

# FlexVPN : IPv6 の基本的な LAN-to-LAN 設定

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ネットワーク図](#)

[基本 IPv6 アドレッシングと関連するスタティック ルーティングの設定](#)

[Flex VPN の基本的な LAN-to-LAN 設定](#)

[IKEv2 プロポーザル、ポリシー、および認証ポリシー](#)

[IKEv2 キーリング、IKEv2 プロファイル、証明書マップおよび IPsec プロファイル](#)

[sVTi を使用したトンネル インターフェイスの作成](#)

[関連情報](#)

## 概要

このドキュメントでは、ローカル認証（事前共有キーおよび証明書）を使用した IPv6 エンドポイント間の FlexVPN LAN-to-LAN トンネル設定について説明します。

## 前提条件

### 要件

このドキュメントに関しては個別の要件はありません。

### 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

### 表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

## ネットワーク図

### [基本 IPv6 アドレッシングと関連するスタティック ルーティングの設定](#)

IPv6 アドレッシングについてはこのドキュメントでは説明しません。詳細については、「[IPv6 アドレッシングおよび基本的な接続の実装](#)」を参照してください。

ルータ R1 :

```
ipv6 unicast-routing
!
interface Ethernet0/0
 no ip address
 ipv6 address 2001:DB8:123:1::2/64
 ipv6 enable
!
ipv6 route ::/0 2001:DB8:123:1::1
!
```

ルータ ISP :

```
ipv6 unicast-routing
!
interface Ethernet0/0
 no ip address
 ipv6 address 2001:DB8:123:1::1/64
 ipv6 enable
!
interface Ethernet0/1
 no ip address
 ipv6 address 2001:DB8:123:2::1/64
 ipv6 enable
!
```

ルータ R2 :

```
ipv6 unicast-routing
!
interface Ethernet0/0
 no ip address
 ipv6 address 2001:DB8:123:2::2/64
 ipv6 enable
!
ipv6 route ::/0 2001:DB8:123:2::1
!
```

## [Flex VPN の基本的な LAN-to-LAN 設定](#)

2 つの IPv6 エンドポイント間での基本的な LAN-to-LAN の設定は、IPv4 と同じです。

### [IKEv2 プロポーザル、ポリシー、および認証ポリシー](#)

この例ではスマート デフォルト (IKEv2 プロポーザル、ポリシー、および認証ポリシー) を使用します。

**注:** スマート デフォルトの設定は必須ではありません。

```
crypto ikev2 authorization policy default
 route set interface
 route accept any
```

```
!  
crypto ikev2 proposal default  
  encryption aes-cbc-256 aes-cbc-192 aes-cbc-128  
  integrity sha512 sha384 sha256 sha1 md5  
  group 5 2  
!  
crypto ikev2 policy default  
  match fvrfl any  
  proposal default  
!
```

## IKEv2 キーリング、IKEv2 プロファイル、証明書マップおよび IPsec プロファイル

### PSK を使用する場合

ルータ R1 :

```
crypto ikev2 keyring key  
  peer R2.cisco.com  
    description Pre-Shared-Key for Router2  
    address 2001:DB8:123:2::2/128  
    hostname Router2  
    identity address 2001:DB8:123:2::2  
    pre-shared-key local cisco123  
    pre-shared-key remote cisco456  
!  
crypto ikev2 profile default  
  match identity remote address 2001:DB8:123:2::2/128  
  authentication remote pre-share  
  authentication local pre-share  
  keyring local key  
!  
crypto ipsec profile default*  
  set ikev2-profile default  
!
```

*\*as of 15.3(3)T the following line need not be explicitly configured anymore and is part of the smart default.*

ルータ R2 :

```
crypto ikev2 keyring key  
  peer R1.cisco.com  
    description Pre-Shared-Key for Router1  
    address 2001:DB8:123:1::2/128  
    hostname Router1  
    identity address 2001:DB8:123:1::2  
    pre-shared-key local cisco456  
    pre-shared-key remote cisco123  
!  
crypto ikev2 profile default  
  match identity remote address 2001:DB8:123:1::2/128  
  authentication remote pre-share  
  authentication local pre-share  
  keyring local key  
!  
crypto ipsec profile default  
  set ikev2-profile default  
!
```

