配置兩台路由器之間的LAN到LAN IPsec隧道

目錄

簡介

本檔案介紹如何在兩個Cisco路由器(Cisco IOS®或Cisco IOS® XE)之間透過網際網路金鑰交換(IKEv1)設定原則型VPN。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據使用Cisco IOS®版本15.7的Cisco路由器。它允許使用者通過IPsec VPN隧道跨站點訪問資源。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

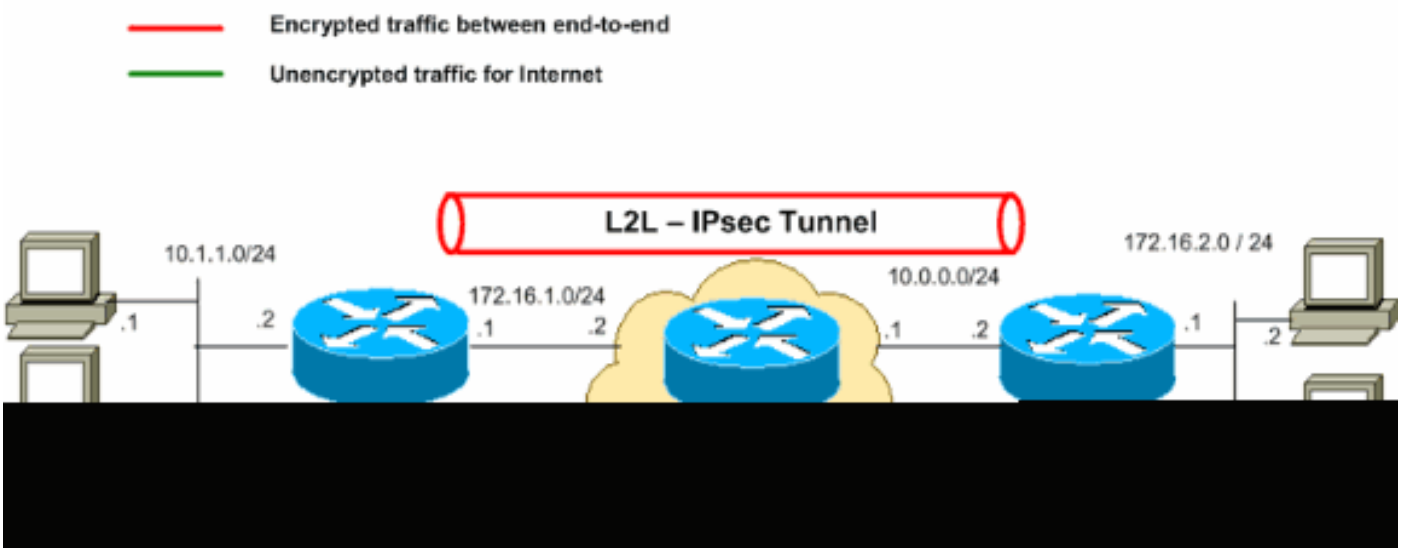
請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

此文件使用以下網路設定：



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RFC 1918位址，已在實驗室環境中使用。

組態

本檔案會使用以下設定：

- 路由器A
- 路由器B

注意：思科建議應用於兩台裝置上的加密對映的ACL是彼此的映象。

路由器A

```
!--- Create an ISAKMP policy for Phase 1 negotiations for the L2L tunnels.

crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14

!--- Specify the pre-shared key and the remote peer address
!--- to match for the L2L tunnel.

crypto isakmp key vpnuser address 10.0.0.2

!--- Create the Phase 2 policy for IPsec negotiation.
```

```
crypto ipsec transform-set myset esp-aes esp-sha256-hmac

!--- Create an ACL for the traffic to be encrypted.
!--- In this example, the traffic from 10.1.1.0/24 to 172.16.2.0/24
!--- is encrypted. The traffic which does not match the access list
!--- is unencrypted for the Internet.

access-list 100 permit ip 10.1.1.0 0.0.0.255 172.16.2.0 0.0.0.255

!--- Create the actual crypto map. Specify an access control list (ACL),
!--- which defines the proxy identities (local and remote host/networks).

crypto map mymap 10 ipsec-isakmp
 set peer 10.0.0.2
 set transform-set myset
 match address 100

interface GigabitEthernet0/1
ip address 10.1.1.2 255.255.255.0

!--- Apply the crypto map on the outside interface.

interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 crypto map mymap

!--- Route to the default gateway

ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

路由器B

