VPN site à site basé sur la route IKEv1 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 IKEv1/ISAKMP (Internet Key Exchange version 1).

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 :

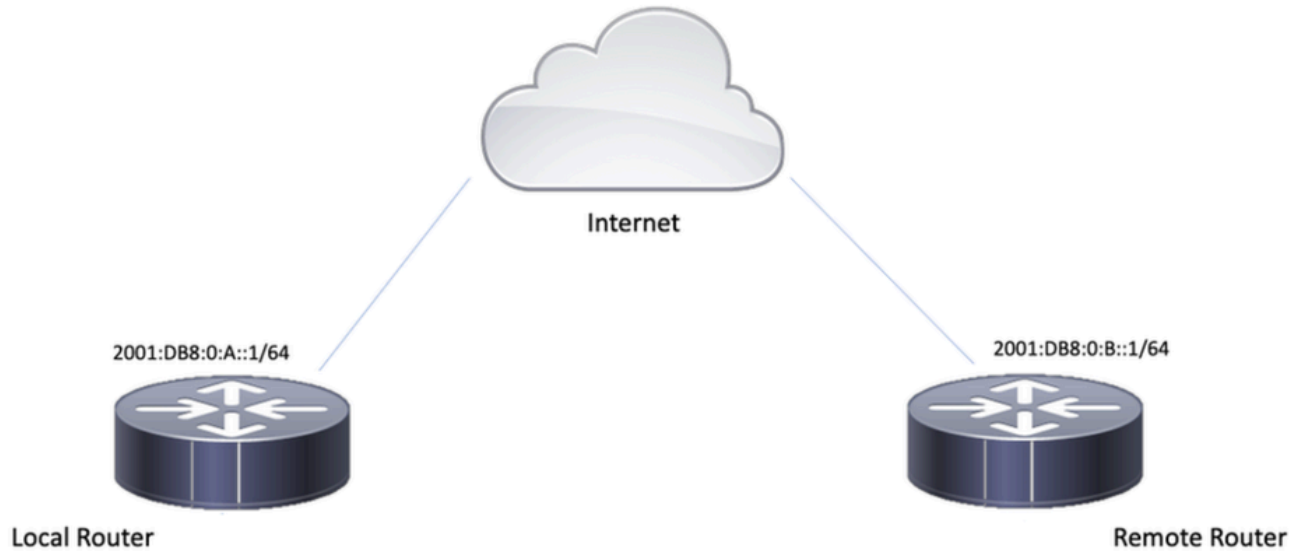
- Cisco IOS XE exécutant 17.03.04a comme routeur local
- Cisco IOS exécutant 17.03.04a en tant que routeur distant

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

Routeur local

Étape 1 : activation du routage de monodiffusion IPv6

```
ipv6 unicast-routing
```

Étape 2 : configuration des interfaces du routeur

```
interface GigabitEthernet1
ipv6 address 2001:DB8:0:A::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 stratégie de phase 1

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

Étape 5. Configuration du trousseau de clés avec une clé pré-partagée

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

Étape 6 : configuration du profil ISAKMP

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

Étape 7 : configuration de la stratégie de phase 2

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

Étape 8. Configuration du profil IPsec

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

Étape 9 : configuration de l’interface du tunnel

```
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
```

Étape 10 : 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:DB8:0: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
```

Configuration finale du routeur distant

```
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
```

Dépannage

Afin de dépanner le tunnel, utilisez les commandes debug :

- debug crypto isakmp
- debug crypto isakmp 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.