在Cisco IOS XE路由器上配置多SA虚拟隧道接口

目录

简介

本文档介绍如何在使用Cisco IOS® XE软件的Cisco路由器上配置多安全关联（多SA）虚拟隧道接口(VTI)。还描述了迁移过程。Multi-SA VTI替代了基于加密映射（基于策略）的VPN配置。它向后兼容基于加密映射和其他基于策略的实现。Cisco IOS XE版本16.12及更高版本支持此功能。

先决条件

要求

Cisco建议您了解Cisco IOS XE路由器上的IPsec VPN配置。

使用的组件

本文档中的信息基于采用Cisco IOS XE版本16.12.01a的集成多业务路由器(ISR)4351。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

VTI相对于加密映射的优点

加密映射是物理接口的输出功能。到不同对等体的隧道是在同一加密映射下配置的。加密映射访问控制列表(ACL)条目用于匹配要发送到特定VPN对等体的流量。这种配置也称为基于策略的VPN。

对于VTI，每个VPN隧道都由一个单独的逻辑隧道接口表示。路由表决定流量发送到哪个VPN对等设备。这种配置也称为基于路由的VPN。

在早于Cisco IOS XE版本16.12的版本中，VTI配置与加密映射配置不兼容。隧道两端必须配置相同类型的VPN才能进行互操作。

在Cisco IOS XE版本16.12中，添加了新配置选项，允许隧道接口在协议级别上充当基于策略的VPN，但具有隧道接口的所有属性。

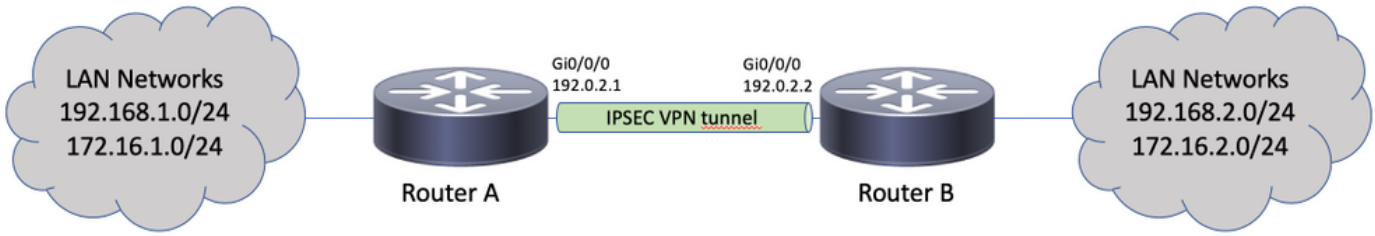
Cisco宣布了Cisco IOS XE版本17.6中Cisco IPsec静态加密映射和动态加密映射功能的寿命终止日期。

VTI相对于加密映射的优势包括：

- 更容易确定隧道的打开/关闭状态。
- 故障排除更容易。
- 它能够基于每个隧道应用服务质量(QoS)、基于区域的防火墙(ZBF)、网络地址转换(NAT)和Netflow等功能。
- 它为所有类型的VPN隧道提供简化的配置。

配置

网络图



路由注意事项

管理员必须确保远程网络的路由指向隧道接口。此 **reverse-route** ipsec配置文件下的选项可用于为加密ACL中指定的网络自动创建静态路由。此类路由也可以手动添加。如果之前配置了更具体的路由，则指向物理接口而不是隧道接口，则必须删除这些路由。

配置示例

基于加密映射的IKEv1隧道迁移至多SA sVTI

两台路由器都预配置了基于互联网密钥交换版本1(IKEv1)加密映射的解决方案：

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
```

要将路由器A迁移到多SA VTI配置，请完成以下步骤。路由器B可以保留旧配置，也可以按类似方式重新配置：

1. 从接口删除加密映射：
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. 创建IPsec配置文件。反向路由可选配置为将远程网络的静态路由自动添加到路由表中：
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. 配置隧道接口。加密ACL作为IPsec策略附加到隧道配置。隧道接口上配置的IP地址不相关，但必须为其配置一些值。IP地址可以从物理接口借用，该接口使用 **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. 加密映射条目随后可以完全删除：

```
no crypto map CMAP 10
```

路由器A的最终配置

```
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
```

基于加密映射的IKEv2隧道迁移至多SA sVTI

两台路由器都预配置了基于互联网密钥交换版本2(IKEv2)加密映射的解决方案：

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
```

