配置IPSec路由器到路由器的中心輻射點以及輻射點之間的通訊

目錄

簡介

此示例配置顯示了三台路由器之間的集中星型IPsec設計。此配置與其他中心輻射型配置不同,因為在本示例中,通過中心輻射型站點啟用通訊。換句話說,兩個分支路由器之間沒有直接IPsec隧道。所有資料包都通過隧道傳送到中心路由器,中心路由器通過與其他分支路由器共用的IPsec隧道將其重新分發。解決思科錯誤ID CSCdp09904(僅限註冊客戶)後,才可能進行此設定。 此修復程式已整合到Cisco IOS®軟體版本12.2(5)中,並且此版本是此配置的最低要求。

要使用OSPF配置通過IPSec的通用路由封裝(GRE)隧道,請參閱使用OSPF配置IPSec上的GRE隧道。

要在使用網路地址轉換(NAT)的GRE通道上配置基本Cisco IOS®防火牆配置,請參閱使用IOS防火牆和NAT在GRE通道上配置路由器到路由器IPSec(預共用金鑰)。

必要條件

需求

本文檔需要對IPsec協定有基本的瞭解。請參閱IP安全(IPSec)加密簡介以瞭解有關IPsec的詳細資訊。

本文的目標是確保在以下路由器之間執行加密：

- 172.16.1.0/24（分支1）到10.1.1.0/24（中心）
- 192.168.1.0/24（分支2）到10.1.1.0/24（中心）
- 172.16.1.0/24（分支1）至192.168.1.0/24（分支2）

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- Cisco IOS軟體版本12.2(24a)(c2500-ik8s-l.122-24a.bin)
- Cisco 2500路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。
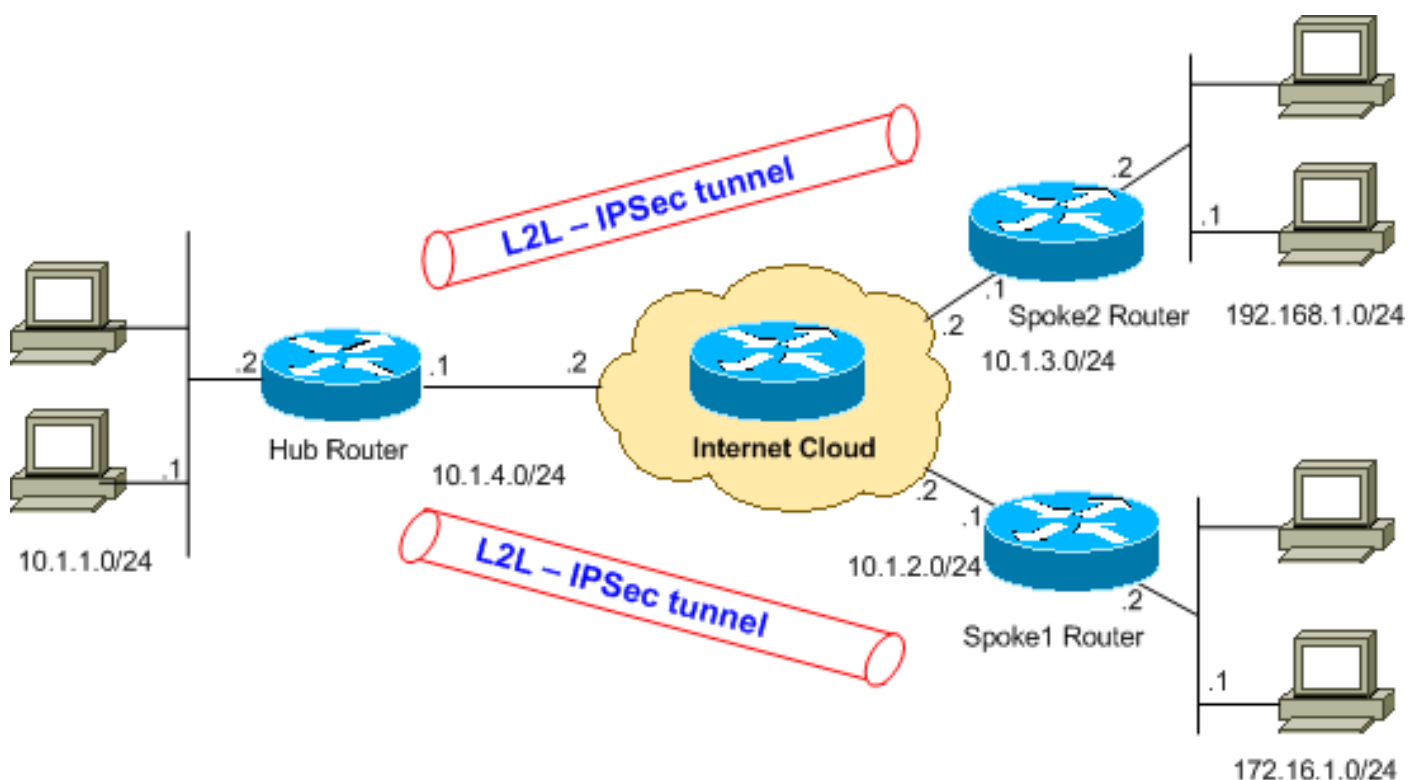
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用下圖中所示的網路設定。

