# Configurar uma interface de túnel virtual Multi-SA em um roteador Cisco IOS XE

## Contents



## Introduction

Este documento descreve como configurar uma Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) de associação de segurança múltipla (Multi-SA - Multi-Security Association) em roteadores Cisco com o software Cisco IOS® XE. O processo de migração também é descrito. O Multi-SA VTI é um substituto para a configuração de VPN baseada em mapa de criptografia (baseada em política). É retrocompatível com mapa de criptografia e outras implementações baseadas em políticas. O suporte para esse recurso está disponível no Cisco IOS XE versão 16.12 e posterior.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento de uma configuração de VPN IPsec em roteadores Cisco IOS XE.

### Componentes Utilizados

As informações neste documento são baseadas em um Integrated Services Router (ISR) 4351 com 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

## Vantagens dos VTIs em relação aos mapas de criptografia

Um mapa de criptografia é um recurso de saída da interface física. Os túneis para diferentes pares são configurados no mesmo mapa de criptografia. As entradas da Lista de Controle de Acesso (ACL - Access Control List) do mapa de criptografia são usadas para corresponder o tráfego a ser enviado a um par de VPN específico. Esse tipo de configuração também é chamado de VPN baseada em políticas.

No caso de VTIs, cada túnel VPN é representado por uma interface de túnel lógica separada. A tabela de roteamento decide para qual par de VPN o tráfego é enviado. Esse tipo de configuração também é chamado de VPN baseada em rota.

Em versões anteriores ao Cisco IOS XE Release 16.12, a configuração do VTI não era compatível com a configuração do mapa de criptografia. As duas extremidades do túnel precisavam ser configuradas com o mesmo tipo de VPN para interoperar.

No Cisco IOS XE versão 16.12, novas opções de configuração foram adicionadas para permitir que a interface de túnel atue como uma VPN baseada em política no nível do protocolo, mas tenha todas as propriedades da interface de túnel.

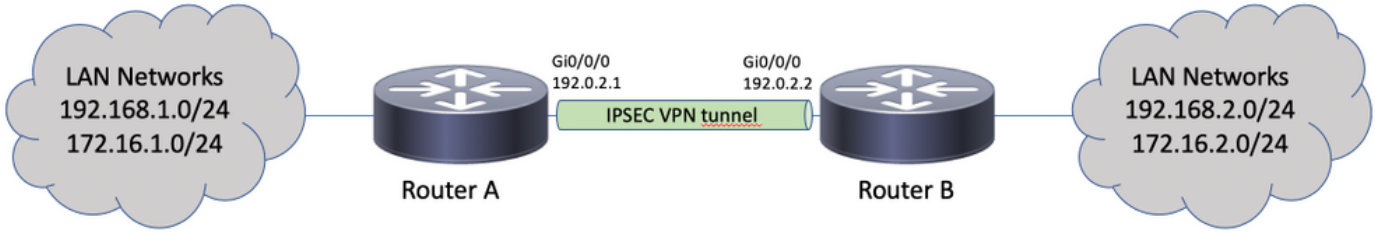
A Cisco anunciou as datas de fim da vida útil para o recurso Cisco IPsec Static Crypto Map e Dynamic Crypto Map no Cisco IOS XE versão 17.6.

As vantagens do VTI sobre o mapa de criptografia incluem:

- Émais fácil determinar o status up/down do túnel.
- Émais fácil solucionar problemas.
- Ele tem a capacidade de aplicar recursos como Qualidade de Serviço (QoS - Quality of Service), Firewall Baseado em Zona (ZBF - Zone-Based Firewall), Conversão de Endereço de Rede (NAT - Network Address Translation) e Netflow por túnel.
- Ele tem uma configuração simplificada para todos os tipos de túneis VPN.

# Configurar

## Diagrama de Rede



## Considerações sobre roteamento

O administrador deve garantir que o roteamento para redes remotas aponte para a interface do túnel. O **reverse-route** no perfil IPsec pode ser usada para criar automaticamente rotas estáticas para as redes especificadas na ACL de criptografia. Essas rotas também podem ser adicionadas manualmente. Se houver rotas previamente configuradas mais específicas, que apontam para uma interface física em vez da interface de túnel, elas devem ser removidas.

## Exemplos de configuração

### Migração de um túnel IKEv1 baseado em mapa de criptografia para um sVTI de várias SAs

Ambos os roteadores são pré-configurados com a solução baseada em mapa de criptografia Internet Key Exchange Version 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 o Roteador A para uma configuração de VTI de vários SAs, conclua estas etapas. O Roteador B pode permanecer com a configuração antiga ou pode ser reconfigurado da mesma forma:

1. Remova o mapa de criptografia da interface:
   ```
   interface GigabitEthernet0/0/0
   no crypto map
   ```
2. Crie o perfil IPsec. A rota inversa é configurada opcionalmente para que as rotas estáticas para redes remotas sejam adicionadas automaticamente à tabela de roteamento:
   ```
   crypto ipsec profile PROF
   set transform-set TSET
   reverse-route
   ```
3. Configure a interface do túnel. A ACL criptografada é anexada à configuração do túnel como uma política IPsec. O endereço IP configurado na interface do túnel é irrelevante, mas deve ser configurado com algum valor. O endereço IP pode ser emprestado da interface física com o comando **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. A entrada do mapa de criptografia pode ser completamente removida depois:
   ```
   no crypto map CMAP 10
   ```

