Dec 21 20:35:14 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:14 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { e6e9e2bb a05d5b04 - b1c0418c 87d2cdd8 } / 0a42aa2f, remote = 50.208.33.177:500

Dec 21 20:35:14 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Not found SA = { e6e9e2bb a05d5b04 - b1c0418c 87d2cdd8 }

Dec 21 20:35:14 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find\_half: Not found half SA = { e6e9e2bb a05d5b04 - 00000000 00000000 }

Dec 21 20:35:14 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Invalid cookie, no sa found, SA = { e6e9e2bb a05d5b04 - b1c0418c 87d2cdd8 } / 0a42aa2f, remote = 50.208.33.177:500

Dec 21 20:35:14 [64.13.163.35 <-> 50.208.33.177] iked\_pv\_audit\_callback: Empty SSH audit event

Dec 21 20:35:14 [64.13.163.35 <-> 50.208.33.177] unknown (unknown) <-> unknown { unknown [unknown] / unknown } unknown; Packet to unknown Isakmp SA, ip = 50.208.33.177:500

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Received IKE Trigger message with local\_gw\_addr = 64.13.163.35 remote\_gw\_addr = 50.208.33.177

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] In iked\_async\_ike\_trigger\_msg\_handler; Tunnel = 12

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Triggering the IKE negotiation ....

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Triggering negotiation for INSTANCE-hq\_0012\_0015\_0000 config block

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_trigger\_callback: non-natt case for gateway hq, lookup peer entry from local\_port=0, remote\_port=500.

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_fetch\_or\_create\_peer\_entry: Create peer entry 0xc38200 for local 64.13.163.35:500 remote 50.208.33.177:500. gw hq, VR id 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_trigger\_callback: FOUND non-natt peer entry for gateway hq

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Initiating new P1 SA for gateway hq

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] P1 SA 194155 start timer. timer duration 30, reason 1.

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_peer\_insert\_p1sa\_entry: Insert p1 sa 194155 in peer entry 0xc38200

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_alloc: Allocated fallback negotiation c4e800

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ike\_spd\_notify\_request: Sending Initial contact

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] IKE SA fill called for negotiation of local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect: Start, remote\_name = 50.208.33.177:500, xchg = 2, flags = 00090000

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_allocate: Start, SA = { d1babaef cf1facac - 00000000 00000000 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_init\_isakmp\_sa: Start, remote = 50.208.33.177:500, initiator = 1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect: SA = { d1babaef cf1facac - 00000000 00000000}, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = Start sa negotiation I (1)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_sa\_proposal: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_isakmp\_vendor\_ids: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM SA I (3)

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0xd1babaef cf1facac - 00000000 00000000 } / 00000000, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 284

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { d1babaef cf1facac - 00000000 00000000}, nego = -1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Not found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 00000000, remote = 50.208.33.177:500

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Not found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find\_half: Found half SA = { d1babaef cf1facac - 00000000 00000000 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: We are intiator, first response packet

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_upgrade: Start, SA = { d1babaef cf1facac - 00000000 00000000 } -> { ... - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8} / 00000000, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_payload\_sa: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_payload\_sa: Found 1 proposals

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_payload\_t: Start, # trans = 1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = MM SA I (3)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_sa\_value: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cr: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cert: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_vid: VID[0..16] = afcad713 68a1f1c9 ...

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_vid: VID[0..16] = 4a131c81 07035845 ...

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_vid: VID[0..28] = 69936922 8741c6d4 ...

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_private: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_ke: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_get\_group: DH Group 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_generate\_sync: Requested DH group 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_generate\_sync: Generated DH keys using hardware for DH group 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_generate\_async: DH Generate Secs [0] USecs [5296]

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_generate\_async: Generated DH using hardware

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_nonce: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_isakmp\_nonce\_data\_len: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM KE I (5)

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0xd1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 00000000, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 228

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = -1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 00000000, remote = 50.208.33.177:500

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8} / 00000000, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = MM KE I (5)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_nonce: Start, nonce[0..16] = ee61523b ca58c99e ...

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_ke: Ke[0..128] = 4a03ae8a 65ba28e9 ...

