使用IPV6的基于IKEv1路由的站点到站点VPN

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[配置](#)

- [网络图](#)
- [配置](#)
  - [本地路由器](#)

[本地路由器最终配置](#)

[远程路由器最终配置](#)

[故障排除](#)

简介

本文档介绍一种配置，用于在使用互联网密钥交换版本1(IKEv1/ISAKMP)协议的两台Cisco路由器之间设置IPv6、基于路由的站点到站点隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS®/Cisco IOS® XE CLI配置的基础知识
- Internet安全关联、密钥管理协议(ISAKMP)和IPsec协议的基础知识
- 了解IPv6编址和路由

使用的组件

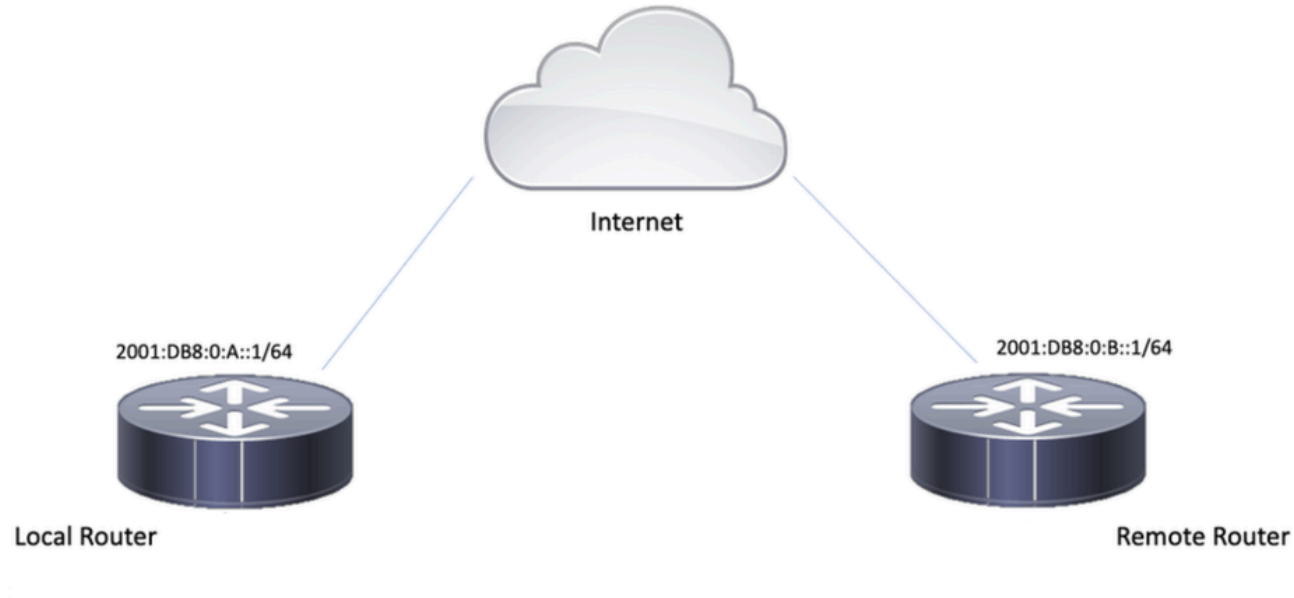
本文档中的信息基于以下软件版本：

- 运行17.03.04a的Cisco IOS XE作为本地路由器
- 运行17.03.04a作为远程路由器的Cisco IOS

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



配置

本地路由器

步骤1.启用IPv6单播路由。

```
ipv6 unicast-routing
```

步骤2.配置路由器接口。

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

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

步骤3.设置IPv6默认路由。

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

步骤4.配置第1阶段策略。

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

步骤5.使用预共享密钥配置密钥环。

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

步骤6.配置ISAKMP配置文件。

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

步骤7.配置第2阶段策略。

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

步骤8.配置IPsec配置文件。

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

步骤9.配置隧道接口。

```
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
```

步骤10.配置相关流量的路由。

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

本地路由器最终配置

```
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
```

远程路由器最终配置

```
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
```

故障排除

要对隧道进行故障排除，请使用debug命令：

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。