Konfigurieren einer virtuellen Multi-SA-Tunnel-Schnittstelle auf einem Cisco IOS XE-Router

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie eine Multi-Security Association (Multi-SA) Virtual Tunnel Interface (VTI) auf Cisco Routern mit der Cisco IOS® XE-Software konfiguriert wird. Der Migrationsprozess wird ebenfalls beschrieben. Multi-SA VTI ist ein Ersatz für die Verschlüsselungs-Map-basierte (richtlinienbasierte) VPN-Konfiguration. Er ist abwärtskompatibel mit Krypto-Map-basierten und anderen richtlinienbasierten Implementierungen. Diese Funktion wird ab Cisco IOS XE Version 16.12 unterstützt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse einer IPsec-VPN-Konfiguration auf Cisco IOS XE-Routern verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Integrated Services Router (ISR) 4351 mit Cisco IOS XE Version 16.12.01a .

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Vorteile von VTIs gegenüber Crypto Maps

Eine Crypto Map ist eine Ausgabefunktion der physischen Schnittstelle. Tunnel zu verschiedenen Peers werden unter derselben Crypto Map konfiguriert. Die Einträge in der Zugriffskontrollliste (ACL) für die Crypto Map werden verwendet, um den an einen bestimmten VPN-Peer zu sendenden Datenverkehr abzugleichen. Dieser Konfigurationstyp wird auch als richtlinienbasiertes VPN bezeichnet.

Bei VTIs wird jeder VPN-Tunnel durch eine separate logische Tunnelschnittstelle dargestellt. Die Routing-Tabelle bestimmt, an welchen VPN-Peer der Datenverkehr gesendet wird. Dieser Konfigurationstyp wird auch als routen VPN bezeichnet.

In Versionen vor Cisco IOS XE Version 16.12 war die VTI-Konfiguration nicht mit der Konfiguration der Crypto Map kompatibel. Beide Tunnelenden mussten mit demselben VPN-Typ konfiguriert werden, um miteinander zu arbeiten.

In der Cisco IOS XE Version 16.12 wurden neue Konfigurationsoptionen hinzugefügt, mit denen die Tunnelschnittstelle auf Protokollebene als richtlinienbasiertes VPN fungieren kann, aber über alle Eigenschaften der Tunnelschnittstelle verfügt.

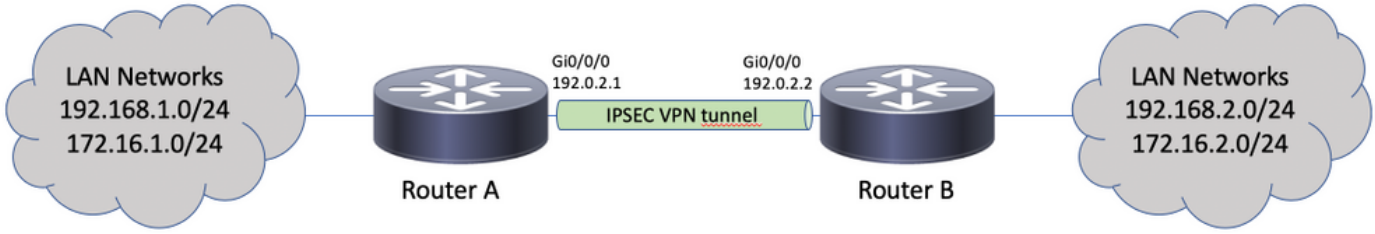
Cisco gab die End-of-Life-Termine für die Cisco IPsec Static Crypto Map- und die Dynamic Crypto Map-Funktion in Cisco IOS XE, Version 17.6, bekannt.

Zu den Vorteilen von VTI gegenüber der Crypto Map gehören:

- Es ist einfacher, den Tunnel-Ein-/Aus-Status zu bestimmen.
- Die Fehlerbehebung ist einfacher.
- Es kann Funktionen wie Quality of Service (QoS), zonenbasierte Firewall (ZBF), Network Address Translation (NAT) und Netflow auf Tunnelbasis anwenden.
- Sie bietet eine optimierte Konfiguration für alle Arten von VPN-Tunneln.

