

IPv6を使用したCiscoルータでのIKEv2ルートベースのサイト間VPNの実装

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ローカルルータの設定](#)

[ローカルルータの最終設定](#)

[ISPの設定](#)

[リモートルータの最終設定](#)

[検証](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、インターネットキーエクスチェンジバージョン2(IKEv2)プロトコルを使用して、2台のCiscoルータ間にIPv6のルートベースのサイト間トンネルを設定する設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IOS®/Cisco IOS® XEのCLI設定に関する基礎知識
- Internet Security Association and Key Management Protocol(ISAKMP)およびIPSecプロトコルに関する基礎知識
- IPv6アドレッシングおよびルーティングの理解

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

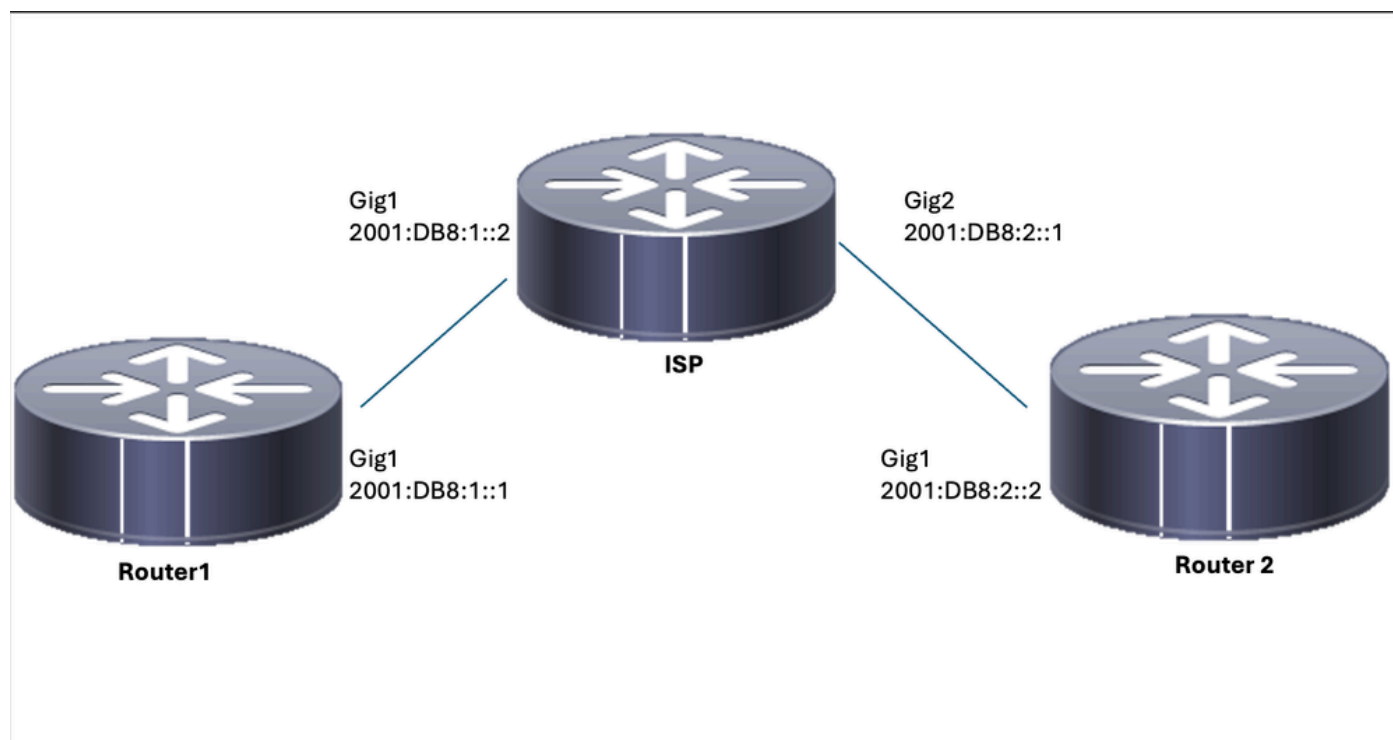
- ローカルルータとして17.03.04aを実行するCisco IOS XE

- リモートルータとして17.03.04aを実行するCisco IOS

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



ローカルルータの設定

ステップ 1：IPv6ユニキャストルーティングを有効にします。

```
ipv6 unicast-routing
```

ステップ 2：ルータ インターフェイスの設定。

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

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

ステップ 3 : IPv6デフォルトルートを設定します。

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

ステップ 4 : Ikev2プロポーザルを設定します。

```
crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14
```

ステップ 5 : Ikev2ポリシーを設定します。

```
crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP
```

手順 6 : 事前共有キーを使用してキーリングを設定します。

```
crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
address 2001:DB8:2::2/64
pre-shared-key cisco123
```

手順 7 : Ikev2プロファイルを設定します。

```
crypto ikev2 profile IKEV2-PROF
match identity remote address 2001:DB8:2::2/64
authentication remote pre-share
authentication local pre-share
keyring local IPV6_KEY
```

ステップ 8 : フェーズ2ポリシーを設定します。

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

ステップ 9 : IPsecプロファイルを設定します。

```
crypto ipsec profile IPSEC-PROF
  set transform-set ESP-AES-SHA
  set ikev2-profile IKEV2-PROF
```

ステップ 10 : トンネル インターフェイスを設定します。

```
interface Tunnel1
  ipv6 address 2001:DB8:3::1/64
  tunnel source GigabitEthernet1
  tunnel mode ipsec ipv6
  tunnel destination 2001:DB8:2::2
  tunnel protection ipsec profile IPSEC-PROF
end
```

