IKEv1 Route Based Site to Site VPN using IPV6

Contents

Introduction

This document describes a configuration to set up an IPv6, route-based, site-to-site tunnel between two Cisco routers using the Internet Key Exchange version 1 (IKEv1/ISAKMP) protocol.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Fundamental knowledge of Cisco IOS®/Cisco IOS® XE CLI configuration
- Fundamental knowledge of Internet Security Association and Key Management Protocol (ISAKMP) and IPsec protocols
- Understanding of IPv6 addressing and routing

Components Used

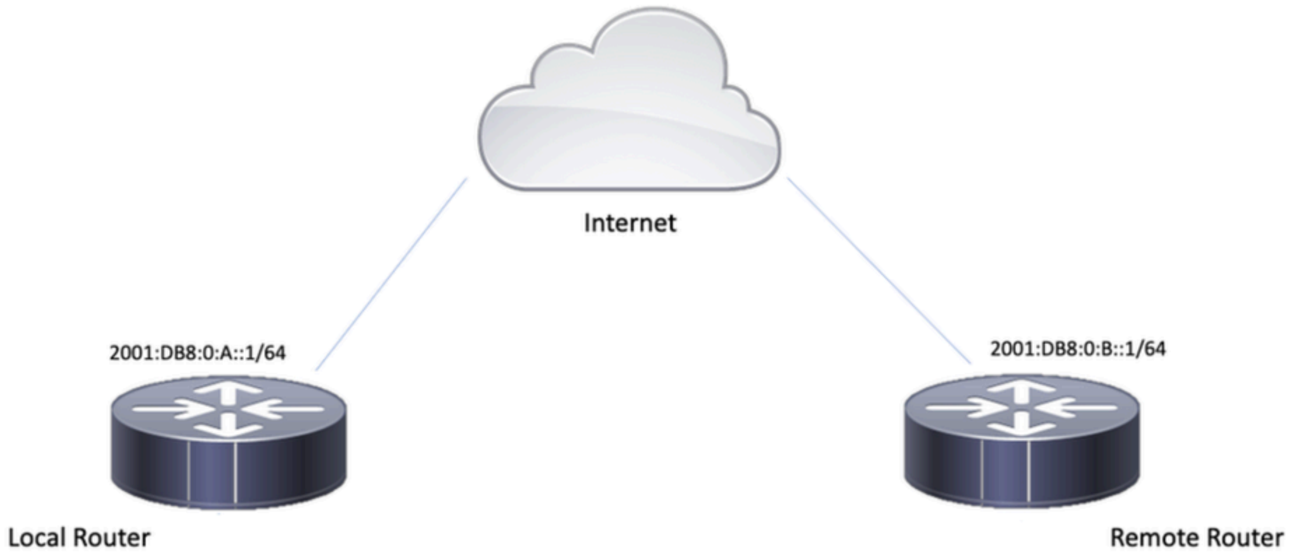
The information in this document is based on these software versions:

- Cisco IOS XE running 17.03.04a as Local Router
- Cisco IOS running 17.03.04a as Remote Router

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configurations

Local Router

Step 1. Enable IPv6 Unicast Routing.

```
ipv6 unicast-routing
```

Step 2. Configure the router interfaces.

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

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

Step 3. Set IPv6 Default Route.

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

Step 4. Configure Phase 1 policy.

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

Step 5. Configure keyring with a pre-shared key.

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

Step 6. Configure the ISAKMP profile.

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

Step 7. Configure the Phase 2 policy.

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

Step 8. Configure the IPsec profile.

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

Step 9. Configure the tunnel interface.

```
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
```

Step 10. Configure the routes for the interesting traffic.

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

Local Router Final Configuration

```
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
```

Remote Router Final Configuration

```
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
```

Troubleshoot

In order to troubleshoot the tunnel, use the debug commands:

- **debug crypto isakmp**
- **debug crypto isakmp error**
- **debug crypto ipsec**
- **debug crypto ipsec error**