要将路由器A迁移到多SA VTI配置，请完成以下步骤。路由器B可以保留旧配置，也可以以类似方式重新配置。

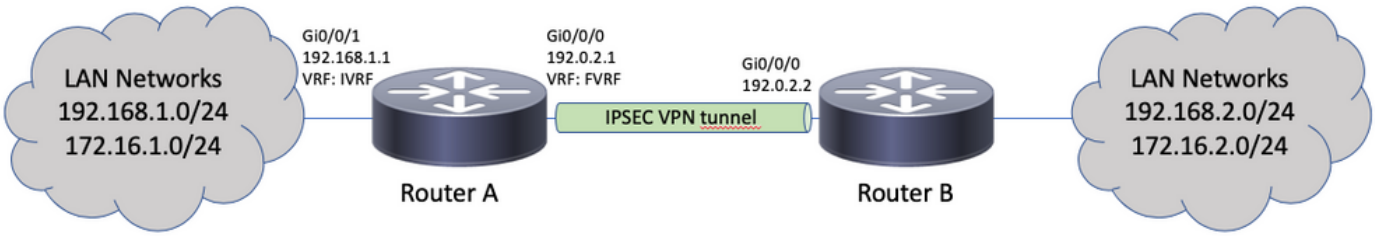
1. 从接口删除加密映射：
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. 创建IPsec配置文件。此 **reverse-route** 命令可以配置为将远程网络的静态路由自动添加到路由表中：
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   set ikev2-profile PROF
   reverse-route
   ```
3. 配置隧道接口。加密ACL作为IPsec策略附加到隧道配置。隧道接口上配置的IP地址不相关，但必须为其配置一些值。IP地址可以从物理接口借用，该接口使用 **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. 之后完全删除加密映射：
   ```
   no crypto map CMAP 10
   ```
   路由器A的最终配置
   ```
   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
```

将VRF感知加密映射迁移到多SA VTI

此示例说明如何迁移VRF感知加密映射配置。

拓扑



加密映射配置

```
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
```

以下是迁移至多SA VTI所需的步骤：

```
! 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
```

最终的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
```

验证

使用本部分可确认配置能否正常运行。

Cisco CLI Analyzer(仅限注册客户)支持 **show** 命令。使用Cisco CLI分析器查看分析 **show** 命令输出.

为了验证是否已成功协商隧道，可以检查隧道接口状态。最后两列 — Status 和 Protocol — 显示状态 up 当隧道运行时：

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

有关当前加密会话状态的更多详细信息，请参阅 **show crypto session** 输出。此 Session status / UP-ACTIVE 表示已正确协商IKE会话：

```
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
```

验证到远程网络的路由是否指向正确的隧道接口：

```
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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

要对IKE协议协商进行故障排除，请使用以下调试：

> **注意：**使用之前，请参阅有关Debug命令的重要信息 **debug** 命令。

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

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

常见问题

隧道是自动启动还是需要流量启动隧道？

与加密映射不同，无论与加密ACL匹配的数据流量是否流经路由器，多SA VTI隧道都会自动出现。即使没有相关流量，隧道也会始终保持运行。

如果流量通过VTI路由，但流量的源或目标与此隧道配置为IPsec策略的加密ACL不匹配，会发生什么情况？

不支持此类场景。只有要加密的流量必须路由到隧道接口。基于策略的路由(PBR)可用于仅将特定流量路由到VTI。PBR可以使用IPsec策略ACL来匹配要路由到VTI的流量。

根据配置的IPsec策略检查每个数据包，并且必须匹配加密ACL。如果不匹配，则不进行加密并以明文形式从隧道源接口发送出去。

如果使用相同的内部VRF(iVRF)和前部VRF(fVRF)(iVRF = fVRF)，则会导致路由环路，并且丢弃数据包是有原因的 **Ipv4RoutingErr**.此类丢弃的统计信息可在以下位置看到： **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与fVRF不同，则进入iVRF中隧道的数据包不匹配IPsec策略，以明文形式退出fVRF中的隧道源接口。它们不会丢弃，因为VRF之间没有路由环路。

多SA VTI是否支持VRF、NAT、QoS等功能？

是的，所有这些功能都以与常规VTI隧道相同的方式受支持。