Configuración de una Interfaz de Túnel Virtual Multi-SA en un Router Cisco IOS XE

Contenido

Introducción

Este documento describe cómo configurar una interfaz de túnel virtual (VTI) de asociación de seguridad múltiple (Multi-SA) en routers Cisco con el software Cisco IOS® XE. También se describe el proceso de migración. Multi-SA VTI es un reemplazo de la configuración de VPN basada en mapa criptográfico (basada en políticas). Es compatible con versiones anteriores con implementaciones basadas en crypto map y otras basadas en políticas. El soporte para esta función está disponible en Cisco IOS XE Release 16.12 y posteriores.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de una configuración de VPN IPsec en los routers Cisco IOS XE.

Componentes Utilizados

La información de este documento se basa en un router de servicios integrados (ISR) 4351 con Cisco IOS XE Release 16.12.01a .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Ventajas de VTI sobre Crypto Maps

Un mapa criptográfico es una función de salida de la interfaz física. Los túneles a diferentes pares se configuran bajo el mismo mapa crypto. Las entradas de la Lista de control de acceso (ACL) de mapa criptográfico se utilizan para hacer coincidir el tráfico que se enviará a un par VPN específico. Este tipo de configuración también se denomina VPN basada en políticas.

En el caso de los VTI, cada túnel VPN se representa mediante una interfaz de túnel lógico independiente. La tabla de ruteo decide a qué par VPN se envía el tráfico. Este tipo de configuración también se denomina VPN basada en rutas.

En las versiones anteriores a Cisco IOS XE Release 16.12, la configuración VTI no era compatible con la configuración de mapa criptográfico. Ambos extremos del túnel debían configurarse con el mismo tipo de VPN para interoperar.

En Cisco IOS XE Release 16.12, se han agregado nuevas opciones de configuración que permiten a la interfaz de túnel actuar como una VPN basada en políticas en el nivel de protocolo, pero que tienen todas las propiedades de la interfaz de túnel.

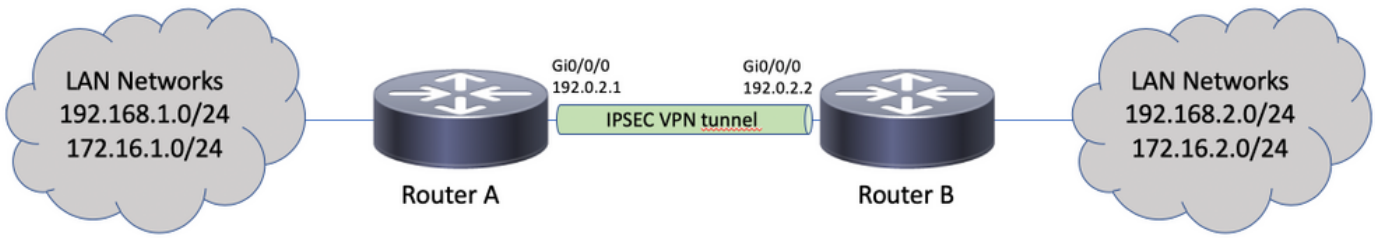
Cisco anunció las fechas de fin de vida útil para la función Cisco IPsec Static Crypto Map y Dynamic Crypto Map en Cisco IOS XE Release 17.6.

Las ventajas de VTI sobre el mapa criptográfico incluyen:

- Es más fácil determinar el estado activo/inactivo del túnel.
- Es más fácil resolver problemas.
- Tiene la capacidad de aplicar funciones como calidad de servicio (QoS), firewall basado en zonas (ZBF), traducción de direcciones de red (NAT) y Netflow por túnel.
- Tiene una configuración optimizada para todos los tipos de túneles VPN.

Configurar

Diagrama de la red



Consideraciones de ruteo

El administrador debe asegurarse de que el ruteo para las redes remotas apunte hacia la interfaz

de túnel. **reverse-route** bajo el perfil IPsec se puede utilizar para crear automáticamente rutas estáticas para las redes especificadas en la ACL crypto. Estas rutas también se pueden agregar manualmente. Si hay rutas previamente configuradas más específicas, ese punto hacia una interfaz física en lugar de hacia la interfaz de túnel, se deben quitar.

Ejemplos de Configuración

Migración de un Túnel IKEv1 Basado en Crypto Map a un Multi-SA sVTI

Ambos routers están preconfigurados con la solución basada en mapa criptográfico de Internet Key Exchange versión 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
```

Para migrar el Router A a una configuración VTI de SA múltiple, complete estos pasos. El router B puede permanecer con la configuración anterior o puede reconfigurarse de forma similar:

1. Quite el mapa crypto de la interfaz:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Cree el perfil IPsec. La ruta inversa se configura opcionalmente para que las rutas estáticas para las redes remotas se agreguen automáticamente a la tabla de ruteo:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. Configure la interfaz de túnel. La ACL criptográfica está conectada a la configuración del túnel como una política IPsec. La dirección IP configurada en la interfaz de túnel es irrelevante, pero debe configurarse con algún valor. La dirección IP se puede tomar prestada desde la interfaz física con el **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 entrada de mapa criptográfico puede eliminarse completamente después:
   ```
   no crypto map CMAP 10
   ```

   ### Configuración final 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
   ```

