ISAKMP Debug - Hub

Dec 11 19:47:31.232 EST: ISAKMP (0): received packet from <Spoke-IP> dport 500 sport 500 Global (N) NEW SA
Dec 11 19:47:31.236 EST: ISAKMP: Created a peer struct for <Spoke-IP>, peer port 500
Dec 11 19:47:31.236 EST: ISAKMP: New peer created peer = 0x88557A64 peer_handle = 0x80000039
Dec 11 19:47:31.236 EST: ISAKMP: Locking peer struct 0x88557A64, refcount 1 for crypto_isakmp_process_block
Dec 11 19:47:31.236 EST: ISAKMP: local port 500, remote port 500
Dec 11 19:47:31.236 EST: ISAKMP:(0):insert sa successfully sa = 885570A0
Dec 11 19:47:31.236 EST: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Dec 11 19:47:31.236 EST: ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1

Dec 11 19:47:31.236 EST: ISAKMP:(0): processing SA payload. message ID = 0
Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
Dec 11 19:47:31.236 EST: ISAKMP (0): vendor ID is NAT-T RFC 3947
Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
Dec 11 19:47:31.236 EST: ISAKMP (0): vendor ID is NAT-T v7
Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID is NAT-T v3
Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID is NAT-T v2
Dec 11 19:47:31.236 EST: ISAKMP:(0):No pre-shared key with <Spoke-IP>!
Dec 11 19:47:31.236 EST: ISAKMP : Scanning profiles for xauth ... VPN-0 VPN-1
Dec 11 19:47:31.236 EST: ISAKMP:(0):Checking ISAKMP transform 1 against priority 3 policy
Dec 11 19:47:31.236 EST: ISAKMP: encryption 3DES-CBC
Dec 11 19:47:31.236 EST: ISAKMP: hash SHA
Dec 11 19:47:31.236 EST: ISAKMP: default group 2
Dec 11 19:47:31.236 EST: ISAKMP: auth RSA sig
Dec 11 19:47:31.236 EST: ISAKMP: life type in seconds
Dec 11 19:47:31.236 EST: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x7F
Dec 11 19:47:31.236 EST: ISAKMP:(0):atts are acceptable. Next payload is 3
Dec 11 19:47:31.236 EST: ISAKMP:(0):Acceptable atts:actual life: 0
Dec 11 19:47:31.236 EST: ISAKMP:(0):Acceptable atts:life: 0
Dec 11 19:47:31.236 EST: ISAKMP:(0):Fill atts in sa vpi_length:4
Dec 11 19:47:31.236 EST: ISAKMP:(0):Fill atts in sa life_in_seconds:86399
Dec 11 19:47:31.236 EST: ISAKMP:(0):Returning Actual lifetime: 86399
Dec 11 19:47:31.236 EST: ISAKMP:(0)::Started lifetime timer: 86399.

Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
Dec 11 19:47:31.236 EST: ISAKMP (0): vendor ID is NAT-T RFC 3947
Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 245 mismatch
Dec 11 19:47:31.236 EST: ISAKMP (0): vendor ID is NAT-T v7
Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 157 mismatch
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID is NAT-T v3
Dec 11 19:47:31.236 EST: ISAKMP:(0): processing vendor id payload
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID seems Unity/DPD but major 123 mismatch
Dec 11 19:47:31.236 EST: ISAKMP:(0): vendor ID is NAT-T v2
Dec 11 19:47:31.236 EST: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Dec 11 19:47:31.236 EST: ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM1

Dec 11 19:47:31.240 EST: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
Dec 11 19:47:31.240 EST: ISAKMP:(0): sending packet to <Spoke-IP> my_port 500 peer_port 500 (R) MM_SA_SETUP
Dec 11 19:47:31.240 EST: ISAKMP:(0):Sending an IKE IPv4 Packet.
Dec 11 19:47:31.240 EST: ISAKMP:(0):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Dec 11 19:47:31.240 EST: ISAKMP:(0):Old State = IKE_R_MM1 New State = IKE_R_MM2