## 証明書を使用する場合

ルータ R1 :

```
crypto pki trustpoint ikev2
  enrollment url http://[2001:DB8:123:1::1]:80
  revocation-check none
crypto pki certificate map cmap 1
  subject-name eq hostname = router2.cisco.com
!
crypto ikev2 profile default
  match identity remote address 2001:DB8:123:2::2/128
  match certificate cmap
  authentication remote rsa-sig
  authentication local rsa-sig
  pki trustpoint ikev2
!
crypto ipsec profile default
  set ikev2-profile default
!
```

ルータ R2 :

```
crypto pki trustpoint ikev2
  enrollment url http://[2001:DB8:123:1::1]:80
  revocation-check none
crypto pki certificate map cmap 1
  subject-name eq hostname = router1.cisco.com
!
crypto ikev2 profile default
  match identity remote address 2001:DB8:123:1::2/128
  match certificate cmap
  authentication remote rsa-sig
  authentication local rsa-sig
  pki trustpoint ikev2
!
crypto ipsec profile default
  set ikev2-profile default
!
```

## sVTi を使用したトンネル インターフェイスの作成

2 種類のトラフィック ( 既存の IPv6 トンネル経由での IPv6 および IPv4 ) を使用できるため、次のような複数の設計があります。

- tunnel mode ipsec ipv6 を使用した IPv6 トンネルでの IPv6
- tunnel mode gre ipv6 を使用した IPv6 トンネルでの IPv4
- tunnel mode gre ipv6 を使用したトンネルでの IPv4 と IPv6 の両方を実行するハイブリッドモード

注: 管理者は SVTI ( IPsec モード ) を介した GRE トンネルを使用することが推奨されます。これは、ほとんどの導入環境では、IPv6 サポートは実際にはデュアル スタックを意味し、GRE/IPSEC ではデュアル スタックがシームレスにサポートされるためです。

## IPv6 トンネルでの IPv6

ルータ R1 :

```

interface Loopback0
  description This is a test endpoint
  no ip address
  ipv6 address 2001:DB8:100:1::1/64
  ipv6 enable
!
interface Tunnel0
  no ip address
  ipv6 address 2001:DB8:99::1/64
  ipv6 enable
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv6
  tunnel destination 2001:DB8:123:2::2
  tunnel protection ipsec profile default
!
ipv6 route 2001:DB8:200:1::/64 Tunnel0
!

```

## ルータ R2 :

```

interface Loopback0
  description This is a test endpoint
  no ip address
  ipv6 address 2001:DB8:200:1::1/64
  ipv6 enable
!
interface Tunnel0
  no ip address
  ipv6 address 2001:DB8:99::2/64
  ipv6 enable
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv6
  tunnel destination 2001:DB8:123:1::2
  tunnel protection ipsec profile default
!
ipv6 route 2001:DB8:100:1::/64 Tunnel0
!

```

## show コマンド :

```

=====
IKEv2 SA:
=====
Using PSK:
-----
Router1#show crypto ikev2 sa detailed
 IPv4 Crypto IKEv2 SA

 IPv6 Crypto IKEv2 SA

Tunnel-id   fvrf/ivrf           Status
2           none/none           READY
Local   2001:DB8:123:1::2/500
Remote  2001:DB8:123:2::2/500
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
      Auth verify: PSK
      Life/Active Time: 86400/14180 sec
      CE id: 0, Session-id: 1
      Status Description: Negotiation done
      Local spi: C73B18AE83F68C11      Remote spi: EF52B3A4454D1AAA
      Local id: 2001:DB8:123:1::2

```

```
Remote id: 2001:DB8:123:2::2
Local req msg id: 4           Remote req msg id: 4
Local next msg id: 4         Remote next msg id: 4
Local req queued: 4          Remote req queued: 4
Local window: 5              Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

-----