   ### Configuração final do roteador 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
```

## Migração de um túnel IKEv2 baseado em mapa de criptografia para um sVTI de várias SAs

Ambos os roteadores são pré-configurados com a solução baseada em mapa de criptografia Internet Key Exchange Version 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 o Roteador A para uma configuração de VTI de vários SAs, conclua estas etapas. O Roteador B pode permanecer com a configuração antiga ou pode ser reconfigurado da mesma forma.

1. Remova o mapa de criptografia da interface:
   ```
   interface GigabitEthernet0/0/0
   ```

```
no crypto map
```

2. Crie o perfil IPsec. O **reverse-route** é configurado opcionalmente para ter as rotas estáticas para redes remotas automaticamente adicionadas à tabela de roteamento:
```
crypto ipsec profile PROF
set transform-set TSET
set ikev2-profile PROF
reverse-route
```
3. Configure a interface do túnel. A ACL criptografada é anexada à configuração do túnel como uma política IPsec. O endereço IP configurado na interface do túnel é irrelevante, mas deve ser configurado com algum valor. O endereço IP pode ser emprestado da interface física com o comando **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. Remova o mapa de criptografia completamente depois:
```
no crypto map CMAP 10
```

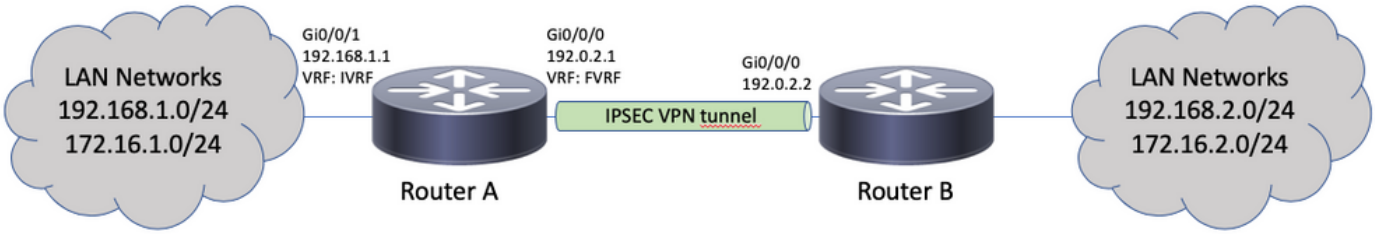
### Configuração final do roteador A

```
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
```

## Migração de um mapa de criptografia com reconhecimento de VRF para um VTI de vários SAs

Este exemplo mostra como migrar a configuração do mapa de criptografia com reconhecimento de VRF.

Topologia




## Configuração do mapa de criptografia

```
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
```

Estas são as etapas necessárias para migrar para VTI de vários SAs:

```
! 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
```

## Configuração final com reconhecimento de 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
```

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O Cisco CLI Analyzer (somente clientes registrados) suporta determinados **show** comandos. Use o Cisco CLI Analyzer para visualizar uma análise de **show** Saída do comando.

Para verificar se o túnel foi negociado com êxito, o status da interface do túnel pode ser verificado. As duas últimas colunas - Status e Protocol - mostrar um status de up Quando o túnel estiver operacional:

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

Mais detalhes sobre o status atual da sessão de criptografia podem ser encontrados no **show crypto session** saída. O Session status de UP-ACTIVE indica que a sessão IKE foi negociada corretamente:

```
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 se o roteamento para a rede remota aponta para a interface de túnel correta:

```
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

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para solucionar problemas de negociação de protocolo IKE, use estas depurações:

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar **debug** comandos.

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

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

# Perguntas mais freqüentes

### O túnel é ativado automaticamente ou o tráfego é necessário para ativá-lo?

Diferentemente dos mapas de criptografia, os túneis VTI de várias SAs surgem automaticamente, independentemente de o tráfego de dados que corresponde à ACL de criptografia fluir pelo roteador ou não. Os túneis permanecem ativos o tempo todo, mesmo que não haja tráfego interessante.

### O que acontece se o tráfego for roteado através do VTI, mas a origem ou o destino do tráfego não corresponder à ACL criptografada configurada como uma política IPsec para esse túnel?

Tal cenário não é suportado. Somente o tráfego destinado a ser criptografado deve ser roteado para a interface de túnel. O roteamento baseado em políticas (PBR) pode ser usado para rotear somente o tráfego específico para o VTI. O PBR pode usar a ACL de política IPsec para corresponder o tráfego a ser roteado para o VTI.

Cada pacote é comparado à política IPsec configurada e deve corresponder à ACL criptografada. Se não corresponder, não será criptografado e será enviado em texto claro para fora da interface origem do túnel.

Caso o mesmo VRF interno (iVRF) e o VRF frontal (fVRF) sejam usados (iVRF = fVRF), isso resulta em um loop de roteamento e os pacotes são descartados com um motivo **Ipv4RoutingErr**. As estatísticas de tais quedas podem ser vistas com o **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
```

Caso o iVRF seja diferente do fVRF, os pacotes que entram no túnel no iVRF e não correspondem à política do IPsec, saia da interface origem do túnel no fVRF em texto claro. Eles não são descartados, pois não há nenhum loop de roteamento entre os VRFs.

### Recursos como VRF, NAT, QoS e assim por diante são suportados no VTI de várias SAs?

Sim, todos esses recursos são suportados da mesma forma que nos túneis VTI regulares.