

# スポーク間の通信における、IPSec ルータ間ハブアンドスポークの設定

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[別のスポークの追加](#)

[確認](#)

[show コマンドの出力例](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[デバッグの出力例](#)

[関連情報](#)

## 概要

この設定例では、3 台のルータ間のハブ アンド スポーク IPSec 設計を示します。この構成は、ハブを経由することでスポーク サイト間の通信が確立されるため、その他のハブ アンド スポーク構成とは異なります。つまり、2 台のスポーク ルータ間を直接結ぶ IPSec トンネルは存在しません。すべてのパケットは、トンネルを経由してハブ ルータに送信され、さらに他のスポーク ルータと共有する IPSec トンネルに再配送されます。この構成は、Cisco Bug ID [CSCdp09904](#) ( [登録ユーザのみ](#) ) の解決策として実現しました。この解決策は、Cisco IOS® ソフトウェア リリース 12.2(5) に統合されており、このリリースがこの構成を実現するための最小要件です。

OSPF を使用した IPsec 環境での総称ルーティング カプセル化 ( GRE ) トンネルを設定するには、[OSPF を使用した IPsec 環境での GRE トンネルの設定](#)を参照してください。

ネットワーク アドレス変換 ( NAT ) を使用した GRE トンネルで基本的な Cisco IOS® ファイアウォールを設定するには、[IOS ファイアウォールと NAT を使用した GRE トンネル上のルータ間 IPsec \( 事前共有鍵 \) の設定](#)を参照してください。

## 前提条件

### 要件

このドキュメントの内容は、IPsec プロトコルに関する基本的知識が前提となっています。IPsec に関する知識を深めるには、[IP Security \( IPsec \) 暗号化の概要](#)を参照してください。

このドキュメントの目的は、次のルータ間で暗号化を実行することです。

- 172.16.1.0/24 ( スポーク 1 ) と 10.1.1.0/24 ( ハブ )
- 192.168.1.0/24 ( スポーク 2 ) と 10.1.1.0/24 ( ハブ )
- 172.16.1.0/24 ( スポーク 1 ) と 192.168.1.0/24 ( スポーク 2 )

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.2(24a) ( c2500-ik8s-l.122-24a.bin )
- Cisco 2500 ルータ

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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 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。

## 設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク図

このドキュメントでは、次の図で示されるネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。これらは、ラボ環境で使用された [RFC 1918](#) のアドレスです。

## 設定

このドキュメントでは、次の設定を使用します。

[show running-config コマンド](#) は、ルータの実行コンフィギュレーションを表示します。

- [ハブ ルータ](#)
- [スポーク 1 ルータ](#)
- [スポーク 2 ルータ](#)

ハブ ルータ
--------

```

Hub#show running-config Building configuration...
Current configuration : 1466 bytes ! version 12.2
service timestamps debug datetime msec service
timestamps log uptime no service password-encryption !
hostname Hub ! ! ip subnet-zero ! ! !--- Configuration
for IKE policies. crypto isakmp policy 10 !--- Enables
the IKE policy configuration (config-isakmp) !---
command mode, where you can specify the parameters that
!--- are used during an IKE negotiation. hash md5
authentication pre-share crypto isakmp key cisco123
address 10.1.2.1 crypto isakmp key cisco123 address
10.1.3.1 !--- Specifies the preshared key "cisco123"
which should !--- be identical at both peers. This is a
global !--- configuration mode command. ! !---
Configuration for IPsec policies. crypto ipsec
transform-set myset esp-des esp-md5-hmac !--- Enables
the crypto transform configuration mode, !--- where you
can specify the transform sets that are used !--- during
an IPsec negotiation. ! crypto map mymap 10 ipsec-isakmp
!--- Indicates that IKE is used to establish !--- the
IPsec security association for protecting the !---
traffic specified by this crypto map entry. set peer
10.1.2.1 !--- Sets the IP address of the remote end. set
transform-set myset !--- Configures IPsec to use the
transform-set !--- "myset" defined earlier in this
configuration. match address 110 !--- Specifies the
traffic to be encrypted. crypto map mymap 20 ipsec-
isakmp set peer 10.1.3.1 set transform-set myset match
address 120 ! ! ! ! interface Ethernet0 ip address
10.1.1.1 255.255.255.0 ! interface Ethernet1 ip address
10.1.4.1 255.255.255.0 no ip route-cache !--- You must
enable process switching for IPsec !--- to encrypt
outgoing packets. This command disables fast switching.
no ip mroute-cache crypto map mymap !--- Configures the
interface to use the !--- crypto map "mymap" for IPsec.
! !--- Output suppressed. ip classless ip route
172.16.1.0 255.255.255.0 Ethernet1 ip route 192.168.1.0
255.255.255.0 Ethernet1 ip route 10.1.0.0 255.255.0.0
Ethernet1 ip http server ! access-list 110 permit ip
10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 access-list 110
permit ip 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 120 permit ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255 access-list 120 permit ip 172.16.1.0 0.0.0.255
192.168.1.0 0.0.0.255 !--- This crypto ACL-permit
identifies the !--- matching traffic flows to be
protected via encryption.