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cr: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cert: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_private: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_id: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_hash: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_get\_group: DH Group 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_compute\_synch: Requested DH group 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_final\_async: DH Compute Secs [0] USecs [4988]

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_final\_async: Computed DH using hardware

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_find\_pre\_shared\_key: Find pre shared key key for 64.13.163.35:500, id = fqdn(any:0,[0..27]=srx240-02.ahprod.adhaven.com) -> 50.208.33.177:500, id = No Id

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_find\_pre\_shared\_key: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_calc\_mac: Start, initiator = true, local = true

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_status\_n: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_encrypt: Marking encryption for packet

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM final I (7)

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0xd1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 00000000, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Encrypting packet

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 116

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = -1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 00000000, remote = 50.208.33.177:500

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8} / 00000000, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Decrypting packet

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = MM final I (7)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_encrypt: Check that packet was encrypted succeeded

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_id: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_hash: Start, hash[0..20] = e46e58aa 8795b58b ...

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_calc\_mac: Start, initiator = true, local = false

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cert: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_private: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_wait\_done: Marking for waiting for done

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_all\_done: MESSAGE: Phase 1 { 0xd1babaef cf1facac - 0x0c3ea32b 96d2b0e8 } / 00000000, version = 1.0, xchg = Identity protect, auth\_method = Pre shared keys, Initiator, cipher = 3des-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 86400 sec, key l

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM done I (9)

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_send\_notify: Connected, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_process\_packet: No output packet, returning

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ike\_sa\_done: local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_id\_validate id NOT matched.

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] P1 SA 194155 stop timer. timer duration 30, reason 1.

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] P1 SA 194155 start timer. timer duration 0, reason 3.

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ipsec\_spi\_allocate: local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Added (spi=0x198f07ec, protocol=0) entry to the spi table

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ipsec\_spi\_allocate: local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Added (spi=0x42a47a67, protocol=0) entry to the spi table

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect\_ipsec: Start, remote\_name = :500, flags = 00000000

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find\_ip\_port: Remote = all:500, Found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Found slot 0, max 1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect\_ipsec: SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_init\_qm\_negotiation: Start, initiator = 1, message\_id = 0be56b24

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = Start QM I (14)/-1, exchange = 32, auth\_method = phase1, Initiator

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_hash\_1: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_sa\_proposals: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_nonce: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_qm\_nonce\_data\_len: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_optional\_ke: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_optional\_ids: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_qm\_optional\_id: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_qm\_optional\_id: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Construction NHTB payload for local:64.13.163.35, remote:50.208.33.177 IKEv1 P1 SA index 194155 sa-cfg INSTANCE-hq\_0012\_0015\_0000

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Not route based VPN. Not sending NHTB notify payload for sa-cfg INSTANCE-hq\_0012\_0015\_0000

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_encrypt: Marking encryption for packet

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = QM HASH SA I (16)

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0xd1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 0be56b24, nego = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_finalize\_qm\_hash\_1: Hash[0..20] = 8c283b70 edf01b6b ...

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Encrypting packet

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 156

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = 0, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] P1 SA 194155 timer expiry. ref cnt 2, timer reason Defer delete timer expired (3), flags 0x130.

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] Initiate IKE P1 SA 194155 delete. curr ref count 2, del flags 0x2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ike\_sa\_delete\_notify\_done\_cb: For p1 sa index 194155, ref cnt 2, status: Error ok

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_expire\_callback: Start, expire SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Found slot 1, max 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_init\_info\_exchange: Created random message id = 24bb2db2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_init\_info\_exchange: Phase 1 done, use HASH and N or D payload

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0xd1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 24bb2db2, nego = 1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Encrypting packet

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 84

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_expire\_callback: Sending notification to 50.208.33.177:500

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = 1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_delete\_negotiation: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = 1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation\_info: Start, nego = 1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation: Start, nego = 1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_remove\_callback: Start, delete SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_delete\_negotiation: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8}, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_tunnel\_table\_entry\_delete: Deleting tunnel\_id: 0 from IKE tunnel table

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_tunnel\_table\_entry\_delete: The tunnel id: 0 doesn't exist in IKE tunnel table

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_delete: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation\_qm: Start, nego = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation: Start, nego = 0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 4

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 4

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation\_isakmp: Start, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation: Start, nego = -1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_fb\_isakmp\_sa\_freed: Received notification from the ISAKMP library that the IKE SA c39000 is freed

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] IKE SA delete called for p1 sa 194155 (ref cnt 2) local:64.13.163.35, remote:50.208.33.177, IKEv1

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] P1 SA 194155 stop timer. timer duration 0, reason 0.

