Een multi-SA virtuele tunnelinterface configureren op een Cisco IOS XE router

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
VTI's via encryptie-kaarten
Configureren
Netwerkdiagram
Routingoverwegingen
Configuratievoorbeelden
Migratie van een op Crypto Map gebaseerde IKEv1-tunnel naar een multi-SA sVTI
Migratie van een Crypto Map gebaseerde IKEv2-tunnelheid naar een Multi-SA sVTI
Migratie van een VRF-bewuste encryptie naar een multi-SA VTI
Verifiëren
Problemen oplossen
Veelgestelde vragen

Inleiding

Dit document beschrijft hoe u een multi-security associatie (Multi-SA) Virtual Tunnel Interface (VTI) op Cisco-routers kunt configureren met Cisco IOS® XE-software. Het migratieproces wordt ook beschreven. Multi-SA VTI is een vervanging voor de crypto kaart-gebaseerde (op beleid gebaseerde) VPN configuratie. Het is achterwaarts compatibel met crypto kaart-gebaseerde en andere beleidsgebaseerde implementaties. Ondersteuning voor deze optie is beschikbaar in Cisco IOS XE release 16.12 en hoger.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van een IPsec VPN-configuratie op Cisco IOS XE-routers.

Gebruikte componenten

De informatie in dit document is gebaseerd op een geïntegreerde services router (ISR) 4351 met Cisco IOS XE release 16.12.01a.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Achtergrondinformatie

VTI's via encryptie-kaarten

Een crypto kaart is een uitvoerfunctie van de fysieke interface. Tunnalen naar verschillende peers worden ingesteld onder dezelfde crypto-kaart. De crypto map Access Control List (ACL's) wordt gebruikt om het verkeer naar een bepaalde VPN-peer te koppelen. Dit type configuratie wordt ook een op beleid gebaseerde VPN genoemd.

In het geval van VTIs wordt elke VPN-tunnel weergegeven door een afzonderlijke logische tunnelinterface. De routingtabel bepaalt naar welke VPN-peer het verkeer wordt verzonden. Dit type configuratie wordt ook een route-gebaseerd VPN genoemd.

In releases eerder dan Cisco IOS XE release 16.12 was de VTI-configuratie niet compatibel met de configuratie van crypto-kaart. Beide uiteinden van de tunnel moesten met hetzelfde type VPN worden geconfigureerd om te kunnen samenwerken.

In Cisco IOS XE release 16.12 zijn nieuwe configuratieopties toegevoegd die de tunnelinterface toestaan om als op beleid gebaseerde VPN op het protocolniveau te fungeren maar alle eigenschappen van de tunnelinterface hebben.

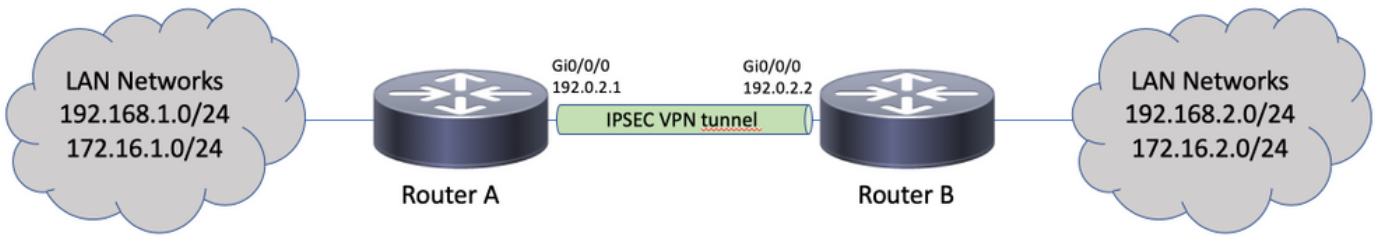
Cisco heeft de end-of-life datums aangekondigd voor de statische encryptie van Cisco IPsec en de functie Dynamische crypto kaart van Cisco IOS XE release 17.6.