```

## スポーク1ルータ

```

Spokel#show running-config Building configuration...
Current configuration : 1203 bytes ! version 12.2
service timestamps debug datetime msec service
timestamps log uptime no service password-encryption !
hostname Spokel ! enable secret 5
$!$DOX3$rIrxEnTVTtw/7LNbxI.akz0 ! ip subnet-zero no ip
domain-lookup ! ! crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco123
address 10.1.4.1 ! ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map mymap 10 ipsec-isakmp
set peer 10.1.4.1 set transform-set myset match address
110 ! ! ! ! interface Ethernet0 ip address 172.16.1.1
255.255.255.0 ! interface Ethernet1 ip address 10.1.2.1
255.255.255.0 no ip route-cache no ip mroute-cache
crypto map mymap ! . . !--- Output suppressed. . . ip
classless ip route 192.168.1.0 255.255.255.0 Ethernet1

```

```
ip route 10.1.0.0 255.255.0.0 Ethernet1 no ip http
server ! access-list 110 permit ip 172.16.1.0 0.0.0.255
10.1.1.0 0.0.0.255 access-list 110 permit ip 172.16.1.0
0.0.0.255 192.168.1.0 0.0.0.255 ! end 2509a#
```

## スポーク 2 ルータ

```
Spoke2#show running-config Building configuration...
Current configuration : 1117 bytes ! version 12.2
service timestamps debug datetime msec service
timestamps log uptime service password-encryption !
hostname Spoke2 ! ! ip subnet-zero no ip domain-lookup !
! crypto isakmp policy 10 hash md5 authentication pre-
share crypto isakmp key cisco123 address 10.1.4.1 ! !
crypto ipsec transform-set myset esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp set peer 10.1.4.1 set
transform-set myset match address 120 ! ! ! ! interface
Ethernet0 ip address 192.168.1.1 255.255.255.0 !
interface Ethernet1 ip address 10.1.3.1 255.255.255.0 !-
-- No ip route-cache. no ip mroute-cache crypto map
mymap ! . . !--- Output suppressed. . . ip classless ip
route 172.16.0.0 255.255.0.0 Ethernet1 ip route 10.1.0.0
255.255.0.0 Ethernet1 no ip http server ! access-list
120 permit ip 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 120 permit ip 192.168.1.0 0.0.0.255 10.1.1.0
0.0.0.255 ! end VPN2509#
```

## 別のスポークの追加

スポーク 1 とスポーク 2 に加えて、既存のハブ ルータに別のスポーク ルータ ( スポーク 3 ) を追加する必要がある場合に必要なのは、ハブからスポーク 3 に新しい LAN-to-LAN ( L2L ) トンネルを作成することです。ただし、1 つの物理インターフェイスに設定できる暗号マップは 1 つだけであるため、このトンネルを追加するときには同じ暗号マップ名を使用する必要があります。このようなケースは、各リモート サイトに異なる回線番号を使用している場合に生じる可能性があります。

注: 新しいトンネル エントリが追加されたときは、暗号マップを削除してインターフェイスに再適用することが必要になる場合があります。暗号マップを削除すると、アクティブなトンネルがすべて削除されます。

## ハブ ルータ

```
Hub#show running-config Building configuration...
Current configuration : 1466 bytes ! version 12.2
service timestamps debug datetime msec service
timestamps log uptime no service password-encryption !
hostname Hub ! ! ip subnet-zero ! ! crypto isakmp policy
10 hash md5 authentication pre-share crypto isakmp key
cisco123 address 10.1.2.1 crypto isakmp key cisco123
address 10.1.3.1 crypto isakmp key cisco123 address
10.1.5.1 ! crypto ipsec transform-set myset esp-des esp-
md5-hmac ! crypto map mymap 10 ipsec-isakmp set peer
10.1.2.1 set transform-set myset match address 110
crypto map mymap 20 ipsec-isakmp set peer 10.1.3.1 set
transform-set myset match address 120 !--- It is
important to specify crypto map line number 30 for !---
the Spoke 3 router with the same crypto map name "mymap"
crypto map mymap 30 ipsec-isakmp set peer 10.1.5.1 set
transform-set myset match address 130 ! ! ! ! interface
Ethernet0 ip address 10.1.1.1 255.255.255.0 ! interface
Ethernet1 ip address 10.1.4.1 255.255.255.0 no ip route-
cache no ip mroute-cache !--- It is important to remove
```

```
and re-apply the crypto !--- map to this interface if it
is used for the termination of other !--- spoke VPN
tunnels. crypto map mymap ! !--- Output suppressed. ip
classless ip route 172.16.1.0 255.255.255.0 Ethernet1 ip
route 192.168.1.0 255.255.255.0 Ethernet1 ip route
10.1.0.0 255.255.0.0 Ethernet1 ip route 172.16.2.0
255.255.255.0 Ethernet1 ip http server ! access-list 110
permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 110 permit ip 192.168.1.0 0.0.0.255
172.16.1.0 0.0.0.255 access-list 110 permit ip
172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 access-list
120 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 120 permit ip 172.16.2.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 120 permit ip
172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255 access-list
130 permit ip 10.1.1.0 0.0.0.255 172.16.2.0 0.0.0.255
access-list 130 permit ip 192.168.1.0 0.0.0.255
172.16.2.0 0.0.0.255 access-list 130 permit ip
172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

### スポーク 3 ルータ