```
Router2#show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA
IPv6 Crypto IKEv2 SA
```

```
Tunnel-id  fvr/ivrf          Status
3           none/none        READY
Local 2001:DB8:123:2::2/500
Remote 2001:DB8:123:1::2/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
Life/Active Time: 86400/14298 sec
CE id: 0, Session-id: 1
Status Description: Negotiation done
Local spi: EF52B3A4454D1AAA      Remote spi: C73B18AE83F68C11
Local id: 2001:DB8:123:2::2
Remote id: 2001:DB8:123:1::2
Local req msg id: 4           Remote req msg id: 4
Local next msg id: 4         Remote next msg id: 4
Local req queued: 4          Remote req queued: 4
Local window: 5              Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

Using Cert Auth:

-----

```
Router1#show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA
```

```
Tunnel-id  fvr/ivrf          Status
1           none/none        READY
Local 2001:DB8:123:1::2/500
Remote 2001:DB8:123:2::2/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/18153 sec
CE id: 1024, Session-id: 3
Status Description: Negotiation done
Local spi: 282FE0B3B5CC7FAB      Remote spi: 0D26F64871399A2B
Local id: 2001:DB8:123:1::2
Remote id: 2001:DB8:123:2::2
Local req msg id: 6           Remote req msg id: 6
Local next msg id: 6         Remote next msg id: 6
Local req queued: 6          Remote req queued: 6
Local window: 5              Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

-----

Router2#show crypto ikev2 sa detail  
IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

```
Tunnel-id   fvrf/ivrf           Status
1           none/none           READY
Local      2001:DB8:123:2::2/500
Remote     2001:DB8:123:1::2/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/17811 sec
CE id: 1024, Session-id: 4
Status Description: Negotiation done
Local spi: 0D26F64871399A2B      Remote spi: 282FE0B3B5CC7FAB
Local id: 2001:DB8:123:2::2
Remote id: 2001:DB8:123:1::2
Local req msg id: 6              Remote req msg id: 6
Local next msg id: 6            Remote next msg id: 6
Local req queued: 6             Remote req queued: 6
Local window: 5                 Remote window: 5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

=====  
IPSec SA:  
=====

Router1#show crypto ipsec sa detail

```
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 2001:DB8:123:1::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:DB8:123:2::2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (rcv) 0, #pkts verify failed: 0
#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts tagged (send): 0, #pkts untagged (rcv): 0
#pkts not tagged (send): 0, #pkts not untagged (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv) 0

local crypto endpt.: 2001:DB8:123:1::2,
remote crypto endpt.: 2001:DB8:123:2::2
path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
current outbound spi: 0xA50C0785(2769028997)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
spi: 0xA065288D(2690984077)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 62, flow_id: SW:62, sibling_flags 80000041, crypto map:
Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4226008/2911)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xA50C0785(2769028997)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 61, flow_id: SW:61, sibling_flags 80000041, crypto map:
Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4226008/2911)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
-----
```

```
Router2#show crypto ipsec sa detail
```

```
interface: Tunnel0
```

```
  Crypto map tag: Tunnel0-head-0, local addr 2001:DB8:123:2::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:DB8:123:1::2 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
```

```
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
```

```
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
```

```
#pkts invalid prot (rcv) 0, #pkts verify failed: 0
```

```
#pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
```

```
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
```

```
##pkts replay failed (rcv): 0
```

```
#pkts tagged (send): 0, #pkts untagged (rcv): 0
```

```
#pkts not tagged (send): 0, #pkts not untagged (rcv): 0
```

```
#pkts internal err (send): 0, #pkts internal err (rcv) 0
```

```
local crypto endpt.: 2001:DB8:123:2::2,
```

```
remote crypto endpt.: 2001:DB8:123:1::2
```

```
path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
```

```
current outbound spi: 0xA065288D(2690984077)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```



