

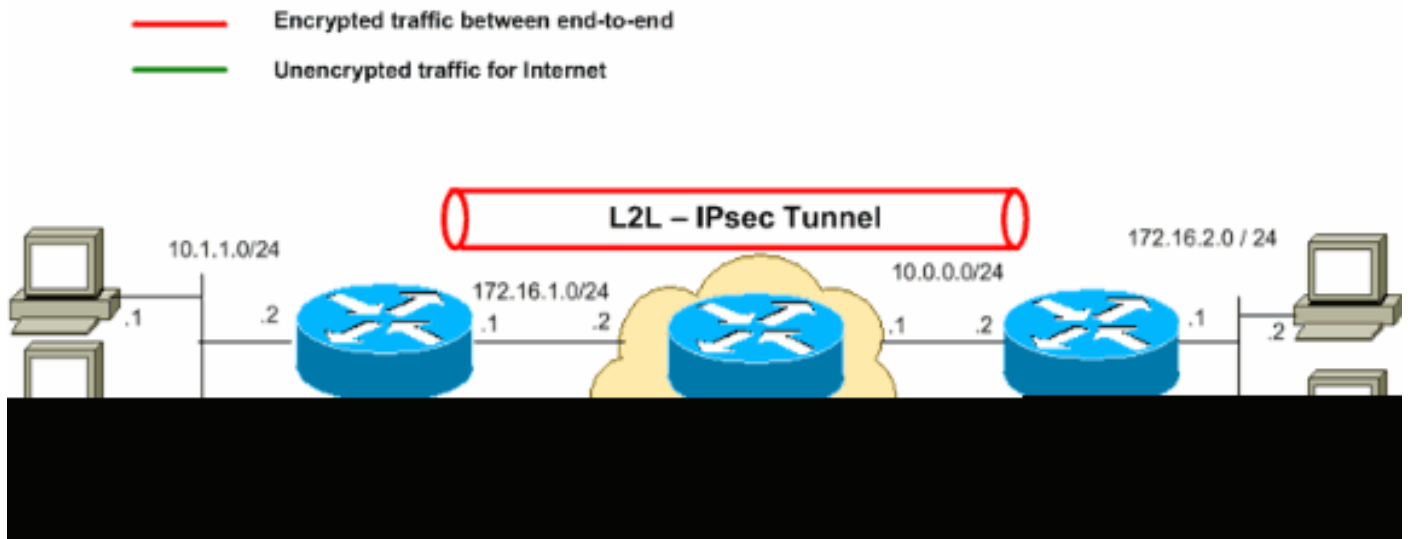
[تادنت سمل](#)

نيوكتال

دنت سمل اذه يف ةحوضوملا تازيمل نيوكت تامولعم كل مّدقّت، مسقلا اذه يف

ةكبش ل ل يطيختال مسرلا

يالاتلا ةكبش ل دادع | دنت سمل اذه مدختسي



✎ رلع routable ايناوناق لليكشت اذه يف لمعتسي ةطخ بطاخي سي ل ip ل :ةظحالم ةيربتم ةئيبي يف اهمادختسا مت ياتال [RFC 1918](#) نيناوانع يهو .تنترتنالا

تانيوكتال

ةيالاتلا تانيوكتال دنت سمل اذه مدختسي

- [هجوم A](#)
- [هجوم B](#)

✎ رلع ةقبطملا (ACL) لوصولا يف مكحتلا ةمئاق نوكت نأ Cisco ي صوت :ةظحالم ضعبلا اهضعبل ةقبطاتم ةروص نيزاهجالا لك رلع ريفشتلا ةطيرخ

هجوم 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

```

B هجوم ل

```

!--- 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 10.0.0.1

```

ةحصلا نم ققحتلا

ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

ضعب (طقف [نيلجس ملإ](#) ءالمعلل) [Cisco](#) نم رماوأل رطس ةهجاو للجم) [Cisco CLI Analyzer](#) معدي
 show ليلحت ضرعل (Cisco نم رماوأل رطس ةهجاو للجم) Cisco CLI Analyzer مدختسا. رماوأل
 show ليلحت ضرعل.

- `show crypto ipsec sa` - ليلحت اذم ءاداعلا راهظا -
 لبق نم ةمدختسملا، ةرداصل او ةدراوأل، (SPIs) نامأل تاملعم سراهفو ةديعبلاو ةيلحمل
 (SAs) ةيلحلا نامأل تانارتقا.

```
<#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 - إظهار حالة IKE والاتصال به.

```
<#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** - مداخلتساب اهؤاشنإ مت يتللا ريفشتلا ةطيرخ ةينب ضرعي
 - ليلسلسلتلا مقرلاو ريفشتلا ةطيرخ مسا.
 - ريفظنللا ناونع.
 - ةديعبلاو ةيلحمللا ليكولا تايوه عم قبطملا (ACL) لوصولاب مكحتلا ةمئاق مسا.
 - ةمدختسمللا IPsec ليوحت ةومجم ميقي.
 - اهليلع ريفشتلا ةطيرخ طبر مت يتللا ةهاولا.

<#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
```

اهحال صاوا ءاطخاا فاشكسا

اهحال صاوا نيوكتاا ءاطخا فاشكساا اهمادختساا كككمي تامولعم مسقلا اذو رفوي

رم اوأا

ضعب (طقف نيلاجس مالا عالم لال) (Cisco نم رماوأا رطس ءهجاو للاحم) Cisco CLI Analyzer م عدي show ليلحت ضرعل (Cisco نم رماوأا رطس ءهجاو للاحم) Cisco CLI Analyzer مدختساا. رماوأا show رماأا جارخا

 رماوأا debug مدختساا نا لبق ءاطخاا حيحصت رماوأا نع ءمهم تامولعم ىلا عجارا: ءطخال م

- debug crypto isakmp - ىلاوأا ءلحرملل ISAKMP تاضوافم ضرع
- debug crypto ipsec - ءلحرملل IPsec تاضوافم ضرع

ءنيعلل ءاطخاا حيحصت جارخا

ءحجان VPN تاضوافم (ئدابلا) RouterA نم ءنيعلل ءاطخاا حيحصت جارخا

ءجوملا

```
<#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_MSG_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_SET
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 peer
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 GigabitEthernet0/24
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_C
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
```

ةلص تاذا تامولعم

- [IKE تالوكوتورب/IPSec ةضوافم](#)
- [تادنتس مل او ينقتلا مع دلا - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا