Implémentation d'un VPN site à site basé sur la route IKEv2 sur des routeurs Cisco utilisant IPv6

Table des matières

Introduction

Ce document décrit une configuration pour configurer un tunnel site à site basé sur la route IPv6 entre deux routeurs Cisco utilisant le protocole IKEv2 (Internet Key Exchange version 2).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances fondamentales de la configuration de l'interface de ligne de commande Cisco IOS®/Cisco IOS® XE
- Connaissances fondamentales des protocoles ISAKMP (Internet Security Association and Key Management Protocol) et IPsec
- Compréhension de l'adressage et du routage IPv6

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

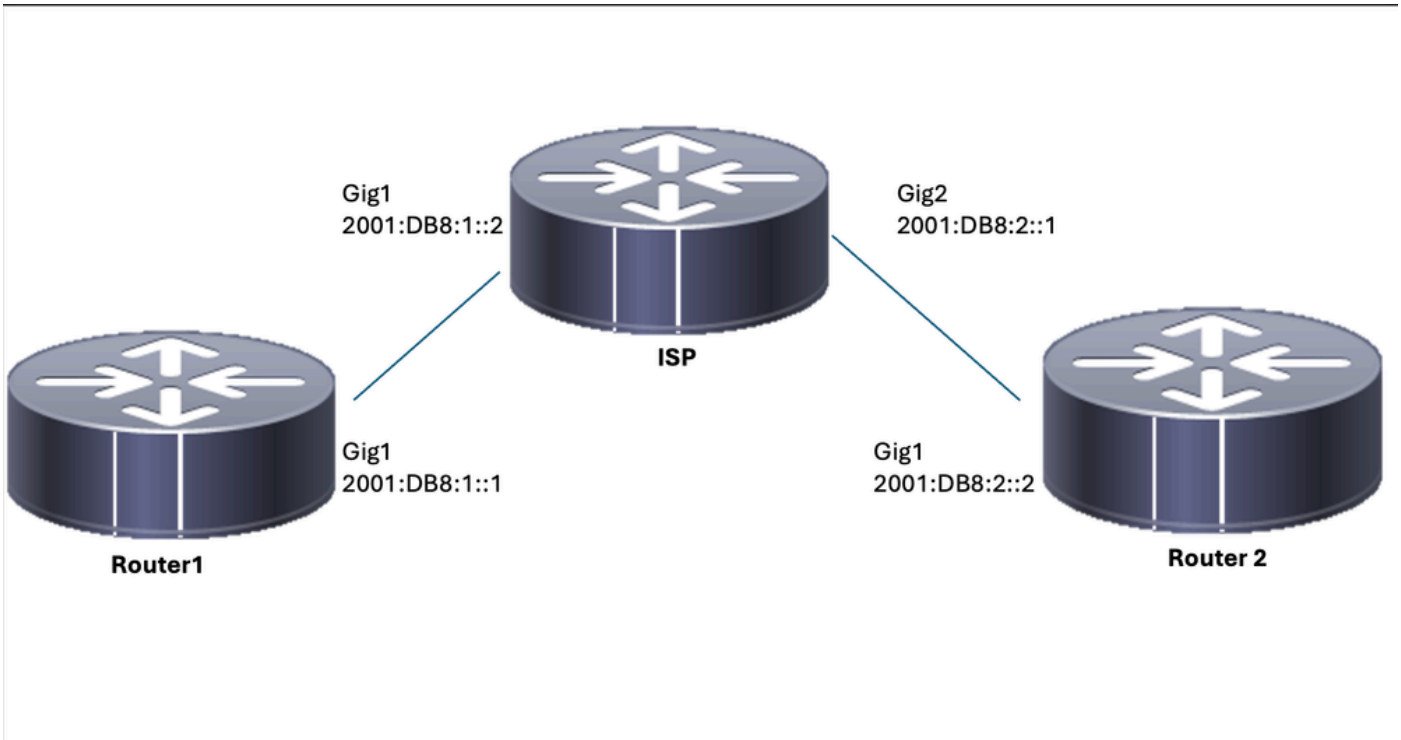
- Cisco IOS XE exécutant 17.03.04a comme routeur local

- Cisco IOS exécutant 17.03.04a en tant que routeur distant

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Configurations des routeurs locaux

Étape 1 : activation du routage de monodiffusion IPv6

```
ipv6 unicast-routing
```

Étape 2 : configuration des interfaces du routeur

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

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

Étape 3 : définition de la route par défaut IPv6

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

Étape 4 : configuration de la proposition Ikev2

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

Étape 5 : configuration de la stratégie Ikev2

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

Étape 6. Configuration du trousseau de clés avec une clé pré-partagée

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

Étape 7 : configuration du profil 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
```

Étape 8 : configuration de la stratégie de phase 2

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

Étape 9. Configuration du profil IPsec

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

Étape 10. Configuration de l'interface du tunnel

```
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
```

Étape 11 : configuration des routes pour le trafic intéressant

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

Configuration finale du routeur 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
```

Configuration du FAI

```
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
!
```

Configuration finale du routeur distant

```
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
```

Vérification

```
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:
```

Dépannage

Afin de dépanner le tunnel, utilisez ces commandes debug :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.