```
spi: 0xA50C0785(2769028997)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 61, flow_id: SW:61, sibling_flags 80000041, crypto map:
  Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4231562/2833)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)
```

inbound ah sas:

inbound pcp sas:

```
outbound esp sas:
spi: 0xA065288D(2690984077)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 62, flow_id: SW:62, sibling_flags 80000041, crypto map:
  Tunnel0-head-0
  sa timing: remaining key lifetime (k/sec): (4231562/2833)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcp sas:

=====  
Routing :

=====

```
Router1#show ipv6 route
IPv6 Routing Table - default - 9 entries
S   ::/0 [1/0]
    via 2001:DB8:123:1::1
C   2001:DB8:99::/64 [0/0]
    via Tunnel0, directly connected
L   2001:DB8:99::1/128 [0/0]
    via Tunnel0, receive
C   2001:DB8:100:1::/64 [0/0]
    via Loopback0, directly connected
L   2001:DB8:100:1::1/128 [0/0]
    via Loopback0, receive
C   2001:DB8:123:1::/64 [0/0]
    via Ethernet0/0, directly connected
L   2001:DB8:123:1::2/128 [0/0]
    via Ethernet0/0, receive
S   2001:DB8:200:1::/64 [1/0]
    via Tunnel0, directly connected
L   FF00::/8 [0/0]
    via Null0, receive
```

-----

```
Router2#show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
```

```

    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1 - LISP
S   ::/0 [1/0]
    via 2001:DB8:123:2::1
C   2001:DB8:99::/64 [0/0]
    via Tunnel0, directly connected
L   2001:DB8:99::2/128 [0/0]
    via Tunnel0, receive
S   2001:DB8:100:1::/64 [1/0]
    via Tunnel0, directly connected
C   2001:DB8:123:2::/64 [0/0]
    via Ethernet0/0, directly connected
L   2001:DB8:123:2::2/128 [0/0]
    via Ethernet0/0, receive
C   2001:DB8:200:1::/64 [0/0]
    via Loopback0, directly connected
L   2001:DB8:200:1::1/128 [0/0]
    via Loopback0, receive
L   FF00::/8 [0/0]
    via Null0, receive

```

```

=====
CEF :
=====

```

```

Router1#show ipv6 cef tu0
2001:DB8:99::/64
    attached to Tunnel0
2001:DB8:200:1::/64
    attached to Tunnel0

```

```

Router1#show ipv6 cef 2001:DB8:200:1::1 int
2001:DB8:200:1::/64, epoch 0, flags attached, RIB[S], refcount 4, per-destination
sharing
sources: RIB
feature space:
  IPRM: 0x00048000
ifnums:
  Tunnel0(14)
path EFE135F8, path list F1BA1F2C, share 1/1, type attached prefix, for IPv6
attached to Tunnel0, adjacency IPV6 midchain out of Tunnel0 F1BBAB80
output chain: IPV6 midchain out of Tunnel0 F1BBAB80 IPV6 adj out of Ethernet0/0,
addr 2001:DB8:123:1::1 F0F7D978

```

```

Router1#show adj int | i IP|erfa|comp
Protocol Interface Address
IPV6      Ethernet0/0 2001:DB8:123:1::1(16)
          IPv6 ND
          IP redirect enabled
          Switching vector: IPv6 adjacency oce
IPV6      Ethernet0/0 FE80::A8BB:CCFF:FE00:6500(2)
          IPv6 ND
          IP redirect enabled
          Switching vector: IPv6 adjacency oce
IPV6      Tunnel0 point2point(10)
          IPv6 adj out of Ethernet0/0, addr 2001:DB8:123:1::1
          IP redirect enabled
          Switching vector: IPv6 midchain adjacency oce
          Post encap features: IPSEC Post-encap output
          classification
          IP Tunnel stack to 2001:DB8:123:2::2 in Default (0x0)
          IPv6 adj out of Ethernet0/0, addr 2001:DB8:123:1::1

