使用IPv6在思科路由器上實施IKEv2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2(IKEv2)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

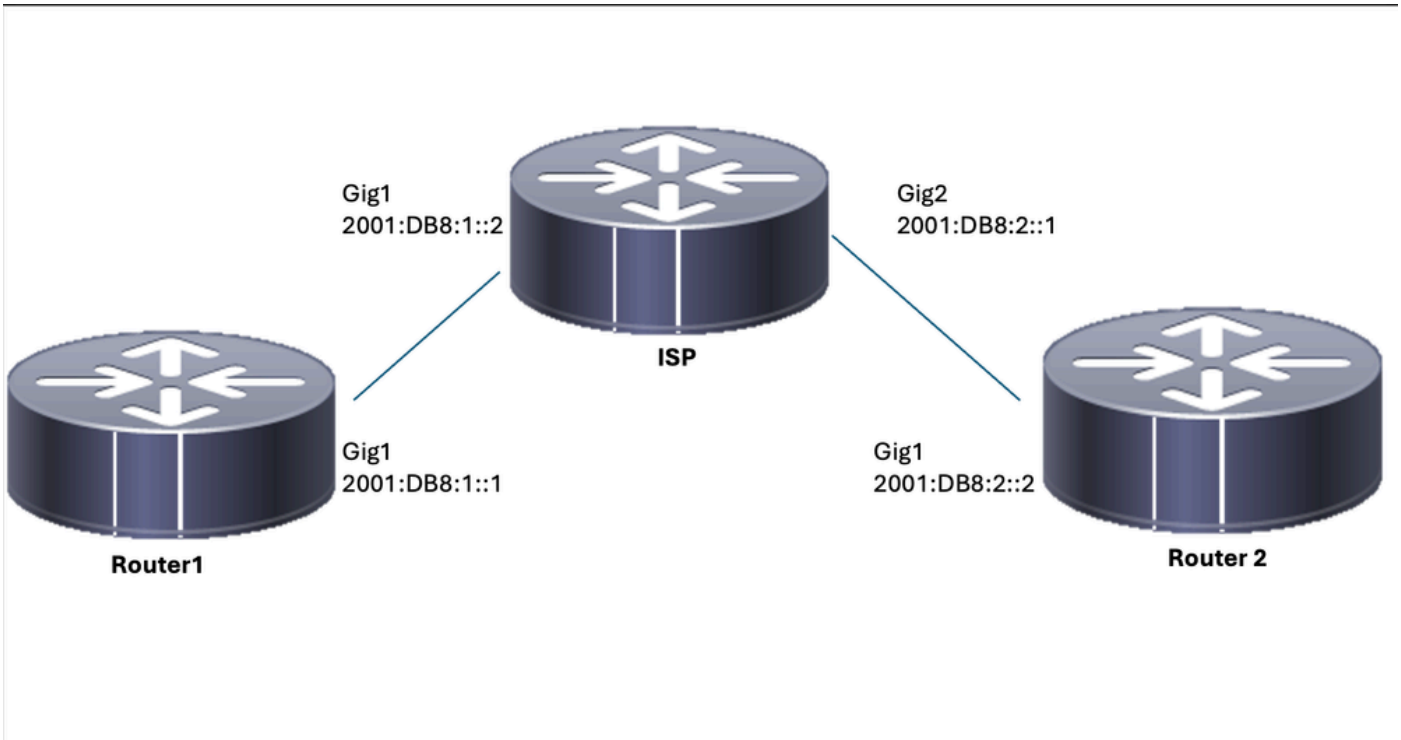
本檔案中的資訊是根據以下軟體版本：

- 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



本地路由器配置

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:DB8:1::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Ikev2建議。

```
crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14
```

步驟5.配置Ikev2策略。

```
crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP
```

步驟6.使用預共用金鑰配置金鑰環。

```
crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
 address 2001:DB8:2::2/64
 pre-shared-key cisco123
```

步驟7.配置Ikev2配置檔案。

```
crypto ikev2 profile IKEV2-PROF
 match identity remote address 2001:DB8:2::2/64
 authentication remote pre-share
 authentication local pre-share
 keyring local IPV6_KEY
```

步驟8.配置第2階段策略。

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

步驟9.配置IPsec配置檔案。

```
crypto ipsec profile IPSEC-PROF
 set transform-set ESP-AES-SHA
 set ikev2-profile IKEV2-PROF
```

步驟10.配置隧道介面。

```
interface Tunnel1
 ipv6 address 2001:DB8:3::1/64
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:2::2
 tunnel protection ipsec profile IPSEC-PROF
end
```

步驟11.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:DB8:1::1/64
no shutdown

!