De voordelen van VTI ten opzichte van crypto-kaart omvatten:

- Het is gemakkelijker om de tunnel op/neer status te bepalen.
- Het is makkelijker om problemen op te lossen.
- Het is in staat om functies als Quality of Service (QoS), Zone-Based Firewall (ZBF), Network Address Translation (NAT) en NetFlow op een basis per tunnel toe te passen.
- Het heeft een gestroomlijnde configuratie voor alle typen VPN-tunnels.

Configureren

Netwerkdiagram



Routingoverwegingen

De beheerder moet ervoor zorgen dat de routing voor externe netwerken naar de tunnelinterface

leidt. Het **reverse-route** De optie onder het profiel van IPsec kan worden gebruikt om automatisch statische routes voor de netwerken te creëren die in crypto ACL worden gespecificeerd. Zulke routes kunnen ook handmatig worden toegevoegd. Als er eerder ingestelde specifiekere routes zijn, die richting een fysieke interface in plaats van de tunnelinterface, moeten deze worden verwijderd.

Configuratievoorbeelden

Migratie van een op Crypto Map gebaseerde IKEv1-tunnel naar een multi-SA sVTI

Beide routers zijn vooraf ingesteld met de encryptie-gebaseerde oplossing van Internet Key Exchange, versie 1 (IKEv1):

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
```

Voltooi deze stappen om router A te migreren naar een VTI-configuratie met meerdere leveranciers. Router B kan bij de oude configuratie blijven of op dezelfde manier worden aangepast:

1. Verwijder de crypto-kaart van de interface:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Maak het IPsec-profiel. Reverse-route wordt naar keuze geconfigureerd om de statische routes voor externe netwerken automatisch aan de routingtabel toe te voegen:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. Configuratie van de tunnelinterface. De crypto ACL wordt aan de tunnelconfiguratie als beleid van IPsec bevestigd. Het IP-adres dat in de tunnelinterface is ingesteld is niet relevant, maar moet met een bepaalde waarde worden geconfigureerd. Het IP-adres kan worden geleend van de fysieke interface met de **ip unnumbered** opdracht:
   ```
   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. De crypto map-ingang kan daarna volledig worden verwijderd:
   ```
   no crypto map CMAP 10
   ```

   ### Configuratie van eindrouter 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
   ```

Migratie van een Crypto Map gebaseerde IKEv2-tunnelheid naar een Multi-SA sVTI

Beide routers zijn vooraf ingesteld met de IKEv2-encryptie (Internet Key Exchange, versie 2) op kaart gebaseerde oplossing:

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
```

Voltooi deze stappen om router A te migreren naar een VTI-configuratie met meerdere leveranciers. Router B kan bij de oude configuratie blijven of op dezelfde manier worden aangepast.

1. Verwijder de crypto-kaart van de interface:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Maak het IPsec-profiel. Het **reverse-route** commando is optioneel ingesteld om de statische

routes voor externe netwerken automatisch aan de routingtabel toe te voegen:

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

3. Configuratie van de tunnelinterface. De crypto ACL wordt aan de tunnelconfiguratie als beleid van IPsec bevestigd. Het IP-adres dat in de tunnelinterface is ingesteld is niet relevant, maar moet met een bepaalde waarde worden geconfigureerd. Het IP-adres kan worden geleend van de fysieke interface met de **ip unnumbered** opdracht:

```
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. Verwijder de crypto kaart volledig daarna:

```
no crypto map CMAP 10
```

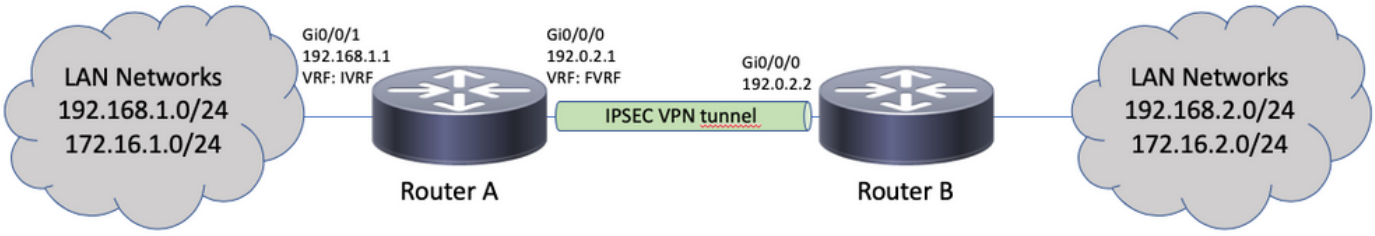
Configuratie van eindrouter A