```

```

-----

```

```
Router2#show ipv6 cef tu0
2001:DB8:99::/64
  attached to Tunnel0
2001:DB8:100:1::/64
  attached to Tunnel0
```

```
Router2# show ipv6 cef 2001:DB8:100:1::1 int
2001:DB8:100:1::/64, epoch 0, flags attached, RIB[S], refcount 4, per-destination
sharing
sources: RIB
feature space:
  IPRM: 0x00048000
ifnums:
  Tunnel0(14)
path F1515E90, path list F2F75774, share 1/1, type attached prefix, for IPv6
attached to Tunnel0, adjacency IPV6 midchain out of Tunnel0 F0FB8E48
output chain: IPV6 midchain out of Tunnel0 F0FB8E48 IPV6 adj out of Ethernet0/0,
addr 2001:DB8:123:2::1 F0FB8F78
```

```
Router2# show adj int | i IP|erfa|comp
Protocol Interface Address
IPV6 Ethernet0/0 2001:DB8:123:2::1(16)
IPv6 ND
IP redirect enabled
Switching vector: IPv6 adjacency oce
IPV6 Ethernet0/0 FE80::A8BB:CCFF:FE00:6510(2)
IPv6 ND
IP redirect enabled
Switching vector: IPv6 adjacency oce
IPV6 Tunnel0 point2point(10)
IPv6 adj out of Ethernet0/0, addr 2001:DB8:123:2::1
IP redirect enabled
Switching vector: IPv6 midchain adjacency oce
Post encap features: IPSEC Post-encap output
classification
IP Tunnel stack to 2001:DB8:123:1::2 in Default (0x0)
IPv6 adj out of Ethernet0/0, addr 2001:DB8:123:2::1
```

## デバッグ

PSK 認証の使用時に実行されたデバッグ :

```
debug crypto ikev2
debug crypto ipsec
```

証明書認証の使用時に実行されたデバッグ :

```
debug crypto ikev2
debug crypto ipsec
debug crypto pki messages
debug crypto pki transaction
```

## IPv6/ハイブリッドトンネルでの IPv4

混合/ハイブリッド モード トンネリングは、GRE ヘッダーを使用してのみ実現できます。 **tunnel mode gre ipv6** コマンドが使用されます。 誤って **tunnel mode ipsec ipv6** コマンドを使用すると、次のように表示されます。

```
%IPSECV6-4-PKT_PROTOCOL_MISMATCH: IP protocol in packet mismatched with tunnel mode,
```

packet from <src> to <dst> dropped by Tunnel0.

## ルータ R1 :

```
interface Loopback1
  description This is a test endpoint
  ip address 10.0.0.1 255.255.255.0
!
interface Tunnel0
  ip address 100.0.0.1 255.255.255.0
  tunnel source Ethernet0/0
  tunnel mode gre ipv6
  tunnel destination 2001:DB8:123:2::2
  tunnel protection ipsec profile default
!
ip route 20.0.0.0 255.255.255.0 Tunnel0
!
```

## ルータ R2 :

```
interface Loopback1
  description This is a test endpoint
  ip address 20.0.0.1 255.255.255.0
!
interface Tunnel0
  ip address 100.0.0.2 255.255.255.0
  tunnel source Ethernet0/0
  tunnel mode gre ipv6
  tunnel destination 2001:DB8:123:1::2
  tunnel protection ipsec profile l2l
!
ip route 10.0.0.0 255.255.255.0 Tunnel0
!
```