```
Spoke3#show running-config Building configuration...
Current configuration : 1117 bytes ! version 12.2
service timestamps debug datetime msec service
timestamps log uptime service password-encryption !
hostname Spoke3 ! ! ip subnet-zero no ip domain-lookup !
! crypto isakmp policy 10 hash md5 authentication pre-
share crypto isakmp key cisco123 address 10.1.4.1 ! !
crypto ipsec transform-set myset esp-des esp-md5-hmac !
crypto map mymap 10 ipsec-isakmp set peer 10.1.4.1 set
transform-set myset match address 130 ! ! ! ! interface
Ethernet0 ip address 172.16.2.1 255.255.255.0 !
interface Ethernet1 ip address 10.1.5.1 255.255.255.0 no
ip mroute-cache crypto map mymap ! . . !--- Output
suppressed. . . ip classless ip route 172.16.0.0
255.255.0.0 Ethernet1 ip route 10.1.0.0 255.255.0.0
Ethernet1 no ip http server ! access-list 130 permit ip
172.168.2.0 0.0.0.255 172.16.1.0 0.0.0.255 access-list
130 permit ip 172.168.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 permit ip 172.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255 ! end VPN2509#
```

## 確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) ( OIT ) ( [登録](#) ユーザ専用 ) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

この設定を確認するために、スポーク 2 の ethernet1 インターフェイス アドレスに向かうスポーク 1 で ethernet1 インターフェイス アドレスからソースをたどられる試みて下さい。

- **ping** : 基本的なネットワークの接続性を診断するのに使用します。Spoke1#ping Protocol [ip]: Target IP address: 192.168.1.1 Repeat count [5]: Datagram size [100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface: 172.16.1.1 Type of service [0]: Set DF bit in IP header? [no]: Validate reply data? [no]: Data pattern [0xABCD]: Loose, Strict, Record, Timestamp, Verbose[none]: Sweep range of sizes [n]: Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
- **show crypto ipsec sa** : 現在の ( IPsec ) セキュリティ アソシエーション ( SA ) で使用されて

いる設定を表示します。

- [show crypto isakmp sa](#) : 現在ピアにあるすべての IKE SA を表示します。
- [show crypto engine connections active](#) : 各 IPSec SA を介して送信されるパケットの数を表示します。

## show コマンドの出力例

この出力は、ハブ ルータで `show crypto engine connections active` コマンドが実行されたときのもので

```
Hub#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
Decrypt 5 Ethernet0 10.1.4.1 set HMAC_MD5+DES_56_CB 0 0 6 <none> <none> set HMAC_MD5+DES_56_CB 0
0 2000 Ethernet0 10.1.4.1 set HMAC_MD5+DES_56_CB 0 10 2001 Ethernet0 10.1.4.1 set
HMAC_MD5+DES_56_CB 10 0 2002 Ethernet0 10.1.4.1 set HMAC_MD5+DES_56_CB 0 10 2003 Ethernet0
10.1.4.1 set HMAC_MD5+DES_56_CB 10 0
```

この例から、各トンネルが 10 パケットを暗号化して復号化したことを確認できます。これにより、トラフィックがハブ ルータを介して到達したことが証明されます。

注: 各ピアに、2 つの IPSec SA ( 各方向に 1 つずつ ) が作成されます。たとえば、ハブ ルータには 2 つのピアに対して 4 つの IPSec SA があります。

## トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

### トラブルシューティングのためのコマンド

注: `debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- [debug crypto ipsec](#) : フェーズ 2 の IPSec ネゴシエーションを表示します。
- [debug crypto isakmp](#) : フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- [debug crypto engine](#) - 暗号化されたトラフィックを表示します。
- [clear crypto isakmp](#) : フェーズ 1 に関連する SA をクリアします。
- [clear crypto sa](#) : フェーズ 2 に関連する SA をクリアします。

### デバッグの出力例

ここに、`debug crypto ipsec` および `debug crypto isakmp` コマンドをハブ ルータ上で実行した出力を示します。