```
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
```

Migratie van een VRF-bewuste encryptie naar een multi-SA VTI

Dit voorbeeld toont hoe te om de VRF-bewuste crypto kaartconfiguratie te migreren.

Topologie



Configuratie van versleuteling

```
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
```

Dit zijn de stappen die vereist zijn om te migreren naar multiSA VTI:

```
! 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
```

Definitieve VRF-bewuste configuratie

```
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
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De Cisco CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde **show** opdrachten. Gebruik de Cisco CLI Analyzer om een analyse van **show** opdrachtoutput.

Om te verifiëren of de tunnel succesvol is onderhandeld kan de status van de tunnelinterface worden gecontroleerd. De laatste twee kolommen - Status en Protocol - een status van up wanneer de tunnel in gebruik is :

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

Meer informatie over de huidige status van de crypto sessie is te vinden in **show crypto session** uitvoer. Het Session status van UP-ACTIVE geeft aan dat de IKE-sessie naar behoren is onderhandeld:

```
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
```

Controleer dat het routeren naar het externe netwerk via de juiste tunnelinterface wijst:

```
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
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Om de IKE-protocolonderhandeling problemen op te lossen, gebruikt u deze specificaties:

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u deze gebruikt **debug** opdrachten.

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

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

Veelgestelde vragen

Komt de tunnel automatisch of is er verkeer nodig om de tunnel op te trekken?

Anders dan met crypto kaarten komen de multi-SA VTI tunnels automatisch op, ongeacht of het gegevensverkeer dat de crypto ACL aanpast over de router stroomt of niet. De tunnels blijven de hele tijd omhoog, zelfs als er geen interessant verkeer is.

Wat gebeurt als het verkeer door het VTI wordt geleid, maar de bron of bestemming van het verkeer komt niet overeen met crypto ACL gevormd als beleid IPsec voor deze tunnel?

Een dergelijk scenario wordt niet ondersteund. Alleen het te versleutelen verkeer moet naar de tunnelinterface worden verstuurd. Op beleid gebaseerde routing (PBR) kan alleen worden gebruikt om specifiek verkeer naar de VTI te leiden. PBR kan het IPsec beleid ACL gebruiken om het verkeer aan VTI te koppelen.

Elk pakket wordt afgevinkt tegen het geconfigureerde IPsec-beleid en moet overeenkomen met de crypto-ACL. Als de tekst niet overeenkomt, wordt hij niet versleuteld en wordt hij in duidelijke tekst uit de interface van de tunnelbron verzonden.

Indien hetzelfde interne VRF (iVRF) en het voorste VRF (fVRF) worden gebruikt (iVRF = fVRF), resulteert dit in een routingloop en worden de pakketten met een reden gemaskeerd **Ipv4RoutingErr**. Statistieken voor dergelijke druppels zijn te zien bij de **show platform hardware qfp active statistics drop** opdracht:

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

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

Indien iVRF anders is dan fVRF, de pakketten die de tunnel in iVRF binnendringen en het beleid niet van IPsec aanpassen, de verbinding van de tunnelbron in fVRF in duidelijke tekst afsluiten. Ze worden niet laten vallen, omdat er geen routinglus tussen de VRF's is.

Zijn functies zoals VRF, NAT, QoS, enzovoort, ondersteund op multiSA VTI?

Ja, al deze functies worden op dezelfde manier ondersteund als in normale VTI-tunnels.