使用IPV6的IKEv1基於路由的站點到站點VPN

目錄

簡介

本文檔介紹如何使用Internet金鑰交換版本1(IKEv1/ISAKMP)協定在兩台Cisco路由器之間設定IPv6、基於路由的站點到站點隧道的配置。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS®/Cisco IOS® XE CLI配置基礎知識
- 網際網路安全關聯和金鑰管理協定(ISAKMP)以及IPsec協定的基礎知識
- 瞭解IPv6編址和路由

採用元件

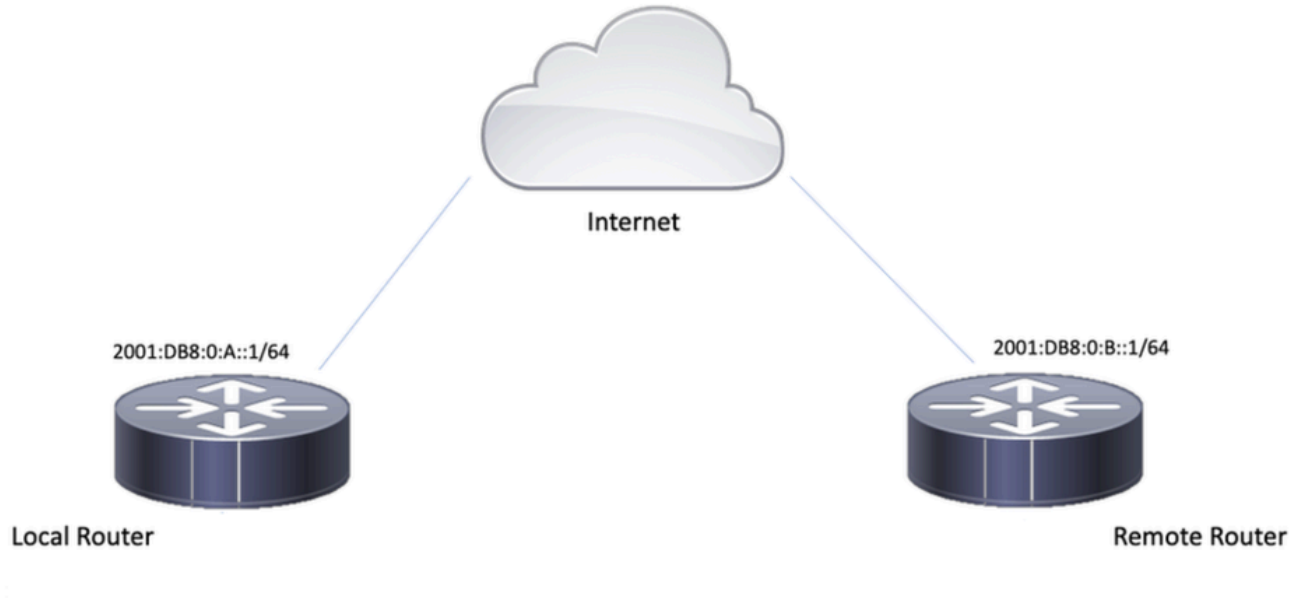
本檔案中的資訊是根據以下軟體版本：

- 運行17.03.04a作為本地路由器的Cisco IOS XE
- 運行17.03.04a作為遠端路由器的Cisco IOS

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



組態

本地路由器

步驟1.啟用IPv6單播路由。

```
ipv6 unicast-routing
```

步驟2.配置路由器介面。

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

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

步驟3.設定IPv6預設路由。

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

步驟4.配置階段1策略。

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

步驟5.使用預共用金鑰配置金鑰環。

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

步驟6.配置ISAKMP配置檔案。

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

步驟7.配置第2階段策略。

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

步驟8.配置IPsec配置檔案。

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

步驟9.配置隧道介面。

```
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
```

步驟10.為相關流量配置路由。

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

本地路由器最終配置

```
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
```

遠端路由器最終配置

```
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
```

疑難排解

若要對通道進行疑難排解，請使用debug指令：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。