```
*Mar 1 00:03:46.887: ISAKMP (0:0): received packet
      from 10.1.2.1 (N) NEW SA
*Mar 1 00:03:46.887: ISAKMP: local port 500, remote port 500
*Mar 1 00:03:46.899: ISAKMP (0:1): processing SA payload. message ID = 0
*Mar 1 00:03:46.899: ISAKMP (0:1): found peer pre-shared key matching 10.1.2.1
*Mar 1 00:03:46.903: ISAKMP (0:1): Checking ISAKMP transform 1 against priority
      10 policy
*Mar 1 00:03:46.903: ISAKMP:      encryption DES-CBC
*Mar 1 00:03:46.907: ISAKMP:      hash MD5
*Mar 1 00:03:46.907: ISAKMP:      default group 1
*Mar 1 00:03:46.911: ISAKMP:      auth pre-share
*Mar 1 00:03:46.911: ISAKMP:      life type in seconds
```

\*Mar 1 00:03:46.911: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80  
\*Mar 1 00:03:46.915: ISAKMP (0:1): **atts are acceptable**. Next payload is 0 *!--- The initial IKE parameters have been !---* successfully exchanged between Spoke 1 and Hub. \*Mar 1 00:03:48.367: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID\_IPV4\_ADDR \*Mar 1 00:03:48.371: ISAKMP (0:1): sending packet to 10.1.2.1 (R) MM\_SA\_SETUP \*Mar 1 00:03:56.895: ISAKMP (0:1): received packet from 10.1.2.1 (R) MM\_SA\_SETUP \*Mar 1 00:03:56.899: ISAKMP (0:1): phase 1 packet is a duplicate of a previous packet. \*Mar 1 00:03:56.899: ISAKMP (0:1): retransmitting due to retransmit phase 1 \*Mar 1 00:03:56.903: ISAKMP (0:1): retransmitting phase 1 MM\_SA\_SETUP... \*Mar 1 00:03:57.403: ISAKMP (0:1): retransmitting phase 1 MM\_SA\_SETUP... \*Mar 1 00:03:57.403: ISAKMP (0:1): incrementing error counter on sa: retransmit phase 1 \*Mar 1 00:03:57.407: ISAKMP (0:1): retransmitting phase 1 MM\_SA\_SETUP \*Mar 1 00:03:57.407: ISAKMP (0:1): sending packet to 10.1.2.1 (R) MM\_SA\_SETUP \*Mar 1 00:03:58.923: ISAKMP (0:1): received packet from 10.1.2.1 (R) MM\_SA\_SETUP \*Mar 1 00:03:58.931: ISAKMP (0:1): processing KE payload. message ID = 0 \*Mar 1 00:04:00.775: ISAKMP (0:1): processing NONCE payload. message ID = 0 \*Mar 1 00:04:00.783: ISAKMP (0:1): found peer pre-shared key matching 10.1.2.1 \*Mar 1 00:04:00.795: ISAKMP (0:1): SKEYID state generated \*Mar 1 00:04:00.799: ISAKMP (0:1): processing vendor id payload \*Mar 1 00:04:00.803: ISAKMP (0:1): speaking to another IOS box! \*Mar 1 00:04:00.811: ISAKMP (0:1): sending packet to 10.1.2.1 (R) MM\_KEY\_EXCH \*Mar 1 00:04:02.751: ISAKMP (0:1): received packet from 10.1.2.1 (R) MM\_KEY\_EXCH \*Mar 1 00:04:02.759: ISAKMP (0:1): processing ID payload. message ID = 0 \*Mar 1 00:04:02.759: ISAKMP (0:1): processing HASH payload. message ID = 0 \*Mar 1 00:04:02.767: ISAKMP (0:1): SA has been authenticated with 10.1.2.1 \*Mar 1 00:04:02.771: ISAKMP (1): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 \*Mar 1 00:04:02.775: ISAKMP (1): Total payload length: 12 \*Mar 1 00:04:02.783: ISAKMP (0:1): sending packet to 10.1.2.1 (R) QM\_IDLE \*Mar 1 00:04:02.871: ISAKMP (0:1): received packet from 10.1.2.1 (R) QM\_IDLE *!--- IKE phase 1 SA has been successfully negotiated !---* between Spoke 1 and Hub. \*Mar 1 00:04:02.891: ISAKMP (0:1): processing HASH payload. message ID = 581713929 \*Mar 1 00:04:02.891: ISAKMP (0:1): processing SA payload. message ID = 581713929 \*Mar 1 00:04:02.895: ISAKMP (0:1): **Checking IPsec proposal 1 !---** IKE exchanges IPsec phase 2 parameters *!--- between Spoke 1 and Hub.* \*Mar 1 00:04:02.895: ISAKMP: transform 1, ESP\_DES \*Mar 1 00:04:02.899: ISAKMP: attributes in transform: \*Mar 1 00:04:02.899: ISAKMP: encaps is 1 \*Mar 1 00:04:02.899: ISAKMP: SA life type in seconds \*Mar 1 00:04:02.903: ISAKMP: SA life duration (basic) of 3600 \*Mar 1 00:04:02.903: ISAKMP: SA life type in kilobytes \*Mar 1 00:04:02.907: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 \*Mar 1 00:04:02.911: ISAKMP: authenticator is HMAC-MD5 \*Mar 1 00:04:02.915: ISAKMP (0:1): **atts are acceptable.** *!--- IPsec phase 2 parameters have been !