Configurar a interface de túnel Multi-SA virtual no roteador IOS-XE

Índice

Introdução

Este documento descreve como configurar a interface de túnel virtual da multi associação de segurança no roteador IOS-XE. O processo de migração é descrito igualmente. O MULTI-SA VTI é uma substituição para (política baseada) a configuração de rede privada virtual baseada em mapas cripto. É para trás compatível com aplicações baseadas política baseadas em mapas e outras criptos. O apoio para este caracteriza está disponível desde a liberação IOS-XE 16.12.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de Virtual Private Network do IPsec no Roteadores IOS-XE

Componentes Utilizados

A informação neste documento é baseada nos 4351 Router ISR que executam a versão de software IOS-XE 16.12.01a.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Vantagens de interfaces de túnel virtuais sobre crypto map

O crypto map é uns recursos de emissor da interface física. Os túneis aos pares diferentes são configurados sob o mesmo crypto map. As entradas de lista de acesso especificam a que tráfego do par deve ser enviado. O este tipo de configuração é chamado igualmente VPN com base em política.

Se as interfaces de túnel virtuais são utilizadas, cada túnel VPN está representado por uma interface de túnel lógico separada. A tabela de roteamento decide a que tráfego do par deve ser enviado. O este tipo de configuração é chamado igualmente VPN rota-baseado.

Antes da liberação IOS-XE 16.12, a configuração VTI não era compatível com configuração do crypto map. O ambas as extremidades do túnel teve que ser configurado com o mesmo tipo de VPN para interoperar.

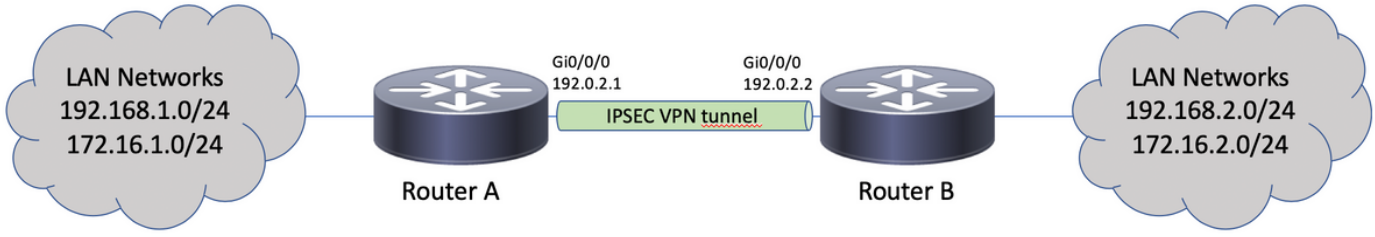
Em IOS-XE 16.12, as opções novas do confiugration foram adicionadas que permitem que a interface de túnel atue como o VPN com base em política no nível de protocolo, mas têm todas as propriedades da interface de túnel.

As vantagens de VTI sobre o crypto map incluem:

- Mais fácil determinar o status up/down do túnel
- Mais fácil pesquisar defeitos
- Capacidade para aplicar características como QoS, ZBF, NAT, Netflow em uma base do por-túnel
- Configuração aerodinâmica para todos os tipos de túneis VPN

Configurar

Diagrama de Rede



Configurações

IKEv1

Ambo o Roteadores preconfigured com solução IKEv1 baseada em mapas cripto:

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 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
```

Roteador 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
```

A fim migrar o roteador à uma configuração multi-SA VTI, o seguinte deve ser configurado. O roteador B pode permanecer com configuraion velho ou pode ser reconfigurado similarmente:

1. Remova o crypto map da relação:

```
interface GigabitEthernet0/0/0
no crypto map
```

2. Crie o perfil IPSec. a Reverso-rota é configurada opcionalmente para ter as rotas estáticas para as redes remotas adicionadas automaticamente à tabela de roteamento:

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

3. Configurar a interface de túnel. A lista de acesso cripto é anexada à configuração de túnel como a política do IPsec. O endereço IP de Um ou Mais Servidores Cisco ICM NT configurado na interface de túnel é irrelevante mas deve ser configurado com algum valor. O endereço IP de Um ou Mais Servidores Cisco ICM NT pode ser pedido da interface física usando “o comando unnumbered IP”:

```
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. O crypto map pode ser removido completamente mais tarde:

```
no crypto map CMAP 10
```

Configuração de roteador A final:

```
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
```

IKEv2

Ambo o Roteadores preconfigured com solução IKEv2 baseada em mapas cripto:

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 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
```

