Configurazione di un'interfaccia del tunnel virtuale multi-SA su un router Cisco IOS XE

Sommario

Introduzione

In questo documento viene descritto come configurare una VTI (Virtual Tunnel Interface) Multi-Security Association (Multi-SA) sui router Cisco con il software Cisco IOS® XE. Viene inoltre descritto il processo di migrazione. Multi-SA VTI sostituisce la configurazione VPN basata su mappa crittografica (basata su policy). È compatibile con le versioni precedenti con le implementazioni basate su mappe crittografiche e altre implementazioni basate su regole. Il supporto per questa funzione è disponibile in Cisco IOS XE versione 16.12 e successive.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di una configurazione VPN IPsec sui router Cisco IOS XE.

Componenti usati

Per questo documento, è stato usato un ISR (Integrated Services Router) 4351 con Cisco IOS XE versione 16.12.01a .

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Vantaggi delle VTI rispetto alle mappe crittografiche

Una mappa crittografica è una funzionalità di output dell'interfaccia fisica. I tunnel verso peer diversi sono configurati con la stessa mappa crittografica. Le voci dell'elenco di controllo di accesso (ACL) della mappa crittografica vengono utilizzate per far corrispondere il traffico da inviare a un peer VPN specifico. Questo tipo di configurazione viene anche definita VPN basata su criteri.

Nel caso delle VTI, ogni tunnel VPN è rappresentato da un'interfaccia tunnel logica separata. La tabella di routing decide a quale peer VPN inviare il traffico. Questo tipo di configurazione è detta anche VPN basata su route.

Nelle versioni precedenti a Cisco IOS XE versione 16.12, la configurazione VTI non era compatibile con la configurazione della mappa crittografica. Per poter interagire, entrambe le estremità del tunnel dovevano essere configurate con lo stesso tipo di VPN.

In Cisco IOS XE release 16.12, sono state aggiunte nuove opzioni di configurazione che consentono all'interfaccia del tunnel di agire come VPN basata su criteri a livello di protocollo, ma che hanno tutte le proprietà dell'interfaccia del tunnel.

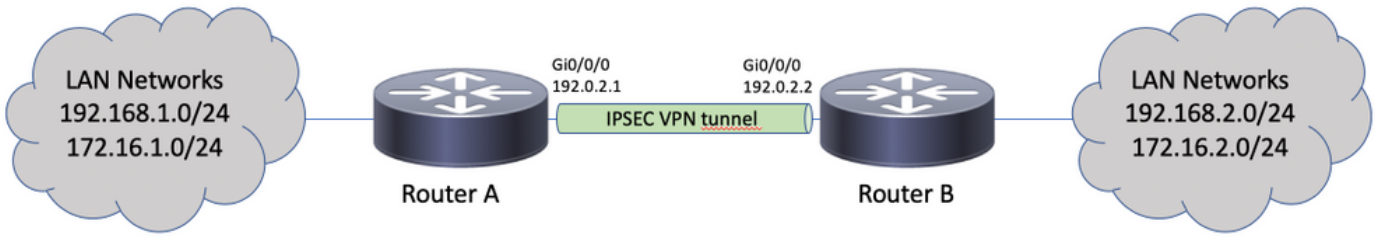
Cisco ha annunciato le date di fine del ciclo di vita delle funzionalità Cisco IPsec Static Crypto Map e Dynamic Crypto Map in Cisco IOS XE versione 17.6.

I vantaggi di VTI rispetto alla mappa crittografica includono:

- Èpiù facile determinare lo stato di attivazione/disattivazione del tunnel.
- La risoluzione dei problemi è più semplice.
- Può applicare funzionalità quali QoS (Quality of Service), ZBF (Zone-Based Firewall), NAT (Network Address Translation) e Netflow per tunnel.
- Offre una configurazione semplificata per tutti i tipi di tunnel VPN.

Configurazione

Esempio di rete



Considerazioni sull'instradamento

L'amministratore deve verificare che il routing delle reti remote punti all'interfaccia del tunnel. OSPF (Open Shortest Path First) **reverse-route** Questa opzione del profilo IPsec può essere utilizzata per creare automaticamente route statiche per le reti specificate nell'ACL crittografico. Tali route possono inoltre essere aggiunte manualmente. Se sono state configurate in precedenza route più specifiche, che puntano a un'interfaccia fisica anziché all'interfaccia del tunnel, devono essere rimosse.

Esempi di configurazione

Migrazione di un tunnel IKEv1 basato su mappa crittografica a un servizio Multi-SA sVTI

Entrambi i router sono preconfigurati con la soluzione basata su mappa crittografica IKEv1 (Internet Key Exchange versione 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
```

Per eseguire la migrazione del router A a una configurazione VTI multi-SA, attenersi alla seguente procedura. Il router B può rimanere con la vecchia configurazione o può essere riconfigurato in modo simile:

1. Rimuovere la mappa crittografica dall'interfaccia:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Creare il profilo IPSec. La funzione Reverse-route è configurata in modo da aggiungere automaticamente alla tabella di routing le route statiche per le reti remote:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. Configurare l'interfaccia del tunnel. L'ACL crittografico è collegato alla configurazione del tunnel come criterio IPsec. L'indirizzo IP configurato sull'interfaccia del tunnel è irrilevante, ma deve essere configurato con un valore. L'indirizzo IP può essere preso in prestito dall'interfaccia fisica con **ip unnumbered** comando:
   ```
   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. La voce della mappa crittografica può essere rimossa completamente in seguito:
   ```
   no crypto map CMAP 10
   ```

Configurazione finale del 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 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
```

Migrazione di un tunnel IKEv2 basato su mappa crittografica a un servizio Multi-SA sVTI

Entrambi i router sono preconfigurati con la soluzione basata su mappa crittografica IKEv2 (Internet Key Exchange versione 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
```

Per eseguire la migrazione del router A a una configurazione VTI multi-SA, attenersi alla seguente procedura. Il router B può rimanere con la precedente configurazione o può essere riconfigurato in modo simile.

