IKEv1-basiertes Site-to-Site-VPN mit IPV6

Inhalt

Einleitung

In diesem Dokument wird eine Konfiguration zum Einrichten eines routenbasierten IPv6-Site-to-Site-Tunnels zwischen zwei Cisco Routern unter Verwendung des Internet Key Exchange Version 1 (IKEv1/ISAKMP)-Protokolls beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der CLI-Konfiguration von Cisco IOS®/Cisco IOS® XE
- Grundlegendes Wissen über ISAKMP- (Internet Security Association and Key Management Protocol) und IPsec-Protokolle
- IPv6-Adressierung und -Routing

Verwendete Komponenten

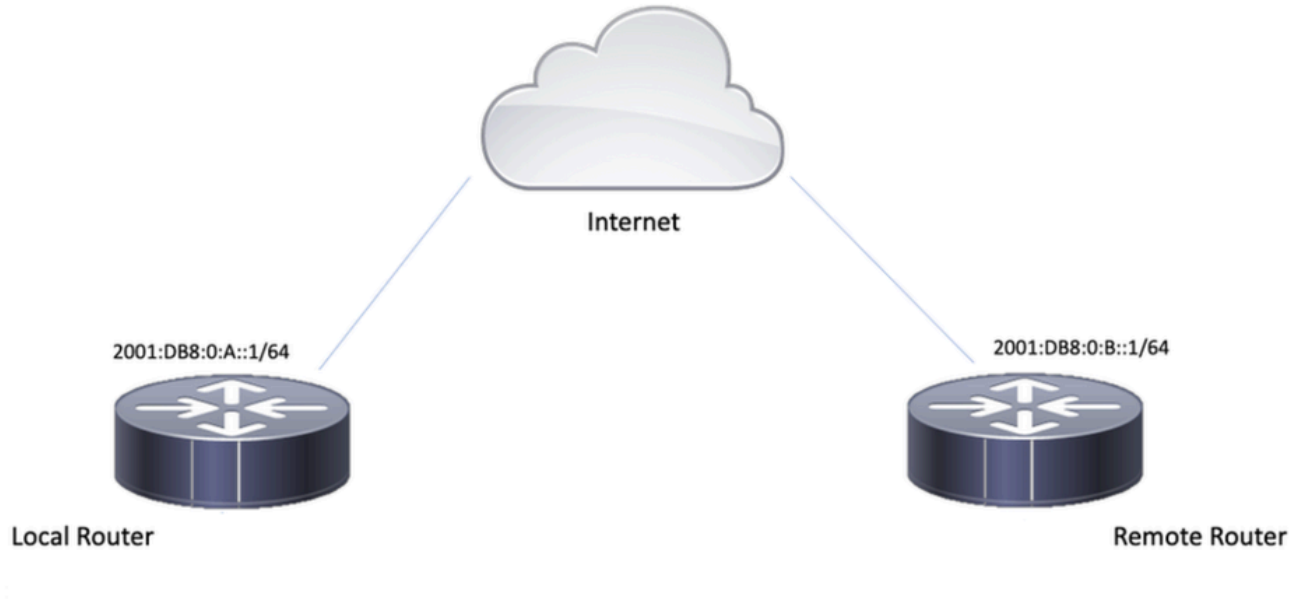
Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco IOS XE mit 17.03.04a als lokalem Router
- Cisco IOS mit 17.03.04a als Remote-Router

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Lokaler Router

Schritt 1: Aktivieren Sie IPv6-Unicast-Routing.

```
ipv6 unicast-routing
```

Schritt 2: Konfigurieren der Router-Schnittstellen

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

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

Schritt 3: Festlegen der IPv6-Standardroute

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

Schritt 4: Konfigurieren der Richtlinie für Phase 1

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

Schritt 5: Konfigurieren Sie den Keyring mit einem Pre-Shared Key.

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

Schritt 6: Konfigurieren Sie das ISAKMP-Profil.

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

Schritt 7: Konfigurieren der Richtlinie für Phase 2

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

Schritt 8: Konfigurieren des IPsec-Profils

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

Schritt 9: Konfigurieren Sie die Tunnelschnittstelle.

```
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
```

Schritt 10: Konfigurieren Sie die Routen für den interessanten Datenverkehr.

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

Endkonfiguration des lokalen Routers

```
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
```

Endkonfiguration des Remote-Routers

```
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
```

Fehlerbehebung

Verwenden Sie die folgenden Debug-Befehle, um eine Fehlerbehebung für den Tunnel durchzuführen:

- debuggen crypto isakmp
- debug crypto isakmp error
- debuggen crypto ipsec
- debuggen crypto ipsec-Fehler

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.