

## ISAKMP Debug - Spoke

```
Dec 11 23:59:02.514 EST: ISAKMP:(0): SA request profile is VPN-0
Dec 11 23:59:02.514 EST: ISAKMP: Created a peer struct for <Hub-IP>, peer port 500
Dec 11 23:59:02.514 EST: ISAKMP: New peer created peer = 0x8642A214 peer_handle = 0x8000004E
Dec 11 23:59:02.514 EST: ISAKMP: Locking peer struct 0x8642A214, refcount 1 for isakmp_initiator
Dec 11 23:59:02.514 EST: ISAKMP: local port 500, remote port 500
Dec 11 23:59:02.518 EST: ISAKMP: set new node 0 to QM_IDLE
Dec 11 23:59:02.518 EST: ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa = 86933958
Dec 11 23:59:02.518 EST: ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
Dec 11 23:59:02.518 EST: ISAKMP:(0):Profile has no keyring, aborting key search
Dec 11 23:59:02.518 EST: ISAKMP:(0):Profile has no keyring, aborting host key search
Dec 11 23:59:02.518 EST: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
Dec 11 23:59:02.522 EST: ISAKMP:(0): constructed NAT-T vendor-07 ID
Dec 11 23:59:0
Dec 11 23:59:02.522 EST: ISAKMP:(0): constructed NAT-T vendor-03 ID
Dec 11 23:59:02.522 EST: ISAKMP:(0): constructed NAT-T vendor-02 ID
Dec 11 23:59:02.522 EST: ISAKMP:(0):Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
Dec 11 23:59:02.522 EST: ISAKMP:(0):Old State = IKE_READY New State = IKE_I_MM1

Dec 11 23:59:02.522 EST: ISAKMP:(0): beginning Main Mode exchange
Dec 11 23:59:02.522 EST: ISAKMP:(0): sending packet to <Hub-IP> my_port 500 peer_port 500 (I) MM_NO_STATE
Dec 11 23:59:02.522 EST: ISAKMP:(0):Sending an IKE IPv4 Packet.
Dec 11 23:59:02.534 EST: ISAKMP (0:0): received packet from <Hub-IP> dport 500 sport 500 Global (I) MM_NO_STATE
Dec 11 23:59:02.538 EST: ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Dec 11 23:59:02.538 EST: ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2

Dec 11 23:59:02.538 EST: ISAKMP:(0): processing SA payload. message ID = 0
Dec 11 23:59:02.538 EST: ISAKMP:(0): processing vendor id payload
Dec 11 23:59:02.542 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
Dec 11 23:59:02.542 EST: ISAKMP (0:0): vendor ID is NAT-T RFC 3947
Dec 11 23:59:02.542 EST: ISAKMP:(0):Profile has no keyring, aborting key search
Dec 11 23:59:02.542 EST: ISAKMP:(0):Profile has no keyring, aborting host key search
Dec 11 23:59:02.542 EST: ISAKMP : Looking for xauth in profile VPN-0
Dec 11 23:59:02.542 EST: ISAKMP:(0):Checking ISAKMP transform 1 against priority 3 policy
Dec 11 23:59:02.542 EST: ISAKMP: encryption 3DES-CBC
Dec 11 23:59:02.542 EST: ISAKMP: hash SHA
Dec 11 23:59:02.542 EST: ISAKMP: default group 2
Dec 11 23:59:02.542 EST: ISAKMP: auth RSA sig
Dec 11 23:59:02.542 EST: ISAKMP: life type in seconds
Dec 11 23:59:02.542 EST: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x7F
Dec 11 23:59:02.546 EST: ISAKMP:(0):atts are acceptable. Next payload is 0
Dec 11 23:59:02.546 EST: ISAKMP:(0):Acceptable atts:actual life: 0
Dec 11 23:59:02.546 EST: ISAKMP:(0):Acceptable atts:life: 0
Dec 11 23:59:02.546 EST: ISAKMP:(0):Fill atts in sa vpi_length:4
Dec 11 23:59:02.546 EST: ISAKMP:(0):Fill atts in sa life_in_seconds:86399
Dec 11 23:59:02.546 EST: ISAKMP:(0):Returning Actual lifetime: 86399
Dec 11 23:59:02.546 EST: ISAKMP:(0)::Started lifetime timer: 86399.

Dec 11 23:59:02.546 EST: ISAKMP:(0): processing vendor id payload
Dec 11 23:59:02.546 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
Dec 11 23:59:02.550 EST: ISAKMP (0:0): vendor ID is NAT-T RFC 3947
Dec 11 23:59:02.550 EST: ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Dec 11 23:59:02.550 EST: ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2
```

```

Dec 11 23:59:02.554 EST: ISAKMP (0:0): constructing CERT_REQ for issuer cn=ca.domain.null