## show コマンド :

```
=====
IPSec SA:
=====
```

```
Router1#show crypto ipsec sa detail
```

```
interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 2001:DB8:123:1::2

protected vrf: (none)
local ident (addr/mask/prot/port): (2001:DB8:123:1::2/128/47/0)
remote ident (addr/mask/prot/port): (2001:DB8:123:2::2/128/47/0)
current_peer 2001:DB8:123:2::2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
  #pkts invalid prot (rcv) 0, #pkts verify failed: 0
  #pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
  ##pkts replay failed (rcv): 0
```

```
#pkts tagged (send): 0, #pkts untagged (rcv): 0
#pkts not tagged (send): 0, #pkts not untagged (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv) 0
```

```
local crypto endpt.: 2001:DB8:123:1::2,
remote crypto endpt.: 2001:DB8:123:2::2
path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
current outbound spi: 0x99D16BE2(2580638690)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
spi: 0xDFF1E2D(234823213)
transform: esp-aes esp-sha-hmac ,
in use settings ={Transport, }
conn id: 90, flow_id: SW:90, sibling_flags 80000001, crypto map:
Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4222891/2971)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x99D16BE2(2580638690)
transform: esp-aes esp-sha-hmac ,
in use settings ={Transport, }
conn id: 89, flow_id: SW:89, sibling_flags 80000001, crypto map:
Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4222891/2971)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
-----
Router2#show crypto ipsec sa detail
```

```
interface: Tunnel0
```

```
  Crypto map tag: Tunnel0-head-0, local addr 2001:DB8:123:2::2
```

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

```
local ident (addr/mask/prot/port): (2001:DB8:123:2::2/128/47/0)
```

```
remote ident (addr/mask/prot/port): (2001:DB8:123:1::2/128/47/0)
```

```
current_peer 2001:DB8:123:1::2 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
```

```
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

```
  #pkts not compressed: 0, #pkts compr. failed: 0
```

```
  #pkts not decompressed: 0, #pkts decompress failed: 0
```

```
  #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
```

```
  #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
```

```
  #pkts invalid prot (rcv) 0, #pkts verify failed: 0
```

```
  #pkts invalid identity (rcv) 0, #pkts invalid len (rcv) 0
```

```
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
```

```
  ##pkts replay failed (rcv): 0
```

```
  #pkts tagged (send): 0, #pkts untagged (rcv): 0
```

```
#pkts not tagged (send): 0, #pkts not untagged (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0
```

```
local crypto endpt.: 2001:DB8:123:2::2,
remote crypto endpt.: 2001:DB8:123:1::2
path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
current outbound spi: 0xDFF1E2D(234823213)
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
spi: 0x99D16BE2(2580638690)
transform: esp-aes esp-sha-hmac ,
in use settings ={Transport, }
conn id: 89, flow_id: SW:89, sibling_flags 80000001, crypto map:
Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4210423/2955)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xDFF1E2D(234823213)
transform: esp-aes esp-sha-hmac ,
in use settings ={Transport, }
conn id: 90, flow_id: SW:90, sibling_flags 80000001, crypto map:
Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4210423/2955)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
=====
Routing :
=====
```

```
Router1#show ip route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/24 is directly connected, Loopback1
L    10.0.0.1/32 is directly connected, Loopback1
20.0.0.0/24 is subnetted, 1 subnets
S    20.0.0.0 is directly connected, Tunnel0
100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    100.0.0.0/24 is directly connected, Tunnel0
L    100.0.0.1/32 is directly connected, Tunnel0
```

```
Router1#show ipv6 route
```

```
IPv6 Routing Table - default - 6 entries
S   ::/0 [1/0]
    via 2001:DB8:123:1::1
C   2001:DB8:100:1::/64 [0/0]
    via Loopback0, directly connected
L   2001:DB8:100:1::1/128 [0/0]
    via Loopback0, receive
```

```
C 2001:DB8:123:1::/64 [0/0]
  via Ethernet0/0, directly connected
L 2001:DB8:123:1::2/128 [0/0]
  via Ethernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
```

-----

```
Router2#sh ip route
Gateway of last resort is not set
```

```
10.0.0.0/24 is subnetted, 1 subnets
S 10.0.0.0 is directly connected, Tunnel0
20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 20.0.0.0/24 is directly connected, Loopback1
L 20.0.0.1/32 is directly connected, Loopback1
100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 100.0.0.0/24 is directly connected, Tunnel0
L 100.0.0.2/32 is directly connected, Tunnel0
```

