Implementando VPN site a site baseada em rota IKEv2 em roteadores Cisco usando IPv6

Contents

Introdução

Este documento descreve uma configuração para configurar um túnel de site a site IPv6 baseado em rota entre dois roteadores Cisco usando o protocolo IKEv2 (Internet Key Exchange versão 2).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento fundamental da configuração da CLI do Cisco IOS®/Cisco IOS® XE
- Conhecimento fundamental dos protocolos Internet Security Association and Key Management Protocol (ISAKMP) e IPsec
- Compreensão do roteamento e endereçamento IPv6

Componentes Utilizados

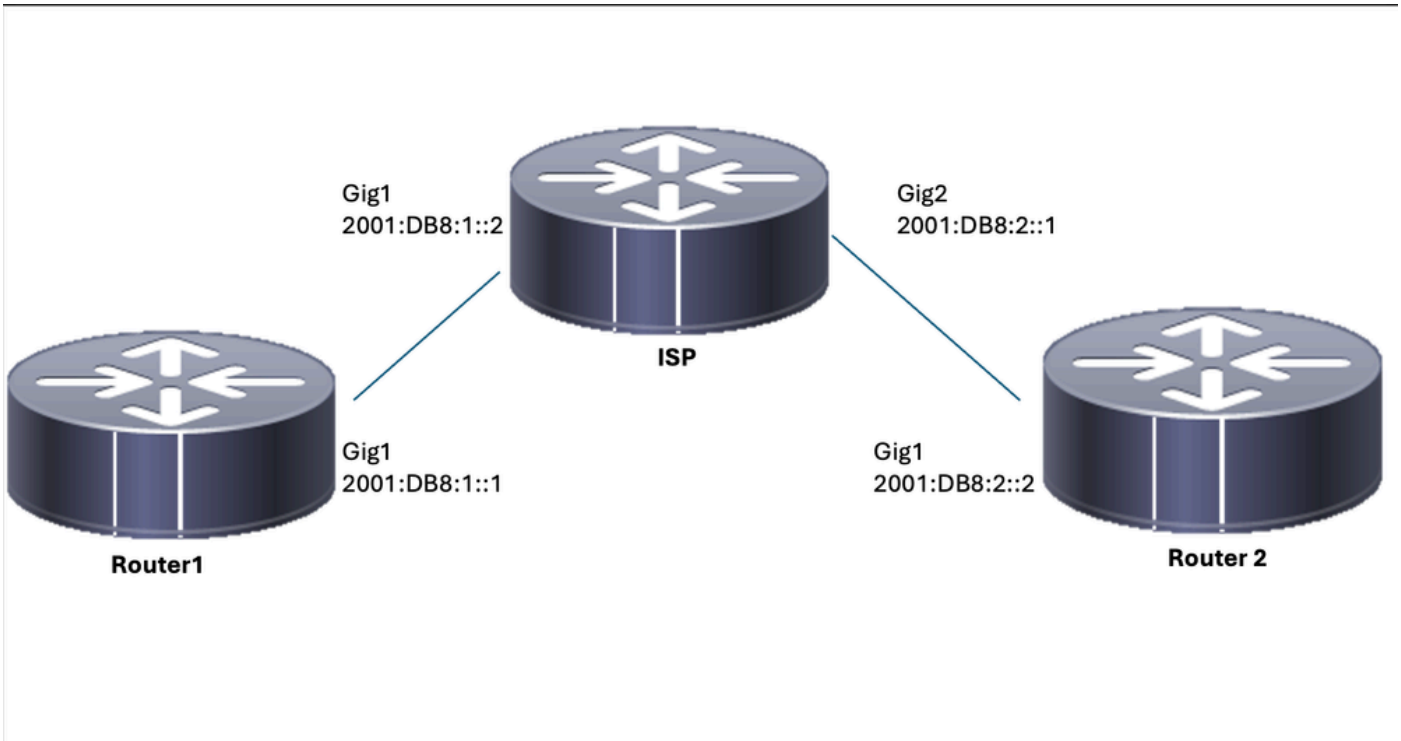
As informações neste documento são baseadas nestas versões de software:

- Cisco IOS XE executando 17.03.04a como roteador local
- Cisco IOS executando 17.03.04a como roteador remoto

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Configurações do roteador local

Etapa 1. Ativar o roteamento unicast IPv6.

```
ipv6 unicast-routing
```

Etapa 2. Configurar as interfaces do roteador.

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

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

Etapa 3. Definir a rota padrão IPv6.

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

Etapa 4. Configurar A Proposta De Ikev2.

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

Etapa 5. Configurar A Política Ikev2.

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

Etapa 6. Configurar o chaveiro com uma chave pré-compartilhada.

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

Etapa 7. Configurar o perfil Ikev2.

```
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
```

Etapa 8. Configurar a política da Fase 2.

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

Etapa 9. Configurar o perfil IPsec.

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

Etapa 10. Configurar a interface túnel.

```
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
```

Etapa 11. Configurar as rotas para o tráfego significativo.

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

Configuração final do roteador local

```
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
```

Configuração do ISP

```
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
!
```

Configuração final do roteador remoto

```
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
```

Verificação

```
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:
```

Troubleshooting

Para solucionar problemas do túnel, use estes comandos debug:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.