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

!

ipv6 route ::/0 GigabitEthernet1

!

crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14

!

crypto ikev2 policy IKEv2-POLI
```

```
proposal IKEv2-PROP

!

crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
 address 2001:DB8:2::2/64
 pre-shared-key cisco123

!

crypto ikev2 profile IKEV2-PROF
 match identity remote address 2001:DB8:2::2/64
 authentication remote pre-share
 authentication local pre-share
 keyring local IPV6_KEY

!

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

!

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

 !

 crypto ipsec profile IPSEC-PROF
 set transform-set ESP-AES-SHA
 set ikev2-profile IKEV2-PROF

!

interface Tunnel1
 ipv6 address 2001:DB8:3::1/64
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:2::2
 tunnel protection ipsec profile IPSEC-PROF
end

!

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

ISP配置

```
ipv6 unicast-routing
!
!
interface GigabitEthernet1
 description Link to R1
 ipv6 address 2001:DB8:1::2/64
!
interface GigabitEthernet2
```

```
 description Link to R3
 ipv6 address 2001:DB8:2::1/64
!
!
!
ipv6 route 2001:DB8:1::/64 GigabitEthernet1
ipv6 route 2001:DB8:2::/64 GigabitEthernet2
!
```

遠端路由器最終配置

```
ipv6 unicast-routing
!
interface GigabitEthernet1
ipv6 address 2001:DB8:2::2/64
no shutdown

!

interface GigabitEthernet2
ipv6 address FC00::2/64
no shutdown

!

ipv6 route ::/0 GigabitEthernet1

!

crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14

!

crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP

!

crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
 address 2001:DB8:1::1/64
 pre-shared-key cisco123

!

crypto ikev2 profile IKEV2-PROF
 match identity remote address 2001:DB8:1::1/64
 authentication remote pre-share
 authentication local pre-share
 keyring local IPV6_KEY

!

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

```
mode tunnel

!

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

 !

 crypto ipsec profile IPSEC-PROF
 set transform-set ESP-AES-SHA
 set ikev2-profile IKEV2-PROF

!

interface Tunnel1
 ipv6 address 2001:DB8:3::2/64
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:1::1
 tunnel protection ipsec profile IPSEC-PROF
end

!

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

驗證

```
On Router 1

R1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
2          none/none             READY
Local  2001:DB8:1::1/500
Remote  2001:DB8:2::2/500
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/75989 sec

R1#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 2001:DB8:1::1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:DB8:2::2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

```
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 2001:DB8:1::1,
     remote crypto endpt.: 2001:DB8:2::2
     plaintext mtu 1422, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet1
     current outbound spi: 0x9DC2A6F6(2646779638)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x18569EF7(408329975)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2104, flow_id: CSR:104, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
         sa timing: remaining key lifetime (k/sec): (4608000/1193)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9DC2A6F6(2646779638)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2103, flow_id: CSR:103, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
         sa timing: remaining key lifetime (k/sec): (4608000/1193)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:


On Router 2

R2#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2001:DB8:2::2/500
Remote  2001:DB8:1::1/500
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/19 sec

R2#show cryto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 2001:DB8:2::2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:DB8:1::1 port 500
     PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

 local crypto endpt.: 2001:DB8:2::2,
 remote crypto endpt.: 2001:DB8:1::1
 plaintext mtu 1422, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet1
 current outbound spi: 0xEF1D3BA2(4011670434)
 PFS (Y/N): N, DH group: none

 inbound esp sas:
  spi: 0x9829B86D(2552871021)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2006, flow_id: CSR:6, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
     sa timing: remaining key lifetime (k/sec): (4608000/3556)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

 inbound ah sas:

 inbound pcp sas:

 outbound esp sas:
  spi: 0xEF1D3BA2(4011670434)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2005, flow_id: CSR:5, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
     sa timing: remaining key lifetime (k/sec): (4607998/3556)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

 outbound ah sas:

 outbound pcp sas:
```

疑難排解

若要對通道進行疑難排解，請使用以下debug指令：

- debug crypto ikev2
- debug crypto ikev2 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）。