IKEv1 routegebaseerde site naar site VPN met IPV6

Inhoud

Inleiding

Dit document beschrijft een configuratie om een IPv6, route-gebaseerde, site-to-site tunnel tussen twee Cisco-routers in te stellen met behulp van het Internet Key Exchange versie 1 (IKEv1/ISAKMP) protocol.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Fundamentele kennis van de configuratie van Cisco IOS®/Cisco IOS® XE CLI
- Fundamentele kennis van Internet Security Association en Key Management Protocol (ISAKMP) en IPsec-protocollen
- Inzicht in IPv6-adressering en -routing

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

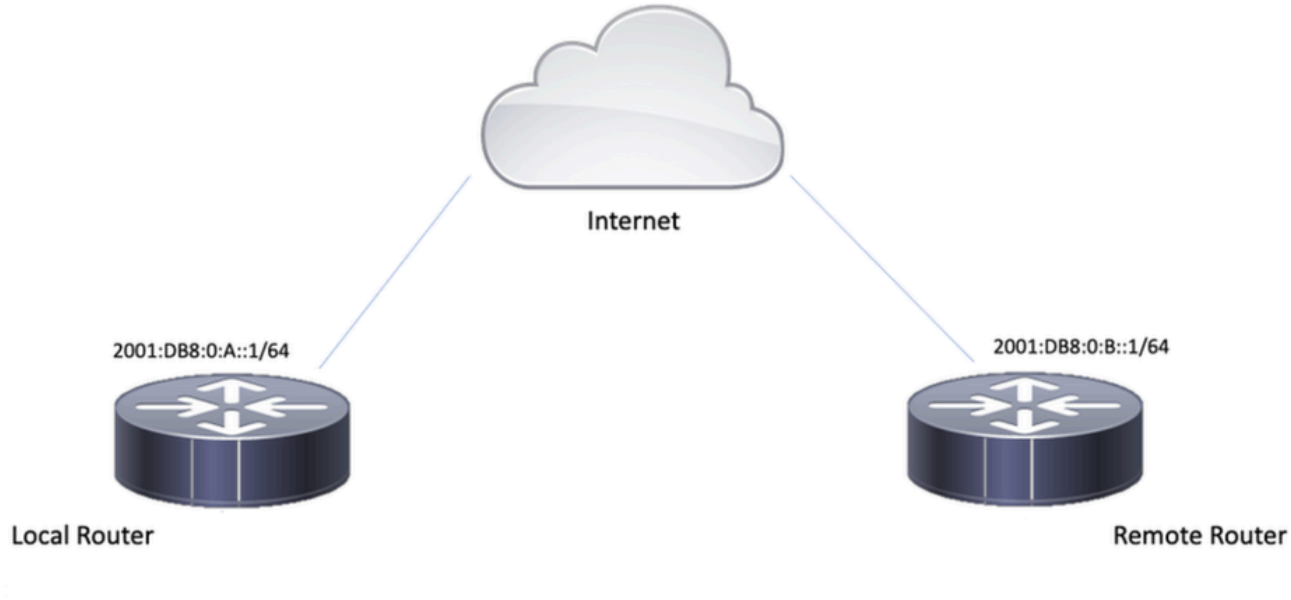
- Cisco IOS XE met 17.03.04a als lokale router
- Cisco IOS-softwarerelease 17.03.04a als externe router

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram



Configuraties

Lokale router

Stap 1. Schakel IPv6 Unicast Routing in.

```
ipv6 unicast-routing
```

Stap 2. Configureer de routerinterfaces.

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

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

Stap 3. Stel IPv6-standaardroute in.

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

Stap 4. Configureer het beleid van fase 1.

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

Stap 5. Configureer de sleutelhanger met een vooraf gedeelde sleutel.

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

Stap 6. Configureer het ISAKMP-profiel.

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

Stap 7. Configureer het fase 2-beleid.

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

Stap 8. Configureer het IPsec-profiel.

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

Stap 9. Configureer de tunnelinterface.

```
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
```

Stap 10. Configureer de routes voor het interessante verkeer.

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

Definitieve configuratie van lokale router

```
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
```

Definitieve configuratie van externe router

```
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
```

Problemen oplossen

Gebruik de debug-opdrachten om problemen met de tunnel op te lossen:

- debug crypto isakmp
- debug crypto isakmp fout
- debug crypto ipsec
- debug crypto ipsec fout

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.