---* successfully exchanged between Spoke 1 and Hub. \*Mar 1 00:04:02.915: IPSEC(validate\_proposal\_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.4.1, remote= 10.1.2.1, local\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), remote\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4 \*Mar 1 00:04:02.931: ISAKMP (0:1): processing NONCE payload. message ID = 581713929 \*Mar 1 00:04:02.935: ISAKMP (0:1): processing ID payload. message ID = 581713929 \*Mar 1 00:04:02.935: ISAKMP (0:1): processing ID payload. message ID = 581713929 \*Mar 1 00:04:02.939: ISAKMP (0:1): asking for 1 spis from ipsec \*Mar 1 00:04:02.943: IPSEC(key\_engine): got a queue event... \*Mar 1 00:04:02.951: IPSEC(spi\_response): getting spi 4208568169 for SA from 10.1.4.1 to 10.1.2.1 for prot 3 \*Mar 1 00:04:02.955: ISAKMP: received ke message (2/1) \*Mar 1 00:04:03.207: ISAKMP (0:1): sending packet to 10.1.2.1 (R) QM\_IDLE \*Mar 1 00:04:03.351: ISAKMP (0:1): received packet from 10.1.2.1 (R) QM\_IDLE \*Mar 1 00:04:03.387: ISAKMP (0:1): Creating IPsec SAs \*Mar 1 00:04:03.387: inbound SA from 10.1.2.1 to 10.1.4.1 (proxy 172.16.1.0 to 192.168.1.0) \*Mar 1 00:04:03.391: has spi 0xFAD9A769 and conn\_id 2000 and flags 4 \*Mar 1 00:04:03.395: lifetime of 3600 seconds \*Mar 1 00:04:03.395: lifetime of 4608000 kilobytes \*Mar 1 00:04:03.399: outbound SA from 10.1.4.1 to 10.1.2.1 (proxy 192.168.1.0 to 172.16.1.0 ) \*Mar 1 00:04:03.403: has spi -732960388 and conn\_id 2001 and flags C \*Mar 1 00:04:03.407: lifetime of 3600 seconds \*Mar 1 00:04:03.407: lifetime of 4608000 kilobytes \*Mar 1 00:04:03.411: ISAKMP (0:1): deleting node 581713929 error FALSE reason " quick mode done (await()) \*Mar 1 00:04:03.415: IPSEC(key\_engine): got a queue event... \*Mar 1 00:04:03.415: IPSEC(initialize\_sas): , (key eng. msg.) INBOUND local= 10.1.4.1, remote= 10.1.2.1, local\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), remote\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0xFAD9A769(4208568169), conn\_id= 2000, keysize= 0, flags= 0x4 \*Mar 1 00:04:03.427: IPSEC(initialize\_sas): , (key eng. msg.) OUTBOUND local= 10.1.4.1, remote= 10.1.2.1, local\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), remote\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0xD44FE97C(3562006908), conn\_id= 2001, keysize= 0, flags= 0xC \*Mar 1 00:04:03.443: IPSEC(create\_sa): sa created, (sa) sa\_dest= 10.1.4.1, sa\_prot= 50, sa\_spi= 0xFAD9A769(4208568169), sa\_trans= esp-des esp-md5-hmac , sa\_conn\_id= 2000 \*Mar 1 00:04:03.447:

IPSEC(create\_sa): sa created, (sa) sa\_dest= 10.1.2.1, sa\_prot= 50, sa\_spi= 0xD44FE97C(3562006908), sa\_trans= esp-des esp-md5-hmac , sa\_conn\_id= 2001 *!--- IPsec tunnel has been created between !--- routers Spoke 1 and Hub.* \*Mar 1 00:05:02.387: IPSEC(sa\_request): , *!--- Since an IPsec tunnel is created between Spoke 1 !--- and Spoke 2 through the Hub, the Hub router !--- initializes a new IPsec tunnel between itself and Spoke 2.* (key eng. msg.) OUTBOUND local= 10.1.4.1, remote= 10.1.3.1, local\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), remote\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi= 0x1B7A414E(460996942), conn\_id= 0, keysize= 0, flags= 0x400C \*Mar 1 00:05:02.399: ISAKMP: received ke message (1/1) \*Mar 1 00:05:02.403: ISAKMP: local port 500, remote port 500 \*Mar 1 00:05:02.411: ISAKMP (0:2): beginning Main Mode exchange \*Mar 1 00:05:02.415: ISAKMP (0:2): sending packet to 10.1.3.1 (I) MM\_NO\_STATE \*Mar 1 00:05:12.419: ISAKMP (0:2): retransmitting phase 1 MM\_NO\_STATE... \*Mar 1 00:05:12.419: ISAKMP (0:2): incrementing error counter on sa: retransmit phase 1 \*Mar 1 00:05:12.423: ISAKMP (0:2): retransmitting phase 1 MM\_NO\_STATE \*Mar 1 00:05:12.423: ISAKMP (0:2): sending packet to 10.1.3.1 (I) MM\_NO\_STATE \*Mar 1 00:05:22.427: ISAKMP (0:2): retransmitting phase 1 MM\_NO\_STATE... \*Mar 1 00:05:22.427: ISAKMP (0:2): incrementing error counter on sa: retransmit phase 1 \*Mar 1 00:05:22.431: ISAKMP (0:2): retransmitting phase 1 MM\_NO\_STATE \*Mar 1 00:05:22.431: ISAKMP (0:2): sending packet to 10.1.3.1 (I) MM\_NO\_STATE \*Mar 1 00:05:22.967: ISAKMP (0:2): received packet from 10.1.3.1 (I) MM\_NO\_STATE \*Mar 1 00:05:22.975: ISAKMP (0:2): processing SA payload. message ID = 0 \*Mar 1 00:05:22.975: ISAKMP (0:2): found peer pre-shared key matching 10.1.3.1 \*Mar 1 00:05:22.979: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 10 policy \*Mar 1 00:05:22.979: ISAKMP: encryption DES-CBC \*Mar 1 00:05:22.983: ISAKMP: hash MD5 \*Mar 1 00:05:22.983: ISAKMP: default group 1 \*Mar 1 00:05:22.987: ISAKMP: auth pre-share \*Mar 1 00:05:22.987: ISAKMP: life type in seconds \*Mar 1 00:05:22.987: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 \*Mar 1 00:05:22.991: ISAKMP (0:2): **atts are acceptable.