두 라우터 간의 LAN-to-LAN IPsec 터널 구성

목차

소개

이 문서에서는 두 Cisco 라우터(Cisco IOS® 또는 Cisco IOS® XE) 간에 IKEv1(Internet Key Exchange)을 통한 정책 기반 VPN을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® 릴리스 15.7을 사용하는 Cisco 라우터를 기반으로 합니다. 사용자는 IPsec VPN 터널을 통해 사이트 전반의 리소스에 액세스할 수 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

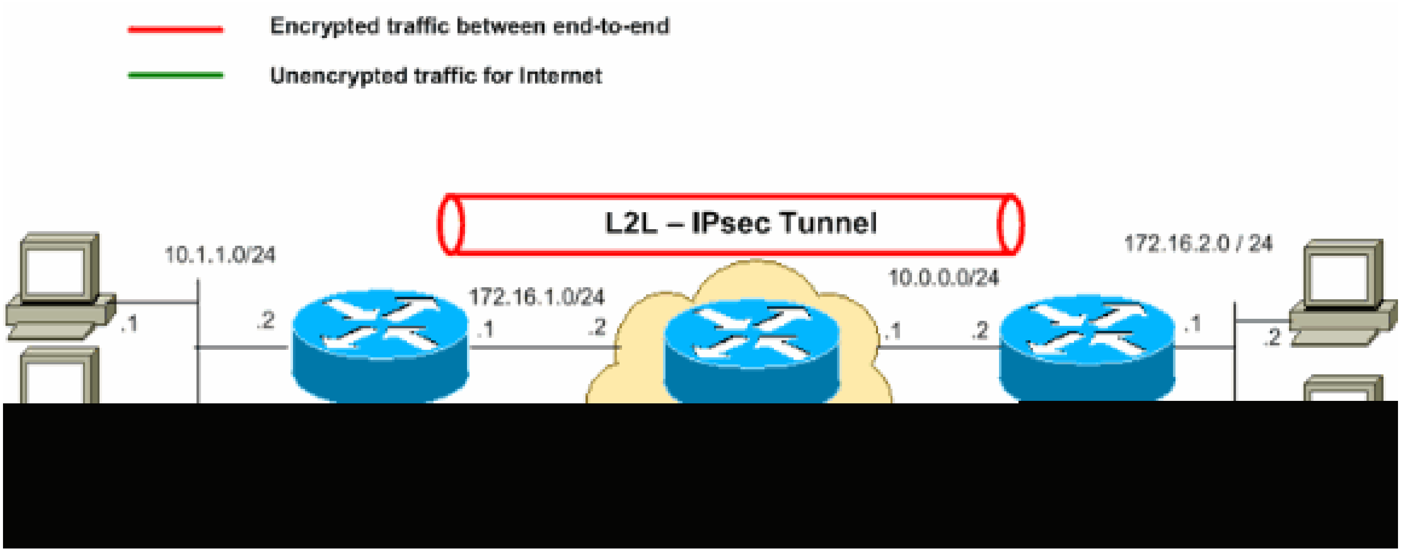
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



[redacted]

참고: 이 컨피그레이션에서 사용되는 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 랩 환경에서 사용된 RFC 1918 주소입니다.

설정

이 문서에서는 다음 설정을 사용합니다.

- 라우터 A
- 라우터 B

참고: 두 디바이스의 암호화 맵에 적용된 ACL은 서로의 미러 이미지가 될 것을 권장합니다.

라우터 A
<code>!--- Create an ISAKMP policy for Phase 1 negotiations for the L2L tunnels.</code> <code>crypto isakmp policy 10</code> <code>encryption aes</code> <code>hash sha256</code> <code>authentication pre-share</code> <code>group 14</code> <code>!--- Specify the pre-shared key and the remote peer address</code> <code>!--- to match for the L2L tunnel.</code>

```
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
```

라우터 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
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Cisco CLI Analyzer(등록된 고객만 해당)는 **show** 명령을 사용합니다. Cisco CLI Analyzer를 사용하여 **show** 명령 출력입니다.

- **show crypto ipsec sa** - 현재 SA(Security Association)에서 사용되는 설정, 캡슐화 및 디캡의 수, 로컬 및 원격 프록시 ID, SPI(Security Parameter Index), 인바운드 및 아웃바운드를 표시합니다.

  <#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** - 모든 현재 IKE SA 및 상태를 표시합니다.

<#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** - 다음으로 생성된 암호화 맵 구조를 표시합니다.
  - 암호화 맵의 이름 및 시퀀스 번호입니다.
  - 피어 주소입니다.
  - 로컬 및 원격 프록시 ID와 함께 적용된 ACL의 이름입니다.
  - 사용된 IPsec transform-set의 값입니다.
  - 암호화 맵이 바인딩된 인터페이스입니다.

<#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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

명령

Cisco CLI Analyzer(등록된 고객만 해당)는 **show** 명령을 사용합니다. Cisco CLI Analyzer를 사용하여 **show** 명령 출력입니다.

참고: Debug 명령에 대한 중요한 정보를 참조한 후 사용하십시오. **debug** 명령을 사용합니다.

- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto ipsec** - 2단계의 IPsec 협상을 표시합니다.

디버그 출력 샘플

성공적인 VPN 협상을 위한 샘플 디버그 출력은 RouterA(initiator)에서 옵니다.

라우터

<#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_IDLE
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
```

관련 정보

- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.