```
!--- Create an ISAKMP policy for Phase 1 negotiations for the L2L tunnels.

crypto isakmp policy 10
encryption aes
hash sha256
authentication pre-share
group 14

!--- Specify the pre-shared key and the remote peer address
!--- to match for the L2L tunnel.

crypto isakmp key vpnuser address 172.16.1.1

!--- Create the Phase 2 policy for IPsec negotiation.

crypto ipsec transform-set myset esp-aes esp-sha256-hmac

!--- Create an ACL for the traffic to be encrypted.
!--- In this example, the traffic from 172.16.2.0/24 to 10.1.1.0/24
!--- is encrypted. The traffic which does not match the access list
!--- is unencrypted for the Internet.

access-list 100 permit ip 172.16.2.0 0.0.0.255 10.1.1.0 0.0.0.255

!--- Create the actual crypto map. Specify an access control list (ACL),
```

```
!--- which defines the proxy identities (local and remote host/networks).

!
crypto map mymap 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set myset
 match address 100

interface GigabitEthernet0/1
ip address 172.16.2.1 255.255.255.0
!

!--- Apply the crypto map on the outside interface.

interface GigabitEthernet0/0
ip address 10.0.0.2 255.255.255.0
crypto map mymap

!--- Route to the default gateway.

ip route 0.0.0.0 0.0.0.0 10.0.01
```

驗證

使用本節內容，確認您的組態是否正常運作。

Cisco CLI Analyzer(僅供已註冊客戶使用)支援 **show** 指令。使用Cisco CLI Analyzer檢視 **show** 命令輸出。

- **show crypto ipsec sa** — 顯示當前安全關聯(SA)使用的設定、封裝和封裝數、本地和遠端代理身份以及安全引數索引(SPI)、入站和出站。

```
<#root>

RouterA#

show crypto ipsec sa


interface: Serial2/0
    Crypto map tag: mymap, local addr 172.16.1.1

    protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.2.0/255.255.255.0/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 21, #pkts decrypt: 21, #pkts verify: 21

    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2

     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x8767D399(2271728537)
     PFS (Y/N): N, DH group: none


  inbound esp sas:
      spi: 0x6E210372(1847657330)
        transform: esp-aes esp-sha256-hmac ,

        in use settings ={Tunnel, }
        conn id: 2007, flow_id: Onboard VPN:7, sibling_flags 80004040, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4338240/3269)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:


   outbound esp sas:
      spi: 0x8767D399(2271728537)
        transform: esp-aes esp-sha256-hmac ,

        in use settings ={Tunnel, }
        conn id: 2008, flow_id: Onboard VPN:8, sibling_flags 80004040, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4338240/3269)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto isakmp sa** — 顯示所有當前IKE SA和狀態。

```
<#root>

RouterA#

show crypto isakmp sa

dst             src             state          conn-id slot status
10.0.0.2        172.16.1.1      QM_IDLE              1    0

ACTIVE
```

- **show crypto map** — 顯示使用建立的加密對映結構：
  - 加密對映的名稱和序列號。
  - 對等體地址。

- 與本地和遠端代理身份一起應用的ACL的名稱。
- 使用的IPsec轉換集的值。
- 繫結加密對映的介面。

<#root>

RouterA#

show crypto map

Crypto Map IPv4 "mymap" 10 ipsec-isakmp
Peer = 10.0.0.2

Extended IP access list

100

access-list 100 permit ip 10.1.1.0 0.0.0.255 172.16.2.0 0.0.0.255

Current peer: 10.0.0.2
Security association lifetime: 4608000 kilobytes/3600 seconds
Responder-Only (Y/N): N
PFS (Y/N): N
Mixed-mode : Disabled