Roteador 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
```

A fim migrar o roteador à uma configuração multi-SA VTI, o seguinte deve ser configurado. O roteador B pode permanecer com configuraion velho ou pode ser reconfigurado similarmente:

1. Remova o crypto map da relação:

```
interface GigabitEthernet0/0/0
no crypto map
```

2. Crie o perfil IPSec. a Reverso-rota é configurada opcionalmente para ter as rotas estáticas para as redes remotas adicionadas automaticamente à tabela de roteamento:

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

3. Configurar a interface de túnel. A lista de acesso cripto é anexada à configuração de túnel como a política do IPsec. O endereço IP de Um ou Mais Servidores Cisco ICM NT configurado na interface de túnel é irrelevante mas deve ser configurado com algum valor. O endereço IP de Um ou Mais Servidores Cisco ICM NT pode ser pedido da interface física usando “o comando unnumbered IP”:

```
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. O crypto map pode ser removido completamente mais tarde:

```
no crypto map CMAP 10
```

Configuração de roteador A final:

```
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
```

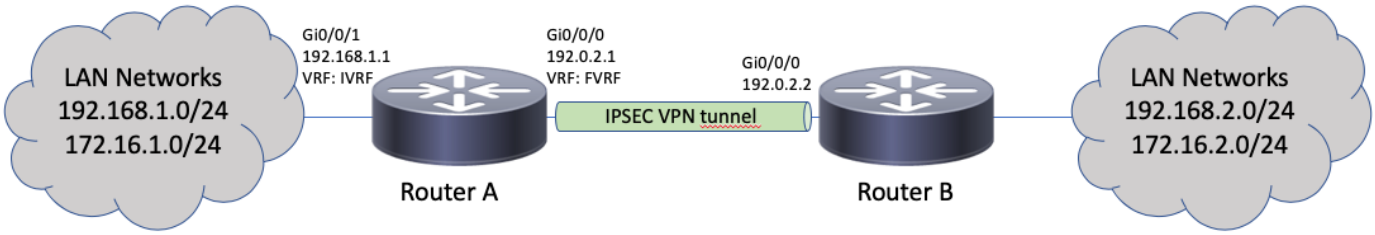
Distribuindo considerações

O administrador deve assegurar-se de que o roteamento para redes remotas esteja apontando para a interface de túnel. a opção da “Reverso-rota” sob o perfil IPSec pode ser usada para criar automaticamente rotas estáticas para as redes especificadas no ACL cripto. Tais rotas podem igualmente ser adicionadas manualmente. Se estava preexistindo umas rotas mais específicas que apontam para a interface física em vez da interface de túnel, estes devem ser removidos.

configuração VRF-ciente

Este exemplo mostra como migrar a configuração VRF-ciente do crypto map.

Topologia



Configuração do crypto map:

```
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
```

A fim migrar a multi-SA VTI, as seguintes etapas devem ser executadas:

```
! 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 VRF-ciente do 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
```

Verificar

A fim verificar se o túnel foi negociado com sucesso, o estado da interface de túnel pode ser verificado. As últimas duas colunas - colunas do “estado” e do “protocolo” - devem indicado “acima” do estado:

```
RouterA#show ip interface brief | i Tunnel0
Tunnel0 192.0.2.1 YES TFTP up up
```

Mais detalhes sobre o estado atual da sessão de criptografia podem ser encontrados da “na saída da sessão de criptografia mostra”. Da “o estado sessão” de “UP-ATIVE” indica que a sessão de IKE esteve 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 que o roteamento à rede remota aponta sobre 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
```

Perguntas mais freqüentes

P: Faz o túnel vem de automaticamente ou é o tráfego necessário trazer acima o túnel?

R: Ao contrário com dos crypto map, os túneis multi-SA VTI vêm acima automaticamente apesar de se o tráfego de dados que combina o ACL cripto está sendo distribuído atualmente. Os túneis ficam acima todo o tempo mesmo se o tráfego para de fluir.

P: Que acontece se o tráfego está distribuído com o VTI mas a fonte ou o destino do tráfego não combinam o ACL cripto configurado como a política do IPsec para este túnel?

R: Tal tráfego será deixado cair. Cada pacote é verificado contra a política configurada do IPsec e deve combinar o ACL cripto. A razão para tal gota é registrada como "Ipv4RoutingErr". As estatísticas para tais gotas podem ser encontradas através do comando seguinte:

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

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

P: As características como VRF, NAT, QoS etc. são apoiadas em multi-SA VTI?

R: Sim, todas aquelas características são apoiadas a mesma maneira que em túneis regulares VTI.

Troubleshooting

A fim pesquisar defeitos a negociação de protocolo IKE, o seguinte debuga pode ser usado:

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

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