注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是<u>RFC 1918</u>，已在實驗室環境中使用。

<u>組態</u>

本檔案會使用這些設定。

<u>show running-config</u>命令會顯示路由器上的運行配置。

- <u>集線器路由器</u>
- <u>分支1路由器</u>
- <u>分支2路由器</u>

集線器路由器

```
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.
```

分支1路由器

```
Spoke1#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 Spoke1
!
enable secret 5 $1$DOX3$rIrxEnTVTw/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#
```

分支2路由器

```
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#
```

新增另一個分支

除了分支1和spoke2之外,如果您需要將另一個分支路由器(spoke3)新增到現有的中心路由器,則只需建立一個從中心路由器到分支3的新LAN到LAN(L2L)隧道。但是,由於每個物理介面只能配置一個加密對映,因此新增此隧道時必須使用相同的加密對映名稱。當您對每個遠端站點使用不同的行號時,這是可能的。

注意: 新增新通道條目時,可能需要刪除加密對映並重新應用到介面。刪除密碼編譯對應後,所有活動的通道都會被清除。

集線器路由器

```
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
```

分支3路由器

```
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#
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析
。

若要驗證此組態，請嘗試使用源自分支1上的ethernet1介面位址（目的地為分支2的ethernet1介面位
址）的延伸型ping命令。

- ping — 用於診斷基本網路連線。
  ```
  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 — 顯示當前(IPSec)安全關聯(SA)使用的設定。
- show crypto isakmp sa — 顯示對等體上的所有當前IKE SA。
- show crypto engine connections active — 顯示通過每個IPSec SA傳輸的資料包數。

show輸出示例

此輸出來自在集線器路由器上發出的show crypto engine connections active命令。

```
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
```

在此範例中，您可以看到每個通道已加密和解密10個封包，這證明流量通過集線器路由器。

注意：為每個對等體建立兩個IPsec SA（每個方向一個）。 例如，在中心路由器中，為兩個對等體建立了四個IPsec SA。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

附註：使用 debug 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- [debug crypto ipsec](#) — 顯示第2階段的IPsec協商。
- [debug crypto isakmp](#) — 顯示第1階段的ISAKMP協商。
- [debug crypto engine](#) — 顯示加密的流量。
- [clear crypto isakmp](#) — 清除與第1階段相關的SA。
- [clear crypto sa](#) — 清除與第2階段相關的SA。

調試輸出示例

這是debug crypto ipsec和debug crypto isakmp命令的中心路由器輸出。

```
*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_SET UP *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 sucessfully 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.
```

這是debug crypto isakmp和debug crypto ipsec命令的Spoke 1路由器輸出。

```
*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.

相關資訊

- IP安全性疑難排解 — 瞭解和使用debug命令
- IPsec配置示例
- IPsec協商/IKE通訊協定
- 技術支援與文件 - Cisco Systems