Migración de un Túnel IKEv2 Basado en Crypto Map a un Multi-SA sVTI

Ambos routers están preconfigurados con la solución basada en mapa criptográfico de Internet Key Exchange versión 2 (IKEv2):

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
```

Para migrar el Router A a una configuración VTI de SA múltiple, complete estos pasos. El router B puede permanecer con la configuración anterior o puede reconfigurarse de forma similar.

1. Quite el mapa crypto de la interfaz:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Cree el perfil IPsec. **reverse-route** se configura opcionalmente para que las rutas estáticas para redes remotas se agreguen automáticamente a la tabla de ruteo:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   set ikev2-profile PROF
   ```

```
reverse-route
```

3. Configure la interfaz de túnel. La ACL criptográfica está conectada a la configuración del túnel como una política IPsec. La dirección IP configurada en la interfaz de túnel es irrelevante, pero debe configurarse con algún valor. La dirección IP se puede tomar prestada desde la interfaz física con el **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. Quite el mapa criptográfico completamente después:

```
no crypto map CMAP 10
```

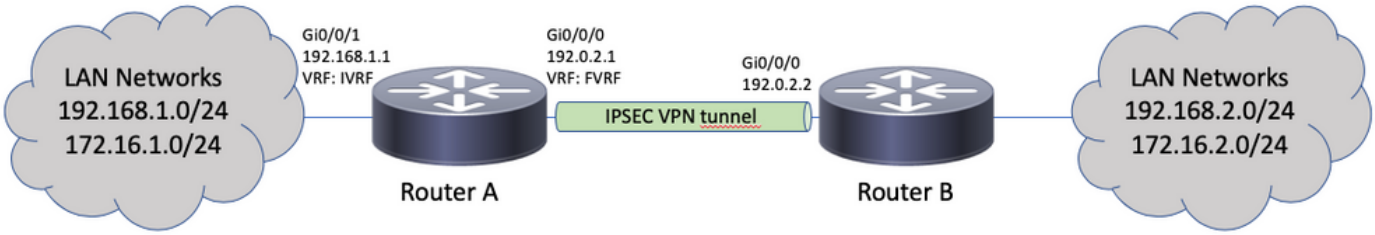
Configuración final del router A

```
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
```

Migración de un Mapa Crypto con Reconocimiento VRF a un VTI Multi-SA

Este ejemplo muestra cómo migrar la configuración de mapa crypto que reconoce VRF.

Topología



Configuración del mapa criptográfico

```
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
```

Estos son los pasos necesarios para migrar a VTI de varias 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
```

Configuración con Reconocimiento de VRF Final

```
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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El Analizador Cisco CLI (sólo clientes registrados) admite ciertos **show** comandos. Utilice Cisco

CLI Analyzer para ver un análisis de **show** resultado del comando.

Para verificar si el túnel se ha negociado correctamente, el estado de la interfaz del túnel se puede verificar. Las dos últimas columnas: Status y Protocol - mostrar un estado de up cuando el túnel está 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
```

En el **show crypto session** resultado. Session status de UP-ACTIVE indica que la sesión IKE se ha negociado correctamente:

```
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
```

Verifique que el ruteo a la red remota apunte a través de la interfaz de túnel correcta:

```
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
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para resolver el problema de la negociación del protocolo IKE, utilice estos debugs:

> **Nota:** Consulte Información Importante sobre Comandos Debug antes de utilizar **debug** comandos.

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

! For IKEv2-based scenarios:
```

```
debug crypto ikev2
debug crypto ipsec
```

Preguntas Frecuentes

¿El túnel se activa automáticamente o se necesita tráfico para activar el túnel?

A diferencia de los mapas criptográficos, los túneles VTI de SA múltiple se activan automáticamente independientemente de si el tráfico de datos que coincide con la ACL criptográfica fluye sobre el router o no. Los túneles permanecen activos todo el tiempo, aunque no haya tráfico interesante.

¿Qué sucede si el tráfico se rutea a través del VTI, pero el origen o el destino del tráfico no coincide con la ACL crypto configurada como política IPsec para este túnel?

No se admite tal escenario. Sólo el tráfico que se pretende cifrar debe enrutarse a la interfaz de túnel. El routing basado en políticas (PBR) se puede utilizar para enrutar solo tráfico específico al VTI. PBR puede utilizar la ACL de política IPsec para hacer coincidir el tráfico que se enrutará al VTI.

Cada paquete se compara con la política IPsec configurada y debe coincidir con la ACL crypto. Si no coincide, no se cifra y se envía en texto sin cifrar desde la interfaz de origen del túnel.

En caso de que se utilice el mismo VRF interno (iVRF) y el VRF frontal (fVRF) (iVRF = fVRF), se producirá un bucle de enrutamiento y los paquetes se descartarán con un motivo **Ipv4RoutingErr**. Las estadísticas para estas caídas se pueden ver con el **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
```

En caso de que iVRF sea diferente de fVRF, los paquetes que ingresan al túnel en iVRF y no coinciden con la política IPsec, salga de la interfaz de origen del túnel en fVRF en texto claro. No se descartan, ya que no hay ningún loop de ruteo entre los VRF.

¿Se admiten funciones como VRF, NAT, QoS, etc. en VTI de SA múltiple?

Sí, todas estas funciones se soportan de la misma manera que en los túneles VTI normales.