** Next payload is 0 *!--- IKE phase 1 parameters have been successfully !--- exchanged between Hub and Spoke 2.* \*Mar 1 00:05:24.447: ISAKMP (0:2): SA is doing pre-shared key authentication using id type ID\_IPV4\_ADDR \*Mar 1 00:05:24.455: ISAKMP (0:2): sending packet to 10.1.3.1 (I) MM\_SA\_SETUP \*Mar 1 00:05:26.463: ISAKMP (0:2): received packet from 10.1.3.1 (I) MM\_SA\_SETUP \*Mar 1 00:05:26.471: ISAKMP (0:2): processing KE payload. message ID = 0 \*Mar 1 00:05:28.303: ISAKMP (0:2): processing NONCE payload. message ID = 0 \*Mar 1 00:05:28.307: ISAKMP (0:2): found peer pre-shared key matching 10.1.3.1 \*Mar 1 00:05:28.319: ISAKMP (0:2): SKEYID state generated \*Mar 1 00:05:28.323: ISAKMP (0:2): processing vendor id payload \*Mar 1 00:05:28.327: ISAKMP (0:2): speaking to another IOS box! \*Mar 1 00:05:28.331: ISAKMP (2): ID payload next-payload : 8 type : 1 protocol : 17 port : 500 length : 8 \*Mar 1 00:05:28.335: ISAKMP (2): Total payload length: 12 \*Mar 1 00:05:28.343: ISAKMP (0:2): sending packet to 10.1.3.1 (I) MM\_KEY\_EXCH \*Mar 1 00:05:28.399: ISAKMP (0:2): received packet from 10.1.3.1 (I) MM\_KEY\_EXCH \*Mar 1 00:05:28.407: ISAKMP (0:2): processing ID payload. message ID = 0 \*Mar 1 00:05:28.411: ISAKMP (0:2): processing HASH payload. message ID = 0 \*Mar 1 00:05:28.419: ISAKMP (0:2): SA has been authenticated with 10.1.3.1 \*Mar 1 00:05:28.419: ISAKMP (0:2): beginning Quick Mode exchange, M-ID of -1872859789 \*Mar 1 00:05:28.439: ISAKMP (0:2): sending packet to 10.1.3.1 (I) QM\_IDLE \*Mar 1 00:05:28.799: ISAKMP (0:2): received packet from 10.1.3.1 (I) **QM\_IDLE** *!--- The IKE phase 1 SA has been successfully !--- negotiated between Hub and Spoke 2.* \*Mar 1 00:05:28.815: ISAKMP (0:2): processing HASH payload. message ID = -1872859789 \*Mar 1 00:05:28.815: ISAKMP (0:2): processing SA payload. message ID = -1872859789 \*Mar 1 00:05:28.819: ISAKMP (0:2): **Checking IPsec proposal 1 !--- IKE exchanges IPsec phase 2 parameters !--- between Hub and Spoke 2.** \*Mar 1 00:05:28.819: ISAKMP: transform 1, ESP\_DES \*Mar 1 00:05:28.823: ISAKMP: attributes in transform: \*Mar 1 00:05:28.823: ISAKMP: encaps is 1 \*Mar 1 00:05:28.827: ISAKMP: SA life type in seconds \*Mar 1 00:05:28.827: ISAKMP: SA life duration (basic) of 3600 \*Mar 1 00:05:28.827: ISAKMP: SA life type in kilobytes \*Mar 1 00:05:28.831: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 \*Mar 1 00:05:28.835: ISAKMP: authenticator is HMAC-MD5 \*Mar 1 00:05:28.839: ISAKMP (0:2): **atts are acceptable.** *!--- IPsec phase 2 parameters have been successfully !--- exchanged between Hub and Spoke 2.* \*Mar 1 00:05:28.843: IPSEC(validate\_proposal\_request): proposal part #1, (key eng. msg.) INBOUND local= 10.1.4.1, remote= 10.1.3.1, local\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), remote\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4 \*Mar 1 00:05:28.855: ISAKMP (0:2): processing NONCE payload. message ID = -1872859789 \*Mar 1 00:05:28.859: ISAKMP (0:2): processing ID payload. message ID = -1872859789 \*Mar 1 00:05:28.863: ISAKMP (0:2): processing ID payload. message ID = -1872859789 \*Mar 1 00:05:28.891: ISAKMP (0:2): Creating IPsec SAs \*Mar 1 00:05:28.891: inbound SA from 10.1.3.1 to 10.1.4.1 (proxy 192.168.1.0 to 172.16.1.0) \*Mar 1 00:05:28.895: has spi 0x1B7A414E and conn\_id 2002 and flags 4 \*Mar 1 00:05:28.899: lifetime of 3600 seconds \*Mar 1 00:05:28.899: lifetime of 4608000 kilobytes \*Mar 1 00:05:28.903: outbound SA from 10.1.4.1 to 10.1.3.1 (proxy 172.16.1.0 to 192.168.1.0 ) \*Mar 1 00:05:28.907: has spi -385025107 and conn\_id 2003 and flags C \*Mar 1