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_del\_ha\_blob: Error deleting blob with type = phase1 mod, tunnel id 0. Error: No such file or directory

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_del\_ha\_blob: Error deleting blob with type = phase1, tunnel id 0. Error: No such file or directory

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] P1 SA 194155 reference count is not zero (1). Delaying deletion of SA

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 2

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_free\_sa: Start

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Freeing fallback negotiation c4e800

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_p1\_sa\_destroy: p1 sa 194155 (ref cnt 0), waiting\_for\_del 0xc3c0c0

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_peer\_remove\_p1sa\_entry: Remove p1 sa 194155 from peer entry 0xc38200

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_peer\_entry\_patricia\_delete:Peer entry c38200 deleted for local 64.13.163.35:1f4 and remote 50.208.33.177:1f4

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Not found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 0be56b24, remote = 50.208.33.177:500

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Not found SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find\_half: Not found half SA = { d1babaef cf1facac - 00000000 00000000 }

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Invalid cookie, no sa found, SA = { d1babaef cf1facac - 0c3ea32b 96d2b0e8 } / 0be56b24, remote = 50.208.33.177:500

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] iked\_pv\_audit\_callback: Empty SSH audit event

Dec 21 20:35:24 [64.13.163.35 <-> 50.208.33.177] unknown (unknown) <-> unknown { unknown [unknown] / unknown } unknown; Packet to unknown Isakmp SA, ip = 50.208.33.177:500

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] Received IKE Trigger message with local\_gw\_addr = 64.13.163.35 remote\_gw\_addr = 50.208.33.177

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] In iked\_async\_ike\_trigger\_msg\_handler; Tunnel = 12

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] Triggering the IKE negotiation ....

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] Triggering negotiation for INSTANCE-hq\_0012\_0015\_0000 config block

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_trigger\_callback: non-natt case for gateway hq, lookup peer entry from local\_port=0, remote\_port=500.

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_fetch\_or\_create\_peer\_entry: Create peer entry 0xc38a00 for local 64.13.163.35:500 remote 50.208.33.177:500. gw hq, VR id 0

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_trigger\_callback: FOUND non-natt peer entry for gateway hq

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] Initiating new P1 SA for gateway hq

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] P1 SA 194156 start timer. timer duration 30, reason 1.

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_peer\_insert\_p1sa\_entry: Insert p1 sa 194156 in peer entry 0xc38a00

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_alloc: Allocated fallback negotiation c4e800

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ike\_spd\_notify\_request: Sending Initial contact

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] IKE SA fill called for negotiation of local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect: Start, remote\_name = 50.208.33.177:500, xchg = 2, flags = 00090000

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_allocate: Start, SA = { 2b7a7afe a6793497 - 00000000 00000000 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_init\_isakmp\_sa: Start, remote = 50.208.33.177:500, initiator = 1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect: SA = { 2b7a7afe a6793497 - 00000000 00000000}, nego = -1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = Start sa negotiation I (1)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_sa\_proposal: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_isakmp\_vendor\_ids: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM SA I (3)

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0x2b7a7afe a6793497 - 00000000 00000000 } / 00000000, nego = -1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 284

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { 2b7a7afe a6793497 - 00000000 00000000}, nego = -1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Not found SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 } / 00000000, remote = 50.208.33.177:500

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Not found SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find\_half: Found half SA = { 2b7a7afe a6793497 - 00000000 00000000 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: We are intiator, first response packet

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_upgrade: Start, SA = { 2b7a7afe a6793497 - 00000000 00000000 } -> { ... - 3e3152b1 90315092 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092} / 00000000, nego = -1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_payload\_sa: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_payload\_sa: Found 1 proposals

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_payload\_t: Start, # trans = 1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = MM SA I (3)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_sa\_value: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cr: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cert: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_vid: VID[0..16] = afcad713 68a1f1c9 ...