```
Router2#show ipv6 route
IPv6 Routing Table - default - 6 entries
```

```
S ::/0 [1/0]
  via 2001:DB8:123:2::1
C 2001:DB8:123:2::/64 [0/0]
  via Ethernet0/0, directly connected
L 2001:DB8:123:2::2/128 [0/0]
  via Ethernet0/0, receive
C 2001:DB8:200:1::/64 [0/0]
  via Loopback0, directly connected
L 2001:DB8:200:1::1/128 [0/0]
  via Loopback0, receive
L FF00::/8 [0/0]
  via Null0, receive
```

```
=====
CEF :
=====
```

```
Router1# sh ip cef tu0
20.0.0.0/24
  attached to Tunnel0
100.0.0.0/24
  attached to Tunnel0
```

```
Router1#show ip cef 20.0.0.1 internal
20.0.0.0/24, epoch 0, flags attached, RIB[S], refcount 5, per-destination
sharing
sources: RIB
feature space:
  IPRM: 0x00048004
ifnums:
  Tunnel0(14)
path EFE136D8, path list F1BA1EDC, share 1/1, type attached prefix,
for IPv4
attached to Tunnel0, adjacency IP midchain out of Tunnel0 F1BBBFA0
output chain: IP midchain out of Tunnel0 F1BBBFA0 IPV6 adj out of Ethernet0/0,
addr 2001:DB8:123:1::1 F0F7D978
```

```
Router1# show adj int | i IP|erfa|comp
Protocol Interface Address
IPV6 Ethernet0/0 2001:DB8:123:1::1(16)
IPv6 ND
```

```

IPV6      Ethernet0/0      IP redirect enabled
Switching vector: IPv6 adjacency oce
FE80::A8BB:CCFF:FE00:6500(2)
IPv6 ND
IP redirect enabled
Switching vector: IPv6 adjacency oce
point2point(10)
  IPV6 adj out of Ethernet0/0, addr
    2001:DB8:123:1::1
    GRE IPv6 tunnel
IP redirect disabled
Switching vector: IPv4 midchain adj oce
Post encap features: IPSEC Post-encap output
  classification
IP Tunnel stack to 2001:DB8:123:2::2 in Default (0x0)
  IPV6 adj out of Ethernet0/0, addr 2001:DB8:123:1::1

```

-----

```

Router2#sh ip cef tu0
10.0.0.0/24
  attached to Tunnel0
100.0.0.0/24
  attached to Tunnel0

```

```

Router2#show ip cef 10.0.0.1 internal
10.0.0.0/24, epoch 0, flags attached, RIB[S], refcount 5, per-destination sharing
sources: RIB
feature space:
  IPRM: 0x00048004
ifnums:
  Tunnel0(14)
path F1515DB0, path list F2F77EBC, share 1/1, type attached prefix, for IPv4
attached to Tunnel0, adjacency IP midchain out of Tunnel0 F0FB8E48
output chain: IP midchain out of Tunnel0 F0FB8E48 IPV6 adj out of Ethernet0/0, addr
2001:DB8:123:2::1 F0FB8F78

```

```

Router2# show adj int | i IP|erfa|comp
Protocol Interface      Address
IPV6      Ethernet0/0      2001:DB8:123:2::1(16)
IPv6 ND
IP redirect enabled
Switching vector: IPv6 adjacency oce
IPV6      Ethernet0/0      FE80::A8BB:CCFF:FE00:6510(2)
IPv6 ND
IP redirect enabled
Switching vector: IPv6 adjacency oce
point2point(10)
  IPV6 adj out of Ethernet0/0, addr 2001:DB8:123:2::1
  GRE IPv6 tunnel
IP redirect disabled
Switching vector: IPv4 midchain adj oce
Post encap features: IPSEC Post-encap output
  classification
IP Tunnel stack to 2001:DB8:123:1::2 in Default (0x0)
  IPV6 adj out of Ethernet0/0, addr 2001:DB8:123:2::1

```

## デバッグ :

```

debug crypto ikev2
debug crypto ipsec

```

## [関連情報](#)



- [テクニカル サポートとドキュメント – Cisco Systems](#)