```
00:05:28.911: lifetime of 3600 seconds *Mar 1 00:05:28.911: lifetime of 4608000 kilobytes *Mar 1
00:05:28.915: ISAKMP (0:2): sending packet to 10.1.3.1 (I) QM_IDLE *Mar 1 00:05:28.919: ISAKMP
(0:2): deleting node -1872859789 error FALSE reason "" *Mar 1 00:05:28.923: IPSEC(key_engine):
got a queue event... *Mar 1 00:05:28.927: IPSEC(initialize_sas): , (key eng. msg.) INBOUND
local= 10.1.4.1, remote= 10.1.3.1, local_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-
hmac , lifedur= 3600s and 4608000kb, spi= 0x1B7A414E(460996942), conn_id= 2002, keysize= 0,
flags= 0x4 *Mar 1 00:05:28.939: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local=
10.1.4.1, remote= 10.1.3.1, local_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), remote_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb, spi= 0xE90CFBAD(3909942189), conn_id= 2003, keysize= 0, flags= 0xC
*Mar 1 00:05:28.951: IPSEC(create_sa): sa created, (sa) sa_dest= 10.1.4.1, sa_prot= 50, sa_spi=
0x1B7A414E(460996942), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2002 *Mar 1 00:05:28.959:
IPSEC(create_sa): sa created, (sa) sa_dest= 10.1.3.1, sa_prot= 50, sa_spi=
0xE90CFBAD(3909942189), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2003 !--- IPsec tunnel has
been created between routers !--- Hub and Spoke 2. This establishes a tunnel between Spoke 1 !--
- and Spoke 2 through Hub.
```

ここには、debug crypto isakmp および debug crypto ipsec コマンドをスプーク 1 ルータ上で実行した出力を示します。