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_vid: VID[0..16] = 4a131c81 07035845 ...

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_vid: VID[0..28] = 69936922 8741c6d4 ...

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_private: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_ke: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_get\_group: DH Group 2

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_generate\_sync: Requested DH group 2

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_generate\_sync: Generated DH keys using hardware for DH group 2

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_generate\_async: DH Generate Secs [0] USecs [4693]

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_generate\_async: Generated DH using hardware

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_nonce: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_isakmp\_nonce\_data\_len: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM KE I (5)

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0x2b7a7afe a6793497 - 3e3152b1 90315092 } / 00000000, nego = -1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 228

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = -1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 } / 00000000, remote = 50.208.33.177:500

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092} / 00000000, nego = -1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = MM KE I (5)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_nonce: Start, nonce[0..16] = 954751a5 37bded35 ...

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_ke: Ke[0..128] = f76dc75d 6d861160 ...

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cr: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cert: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_private: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_id: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_hash: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_get\_group: DH Group 2

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] iked\_dh\_compute\_synch: Requested DH group 2

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_final\_async: DH Compute Secs [0] USecs [4373]

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] juniper\_dlp\_diffie\_hellman\_final\_async: Computed DH using hardware

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_find\_pre\_shared\_key: Find pre shared key key for 64.13.163.35:500, id = fqdn(any:0,[0..27]=srx240-02.ahprod.adhaven.com) -> 50.208.33.177:500, id = No Id

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_find\_pre\_shared\_key: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_calc\_mac: Start, initiator = true, local = true

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_status\_n: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_encrypt: Marking encryption for packet

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM final I (7)

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0x2b7a7afe a6793497 - 3e3152b1 90315092 } / 00000000, nego = -1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Encrypting packet

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 116

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = -1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ikev2\_packet\_v1\_start: Passing IKE v1.0 packet to IKEv1 library

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_get\_sa: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 } / 00000000, remote = 50.208.33.177:500

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find: Found SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 }

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092} / 00000000, nego = -1

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_decode\_packet: Decrypting packet

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = MM final I (7)/-1, exchange = 2, auth\_method = pre shared key, Initiator

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_encrypt: Check that packet was encrypted succeeded

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_id: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_hash: Start, hash[0..20] = 3c864238 3fc08b3d ...

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_calc\_mac: Start, initiator = true, local = false

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_cert: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_i\_private: Start

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_wait\_done: Marking for waiting for done

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_all\_done: MESSAGE: Phase 1 { 0x2b7a7afe a6793497 - 0x3e3152b1 90315092 } / 00000000, version = 1.0, xchg = Identity protect, auth\_method = Pre shared keys, Initiator, cipher = 3des-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 86400 sec, key l

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = MM done I (9)

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:34 [64.13.163.35 <-> 50.208.33.177] ike\_send\_notify: Connected, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = -1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_process\_packet: No output packet, returning

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ike\_sa\_done: local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_id\_validate id NOT matched.

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] P1 SA 194156 stop timer. timer duration 30, reason 1.

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] P1 SA 194156 start timer. timer duration 0, reason 3.

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ipsec\_spi\_allocate: local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Added (spi=0x58e45da2, protocol=0) entry to the spi table

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ipsec\_spi\_allocate: local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Added (spi=0x3ad0aa7a, protocol=0) entry to the spi table

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Parsing notification payload for local:64.13.163.35, remote:50.208.33.177 IKEv1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect\_ipsec: Start, remote\_name = :500, flags = 00000000

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_find\_ip\_port: Remote = all:500, Found SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Found slot 0, max 1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_connect\_ipsec: SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = 0

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_init\_qm\_negotiation: Start, initiator = 1, message\_id = 5288cf4e

