Configurer une interface de tunnel virtuel multi-SA sur un routeur Cisco IOS XE

Contenu

Introduction

Ce document décrit comment configurer une interface VTI (Virtual Tunnel Interface) multi-sécurité (Multi-SA) sur les routeurs Cisco avec le logiciel Cisco IOS® XE. Le processus de migration est également décrit. Multi-SA VTI remplace la configuration VPN basée sur une carte de chiffrement (basée sur des politiques). Il est rétrocompatible avec les mises en oeuvre basées sur des cartes de chiffrement et d'autres stratégies. La prise en charge de cette fonctionnalité est disponible dans Cisco IOS XE version 16.12 et ultérieure.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître une configuration VPN IPsec sur les routeurs Cisco IOS XE.

Components Used

Les informations de ce document sont basées sur un routeur à services intégrés (ISR) 4351 avec Cisco IOS XE version 16.12.01a .

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Avantages des VTI par rapport aux cartes cryptographiques

Une carte de chiffrement est une fonction de sortie de l'interface physique. Les tunnels vers différents homologues sont configurés sous la même carte de chiffrement. Les entrées ACL (crypto map Access Control List) sont utilisées pour faire correspondre le trafic à envoyer à un homologue VPN spécifique. Ce type de configuration est également appelé VPN basé sur des politiques.

Dans le cas des VTI, chaque tunnel VPN est représenté par une interface de tunnel logique distincte. La table de routage décide à quel homologue VPN le trafic est envoyé. Ce type de configuration est également appelé VPN basé sur une route.

Dans les versions antérieures à la version 16.12 de Cisco IOS XE, la configuration VTI n'était pas compatible avec la configuration de la carte de chiffrement. Les deux extrémités du tunnel devaient être configurées avec le même type de VPN afin d'interagir.

Dans la version 16.12 de Cisco IOS XE, de nouvelles options de configuration ont été ajoutées qui permettent à l'interface de tunnel d'agir comme un VPN basé sur des politiques au niveau du protocole, mais ont toutes les propriétés de l'interface de tunnel.

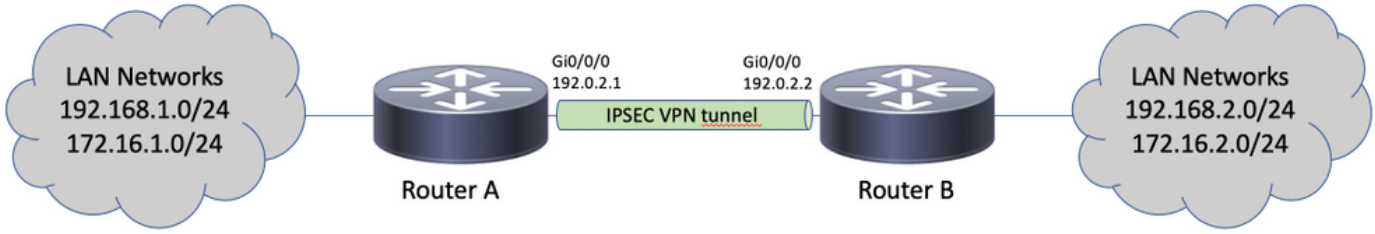
Cisco a annoncé les dates de fin de vie de la fonction Cisco IPsec Static Crypto Map et Dynamic Crypto Map de la version 17.6 de Cisco IOS XE.

Les avantages de VTI par rapport à la crypto-carte sont les suivants :

- Il est plus facile de déterminer l'état actif/inactif du tunnel.
- Il est plus facile à dépanner.
- Il peut appliquer des fonctionnalités telles que QoS (Quality of Service), ZBF (Zone-Based Firewall), NAT (Network Address Translation) et Netflow par tunnel.
- Il possède une configuration rationalisée pour tous les types de tunnels VPN.