Transform sets={
myset: { esp-aes esp-sha256-hmac } ,

}
Interfaces using crypto map mymap:

GigabitEthernet0/0

RouterB#

show crypto map

Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "mymap" 10 ipsec-isakmp

Peer = 172.16.1.1

Extended IP access list

100

access-list 100 permit ip 172.16.2.0 0.0.0.255 10.1.1.0 0.0.0.255

Current peer: 10.0.0.1
Security association lifetime: 4608000 kilobytes/3600 seconds
Responder-Only (Y/N): N
PFS (Y/N): N
Mixed-mode : Disabled

```
Transform sets={
                                myset:  { esp-aes esp-sha256-hmac  } ,

               }
               Interfaces using crypto map mymap:


 GigabitEthernet0/0
```

- **show crypto session remote**

  detail

  <#root>

  RouterA#

  show crypto session remote 10.0.0.2 detail

  Crypto session current status

  Interface: GigabitEthernet0/0

  Uptime: 00:39:16
  Session status: UP-ACTIVE   >>>>> Status of the VPN

  Peer: 10.0.0.2 port 500 fvrf: (none) ivrf: (none)
        Phase1_id: 10.0.0.2
        Desc: (none)
    Session ID: 0
    IKEv1 SA: local 172.16.1.1/500 remote 10.0.0.2/500 Active
            Capabilities:(none) connid:1004 lifetime:23:20:43
    IPSEC FLOW: permit ip 10.1.1.0/255.255.255.0 172.16.2.0/255.255.255.0
          Active SAs: 2, origin: crypto map
          Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4338240/1243
          Outbound: #pkts enc'ed 21 drop 0 life (KB/Sec) 4338240/1243

  RouterB#

  show crypto session remote 172.16.1.1 detail

  Crypto session current status

  Interface: GigabitEthernet0/0

  Uptime: 00:40:43
  Session status: UP-ACTIVE   >>>>> Status of the VPN

  Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
        Phase1_id: 172.16.1.1
        Desc: (none)
    Session ID: 0
    IKEv1 SA: local 10.0.0.2/500 remote 172.16.1.1/500 Active
            Capabilities:(none) connid:1004 lifetime:23:19:16
    IPSEC FLOW: permit ip 172.16.2.0/255.255.255.0 10.1.1.0/255.255.255.0
          Active SAs: 2, origin: crypto map
          Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4271304/1156
          Outbound: #pkts enc'ed 21 drop 0 life (KB/Sec) 4271304/1156

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

指令

Cisco CLI Analyzer(僅供已註冊客戶使用)支援 **show** 指令。使用Cisco CLI Analyzer檢視 **show** 命令輸出。

注意：使用前，請先參閱有關Debug命令的重要資訊 **debug** 指令。

- **debug crypto isakmp** — 顯示第1階段的ISAKMP協商。
- **debug crypto ipsec** — 顯示第2階段的IPsec協商。

