在Cisco IOS XE路由器上配置多SA虛擬隧道介面

目錄

簡介

本檔案介紹如何在使用Cisco IOS® XE軟體的Cisco路由器上設定多重安全關聯（多SA）虛擬通道介面(VTI)。還描述了遷移過程。多SA VTI是密碼編譯對應的（原則型）VPN配置的替代方案。它與基於加密對映的實現和其它基於策略的實現向後相容。Cisco IOS XE版本16.12及更高版本提供對此功能的支援。

必要條件

需求

Cisco建議您瞭解Cisco IOS XE路由器上的IPsec VPN配置。

採用元件

本檔案中的資訊是根據整合式服務路由器(ISR)4351，其採用Cisco IOS XE版本16.12.01a 。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

VTI優於密碼編譯對應

加密對映是物理介面的輸出功能。到不同對等體的隧道是在同一個加密對映下配置的。加密對映訪問控制清單(ACL)條目用於匹配要傳送到特定VPN對等體的流量。這種型別的配置也稱為基於策略的VPN。

對於VTI，每個VPN隧道都由一個單獨的邏輯隧道介面表示。路由表決定流量傳送到哪個VPN對等裝置。這種型別的配置也稱為基於路由的VPN。

在低於Cisco IOS XE版本16.12的版本中，VTI配置與加密對映配置不相容。隧道的兩端必須配置相同型別的VPN才能實現互操作。

在Cisco IOS XE版本16.12中，新增了新配置選項，允許隧道介面在協定級別上充當基於策略的VPN，但具有隧道介面的所有屬性。

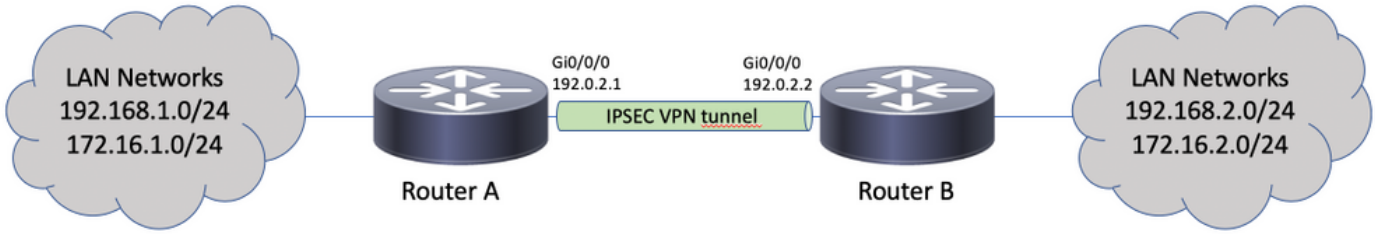
Cisco宣佈Cisco IOS XE 17.6版中的Cisco IPsec靜態加密對映和動態加密對映功能的壽命終止日期。

VTI相對於加密對映的優勢包括：

- 更容易確定通道的開啟/關閉狀態。
- 故障排除更容易。
- 它能夠根據隧道應用服務品質(QoS)、基於區域的防火牆(ZBF)、網路地址轉換(NAT)和Netflow等功能。
- 它為所有型別的VPN隧道提供了簡化的配置。

設定

網路圖表



路由注意事項

管理員必須確保遠端網路的路由指向隧道介面。其 **reverse-route** ipsec配置檔案下的選項可用於為加密ACL中指定的網路自動建立靜態路由。此類路由也可以手動新增。如果之前配置了更具體的路由，則指向物理介面而不是隧道介面，必須刪除這些路由。

組態範例

基於加密對映的IKEv1隧道到多SA sVTI的遷移

兩台路由器都預配置了基於網際網路金鑰交換版本1(IKEv1)加密對映的解決方案：

路由器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
```

路由器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
```

若要將路由器A遷移到多SA VTI配置，請完成以下步驟。路由器B可以保留舊的配置，也可以類似地重新配置：

1. 從介面移除密碼編譯對應：
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. 建立IPsec配置檔案。也可將Reverse-route配置為將遠端網路的靜態路由自動新增到路由表中：
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. 配置隧道介面。加密ACL作為IPsec策略附加到隧道配置。通道介面上設定的IP位址不相關

，但必須設定一些值。IP地址可以從物理介面借用 **ip unnumbered** 指令:

```
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. 之後可以完全移除密碼編譯對應專案：

```
no crypto map CMAP 10
```

路由器A的最終配置

```
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
```

基於加密對映的IKEv2隧道到多SA sVTI的遷移

兩台路由器都預配置了基於網際網路金鑰交換版本2(IKEv2)加密對映的解決方案：

路由器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
```