Configuration

Diagramme du réseau



Considérations relatives au routage

L’administrateur doit s’assurer que le routage des réseaux distants pointe vers l’interface du tunnel. Les **reverse-route** sous le profil IPsec peut être utilisé pour créer automatiquement des routes statiques pour les réseaux spécifiés dans la liste de contrôle d'accès de chiffrement. De telles routes peuvent également être ajoutées manuellement. S'il existe des routes plus spécifiques précédemment configurées, qui pointent vers une interface physique au lieu de l'interface de tunnel, elles doivent être supprimées.

Exemples de configuration

Migration d'un tunnel IKEv1 basé sur une carte de chiffrement vers une infrastructure sVTI multi-SA

Les deux routeurs sont préconfigurés avec la solution crypto-map IKEv1 (Internet Key Exchange Version 1) :

Router A

```
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp key cisco123 address 192.0.2.2
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
match address CACL
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
```

Router B

```
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp key cisco123 address 192.0.2.1
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.1
set transform-set TSET
match address CACL
!
```

```
ip access-list extended CACL
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.2 255.255.255.0
crypto map CMAP
```

Afin de migrer le routeur A vers une configuration VTI multi-SA, complétez ces étapes. Le routeur B peut conserver l'ancienne configuration ou être reconfiguré de la même manière :

1. Supprimez la carte de chiffrement de l'interface :
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Créez le profil IPsec. Reverse-route est éventuellement configuré pour que les routes statiques des réseaux distants soient automatiquement ajoutées à la table de routage :
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. Configurez l'interface de tunnel. La liste de contrôle d'accès de chiffrement est connectée à la configuration du tunnel en tant que stratégie IPsec. L'adresse IP configurée sur l'interface de tunnel n'est pas pertinente, mais elle doit être configurée avec une certaine valeur. L'adresse IP peut être empruntée à l'interface physique avec le **ip unnumbered** commande :
   ```
   interface Tunnel0
   ip unnumbered GigabitEthernet0/0/0
   tunnel source GigabitEthernet0/0/0
   tunnel mode ipsec ipv4
   tunnel destination 192.0.2.2
   tunnel protection ipsec policy ipv4 CACL
   tunnel protection ipsec profile PROF
   ```
4. L'entrée de la carte de chiffrement peut être supprimée complètement après :
   ```
   no crypto map CMAP 10
   ```

Configuration finale du routeur A

```
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp key cisco123 address 192.0.2.2
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ipsec profile PROF
set transform-set TSET
reverse-route
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
!
interface Tunnel0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

Migration d'un tunnel IKEv2 basé sur une carte de chiffrement vers une sVTI multi-SA

Les deux routeurs sont préconfigurés avec la solution crypto-map IKEv2 (Internet Key Exchange Version 2) :

Router A

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.2 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
set ikev2-profile PROF
match address CACL
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
```

Router B

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.1 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.1
set transform-set TSET
set ikev2-profile PROF
match address CACL
!
ip access-list extended CACL
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.2 255.255.255.0
crypto map CMAP
```

Afin de migrer le routeur A vers une configuration VTI multi-SA, complétez ces étapes. Le routeur B peut conserver l'ancienne configuration ou être reconfiguré de la même manière.

1. Supprimez la carte de chiffrement de l'interface :
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Créez le profil IPsec. Les **reverse-route** est éventuellement configurée pour que les routes statiques des réseaux distants soient automatiquement ajoutées à la table de routage :

```
crypto ipsec profile PROF
set transform-set TSET
set ikev2-profile PROF
reverse-route
```

3. Configurez l'interface de tunnel. La liste de contrôle d'accès de chiffrement est connectée à la configuration du tunnel en tant que stratégie IPsec. L'adresse IP configurée sur l'interface de tunnel n'est pas pertinente, mais elle doit être configurée avec une certaine valeur. L'adresse IP peut être empruntée à l'interface physique avec le **ip unnumbered** commande :