調試輸出示例

調試輸出示例來自RouterA（啟動器），用於成功進行VPN協商。

路由器

<#root>

```
RouterA#
```

debug crypto isakmp

```
Jul  1 04:08:49.558: ISAKMP: (0):SA request profile is (NULL)
Jul  1 04:08:49.558: ISAKMP: (0):Created a peer struct for 10.0.0.2, peer port 500
Jul  1 04:08:49.558: ISAKMP: (0):New peer created peer = 0x2108BC48 peer_handle = 0x80000005
Jul  1 04:08:49.558: ISAKMP: (0):Locking peer struct 0x2108BC48, refcount 1 for isakmp_initiator
Jul  1 04:08:49.558: ISAKMP: (0):local port 500, remote port 500
Jul  1 04:08:49.558: ISAKMP: (0):set new node 0 to QM_IDLE
Jul  1 04:08:49.558: ISAKMP: (0):Find a dup sa in the avl tree during calling isadb_insert sa = 3DA022D
Jul  1 04:08:49.558: ISAKMP: (0):Can not start Aggressive mode,.!
Success rate is 50 percent (1/2), round-trip min/avg/max = 1/1/1 ms
Router# trying Main mode.
Jul  1 04:08:49.558: ISAKMP: (0):found peer pre-shared key matching 10.0.0.2
Jul  1 04:08:49.558: ISAKMP: (0):constructed NAT-T vendor-rfc3947 ID
Jul  1 04:08:49.558: ISAKMP: (0):constructed NAT-T vendor-07 ID
Jul  1 04:08:49.558: ISAKMP: (0):constructed NAT-T vendor-03 ID
Jul  1 04:08:49.558: ISAKMP: (0):constructed NAT-T vendor-02 ID
Jul  1 04:08:49.558: ISAKMP: (0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
Jul  1 04:08:49.558: ISAKMP: (0):Old State = IKE_READY  New State = IKE_I_MM1

Jul  1 04:08:49.562: ISAKMP: (0):beginning Main Mode exchange
Jul  1 04:08:49.562: ISAKMP-PAK: (0):sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) MM_NO_STA
Jul  1 04:08:49.562: ISAKMP: (0):Sending an IKE IPv4 Packet.
Jul  1 04:08:49.690: ISAKMP-PAK: (0):received packet from 10.0.0.2 dport 500 sport 500 Global (I) MM_NO
Jul  1 04:08:49.690: ISAKMP: (0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Jul  1 04:08:49.690: ISAKMP: (0):Old State = IKE_I_MM1  New State = IKE_I_MM2

Jul  1 04:08:49.690: ISAKMP: (0):processing SA payload. message ID = 0
Jul  1 04:08:49.690: ISAKMP: (0):processing vendor id payload
```

```
Jul  1 04:08:49.690: ISAKMP: (0):vendor ID seems Unity/DPD but major 69 mismatch
Jul  1 04:08:49.690: ISAKMP: (0):vendor ID is NAT-T RFC 3947
Jul  1 04:08:49.690: ISAKMP: (0):found peer pre-shared key matching 10.0.0.2
Jul  1 04:08:49.690: ISAKMP: (0):local preshared key found
Jul  1 04:08:49.690: ISAKMP: (0):Scanning profiles for xauth ...
Jul  1 04:08:49.690: ISAKMP: (0):Checking ISAKMP transform 1 against priority 10 policy
Jul  1 04:08:49.690: ISAKMP: (0):      encryption AES-CBC
Jul  1 04:08:49.690: ISAKMP: (0):      keylength of 128
Jul  1 04:08:49.690: ISAKMP: (0):      hash SHA256
Jul  1 04:08:49.690: ISAKMP: (0):      default group 14
Jul  1 04:08:49.690: ISAKMP: (0):      auth pre-share
Jul  1 04:08:49.690: ISAKMP: (0):      life type in seconds