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: Current state = Start QM I (14)/-1, exchange = 32, auth\_method = phase1, Initiator

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_hash\_1: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_sa\_proposals: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_nonce: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_qm\_nonce\_data\_len: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_optional\_ke: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_qm\_optional\_ids: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_qm\_optional\_id: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_qm\_optional\_id: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_private: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Construction NHTB payload for local:64.13.163.35, remote:50.208.33.177 IKEv1 P1 SA index 194156 sa-cfg INSTANCE-hq\_0012\_0015\_0000

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Not route based VPN. Not sending NHTB notify payload for sa-cfg INSTANCE-hq\_0012\_0015\_0000

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_policy\_reply\_private\_payload\_out: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_st\_o\_encrypt: Marking encryption for packet

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_state\_step: All done, new state = QM HASH SA I (16)

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0x2b7a7afe a6793497 - 3e3152b1 90315092 } / 5288cf4e, nego = 0

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_finalize\_qm\_hash\_1: Hash[0..20] = 4b26cf84 3023eb50 ...

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Encrypting packet

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 156

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = 0, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] P1 SA 194156 timer expiry. ref cnt 2, timer reason Defer delete timer expired (3), flags 0x130.

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] Initiate IKE P1 SA 194156 delete. curr ref count 2, del flags 0x2

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_ike\_sa\_delete\_notify\_done\_cb: For p1 sa index 194156, ref cnt 2, status: Error ok

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_expire\_callback: Start, expire SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = -1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_alloc\_negotiation: Found slot 1, max 2

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_init\_info\_exchange: Created random message id = 1dba916f

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_init\_info\_exchange: Phase 1 done, use HASH and N or D payload

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Start, SA = { 0x2b7a7afe a6793497 - 3e3152b1 90315092 } / 1dba916f, nego = 1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Encrypting packet

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_encode\_packet: Final length = 84

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_expire\_callback: Sending notification to 50.208.33.177:500

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_send\_packet: Start, send SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = 1, dst = 50.208.33.177:500, routing table id = 0

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_delete\_negotiation: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = 1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation\_info: Start, nego = 1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation: Start, nego = 1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_remove\_callback: Start, delete SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = -1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_delete\_negotiation: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092}, nego = -1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_tunnel\_table\_entry\_delete: Deleting tunnel\_id: 0 from IKE tunnel table

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ssh\_ike\_tunnel\_table\_entry\_delete: The tunnel id: 0 doesn't exist in IKE tunnel table

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_sa\_delete: Start, SA = { 2b7a7afe a6793497 - 3e3152b1 90315092 }

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation\_qm: Start, nego = 0

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation: Start, nego = 0

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Fallback negotiation c4e800 has still 1 references

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 4

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 4

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation\_isakmp: Start, nego = -1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_negotiation: Start, nego = -1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ikev2\_fb\_isakmp\_sa\_freed: Received notification from the ISAKMP library that the IKE SA c39000 is freed

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] IKE SA delete called for p1 sa 194156 (ref cnt 2) local:64.13.163.35, remote:50.208.33.177, IKEv1

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] P1 SA 194156 stop timer. timer duration 0, reason 0.

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_del\_ha\_blob: Error deleting blob with type = phase1 mod, tunnel id 0. Error: No such file or directory

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_del\_ha\_blob: Error deleting blob with type = phase1, tunnel id 0. Error: No such file or directory

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] P1 SA 194156 reference count is not zero (1). Delaying deletion of SA

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 2

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_id\_payload: Start, id type = 2

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ike\_free\_sa: Start

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] ikev2\_fallback\_negotiation\_free: Freeing fallback negotiation c4e800

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_pm\_p1\_sa\_destroy: p1 sa 194156 (ref cnt 0), waiting\_for\_del 0xc52100

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_peer\_remove\_p1sa\_entry: Remove p1 sa 194156 from peer entry 0xc38a00

Dec 21 20:35:35 [64.13.163.35 <-> 50.208.33.177] iked\_peer\_entry\_patricia\_delete:Peer entry c38a00 deleted for local 64.13.163.35:1f4 and remote 50.208.33.177:1f4