```
interface Tunnel0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

4. Supprimez complètement la carte de chiffrement après :

```
no crypto map CMAP 10
```

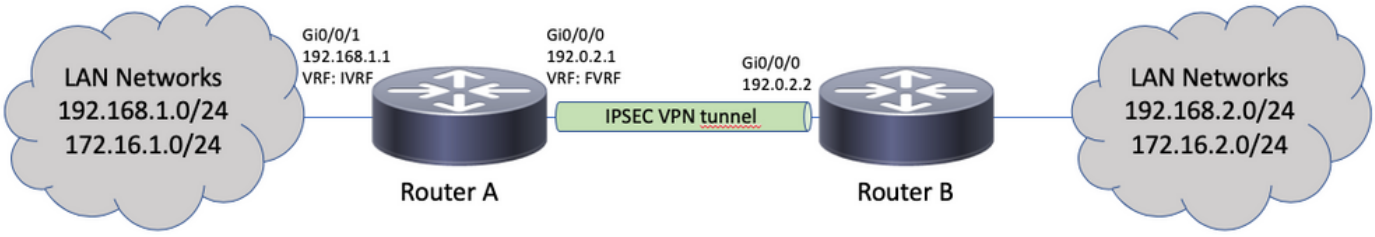
Configuration finale du routeur A

```
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto ikev2 profile PROF
match identity remote address 192.0.2.2 255.255.255.255
authentication remote pre-share key cisco123
authentication local pre-share key cisco123
!
crypto ipsec profile PROF
set transform-set TSET
set ikev2-profile PROF
reverse-route
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
interface GigabitEthernet0/0/0
ip address 192.0.2.1 255.255.255.0
!
interface Tunnel0
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

Migration d'une carte de chiffrement VRF vers une VTI multi-SA

Cet exemple montre comment migrer la configuration de crypto-carte compatible VRF.

Topologie



Configuration de la carte de chiffrement

```
ip vrf fvrf
ip vrf ivrf
!
crypto keyring KEY vrf fvrf
pre-shared-key address 192.0.2.2 key cisco123
!
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp profile PROF
vrf ivrf
keyring KEY
match identity address 192.0.2.2 255.255.255.255 fvrf
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 192.0.2.2
set transform-set TSET
set isakmp-profile PROF
match address CACL
!
interface GigabitEthernet0/0/0
ip vrf forwarding fvrf
ip address 192.0.2.1 255.255.255.0
crypto map CMAP
!
interface GigabitEthernet0/0/1
ip vrf forwarding ivrf
ip address 192.168.1.1 255.255.255.0
!
ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

Voici les étapes requises pour migrer vers VTI multi-SA :

```
! vrf configuration under isakmp profile is only for crypto map based configuration
!
crypto isakmp profile PROF
no vrf ivrf
!
interface GigabitEthernet0/0/0
no crypto map
!
no crypto map CMAP 10
!
no ip route vrf ivrf 172.16.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
no ip route vrf ivrf 192.168.2.0 255.255.255.0 GigabitEthernet0/0/0 192.0.2.2
!
crypto ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
```

```
reverse-route
!
interface tunnel0
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel vrf fvrf
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

Configuration VRF finale

```
ip vrf fvrf
ip vrf ivrf
!
crypto keyring KEY vrf fvrf
pre-shared-key address 192.0.2.2 key cisco123
!
crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14
!
crypto isakmp profile PROF
keyring KEY
match identity address 192.0.2.2 255.255.255.255 fvrf
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
!
interface GigabitEthernet0/0/0
ip vrf forwarding fvrf
ip address 192.0.2.1 255.255.255.0
!
interface GigabitEthernet0/0/1
ip vrf forwarding ivrf
ip address 192.168.1.1 255.255.255.0
!
ip access-list extended CACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
!
crypto ipsec profile PROF
set transform-set TSET
set isakmp-profile PROF
reverse-route
!
interface tunnel0
ip vrf forwarding ivrf
ip unnumbered GigabitEthernet0/0/0
tunnel source GigabitEthernet0/0/0
tunnel mode ipsec ipv4
tunnel destination 192.0.2.2
tunnel vrf fvrf
tunnel protection ipsec policy ipv4 CACL
tunnel protection ipsec profile PROF
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'analyseur CLI de Cisco (clients enregistrés uniquement) prend en charge certaines **show** . Utiliser l'analyseur CLI de Cisco afin d'afficher une analyse de **show** sortie de commande.