Jul  1 04:08:49.690: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
Jul  1 04:08:49.690: ISAKMP: (0):atts are acceptable. Next payload is 0
Jul  1 04:08:49.690: ISAKMP: (0):Acceptable atts:actual life: 0
Jul  1 04:08:49.690: ISAKMP: (0):Acceptable atts:life: 0
Jul  1 04:08:49.690: ISAKMP: (0):Fill atts in sa vpi_length:4
Jul  1 04:08:49.690: ISAKMP: (0):Fill atts in sa life_in_seconds:86400
Jul  1 04:08:49.690: ISAKMP: (0):Returning Actual lifetime: 86400
Jul  1 04:08:49.690: ISAKMP: (0):Started lifetime timer: 86400.

Jul  1 04:08:49.814: ISAKMP: (0):processing vendor id payload
Jul  1 04:08:49.814: ISAKMP: (0):vendor ID seems Unity/DPD but major 69 mismatch
Jul  1 04:08:49.814: ISAKMP: (0):vendor ID is NAT-T RFC 3947
Jul  1 04:08:49.814: ISAKMP: (0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Jul  1 04:08:49.814: ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM2

Jul  1 04:08:49.818: ISAKMP-PAK: (0):sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) MM_SA_SETU
Jul  1 04:08:49.818: ISAKMP: (0):Sending an IKE IPv4 Packet.
Jul  1 04:08:49.818: ISAKMP: (0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Jul  1 04:08:49.818: ISAKMP: (0):Old State = IKE_I_MM2  New State = IKE_I_MM3

Jul  1 04:08:49.978: ISAKMP-PAK: (0):received packet from 10.0.0.2 dport 500 sport 500 Global (I) MM_SA_
Jul  1 04:08:49.978: ISAKMP: (0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Jul  1 04:08:49.978: ISAKMP: (0):Old State = IKE_I_MM3  New State = IKE_I_MM4

Jul  1 04:08:49.978: ISAKMP: (0):processing KE payload. message ID = 0
Jul  1 04:08:50.138: ISAKMP: (0):processing NONCE payload. message ID = 0
Jul  1 04:08:50.138: ISAKMP: (0):found peer pre-shared key matching 10.0.0.2
Jul  1 04:08:50.138: ISAKMP: (1004):processing vendor id payload
Jul  1 04:08:50.138: ISAKMP: (1004):vendor ID is Unity
Jul  1 04:08:50.138: ISAKMP: (1004):processing vendor id payload
Jul  1 04:08:50.138: ISAKMP: (1004):vendor ID is DPD
Jul  1 04:08:50.138: ISAKMP: (1004):processing vendor id payload
Jul  1 04:08:50.138: ISAKMP: (1004):speaking to another IOS box!
Jul  1 04:08:50.138: ISAKMP: (1004):received payload type 20
Jul  1 04:08:50.138: ISAKMP: (1004):His hash no match - this node outside NAT
Jul  1 04:08:50.138: ISAKMP: (1004):received payload type 20
Jul  1 04:08:50.138: ISAKMP: (1004):No NAT Found for self or peer
Jul  1 04:08:50.138: ISAKMP: (1004):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Jul  1 04:08:50.138: ISAKMP: (1004):Old State = IKE_I_MM4  New State = IKE_I_MM4

Jul  1 04:08:50.138: ISAKMP: (1004):Send initial contact
Jul  1 04:08:50.138: ISAKMP: (1004):SA is doing
Jul  1 04:08:50.138: ISAKMP: (1004):pre-shared key authentication using id type ID_IPV4_ADDR
Jul  1 04:08:50.138: ISAKMP: (1004):
```

