IPv6를 사용하여 Cisco 라우터에 IKEv2 경로 기반 Site-to-Site VPN 구현

목차

소개

이 문서에서는 IKEv2(Internet Key Exchange version 2) 프로토콜을 사용하여 두 Cisco 라우터 간에 IPv6 경로 기반 사이트 대 사이트 터널을 설정하는 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS®/Cisco IOS® XE CLI 구성에 대한 기본 지식
- ISAKMP(Internet Security Association and Key Management Protocol) 및 IPsec 프로토콜에 대한 기본 지식
- IPv6 주소 지정 및 라우팅에 대한 이해

사용되는 구성 요소

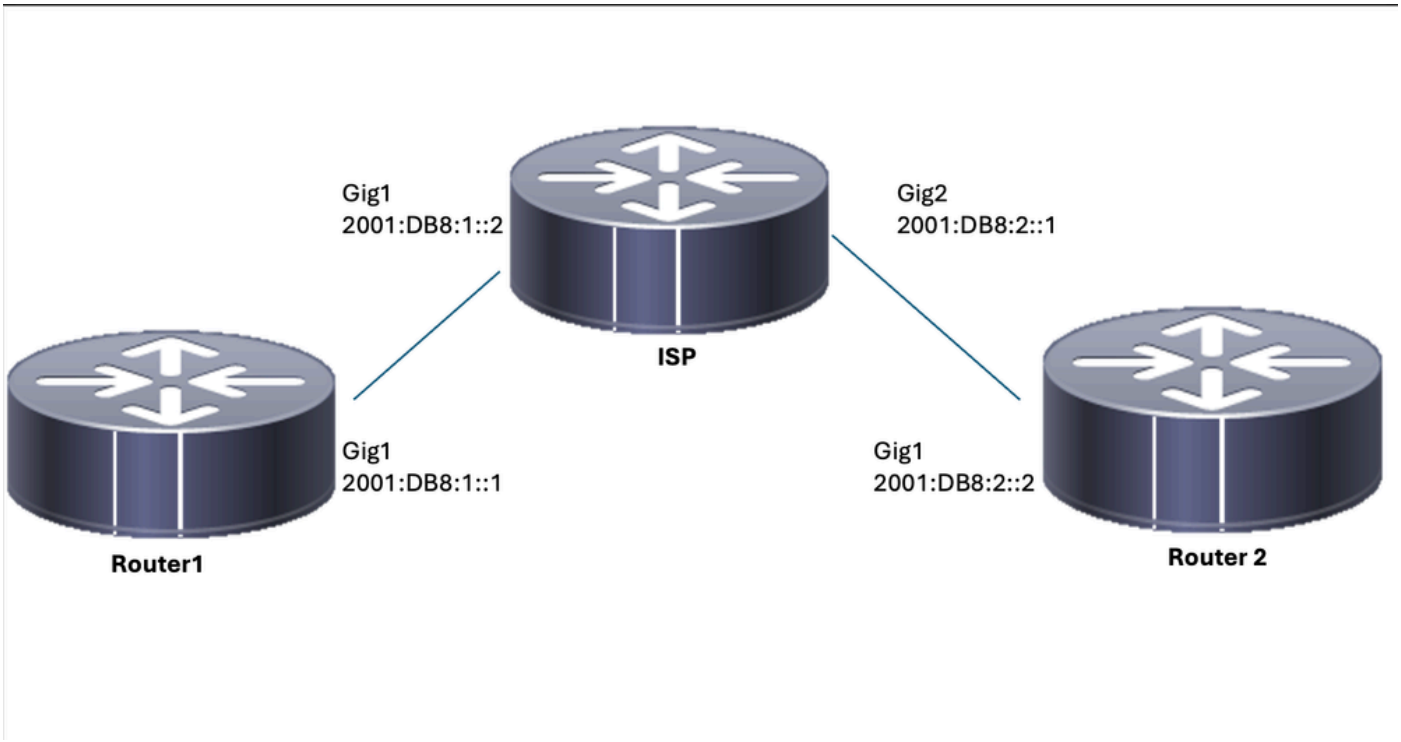
이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- 로컬 라우터로 17.03.04a를 실행하는 Cisco IOS XE
- 17.03.04a를 원격 라우터로 실행하는 Cisco IOS

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



로컬 라우터 컨피그레이션

1단계. IPv6 유니캐스트 라우팅을 활성화합니다.

```
ipv6 unicast-routing
```

2단계. 라우터 인터페이스를 구성합니다.

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

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

3단계. IPv6 기본 경로를 설정합니다.

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

4단계. Ikev2 제안서를 구성합니다.

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

5단계. Ikev2 정책을 구성합니다.

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

6단계. 사전 공유 키로 키링을 구성합니다.

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

7단계. Ikev2 프로파일을 구성합니다.

```
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
```

8단계. 2단계 정책을 구성합니다.

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

9단계. IPsec 프로필을 구성합니다.

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

10단계. 터널 인터페이스를 구성합니다.

```
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
```

11단계. 관심 트래픽에 대한 경로를 구성합니다.

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

로컬 라우터 최종 컨피그레이션

```
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 컨피그레이션

```
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
!
```

원격 라우터 최종 컨피그레이션

```
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
```

확인

```
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:
```

문제 해결

터널 문제를 해결하려면 다음 debug 명령을 사용합니다.

- debug crypto ikev2
- debug crypto ikev2 error
- debug crypto ipsec
- debug crypto ipsec error

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.