Afin de vérifier si le tunnel a été négocié avec succès, l'état de l'interface du tunnel peut être vérifié. Les deux dernières colonnes : Status et Protocol - afficher un état de up lorsque le tunnel est opérationnel :

```
RouterA#show ip interface brief | include Interface|Tunnel0
Interface IP-Address OK? Method Status Protocol
Tunnel0 192.0.2.1 YES TFTP up                    up
```

Pour plus d'informations sur l'état actuel de la session de chiffrement, reportez-vous à la section **show crypto session** sortie. Les Session status de UP-ACTIVE indique que la session IKE a été négociée correctement :

```
RouterA#show crypto session interface tunnel0
Crypto session current status

Interface: Tunnel0
Profile: PROF
Session status: UP-ACTIVE
Peer: 192.0.2.2 port 500
Session ID: 2
IKEv2 SA: local 192.0.2.1/500 remote 192.0.2.2/500 Active
IPSEC FLOW: permit ip 172.16.1.0/255.255.255.0 172.16.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

Vérifiez que le routage vers le réseau distant pointe sur l'interface de tunnel correcte :

```
RouterA#show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
Known via "static", distance 1, metric 0 (connected)
Routing Descriptor Blocks:
* directly connected, via Tunnel0
Route metric is 0, traffic share count is 1

RouterA#show ip cef 192.168.2.100
192.168.2.0/24
attached to Tunnel0
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Afin de dépanner la négociation de protocole IKE, utilisez ces débogages :

> **Note**: Référez-vous à Informations importantes sur les commandes de débogage avant d'utiliser **debug** .

```
! For IKEv1-based scenarios:
debug crypto isakmp
debug crypto ipsec
```

```
! For IKEv2-based scenarios:
debug crypto ikev2
debug crypto ipsec
```

Forum aux questions

Le tunnel s'active-t-il automatiquement ou le trafic est-il nécessaire pour le faire passer ?

Contrairement aux crypto-cartes, les tunnels VTI multi-SA s'activent automatiquement, que le trafic de données correspondant à la liste de contrôle d'accès cryptographique circule ou non sur le routeur. Les tunnels restent en service tout le temps, même s'il n'y a pas de trafic intéressant.

Que se passe-t-il si le trafic est acheminé via le VTI, mais que la source ou la destination du trafic ne correspond pas à la liste de contrôle d'accès de chiffrement configurée comme stratégie IPsec pour ce tunnel ?

Un tel scénario n'est pas pris en charge. Seul le trafic destiné à être chiffré doit être acheminé vers l'interface du tunnel. Le routage basé sur des politiques (PBR) peut être utilisé pour acheminer uniquement le trafic spécifique vers le VTI. PBR peut utiliser la liste de contrôle d'accès de la stratégie IPsec pour correspondre au trafic à acheminer vers le VTI.

Chaque paquet est vérifié par rapport à la stratégie IPsec configurée et doit correspondre à la liste de contrôle d'accès de chiffrement. S'il ne correspond pas, il n'est pas chiffré et est envoyé en texte clair depuis l'interface source du tunnel.

Dans le cas où le même VRF interne (iVRF) et le VRF avant (fVRF) sont utilisés (iVRF = fVRF), cela entraîne une boucle de routage et les paquets sont abandonnés avec une raison **Ipv4RoutingErr**. Les statistiques relatives à ces pertes peuvent être lues à l'aide de **show platform hardware qfp active statistics drop** commande :

```
RouterA#show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats Packets Octets
-------------------------------------------------------------------------
Ipv4RoutingErr 5 500
```

Si iVRF est différent de fVRF, les paquets qui entrent dans le tunnel dans iVRF et ne correspondent pas à la stratégie IPsec, quittez l'interface source du tunnel dans fVRF en texte clair. Ils ne sont pas abandonnés, car il n'y a pas de boucle de routage entre les VRF.

Les fonctionnalités telles que VRF, NAT, QoS, etc. sont-elles prises en charge sur les VTI multi-SA ?

Oui, toutes ces fonctionnalités sont prises en charge de la même manière que sur les tunnels VTI standard.