Dec 11 19:47:31.268 EST: ISAKMP (0): received packet from <Spoke-IP> dport 500 sport 500 Global (R) MM_SA_SETUP
Dec 11 19:47:31.268 EST: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Dec 11 19:47:31.268 EST: ISAKMP:(0):Old State = IKE_R_MM2 New State = IKE_R_MM3

Dec 11 19:47:31.268 EST: ISAKMP:(0): processing KE payload. message ID = 0
Dec 11 19:47:31.292 EST: ISAKMP:(0): processing NONCE payload. message ID = 0
Dec 11 19:47:31.292 EST: ISAKMP:(2110): processing CERT_REQ payload. message ID = 0
Dec 11 19:47:31.292 EST: ISAKMP:(2110): peer wants a CT_X509_SIGNATURE cert
Dec 11 19:47:31.292 EST: ISAKMP:(2110): peer wants cert issued by cn=ca.domain.null CA common to both trusts
Dec 11 19:47:31.292 EST: Choosing trustpoint VPN-1 as issuer Would like to see VPN-0
Dec 11 19:47:31.292 EST: ISAKMP:(2110): processing vendor id payload
Dec 11 19:47:31.292 EST: ISAKMP:(2110): vendor ID is Unity
Dec 11 19:47:31.292 EST: ISAKMP:(2110): processing vendor id payload
Dec 11 19:47:31.292 EST: ISAKMP:(2110): vendor ID is DPD
Dec 11 19:47:31.292 EST: ISAKMP:(2110): processing vendor id payload
Dec 11 19:47:31.292 EST: ISAKMP:(2110): speaking to another IOS box!
Dec 11 19:47:31.292 EST: ISAKMP:received payload type 20
Dec 11 19:47:31.292 EST: ISAKMP (2110): His hash no match - this node outside NAT
Dec 11 19:47:31.292 EST: ISAKMP:received payload type 20
Dec 11 19:47:31.292 EST: ISAKMP (2110): No NAT Found for self or peer
Dec 11 19:47:31.292 EST: ISAKMP:(2110):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Dec 11 19:47:31.292 EST: ISAKMP:(2110):Old State = IKE_R_MM3 New State = IKE_R_MM3

Dec 11 19:47:31.296 EST: ISAKMP (2110): constructing CERT_REQ for issuer cn=ca.domain.null
Dec 11 19:47:31.296 EST: ISAKMP:(2110): sending packet to <Spoke-IP> my_port 500 peer_port 500 (R) MM_KEY_EXCH
Dec 11 19:47:31.296 EST: ISAKMP:(2110):Sending an IKE IPv4 Packet.
Dec 11 19:47:31.296 EST: ISAKMP:(2110):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Dec 11 19:47:31.296 EST: ISAKMP:(2110):Old State = IKE_R_MM3 New State = IKE_R_MM4

Dec 11 19:47:31.916 EST: ISAKMP (2110): received packet from <Spoke-IP> dport 500 sport 500 Global (R) MM_KEY_EXCH
Dec 11 19:47:31.920 EST: ISAKMP:(2110):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Dec 11 19:47:31.920 EST: ISAKMP:(2110):Old State = IKE_R_MM4 New State = IKE_R_MM5

Dec 11 19:47:31.920 EST: ISAKMP:(2110): processing ID payload. message ID = 0
Dec 11 19:47:31.920 EST: ISAKMP (2110): 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 19:47:31.920 EST: ISAKMP:(0):: peer matches *none* of the profiles
Dec 11 19:47:31.920 EST: ISAKMP:(2110): processing CERT payload. message ID = 0
Dec 11 19:47:31.920 EST: ISAKMP:(2110): processing a CT_X509_SIGNATURE cert
Dec 11 19:47:31.920 EST: ISAKMP:(2110): peer's pubkey is cached
Dec 11 19:47:31.924 EST: ISAKMP:(2110): OU = wan
Dec 11 19:47:31.924 EST: %CRYPTO-6-IKMP_NO_ID_CERT_FQDN_MATCH: ID of sp08-edg01.domain.null (type 2) and certificate fqdn with vpn-0.sp08-edg01.domain.null received correct certificate
Dec 11 19:47:31.924 EST: %CRYPTO-6-IKMP_NO_ID_CERT_FQDN_MATCH: ID of sp08-edg01.domain.null (type 2) and certificate fqdn with vpn-0.sp08-edg01.domain.null
Dec 11 19:47:31.928 EST: ISAKMP:(0): certificate map matches VPN-0 profile
Dec 11 19:47:31.928 EST: ISAKMP:(0): Trying to re-validate CERT using new profile
Dec 11 19:47:31.928 EST: ISAKMP:(0): Creating CERT validation list: VPN-0, attempt to reset validated peer object for session 1

