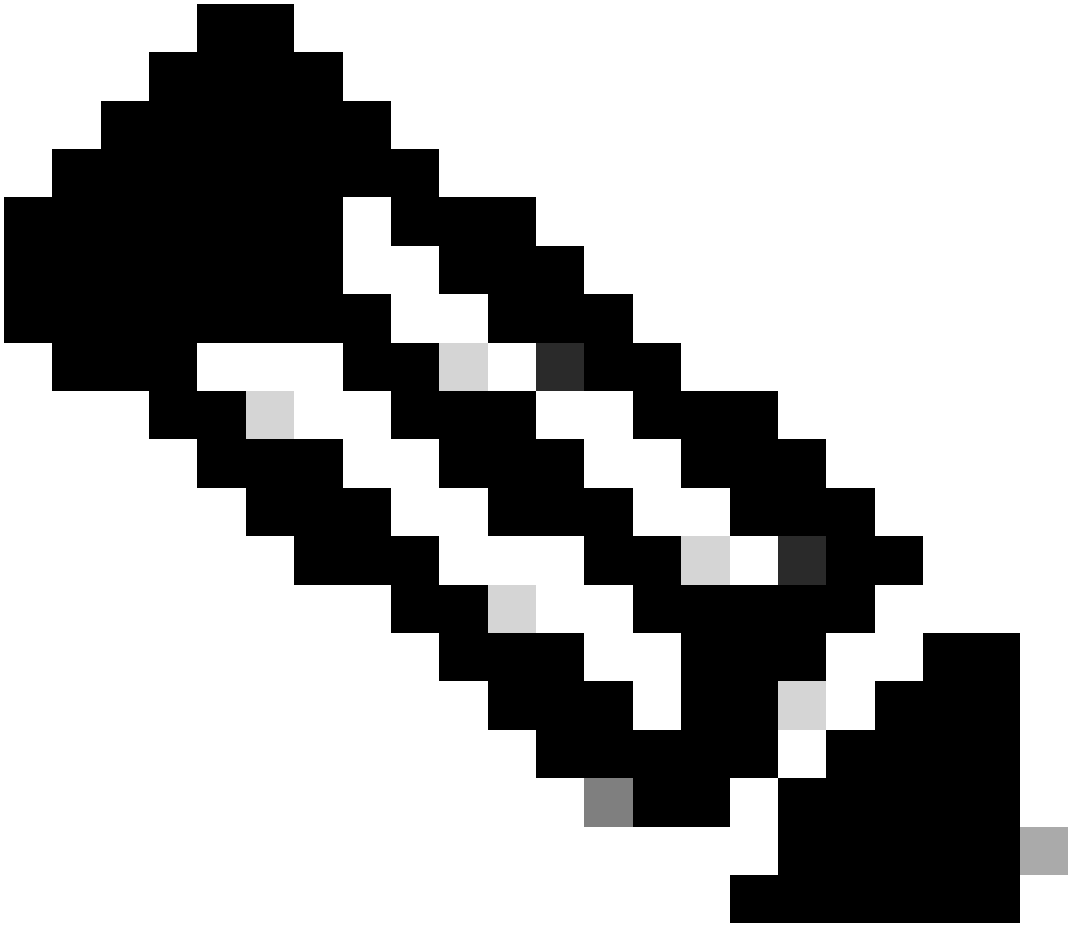
```
Crypto session current status

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
```

Pour obtenir des informations sur les abandons de paquets liés à IPSec dans le processeur de paquets du périphérique, vous pouvez exécuter :

show platform hardware qfp active feature ipsec datapath drops clear

show platform hardware qfp active statistics drop clear

Ces commandes doivent être placées avant pour fermer et ne pas fermer l'interface du tunnel pour effacer les compteurs et les statistiques, cela peut aider à obtenir des informations sur les abandons de paquets liés à IPsec dans un chemin de données de processeur de paquets de périphérique.



Remarque : ces commandes peuvent être exécutées sans que l'option soit désactivée. Il est important de souligner que les compteurs de gouttes sont historiques.

<#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#

Après avoir fermé et non fermé l'interface de tunnel, vous pouvez exécuter ces commandes pour voir s'il y avait un enregistrement de nouvelles statistiques ou compteurs :

Show ip interface brief (afficher un aperçu de l'interface IP) | inclure 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#
```

Commandes utiles

<#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

Informations connexes

Clés IPsec par paire

Guide de configuration de la sécurité Cisco Catalyst SD-WAN, Cisco IOS® XE Catalyst SD-WAN version 17.x

Présentation de la technologie Cisco IPsec

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.