路由器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
```

若要將路由器A遷移到多SA VTI配置，請完成以下步驟。路由器B可以保留舊的配置，也可以類似地重新配置。

1. 從介面移除密碼編譯對應：
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. 建立IPsec配置檔案。其 **reverse-route** 命令可以配置為將遠端網路的靜態路由自動新增到路由表中：
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   set ikev2-profile PROF
   reverse-route
   ```
3. 配置隧道介面。加密ACL作為IPsec策略附加到隧道配置。通道介面上設定的IP位址不相關，但必須設定一些值。IP地址可以從物理介面借用 **ip unnumbered** 指令:
   ```
   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. 之後完全移除密碼編譯對應：
   ```
   no crypto map CMAP 10
   ```

   路由器A的最終配置

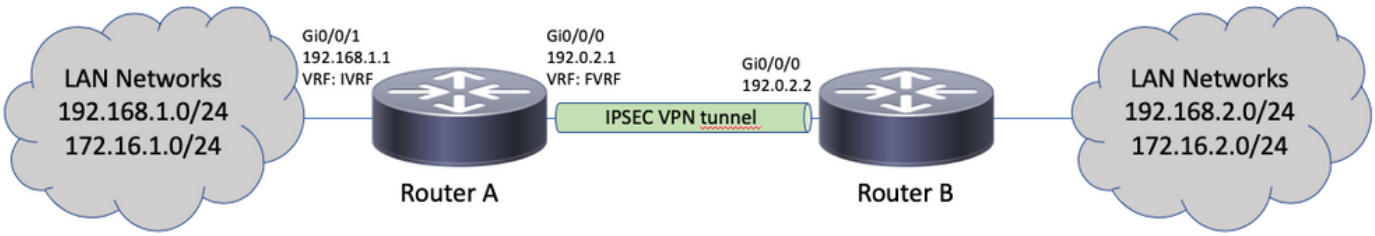
   ```
   crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
   !
   crypto ikev2 profile PROF
   match identity remote address 192.0.2.2 255.255.255.255
   authentication remote pre-share key cisco123
   authentication local pre-share key cisco123
   ```

```
!
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
```

將VRF感知加密對映遷移到多SA VTI

此示例說明如何遷移VRF感知加密對映配置。

拓撲



加密對映配置

```
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
```

以下是遷移至多SA VTI所需的步驟：

```
! 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
```

最終的VRF感知配置

```
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
```

驗證

使用本節內容，確認您的組態是否正常運作。

Cisco CLI Analyzer(僅供已註冊客戶使用)支援 **show** 指令。使用Cisco CLI Analyzer檢視 **show** 命令輸出。

若要確認通道是否已成功交涉，可以檢查通道介面狀態。最後兩列 — Status 和 Protocol — 顯示狀態 up 當通道運作時：

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

有關當前加密會話狀態的更多詳細資訊，請參見 **show crypto session** 輸出。其 Session status 的 UP-ACTIVE 表示已正確協商IKE會話：

```
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
```

驗證通往遠端網路的路由是否通過正確的隧道介面指向：

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

要排除IKE協定協商故障，請使用以下調試：

> **附註**：使用之前，請先參閱有關Debug命令的重要資訊 **debug** 指令。

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

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

常見問題

通道是自動啟動還是需要流量啟動通道？

與加密對映不同，無論與加密ACL匹配的資料流量是否流經路由器，多SA VTI隧道都會自動啟動。即使沒有有趣的流量，隧道也會一直保持運行。

如果流量通過VTI路由，但流量的源或目標與此通道配置為IPsec策略的加密ACL不匹配，會發生什麼情況？

不支援此類情況。只有要加密的流量才能路由到通道介面。原則型路由(PBR)只能將特定流量路由到VTI。PBR可以使用IPsec策略ACL來匹配要路由到VTI的流量。

根據配置的IPsec策略檢查每個資料包，並且必須與加密ACL匹配。如果不相符，則不會加密並以明文形式從隧道源介面傳送出去。

如果使用相同的內部VRF(iVRF)和前部VRF(fVRF)(iVRF = fVRF)，則會導致路由回圈，且丟棄資料包是有原因的 **Ipv4RoutingErr**.此類丟棄的統計資訊可使用 **show platform hardware qfp active statistics drop** 指令:

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

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

如果iVRF與fVRF不同，則在iVRF中進入隧道的資料包與IPsec策略不匹配，以明文退出fVRF中的隧道源介面。它們不會被丟棄，因為VRF之間沒有路由環路。

多SA VTI是否支援VRF、NAT、QoS等功能？

是的，所有這些功能都以與常規VTI隧道相同的方式受支援。