ID payload

```
                next-payload : 8
                type         : 1
Jul  1 04:08:50.138: ISAKMP: (1004):        address      :
```

172.16.1.1   >>>>> IKE ID sent

```
Jul  1 04:08:50.138: ISAKMP: (1004):        protocol     : 17
                port         : 500
                length       : 12
Jul  1 04:08:50.138: ISAKMP: (1004):Total payload length: 12
Jul  1 04:08:50.138: ISAKMP-PAK: (1004):sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) MM_KEY
Jul  1 04:08:50.138: ISAKMP: (1004):Sending an IKE IPv4 Packet.
Jul  1 04:08:50.138: ISAKMP: (1004):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Jul  1 04:08:50.138: ISAKMP: (1004):Old State = IKE_I_MM4  New State = IKE_I_MM5

Jul  1 04:08:50.138: ISAKMP-PAK: (1004):received packet from 10.0.0.2 dport 500 sport 500 Global (I) MM
Jul  1 04:08:50.142: ISAKMP: (1004):processing ID payload. message ID = 0
Jul  1 04:08:50.142: ISAKMP: (1004):
```

ID payload

```
                next-payload : 8
                type         : 1
Jul  1 04:08:50.142: ISAKMP: (1004):        address      :
```

10.0.0.2   >>>>> IKE ID received

```
Jul  1 04:08:50.142: ISAKMP: (1004):        protocol     : 17
                port         : 500
                length       : 12
Jul  1 04:08:50.142: ISAKMP: (0):peer matches *none* of the profiles
Jul  1 04:08:50.142: ISAKMP: (1004):processing HASH payload. message ID = 0
Jul  1 04:08:50.142: ISAKMP: (1004):SA authentication status:
                authenticated
Jul  1 04:08:50.142: ISAKMP: (1004):SA has been authenticated with 10.0.0.2
Jul  1 04:08:50.142: ISAKMP: (0):Trying to insert a peer 172.16.1.1/10.0.0.2/500/,
Jul  1 04:08:50.142: ISAKMP: (0): and inserted successfully 2108BC48.
Jul  1 04:08:50.142: ISAKMP: (1004):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Jul  1 04:08:50.142: ISAKMP: (1004):Old State = IKE_I_MM5  New State = IKE_I_MM6

Jul  1 04:08:50.142: ISAKMP: (1004):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Jul  1 04:08:50.142: ISAKMP: (1004):Old State = IKE_I_MM6  New State = IKE_I_MM6

Jul  1 04:08:50.142: ISAKMP: (1004):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Jul  1 04:08:50.142: ISAKMP: (1004):Old State = IKE_I_MM6  New State = IKE_P1_COMPLETE

Jul  1 04:08:50.142: ISAKMP: (1004):beginning Quick Mode exchange, M-ID of 3184909968
Jul  1 04:08:50.142: ISAKMP: (1004):QM Initiator gets spi
Jul  1 04:08:50.142: ISAKMP-PAK: (1004):sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) QM_IDL
Jul  1 04:08:50.142: ISAKMP: (1004):Sending an IKE IPv4 Packet.
Jul  1 04:08:50.142: ISAKMP: (1004):Node 3184909968, Input = IKE_MESG_INTERNAL, IKE_INIT_QM
Jul  1 04:08:50.142: ISAKMP: (1004):Old State = IKE_QM_READY  New State = IKE_QM_I_QM1
```