Konfigurieren

Netzwerkdiagramm



Überlegungen zum Routing

Der Administrator muss sicherstellen, dass das Routing für Remote-Netzwerke auf die Tunnelschnittstelle zeigt. Die Fehlermeldung **reverse-route** unter dem IPsec-Profil können automatisch statische Routen für die in der Krypto-ACL angegebenen Netzwerke erstellt werden. Solche Routen können auch manuell hinzugefügt werden. Wenn zuvor spezifischere Routen konfiguriert wurden, muss diese auf eine physische Schnittstelle und nicht auf die Tunnelschnittstelle ausgerichtet sein, und diese müssen entfernt werden.

Konfigurationsbeispiele

Migration eines Crypto Map-basierten IKEv1-Tunnels zu einem Multi-SA sVTI

Beide Router sind mit der Krypto-Map-Lösung für Internet Key Exchange Version 1 (IKEv1) vorkonfiguriert:

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
```

Führen Sie die folgenden Schritte aus, um Router A zu einer VTI-Konfiguration mit mehreren SAs zu migrieren. Router B kann mit der alten Konfiguration beibehalten oder auf ähnliche Weise neu konfiguriert werden:

1. Entfernen Sie die Crypto Map von der Schnittstelle:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Erstellen Sie das IPsec-Profil. Reverse-Route wird optional so konfiguriert, dass die statischen Routen für Remote-Netzwerke automatisch der Routing-Tabelle hinzugefügt werden:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. Konfigurieren Sie die Tunnelschnittstelle. Die Krypto-ACL wird als IPsec-Richtlinie an die Tunnelkonfiguration angeschlossen. Die auf der Tunnelschnittstelle konfigurierte IP-Adresse ist irrelevant, muss jedoch mit einem gewissen Wert konfiguriert werden. Die IP-Adresse kann von der physischen Schnittstelle mit dem **ip unnumbered** command:
   ```
   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. Der Crypto Map-Eintrag kann anschließend vollständig entfernt werden:
   ```
   no crypto map CMAP 10
   ```

Endgültige Router-A-Konfiguration

```
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 eines Crypto Map-basierten IKEv2-Tunnels zu einem Multi-SA sVTI

Beide Router sind mit der auf der Internet Key Exchange Version 2 (IKEv2) basierenden Krypto-Map-Lösung vorkonfiguriert:

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
```

Führen Sie die folgenden Schritte aus, um Router A zu einer VTI-Konfiguration mit mehreren SAs zu migrieren. Router B kann mit der alten Konfiguration beibehalten oder auf ähnliche Weise neu konfiguriert werden.

1. Entfernen Sie die Crypto Map von der Schnittstelle:

```
interface GigabitEthernet0/0/0
no crypto map
```

2. Erstellen Sie das IPsec-Profil. Die Fehlermeldung **reverse-route** ist optional so konfiguriert, dass die statischen Routen für Remote-Netzwerke automatisch der Routing-Tabelle hinzugefügt werden:

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

3. Konfigurieren Sie die Tunnelschnittstelle. Die Krypto-ACL wird als IPsec-Richtlinie an die Tunnelkonfiguration angeschlossen. Die auf der Tunnelschnittstelle konfigurierte IP-Adresse ist irrelevant, muss jedoch mit einem gewissen Wert konfiguriert werden. Die IP-Adresse kann von der physischen Schnittstelle mit dem **ip unnumbered** command:

```
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. Entfernen Sie anschließend die Crypto Map vollständig:

```
no crypto map CMAP 10
```

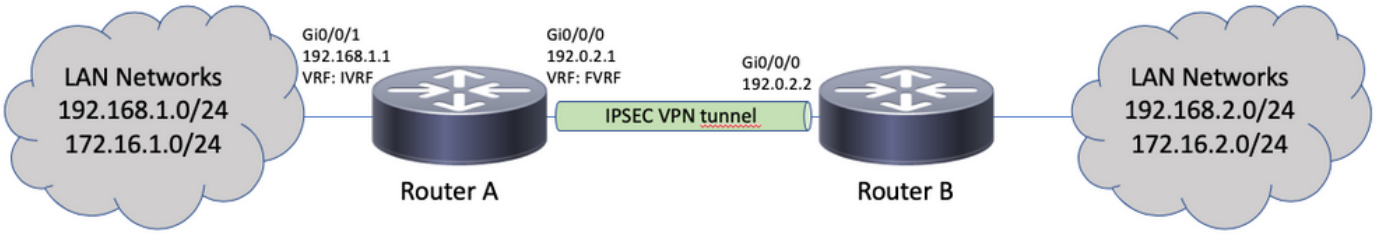
Endgültige Router-A-Konfiguration

```
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 einer VRF-kompatiblen Crypto Map zu einem Multi-SA VTI

Dieses Beispiel zeigt, wie die Konfiguration der VRF-kompatiblen Crypto Map migriert wird.