Dec 11 23:59:02.554 EST: ISAKMP:(0): sending packet to <Hub-IP> my_port 500 peer_port 500 (I) MM_SA_SETUP
Dec 11 23:59:02.554 EST: ISAKMP:(0):Sending an IKE IPv4 Packet.
Dec 11 23:59:02.558 EST: ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Dec 11 23:59:02.558 EST: ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3

Dec 11 23:59:02.586 EST: ISAKMP (0:0): received packet from <Hub-IP> dport 500 sport 500 Global (I) MM_SA_SETUP
Dec 11 23:59:02.590 EST: ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Dec 11 23:59:02.590 EST: ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4

Dec 11 23:59:02.594 EST: ISAKMP:(0): processing KE payload. message ID = 0
Dec 11 23:59:02.838 EST: ISAKMP:(0): processing NONCE payload. message ID = 0
Dec 11 23:59:02.878 EST: ISAKMP:(1077): processing CERT_REQ payload. message ID = 0
Dec 11 23:59:02.878 EST: ISAKMP:(1077): peer wants a CT_X509_SIGNATURE cert
Dec 11 23:59:02.882 EST: ISAKMP:(1077): peer wants cert issued by cn=ca.domain.null CA common to both trusts
Dec 11 23:59:02.882 EST: ISAKMP: Examining profile list for trustpoint VPN-1
Dec 11 23:59:02.882 EST: ISAKMP: No matching found for VPN-1
Dec 11 23:59:02.882 EST: ISAKMP: Examining profile list for trustpoint VPN-0
Dec 11 23:59:02.882 EST: ISAKMP: Found matching profile for VPN-0 Correct
Dec 11 23:59:02.882 EST: Choosing trustpoint VPN-0 as issuer
Dec 11 23:59:02.882 EST: ISAKMP:(1077): processing vendor id payload
Dec 11 23:59:02.882 EST: ISAKMP:(1077): vendor ID is Unity
Dec 11 23:59:02.886 EST: ISAKMP:(1077): processing vendor id payload
Dec 11 23:59:02.886 EST: ISAKMP:(1077): vendor ID is DPD
Dec 11 23:59:02.886 EST: ISAKMP:(1077): processing vendor id payload
Dec 11 23:59:02.886 EST: ISAKMP:(1077): speaking to another IOS box!
Dec 11 23:59:02.886 EST: ISAKMP:received payload type 20
Dec 11 23:59:02.886 EST: ISAKMP:received payload type 20
Dec 11 23:59:02.886 EST: ISAKMP:(1077):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Dec 11 23:59:02.890 EST: ISAKMP:(1077):Old State = IKE_I_MM4 New State = IKE_I_MM4

Dec 11 23:59:02.890 EST: ISAKMP:(1077):Send initial contact
Dec 11 23:59:02.902 EST: ISAKMP:(1077):SA is doing RSA signature authentication using id type ID_FQDN
Dec 11 23:59:02.902 EST: ISAKMP (0:1077): ID payload
  next-payload : 6
  type          : 2
  FQDN name     : sp08-edg01.domain.null ~ Correct (spoke doesn't support label with self-identity command)
  protocol      : 17
  port          : 500
  length        : 30
Dec 11 23:59:02.902 EST: ISAKMP:(1077):Total payload length: 30
Dec 11 23:59:02.926 EST: ISAKMP (0:1077): constructing CERT payload for hostname=vpn-0.sp08-edg01.domain.null,ou=vpn-0,ou=wan,cn=vpn-0.sp08-edg01.domain.null Sending correct certificate
Dec 11 23:59:02.934 EST: ISAKMP:(1077): using the VPN-0 trustpoint's keypair to sign
Dec 11 23:59:03.134 EST: ISKAMP: growing send buffer from 1024 to 3072
Dec 11 23:59:03.138 EST: ISAKMP:(1077): sending packet to <Hub-IP> my_port 500 peer_port 500 (I) MM_KEY_EXCH
Dec 11 23:59:03.138 EST: ISAKMP:(1077):Sending an IKE IPv4 Packet.
Dec 11 23:59:03.142 EST: ISAKMP:(1077):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Dec 11 23:59:03.142 EST: ISAKMP:(1077):Old State = IKE_I_MM4 New State = IKE_I_MM5

Dec 11 23:59:03.178 EST: ISAKMP (0:1076): received packet from <Hub-IP> dport 500 sport 500 Global (I) MM_NO_STATE
Dec 11 23:59:03.226 EST: ISAKMP (0:1077): received packet from <Hub-IP> dport 500 sport 500 Global (I) MM_KEY_EXCH
Dec 11 23:59:03.234 EST: ISAKMP:(1077): processing ID payload. message ID = 0
Dec 11 23:59:03.234 EST: ISAKMP (0:1077): ID payload
  next-payload : 6
  type          : 2
  FQDN name     : vpn-0.hub-edg01.domain.null Correct
  protocol      : 17
  port          : 500
  length        : 36