ステップ 11対象トラフィックのルートを設定します。

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

ローカルルータの最終設定

```
ipv6 unicast-routing
!
interface GigabitEthernet1
  ipv6 address 2001:DB8:1::1/64
  no shutdown

!

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

!

ipv6 route ::/0 GigabitEthernet1

!

crypto ikev2 proposal IKEv2-PROP
  encryption aes-cbc-128
  integrity sha1
  group 14
```

```

!

crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP

!

crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
  address 2001:DB8:2::2/64
  pre-shared-key cisco123

!

crypto ikev2 profile IKEV2-PROF
  match identity remote address 2001:DB8:2::2/64
  authentication remote pre-share
  authentication local pre-share
  keyring local IPV6_KEY

!

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

!

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

!

crypto ipsec profile IPSEC-PROF
  set transform-set ESP-AES-SHA
  set ikev2-profile IKEV2-PROF

!

interface Tunnel1
  ipv6 address 2001:DB8:3::1/64
  tunnel source GigabitEthernet1
  tunnel mode ipsec ipv6
  tunnel destination 2001:DB8:2::2
  tunnel protection ipsec profile IPSEC-PROF
end

!

ipv6 route FC00::/64 2012::1

```

ISPの設定

```

ipv6 unicast-routing
!
!
interface GigabitEthernet1

```

```

description Link to R1
ipv6 address 2001:DB8:1::2/64
!
interface GigabitEthernet2
description Link to R3
ipv6 address 2001:DB8:2::1/64
!
!
!
ipv6 route 2001:DB8:1::/64 GigabitEthernet1
ipv6 route 2001:DB8:2::/64 GigabitEthernet2
!

```

リモートルータの最終設定

```

ipv6 unicast-routing
!
interface GigabitEthernet1
ipv6 address 2001:DB8:2::2/64
no shutdown

!

interface GigabitEthernet2
ipv6 address FC00::2/64
no shutdown

!

ipv6 route ::/0 GigabitEthernet1

!

crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14

!

crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP

!

crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
address 2001:DB8:1::1/64
pre-shared-key cisco123

!

crypto ikev2 profile IKEV2-PROF
match identity remote address 2001:DB8:1::1/64
authentication remote pre-share
authentication local pre-share
keyring local IPV6_KEY

```

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

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

```
!  
  
crypto ipsec profile IPSEC-PROF  
set transform-set ESP-AES-SHA  
set ikev2-profile IKEV2-PROF
```

```
!  
  
interface Tunnel1  
ipv6 address 2001:DB8:3::2/64  
tunnel source GigabitEthernet1  
tunnel mode ipsec ipv6  
tunnel destination 2001:DB8:1::1  
tunnel protection ipsec profile IPSEC-PROF  
end
```

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

検証

On Router 1

```
R1#show crypto ikev2 sa  
IPv4 Crypto IKEv2 SA
```

```
IPv6 Crypto IKEv2 SA
```

```
Tunnel-id    fvrfr/ivrf          Status  
2            none/none          READY
```

```
Local  2001:DB8:1::1/500
```

```
Remote 2001:DB8:2::2/500
```

```
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: P  
Life/Active Time: 86400/75989 sec
```

```
R1#show crypto ipsec sa
```

```
interface: Tunnel1  
Crypto map tag: Tunnel1-head-0, local addr 2001:DB8:1::1
```

```
protected vrf: (none)  
local ident (addr/mask/prot/port): (::/0/0/0)  
remote ident (addr/mask/prot/port): (::/0/0/0)  
current_peer 2001:DB8:2::2 port 500  
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 2001:DB8:1::1,
remote crypto endpt.: 2001:DB8:2::2
plaintext mtu 1422, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet1
current outbound spi: 0x9DC2A6F6(2646779638)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
spi: 0x18569EF7(408329975)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2104, flow_id: CSR:104, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4608000/1193)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcg sas:
```

```
outbound esp sas:
spi: 0x9DC2A6F6(2646779638)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2103, flow_id: CSR:103, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4608000/1193)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcg sas:
```

On Router 2

```
R2#show crypto ikev2 sa
```

```
IPv4 Crypto IKEv2 SA
```

```
IPv6 Crypto IKEv2 SA
```

```
Tunnel-id    fvrf/ivrf          Status
1            none/none          READY
```

```
Local  2001:DB8:2::2/500
```

```
Remote 2001:DB8:1::1/500
```

```
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: P
Life/Active Time: 86400/19 sec
```

```
R2#show crypto ipsec sa
```

```
interface: Tunnel1
```

```
Crypto map tag: Tunnel1-head-0, local addr 2001:DB8:2::2
```

```
protected vrf: (none)
```



```
local ident (addr/mask/prot/port): (::/0/0/0)
remote ident (addr/mask/prot/port): (::/0/0/0)
current_peer 2001:DB8:1::1 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
#pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 2001:DB8:2::2,
remote crypto endpt.: 2001:DB8:1::1
plaintext mtu 1422, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet1
current outbound spi: 0xEF1D3BA2(4011670434)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x9829B86D(2552871021)
    transform: esp-aes esp-sha-hmac ,
    in use settings = {Tunnel, }
    conn id: 2006, flow_id: CSR:6, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4608000/3556)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xEF1D3BA2(4011670434)
    transform: esp-aes esp-sha-hmac ,
    in use settings = {Tunnel, }
    conn id: 2005, flow_id: CSR:5, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
    sa timing: remaining key lifetime (k/sec): (4607998/3556)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

トラブルシューティング

トンネルをトラブルシューティングするには、次のdebugコマンドを使用します。

- debug crypto ikev2
- debug crypto ikev2 error
- debug crypto ipsec
- debug crypto ipsec error

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。