1. Rimuovere la mappa crittografica dall'interfaccia:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Creare il profilo IPSec. OSPF (Open Shortest Path First) **reverse-route** Il comando è configurato

in modo da aggiungere automaticamente le route statiche per le reti remote alla tabella di routing:

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

3. Configurare l'interfaccia del tunnel. L'ACL crittografico è collegato alla configurazione del tunnel come criterio IPsec. L'indirizzo IP configurato sull'interfaccia del tunnel è irrilevante, ma deve essere configurato con un valore. L'indirizzo IP può essere preso in prestito dall'interfaccia fisica con **ip unnumbered** comando:

```
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. Rimuovere la mappa crittografica completamente dopo:

```
no crypto map CMAP 10
```

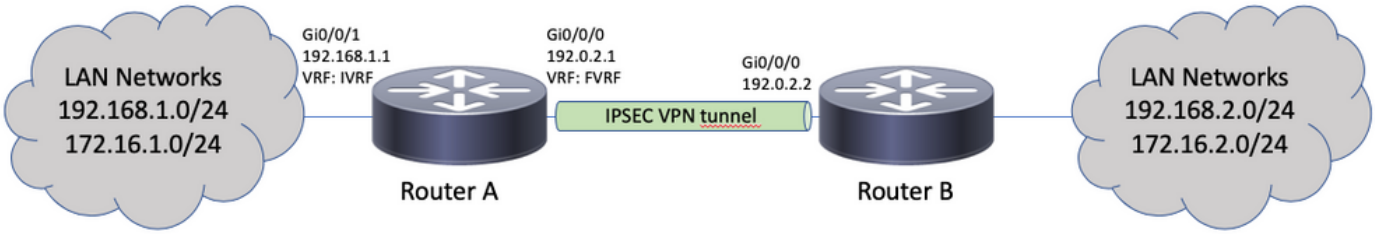
Configurazione finale del router A

```
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 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
```

Migrazione di una mappa crittografica compatibile con VRF a una VTI multi-SA

Nell'esempio viene mostrato come eseguire la migrazione della configurazione della mappa crittografica con riconoscimento VRF.

Topologia



Configurazione mappa crittografica

```
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
```

Di seguito sono riportati i passaggi necessari per eseguire la migrazione a 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
```

Configurazione finale compatibile con VRF

```
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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Cisco CLI Analyzer (solo utenti registrati) supporta alcuni **show** comandi. Usare Cisco CLI Analyzer per visualizzare un'analisi di **show** output del comando.

Per verificare se la negoziazione del tunnel ha esito positivo, è possibile controllare lo stato dell'interfaccia del tunnel. Le ultime due colonne: Status e Protocol - visualizzare lo stato up quando il tunnel è operativo:

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

Per ulteriori dettagli sullo stato corrente della sessione crittografica, consultare la **show crypto session** uscita. OSPF (Open Shortest Path First) Session status di UP-ACTIVE indica che la sessione IKE è stata negoziata correttamente:

```
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
```

Verificare che il routing alla rete remota punti sull'interfaccia del tunnel corretta:

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per risolvere i problemi relativi alla negoziazione del protocollo IKE, utilizzare i seguenti debug:

Nota: consultare le informazioni importanti sui comandi di debug prima di usare **debug** comandi.

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

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

Domande frequenti

Il tunnel viene attivato automaticamente o è necessario il traffico per attivare il tunnel?

A differenza delle mappe crittografiche, i tunnel VTI multi-SA vengono visualizzati automaticamente a prescindere dal fatto che il traffico di dati che corrisponde all'ACL crittografico fluisca o meno sul router. I tunnel rimangono sempre in piedi, anche se non c'è traffico interessante.

Cosa succede se il traffico viene instradato attraverso la VTI, ma l'origine o la destinazione del traffico non corrisponde all'ACL di crittografia configurato come criterio IPsec per il tunnel?

Questo scenario non è supportato. Solo il traffico che si desidera crittografare deve essere indirizzato all'interfaccia del tunnel. Il PBR (Policy-Based Routing) può essere utilizzato per indirizzare solo il traffico specifico alla VTI. PBR può utilizzare l'ACL del criterio IPsec per far corrispondere il traffico da instradare alla VTI.

Ogni pacchetto viene controllato in base al criterio IPsec configurato e deve corrispondere all'ACL di crittografia. Se non corrisponde, non viene crittografato e inviato in formato testo non crittografato dall'interfaccia di origine del tunnel.

Se si usa lo stesso VRF (iVRF) interno e lo stesso VRF (fVRF) anteriore (iVRF = fVRF), si verifica un loop di routing e i pacchetti vengono scartati, indicando il motivo **Ipv4RoutingErr**. Le statistiche relative a tali cadute possono essere visualizzate con **show platform hardware qfp active statistics drop** comando:

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

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

Se il protocollo iVRF è diverso da fVRF, i pacchetti che entrano nel tunnel in iVRF e non corrispondono ai criteri IPsec, uscire dall'interfaccia dell'origine del tunnel in fVRF in testo non crittografato. Non vengono scartati, in quanto non vi è alcun loop di routing tra i VRF.

Caratteristiche quali VRF, NAT, QoS e così via sono supportate su VTI multi-SA?

Sì, tutte queste funzionalità sono supportate allo stesso modo dei normali tunnel VTI.