Topologie



Konfiguration der Crypto Map

```
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
```

Dies sind die erforderlichen Schritte für die Migration zu Multi-SA 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
```

Endgültige VRF-sensitive Konfiguration

```
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
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Der Cisco CLI Analyzer (nur registrierte Kunden) unterstützt bestimmte **show** Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse von **show** Befehlsausgabe.

Um zu überprüfen, ob der Tunnel erfolgreich verhandelt wurde, kann der Tunnelschnittstellenstatus überprüft werden. Die letzten beiden Spalten - Status und Protocol - den Status von up bei Betrieb des Tunnels:

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

Weitere Informationen zum aktuellen Status der Crypto-Sitzung finden Sie im . **show crypto session** Ausgabe. Die Fehlermeldung Session status von UP-ACTIVE gibt an, dass die IKE-Sitzung ordnungsgemäß verhandelt wurde:

```
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
```

Überprüfen Sie, ob das Routing zum Remote-Netzwerk über die richtige Tunnelschnittstelle erfolgt:

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Verwenden Sie zur Fehlerbehebung bei der IKE-Protokollverhandlung die folgenden Debugger:

> **Anmerkung:** Weitere Informationen zu Debug-Befehlen vor der Verwendung finden Sie unter Wichtige Informationen **debug** Befehle.

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

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

Häufig gestellte Fragen

Wird der Tunnel automatisch aktiviert oder ist für die Tunnelherstellung Datenverkehr erforderlich?

Im Gegensatz zu Crypto Maps werden die Multi-SA-VTI-Tunnel automatisch eingerichtet, unabhängig davon, ob der Datenverkehr, der mit der Krypto-ACL übereinstimmt, über den Router fließt oder nicht. Die Tunnel sind ständig verfügbar, auch wenn kein interessanter Verkehr vorhanden ist.

Was geschieht, wenn der Datenverkehr über das VTI weitergeleitet wird, die Quelle oder das Ziel des Datenverkehrs jedoch nicht mit der als IPsec-Richtlinie für diesen Tunnel konfigurierten Krypto-ACL übereinstimmt?

Ein solches Szenario wird nicht unterstützt. Nur der zur Verschlüsselung bestimmte Datenverkehr muss an die Tunnelschnittstelle weitergeleitet werden. Richtlinienbasiertes Routing (Policy-Based Routing, PBR) kann verwendet werden, um nur bestimmten Datenverkehr an das VTI weiterzuleiten. Der PBR kann die IPsec-Richtlinie-ACL verwenden, um den an das VTI weiterzuleitenden Datenverkehr abzugleichen.

Jedes Paket wird anhand der konfigurierten IPsec-Richtlinie geprüft und muss mit der Krypto-ACL übereinstimmen. Wenn sie nicht übereinstimmt, wird sie nicht verschlüsselt und in unverschlüsseltem Text aus der Tunnelquellenschnittstelle gesendet.

Falls dasselbe interne VRF (iVRF) und das Front-VRF (fVRF) verwendet werden (iVRF = fVRF), führt dies zu einer Routing-Schleife, und die Pakete werden aus einem Grund verworfen **Ipv4RoutingErr**. Statistiken zu solchen Fallstricken sind in der **show platform hardware qfp active statistics drop** command:

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

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

Falls sich die iVRF-Instanz von der fVRF-Instanz unterscheidet, verlassen die Pakete, die in iVRF in den Tunnel gelangen und nicht mit der IPsec-Richtlinie übereinstimmen, die Tunnelquellenschnittstelle in fVRF in Klartext. Sie werden nicht verworfen, da zwischen den VRFs keine Routingschleife besteht.

Werden Funktionen wie VRF, NAT, QoS usw. auf Multi-SA-VTI unterstützt?

Ja, alle diese Funktionen werden auf die gleiche Weise unterstützt wie bei regulären VTI-Tunneln.