Jul 1 04:08:50.142: ISAKMP: (1004):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE   >>>>> Phase1 negoti

```
Jul  1 04:08:50.142: ISAKMP: (1004):Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

Jul  1 04:08:50.146: ISAKMP-PAK: (1004):received packet from 10.0.0.2 dport 500 sport 500 Global (I) QM
Jul  1 04:08:50.146: ISAKMP: (1004):processing HASH payload. message ID = 3184909968
Jul  1 04:08:50.146: ISAKMP: (1004):processing SA payload. message ID = 3184909968
Jul  1 04:08:50.146: ISAKMP: (1004):Checking IPSec proposal 1
Jul  1 04:08:50.146: ISAKMP: (1004):transform 1, ESP_AES
Jul  1 04:08:50.146: ISAKMP: (1004):   attributes in transform:
Jul  1 04:08:50.146: ISAKMP: (1004):      encaps is 1 (Tunnel)
Jul  1 04:08:50.146: ISAKMP: (1004):      SA life type in seconds
Jul  1 04:08:50.146: ISAKMP: (1004):      SA life duration (basic) of 3600
Jul  1 04:08:50.146: ISAKMP: (1004):      SA life type in kilobytes
Jul  1 04:08:50.146: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
```

```
Jul  1 04:08:50.146: ISAKMP: (1004):      authenticator is HMAC-SHA256
Jul  1 04:08:50.146: ISAKMP: (1004):      key length is 128
Jul  1 04:08:50.146: ISAKMP: (1004):atts are acceptable.
Jul  1 04:08:50.146: IPSEC(validate_proposal_request): proposal part #1
Jul  1 04:08:50.146: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 172.16.1.1:0, remote= 10.0.0.2:0,
    local_proxy= 10.1.1.0/255.255.255.0/256/0,
    remote_proxy= 172.16.2.0/255.255.255.0/256/0,
    protocol= ESP, transform= esp-aes esp-sha256-hmac  (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
Jul  1 04:08:50.146: Crypto mapdb : proxy_match
                src addr     : 10.1.1.0
                dst addr     : 172.16.2.0
                protocol     : 0
                src port     : 0
                dst port     : 0

Jul  1 04:08:50.146: (ipsec_process_proposal)Map Accepted: mymap, 10

Jul  1 04:08:50.146: ISAKMP: (1004):processing NONCE payload. message ID = 3184909968
Jul  1 04:08:50.146: ISAKMP: (1004):processing ID payload. message ID = 3184909968
Jul  1 04:08:50.146: ISAKMP: (1004):processing ID payload. message ID = 3184909968
Jul  1 04:08:50.146: ISAKMP: (1004):Node 3184909968, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Jul  1 04:08:50.146: ISAKMP: (1004):Old State = IKE_QM_I_QM1  New State = IKE_QM_IPSEC_INSTALL_AWAIT
Jul  1 04:08:50.146: IPSEC(key_engine): got a queue event with 1 KMI message(s)
Jul  1 04:08:50.146: Crypto mapdb : proxy_match
                src addr     : 10.1.1.0
                dst addr     : 172.16.2.0
                protocol     : 256
                src port     : 0
                dst port     : 0
Jul  1 04:08:50.146: IPSEC(crypto_ipsec_create_ipsec_sas): Map found mymap, 10
Jul  1 04:08:50.146: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and pee
Jul  1 04:08:50.146: IPSEC(get_old_outbound_sa_for_peer): No outbound SA found for peer 22C55798
Jul  1 04:08:50.146: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.1, sa_proto= 50,


sa_spi= 0x6E210372(1847657330),    >>>>> Inbound SPI

    sa_trans= esp-aes esp-sha256-hmac , sa_conn_id= 2007
    sa_lifetime(k/sec)= (4608000/3600),
  (identity) local= 172.16.1.1:0, remote= 10.0.0.2:0,
    local_proxy= 10.1.1.0/255.255.255.0/256/0,
    remote_proxy= 172.16.2.0/255.255.255.0/256/0
Jul  1 04:08:50.146: IPSEC(create_sa): sa created,
  (sa) sa_dest= 10.0.0.2, sa_proto= 50,


sa_spi= 0x8767D399(2271728537),   >>>>> Outbound SPI

    sa_trans= esp-aes esp-sha256-hmac , sa_conn_id= 2008
    sa_lifetime(k/sec)= (4608000/3600),
  (identity) local= 172.16.1.1:0, remote= 10.0.0.2:0,
    local_proxy= 10.1.1.0/255.255.255.0/256/0,
    remote_proxy= 172.16.2.0/255.255.255.0/256/0
Jul  1 04:08:50.150: IPSEC: Expand action denied, notify RP
Jul  1 04:08:50.150: ISAKMP-ERROR: (0):Failed to find peer index node to update peer_info_list
Jul  1 04:08:50.150: ISAKMP: (1004):Received IPSec Install callback... proceeding with the negotiation

Jul  1 04:08:50.150: ISAKMP: (1004):Successfully installed IPSEC SA (SPI:0x6E210372) on GigabitEthernet0

Jul  1 04:08:50.150: ISAKMP-PAK: (1004):sending packet to 10.0.0.2 my_port 500 peer_port 500 (I) QM_IDL
```

```
Jul  1 04:08:50.150: ISAKMP: (1004):Sending an IKE IPv4 Packet.
Jul  1 04:08:50.150: ISAKMP: (1004):deleting node -1110057328 error FALSE reason "No Error"
Jul  1 04:08:50.150: ISAKMP: (1004):Node 3184909968, Input = IKE_MESG_FROM_IPSEC, IPSEC_INSTALL_DONE

Jul  1 04:08:50.150: ISAKMP: (1004):Old State = IKE_QM_IPSEC_INSTALL_AWAIT  New State = IKE_QM_PHASE2_CO

Jul  1 04:08:50.950: ISAKMP: (1003):purging node -262896492
Jul  1 04:09:09.710: ISAKMP: (1003):purging SA., sa=3DA05D84, delme=3DA05D84
```

相關資訊

- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。