Dec 11 19:47:31.948 EST: ISAKMP:(0): CERT validity confirmed.
Dec 11 19:47:31.948 EST: ISAKMP:(2110):Profile has no keyring, aborting key search
Dec 11 19:47:31.948 EST: ISAKMP:(2110): processing SIG payload. message ID = 0
Dec 11 19:47:31.948 EST: ISAKMP:(2110): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 885570A0
Dec 11 19:47:31.948 EST: ISAKMP:(2110):SA authentication status:
authenticated
Dec 11 19:47:31.948 EST: ISAKMP:(2110):SA has been authenticated with <Spoke-IP>
Dec 11 19:47:31.948 EST: ISAKMP:(2110):SA authentication status:
authenticated
Dec 11 19:47:31.948 EST: ISAKMP:(2110): Process initial contact,
bring down existing phase 1 and 2 SA's with local <Hub-IP> remote <Spoke-IP> remote port 500
Dec 11 19:47:31.948 EST: ISAKMP: Trying to insert a peer <Hub-IP>/<Spoke-IP>/500/, and inserted successfully 88557A64.
Dec 11 19:47:31.948 EST: ISAKMP:(2110):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Dec 11 19:47:31.948 EST: ISAKMP:(2110):Old State = IKE_R_MM5 New State = IKE_R_MM5

Dec 11 19:47:31.952 EST: ISAKMP:(2110):SA is doing RSA signature authentication using id type ID_FQDN
Dec 11 19:47:31.952 EST: ISAKMP (2110): ID payload
next-payload : 6
type : 2
FQDN name : **vpn-0**.hub-edg01.domain.null Correct Hub Identity
protocol : 17
port : 500
length : 36
Dec 11 19:47:31.952 EST: ISAKMP:(2110):Total payload length: 36
Dec 11 19:47:31.956 EST: ISAKMP (2110): constructing CERT payload for serialNumber=<removed>+hostname=**vpn-1**.hub-edg01.domain.null,ou=vpn-1,ou=wan,cn=vpn-1.hub-edg01.domain.null Sending wrong certificate
Dec 11 19:47:31.956 EST: ISAKMP:(2110): using the VPN-1 trustpoint's keypair to sign Would like to see VPN-0
Dec 11 19:47:31.996 EST: ISKAMP: growing send buffer from 1024 to 3072
Dec 11 19:47:32.000 EST: ISAKMP:(2110): sending packet to <Spoke-IP> my_port 500 peer_port 500 (R) MM_KEY_EXCH
Dec 11 19:47:32.000 EST: ISAKMP:(2110):Sending an IKE IPv4 Packet.
Dec 11 19:47:32.000 EST: ISAKMP:(2110):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Dec 11 19:47:32.000 EST: ISAKMP:(2110):Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

Dec 11 19:47:32.000 EST: ISAKMP:(2110):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

Dec 11 19:47:32.000 EST: ISAKMP:(2110):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

Note: The NHRP Server (local) is supposed to construct a certificate payload for "vpn-0.hub-edg01.domain.null", correctly identified above, but instead constructs a payload for "vpn-1.hub-edg01.domain.null", which is mapped to a different ISAKMP Profile (VPN-1) via the self-identity command.

Note: Process keeps repeating.