```

Dec 11 23:59:03.234 EST: ISAKMP:(1077): processing CERT payload. message ID = 0  
Dec 11 23:59:03.234 EST: ISAKMP:(1077): processing a CT\_X509\_SIGNATURE cert  
Dec 11 23:59:03.246 EST: ISAKMP:(1077): peer's pubkey isn't cached  
Dec 11 23:59:03.246 EST: ISAKMP:(0): Creating CERT validation list: VPN-0,  
Dec 11 23:59:03.342 EST: ISAKMP:(1077): OU = wan  
Dec 11 23:59:03.346 EST: %CRYPTO-6-IKMP\_NO\_ID\_CERT\_FQDN\_MATCH: ID of vpn-0.hub-edg01.domain.null (type 2) and certificate fqdn with vpn-1.hub-edg01.domain.null Received Wrong Hub Certificate  
Dec 11 23:59:03.346 EST: %CRYPTO-6-IKMP\_NO\_ID\_CERT\_FQDN\_MATCH: ID of vpn-0.hub-edg01.domain.null (type 2) and certificate fqdn with vpn-1.hub-edg01.domain.null  
Dec 11 23:59:03.358 EST: ISAKMP:(0): certificate map matches VPN-1 profile Would like to see VPN-0  
Dec 11 23:59:03.358 EST: ISAKMP:(0): expected profile VPN-0 but matched VPN-1 exchange aborted  
Dec 11 23:59:03.358 EST: ISAKMP (0:1077): FSM action returned error: 2  
Dec 11 23:59:03.358 EST: ISAKMP:(1077):Input = IKE\_MESG\_FROM\_PEER, IKE\_MM\_EXCH  
Dec 11 23:59:03.358 EST: ISAKMP:(1077):Old State = IKE\_I\_MM5 New State = IKE\_I\_MM6  
  
Dec 11 23:59:03.358 EST: ISAKMP:(1077):peer does not do paranoid keepalives.  
  
Dec 11 23:59:03.362 EST: ISAKMP:(1077):deleting SA reason "IKMP\_ERR\_NO\_RETRANS" state (I) MM\_KEY\_EXCH (peer <Hub-IP>)  
Dec 11 23:59:03.362 EST: ISAKMP:(1077):Input = IKE\_MESG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
Dec 11 23:59:03.362 EST: ISAKMP:(1077):Old State = IKE\_I\_MM6 New State = IKE\_I\_MM6  
  
Dec 11 23:59:03.366 EST: ISAKMP:(1077):peer does not do paranoid keepalives.  
  
Dec 11 23:59:03.366 EST: ISAKMP (0:1077): FSM action returned error: 2  
Dec 11 23:59:03.366 EST: ISAKMP:(1077):Input = IKE\_MESG\_INTERNAL, IKE\_PROCESS\_ERROR  
Dec 11 23:59:03.366 EST: ISAKMP:(1077):Old State = IKE\_I\_MM6 New State = IKE\_I\_MM5  
  
Dec 11 23:59:03.366 EST: ISAKMP:(1077):deleting SA reason "IKMP\_ERR\_NO\_RETRANS" state (I) MM\_KEY\_EXCH (peer <Hub-IP>)  
Dec 11 23:59:03.370 EST: ISAKMP: Unlocking peer struct 0x8642A214 for isadb\_mark\_sa\_deleted(), count 0  
Dec 11 23:59:03.370 EST: ISAKMP: Deleting peer node by peer\_reap for <Hub-IP>: 8642A214  
Dec 11 23:59:03.370 EST: ISAKMP:(1077):deleting node -34960790 error FALSE reason "IKE deleted"  
Dec 11 23:59:03.374 EST: ISAKMP:(1077):Input = IKE\_MESG\_INTERNAL, IKE\_PHASE1\_DEL  
Dec 11 23:59:03.374 EST: ISAKMP:(1077):Old State = IKE\_I\_MM5 New State = IKE\_DEST\_SA  
  
Dec 11 23:59:23.366 EST: ISAKMP:(1076):purging node -723462747  
  
Dec 11 23:59:33.366 EST: ISAKMP:(1076):purging SA., sa=865CC264, delme=865CC264

*Note: Process keeps repeating.*