VPN de sitio a sitio basada en ruta IKEv1 mediante IPV6

Contenido

Introducción

Este documento describe una configuración para configurar un túnel IPv6, basado en ruta, de sitio a sitio entre dos routers Cisco que utilizan el protocolo Intercambio de claves de Internet versión 1 (IKEv1/ISAKMP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos fundamentales de la configuración CLI de Cisco IOS®/Cisco IOS® XE
- Conocimientos fundamentales de los protocolos IPsec y ISAKMP (Internet Security Association and Key Management Protocol)
- Comprensión del direccionamiento y el routing IPv6

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

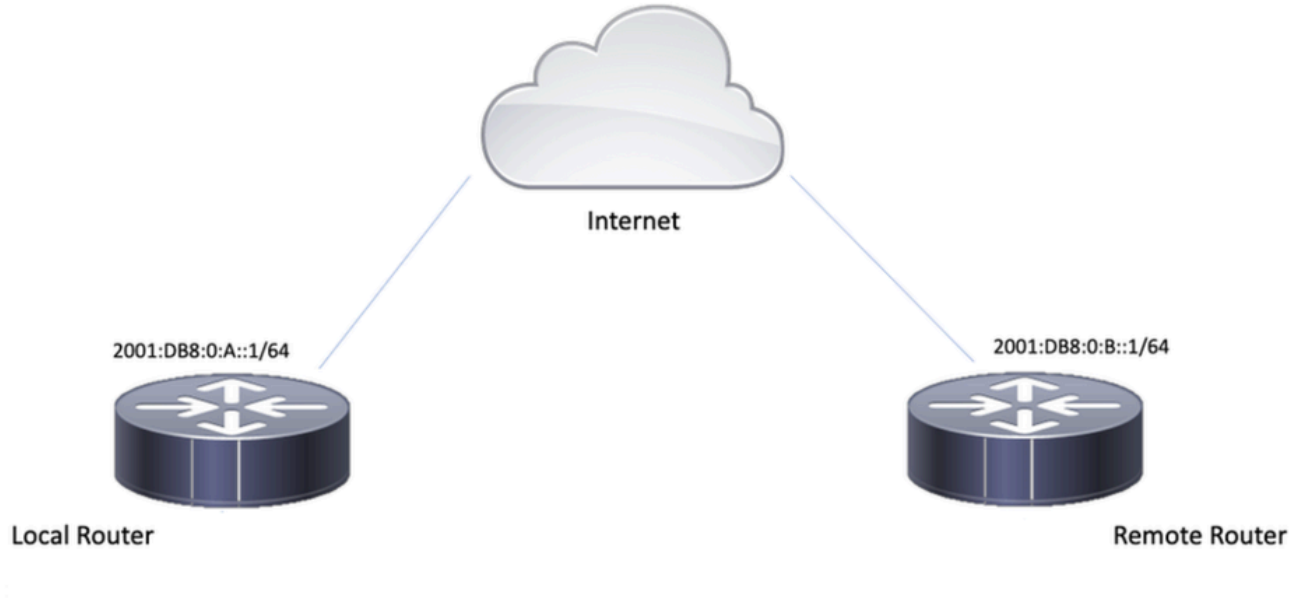
- Cisco IOS XE con 17.03.04a como router local
- Cisco IOS que ejecuta 17.03.04a como router remoto

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Configuraciones

Router local

Paso 1. Habilitación del routing unidifusión IPv6.

```
ipv6 unicast-routing
```

Paso 2. Configure las interfaces del router.

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

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

Paso 3. Establecer la ruta predeterminada de IPv6.

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

Paso 4. Configuración de la política de la fase 1.

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

Paso 5. Configure el llavero con una clave previamente compartida.

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

Paso 6. Configure el perfil ISAKMP.

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

Paso 7. Configure la política de Fase 2.

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

Paso 8. Configure el perfil IPsec.

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

Paso 9. Configuración de la interfaz de 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
```

Paso 10. Configure las rutas para el tráfico interesante.

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

Configuración final del router 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
```

Configuración final del router 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
```

Troubleshoot

Para resolver problemas del túnel, utilice los comandos debug:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).