```
*Mar 1 00:03:28.771: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 10.1.2.1, remote=
10.1.4.1, local_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), remote_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb, spi= 0xD44FE97C(3562006908), conn_id= 0, keysize= 0, flags= 0x400C
!--- Request sent after the ping. *Mar 1 00:03:28.787: ISAKMP: received ke message (1/1) *Mar 1
00:03:28.791: ISAKMP: local port 500, remote port 500 *Mar 1 00:03:28.799: ISAKMP (0:1):
beginning Main Mode exchange !--- Initial IKE phase 1 parameters are exchanged !--- between
Spoke 1 and Hub. *Mar 1 00:03:28.803: ISAKMP (0:1): sending packet to 10.1.4.1 (I) MM_NO_STATE.
*Mar 1 00:03:38.807: ISAKMP (0:1): retransmitting phase 1 MM_NO_STATE... *Mar 1 00:03:38.807:
ISAKMP (0:1): incrementing error counter on sa: retransmit phase 1 *Mar 1 00:03:38.811: ISAKMP
(0:1): retransmitting phase 1 MM_NO_STATE *Mar 1 00:03:38.811: ISAKMP (0:1): sending packet to
10.1.4.1 (I) MM_NO_STATE *Mar 1 00:03:48.815: ISAKMP (0:1): retransmitting phase 1
MM_NO_STATE... *Mar 1 00:03:48.815: ISAKMP (0:1): incrementing error counter on sa: retransmit
phase 1 *Mar 1 00:03:48.819: ISAKMP (0:1): retransmitting phase 1 MM_NO_STATE *Mar 1
00:03:48.819: ISAKMP (0:1): sending packet to 10.1.4.1 (I) MM_NO_STATE *Mar 1 00:03:49.355:
ISAKMP (0:1): received packet from 10.1.4.1 (I) MM_NO_STATE *Mar 1 00:03:49.363: ISAKMP (0:1):
processing SA payload. message ID = 0 *Mar 1 00:03:49.363: ISAKMP (0:1): found peer pre-shared
key matching 10.1.4.1 *Mar 1 00:03:49.367: ISAKMP (0:1): Checking ISAKMP transform 1 against
priority 10 policy *Mar 1 00:03:49.367: ISAKMP: encryption DES-CBC *Mar 1 00:03:49.371: ISAKMP:
hash MD5 *Mar 1 00:03:49.371: ISAKMP: default group 1 *Mar 1 00:03:49.375: ISAKMP: auth pre-
share *Mar 1 00:03:49.375: ISAKMP: life type in seconds *Mar 1 00:03:49.375: ISAKMP: life
duration (VPI) of 0x0 0x1 0x51 0x80 *Mar 1 00:03:49.379: ISAKMP (0:1): atts are acceptable. Next
payload is 0 !--- IKE phase 1 parameters have been sucessfully !--- negotiated between Spoke 1
and Hub. *Mar 1 00:03:50.835: ISAKMP (0:1): SA is doing pre-shared key authentication using id
type ID_IPV4_ADDR *Mar 1 00:03:50.851: ISAKMP (0:1): sending packet to 10.1.4.1 (I) MM_SA_SETUP
*Mar 1 00:03:52.759: ISAKMP (0:1): received packet from 10.1.4.1 (I) MM_SA_SETUP *Mar 1
00:03:52.763: ISAKMP (0:1): processing KE payload. message ID = 0 *Mar 1 00:03:54.635: ISAKMP
(0:1): processing NONCE payload. message ID = 0 *Mar 1 00:03:54.639: ISAKMP (0:1): found peer
pre-shared key matching 10.1.4.1 *Mar 1 00:03:54.651: ISAKMP (0:1): SKEYID state generated *Mar
1 00:03:54.655: ISAKMP (0:1): processing vendor id payload *Mar 1 00:03:54.663: ISAKMP (0:1):
speaking to another IOS box! *Mar 1 00:03:54.663: ISAKMP (1): ID payload next-payload : 8 type :
1 protocol : 17 port : 500 length : 8 *Mar 1 00:03:54.667: ISAKMP (1): Total payload length: 12
*Mar 1 00:03:54.675: ISAKMP (0:1): sending packet to 10.1.4.1 (I) MM_KEY_EXCH *Mar 1
00:03:54.759: ISAKMP (0:1): received packet from 10.1.4.1 (I) MM_KEY_EXCH *Mar 1 00:03:54.767:
ISAKMP (0:1): processing ID payload. message ID = 0 *Mar 1 00:03:54.767: ISAKMP (0:1):
processing HASH payload. message ID = 0 *Mar 1 00:03:54.775: ISAKMP (0:1): SA has been
authenticated with 10.1.4.1 *Mar 1 00:03:54.779: ISAKMP (0:1): beginning Quick Mode exchange, M-
ID of 581713929 *Mar 1 00:03:54.799: ISAKMP (0:1): sending packet to 10.1.4.1 (I) QM_IDLE *Mar 1
00:03:55.155: ISAKMP (0:1): received packet from 10.1.4.1 (I) QM_IDLE *Mar 1 00:03:55.171:
ISAKMP (0:1): processing HASH payload. message ID = 581713929 *Mar 1 00:03:55.175: ISAKMP (0:1):
processing SA payload. message ID = 581713929 *Mar 1 00:03:55.179: ISAKMP (0:1): Checking IPsec
proposal 1 !--- IKE exchanges the IPsec phase 2 parameters between !--- Spoke 1 and Hub. *Mar 1
00:03:55.179: ISAKMP: transform 1, ESP_DES *Mar 1 00:03:55.183: ISAKMP: attributes in transform:
```

\*Mar 1 00:03:55.183: ISAKMP: encaps is 1 \*Mar 1 00:03:55.183: ISAKMP: SA life type in seconds  
\*Mar 1 00:03:55.187: ISAKMP: SA life duration (basic) of 3600 \*Mar 1 00:03:55.187: ISAKMP: SA  
life type in kilobytes \*Mar 1 00:03:55.191: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0  
\*Mar 1 00:03:55.195: ISAKMP: authenticator is HMAC-MD5 \*Mar 1 00:03:55.199: ISAKMP (0:1): **atts  
are acceptable. !---** *IKE has successfully negotiated phase 2 IPsec !---* *SA between Hub and Spoke  
2.* \*Mar 1 00:03:55.203: IPSEC(validate\_proposal\_request): proposal part #1, (key eng. msg.)  
INBOUND local= 10.1.2.1, remote= 10.1.4.1, local\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4),  
remote\_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-  
hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4 \*Mar 1 00:03:55.219:  
ISAKMP (0:1): processing NONCE payload. message ID = 581713929 \*Mar 1 00:03:55.219: ISAKMP  
(0:1): processing ID payload. message ID = 581713929 \*Mar 1 00:03:55.223: ISAKMP (0:1):  
processing ID payload. message ID = 581713929 \*Mar 1 00:03:55.251: ISAKMP (0:1): Creating IPsec  
SAs \*Mar 1 00:03:55.255: inbound SA from 10.1.4.1 to 10.1.2.1 (proxy 192.168.1.0 to 172.16.1.0)  
\*Mar 1 00:03:55.259: has spi 0xD44FE97C and conn\_id 2000 and flags 4 \*Mar 1 00:03:55.263:  
lifetime of 3600 seconds \*Mar 1 00:03:55.263: lifetime of 4608000 kilobytes \*Mar 1 00:03:55.267:  
outbound SA from 10.1.2.1 to 10.1.4.1 (proxy 172.16.1.0 to 192.168.1.0 ) \*Mar 1 00:03:55.271:  
has spi -86399127 and conn\_id 2001 and flags C \*Mar 1 00:03:55.271: lifetime of 3600 seconds  
\*Mar 1 00:03:55.275: lifetime of 4608000 kilobytes \*Mar 1 00:03:55.279: ISAKMP (0:1): sending  
packet to 10.1.4.1 (I) QM\_IDLE \*Mar 1 00:03:55.283: ISAKMP (0:1): deleting node 581713929 error  
FALSE reason " " \*Mar 1 00:03:55.287: IPSEC(key\_engine): got a queue event... \*Mar 1  
00:03:55.291: IPSEC(initialize\_sas): , (key eng. msg.) INBOUND local= 10.1.2.1, remote=  
10.1.4.1, local\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), remote\_proxy=  
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac ,  
lifedur= 3600s and 4608000kb, spi= 0xD44FE97C(3562006908), conn\_id= 2000, keysize= 0, flags= 0x4  
\*Mar 1 00:03:55.303: IPSEC(initialize\_sas): , (key eng. msg.) OUTBOUND local= 10.1.2.1, remote=  
10.1.4.1, local\_proxy= 172.16.1.0/255.255.255.0/0/0 (type=4), remote\_proxy=  
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac ,  
lifedur= 3600s and 4608000kb, spi= 0xFAD9A769(4208568169), conn\_id= 2001, keysize= 0, flags= 0xC  
\*Mar 1 00:03:55.319: IPSEC(create\_sa): sa created, (sa) sa\_dest= 10.1.2.1, sa\_prot= 50, sa\_spi=  
0xD44FE97C(3562006908), sa\_trans= esp-des esp-md5-hmac , sa\_conn\_id= 2000 \*Mar 1 00:03:55.323:  
IPSEC(create\_sa): sa created, (sa) sa\_dest= 10.1.4.1, sa\_prot= 50, sa\_spi=  
0xFAD9A769(4208568169), sa\_trans= esp-des esp-md5-hmac , sa\_conn\_id= 2001 *!---* *The IPsec tunnel  
between Spoke 1 and Hub is set up.*

## 関連情報

- [IP Security のトラブルシューティング : debug コマンドの説明と使用](#)
- [IPsec 設定例](#)
- [IPsec ネゴシエーション/IKE プロトコル](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)