VPN site a site baseada em rota IKEv1 usando IPV6

Contents

Introdução

Este documento descreve uma configuração para configurar um túnel de site a site IPv6, baseado em rota, entre dois roteadores Cisco usando o protocolo Internet Key Exchange versão 1 (IKEv1/ISAKMP).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento fundamental da configuração da CLI do Cisco IOS®/Cisco IOS® XE
- Conhecimento fundamental dos protocolos Internet Security Association and Key Management Protocol (ISAKMP) e IPsec
- Compreensão do roteamento e endereçamento IPv6

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

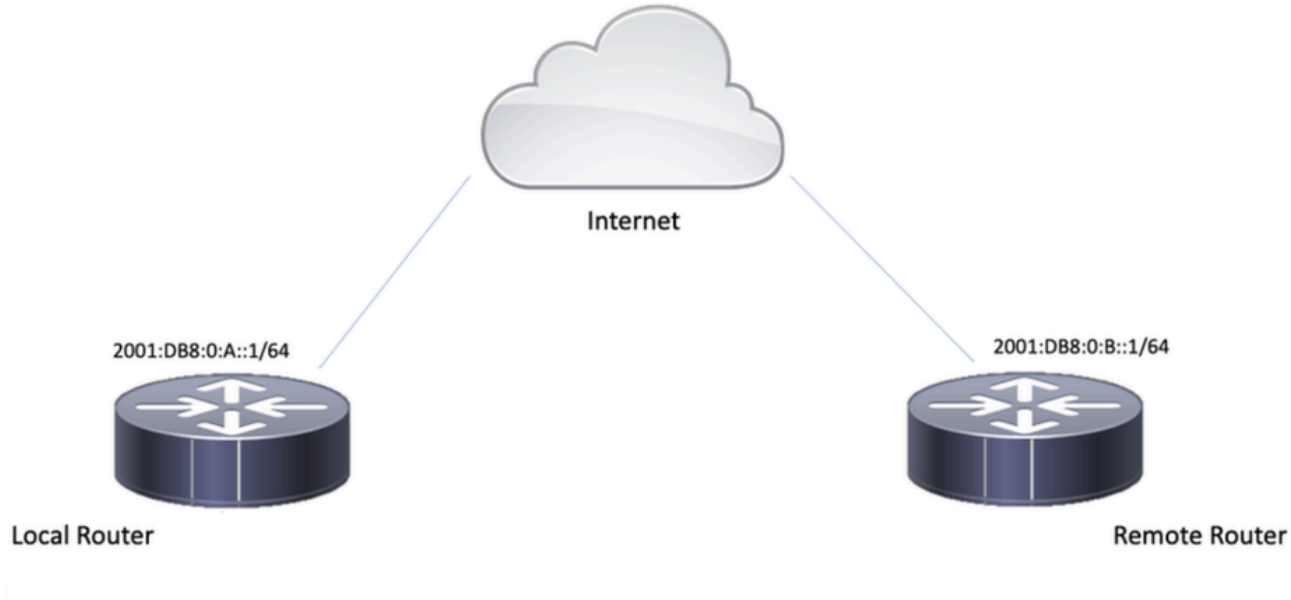
- Cisco IOS XE executando 17.03.04a como roteador local
- Cisco IOS executando 17.03.04a como roteador remoto

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.

Configurar

Diagrama de Rede



Configurações

Roteador local

Etapa 1. Ativar o roteamento unicast IPv6.

```
ipv6 unicast-routing
```

Etapa 2. Configurar as interfaces do roteador.

```
interface GigabitEthernet1
ipv6 address 2001:DB8:0:A::1/64
no shutdown

interface GigabitEthernet2
ipv6 address FC00::1/64
no shutdown
```

Etapa 3. Definir a rota padrão IPv6.

```
ipv6 route ::/0 GigabitEthernet1
```

Etapa 4. Configurar a política da Fase 1.

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 14
```

Etapa 5. Configurar o chaveiro com uma chave pré-compartilhada.

```
crypto keyring IPV6_KEY
pre-shared-key address ipv6 2001:DB8:0:B::1/128 key cisco123
```

Etapa 6. Configurar o perfil ISAKMP.

```
crypto isakmp profile ISAKMP_PROFILE_LAB
keyring IPV6_KEY
match identity address ipv6 2001:DB8:0:B::1/128
```

Etapa 7. Configurar a política da Fase 2.

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel
```

Etapa 8. Configurar o perfil IPsec.

```
crypto ipsec profile Prof1
 set transform-set ESP-AES-SHA
```

Etapa 9. Configurar a interface túnel.

```
interface Tunnel0
 no ip address
 ipv6 address 2012::1/64
 ipv6 enable
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:0:B::1
 tunnel protection ipsec profile Prof1
end
```

Etapa 10. Configurar as rotas para o tráfego significativo.

```
ipv6 route FC00::/64 2012::1
```

Configuração final do roteador local

```
ipv6 unicast-routing
!
interface GigabitEthernet1
ipv6 address 2001:DB8:0:A::1/64
no shutdown

!

interface GigabitEthernet2
ipv6 address FC00::1/64
no shutdown

!

ipv6 route ::/0 GigabitEthernet1

!

crypto isakmp policy 10
encryption aes
authentication pre-share
group 14

!

crypto keyring IPV6_KEY
pre-shared-key address ipv6 2001:DB8:0:B::1/128 key cisco123

!

crypto isakmp profile ISAKMP_PROFILE_LAB
keyring IPV6_KEY
match identity address ipv6 2001:DB8:0:B::1/128

!
```

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel

!

crypto ipsec profile Prof1
 set transform-set ESP-AES-SHA

!

interface Tunnel0
 no ip address
 ipv6 address 2012::1/64
 ipv6 enable
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:0:B::1
 tunnel protection ipsec profile Prof1
end

!

ipv6 route FC00::/64 2012::1
```

Configuração final do roteador remoto

```
ipv6 unicast-routing
!
interface GigabitEthernet1
ipv6 address 2001:DB8:0:B::1/64
no shutdown

!

interface GigabitEthernet2
ipv6 address FC01::1/64
no shutdown

!

ipv6 route ::/0 GigabitEthernet1

!

crypto isakmp policy 10
encryption aes
authentication pre-share
group 14

!

crypto keyring IPV6_KEY
pre-shared-key address ipv6 2001:DB8:0:A::1/128 key cisco123

!

crypto isakmp profile ISAKMP_PROFILE_LAB
```

```
keyring IPV6_KEY
match identity address ipv6 2001:DB8:0:A::1/128

!

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel

!

crypto ipsec profile Prof1
 set transform-set ESP-AES-SHA

!

interface Tunnel0
 no ip address
 ipv6 address 2012::2/64
 ipv6 enable
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:0:A::1
 tunnel protection ipsec profile Prof1
end

!

ipv6 route FC00::/64 2012::1
```

Troubleshooting

Para solucionar problemas do túnel, use os comandos debug:

- debug crypto isakmp
- debug crypto isakmp error
- debug crypto ipsec
- debug crypto ipsec error

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.