VPN da sito a sito basata su route IKEv1 con IPV6

Sommario

Introduzione

In questo documento viene descritta la configurazione per configurare un tunnel da sito a sito IPv6 basato su routing tra due router Cisco con protocollo IKEv1/ISAKMP (Internet Key Exchange versione 1).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze fondamentali della configurazione CLI di Cisco IOS®/Cisco IOS® XE
- Conoscenze base dei protocolli ISAKMP (Internet Security Association and Key Management Protocol) e IPsec
- Informazioni sull'indirizzamento e il routing IPv6

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

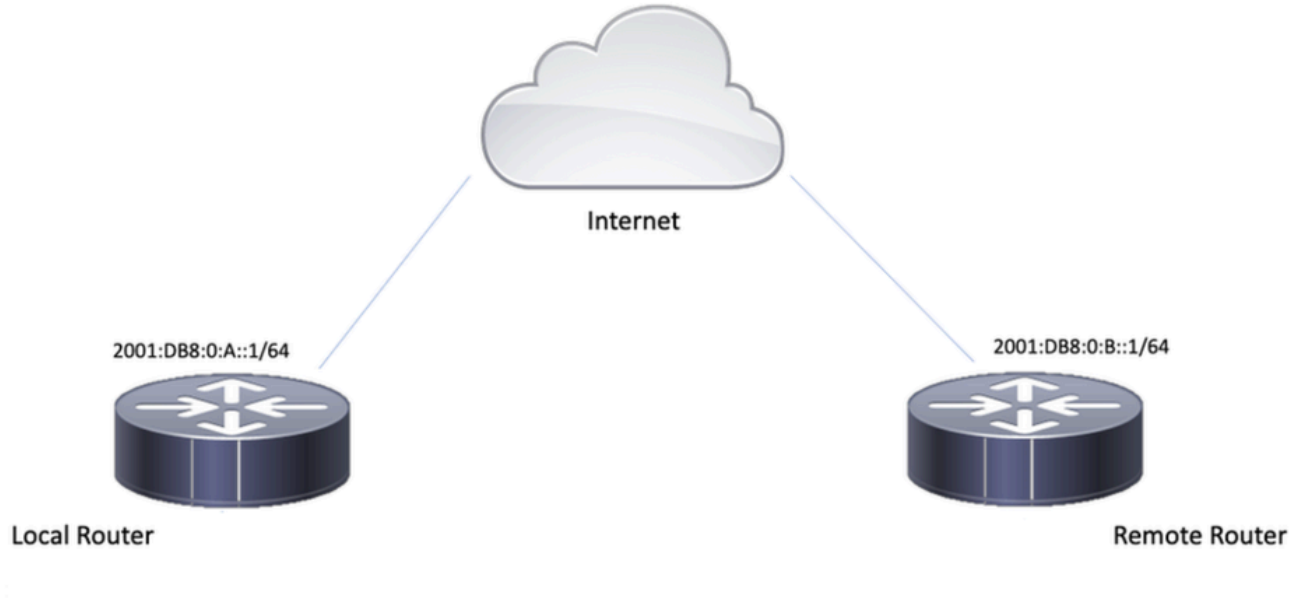
- Cisco IOS XE con 17.03.04a come router locale
- Cisco IOS con versione 17.03.04a come router remoto

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazioni

Router locale

Passaggio 1. Abilitare il routing unicast IPv6.

```
ipv6 unicast-routing
```

Passo 2: configurare le interfacce del router.

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

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

Passaggio 3. Impostare la route predefinita IPv6.

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

Passaggio 4. Configurare i criteri della fase 1.

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

Passaggio 5. Configurare il keyring con una chiave già condivisa.

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

Passaggio 6. Configurare il profilo ISAKMP.

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

Passaggio 7. Configurare il criterio Fase 2.

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

Passaggio 8. Configurare il profilo IPSec.

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

Passaggio 9. Configurare l'interfaccia del 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
```

Passaggio 10. Configurare le route per il traffico interessante.

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

Configurazione finale router locale

```
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
```

Configurazione finale router remoto

```
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
```

Risoluzione dei problemi

Per risolvere i problemi del tunnel, usare i comandi di debug:

- debug crypto isakmp
- errore debug crypto isakmp
- debug crypto ipsec
- errore debug crypto ipsec

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).