Hi,

it looks there is a problem with DPD or interoperability. Always after an IKE and SA is established, I got an error on the AVM IKE Server.

    fehlerhafte Paketlaenge: Hdr-length > read-Data

-> meaning wrong packet length

So I started debugging on this. As you can see in the tcpdump, the packet sent at 16:39:14.929827 has 16 bytes less than the other packets. I do not have an explanation for this, that is why I added a debug log of strongswan. Perhaps it has to do with the new SA created in that moment and the dpd job does not already know it and sends "empty" instead.

Consequences:
This results in an unstable VPN connection if I do not add a rightip to this conn (which may result in strongswan setting up the connection). But the strongswan gateway should only act as a responder, not as an initiator.

Please help,

André

If more details are needed, I will provide any information.

Log of Fritzbox

2013-09-09 16:34:03 avmike:marcant: Phase 2 ready
2013-09-09 16:34:03 avmike:< cb_sa_created(name=marcant,id=160,...,flags=0x00002001)
2013-09-09 16:34:03 avmike:marcant: start waiting connections
2013-09-09 16:34:03 avmike:marcant: NO waiting connections
2013-09-09 16:39:14 avmike:marcant
    fehlerhafte Paketlaenge: Hdr-length > read-Data

tcpdump on charon side

16:37:35.421216 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 120) 
   strongswan-server.net.isakmp > avmclient.net.isakmp: [bad udp cksum 788a!] isakmp 1.0 msgid e976c4c5 cookie 4dad7d9ab6375f48->12a805313f7b7287: phase 2/others I inf[E]: [encrypted hash]
16:39:14.929827 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 104) 
   strongswan-server.net.isakmp > avmclient.net.isakmp: [bad udp cksum 15c3!] isakmp 1.0 msgid 8440d00c cookie 4dad7d9ab6375f48->12a805313f7b7287: phase 2/others I inf[E]: [encrypted hash]
16:39:35.485101 IP (tos 0x0, ttl 53, id 29272, offset 0, flags [none], proto UDP (17), length 120) 
   avmclient.net.isakmp > strongswan-server.net.isakmp: [udp sum ok] isakmp 1.0 msgid 69079b39 cookie 4dad7d9ab6375f48->12a805313f7b7287: phase 2/others R inf[E]: [encrypted hash]
16:39:35.490312 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 120) 
   strongswan-server.net.isakmp > avmclient.net.isakmp: [bad udp cksum 9fa!] isakmp 1.0 msgid f2b
Sep 9 16:39:14 rossini charon: 09[MGR] checkout IKE_SA by ID
Sep 9 16:39:14 rossini charon: 14[KNL] received a XFRM_MSG_EXPIRE
Sep 9 16:39:14 rossini charon: 14[KNL] creating delete job for ESP CHILD_SA with SPI c779dcad and
reqid {1}
Sep 9 16:39:14 rossini charon: 09[MGR] checkout IKE_SA by ID
Sep 9 16:39:14 rossini charon: 09[IKE] queueing QUICK_DELETE task
Sep 9 16:39:14 rossini charon: 09[MGR] checkout IKE_SA by ID
Sep 9 16:39:14 rossini charon: 09[IKE] activating QUICK_DELETE task
Sep 9 16:39:14 rossini charon: 09[IKE] closing expired CHILD_SA rw-test1{1} with SPIs c779dcad_i3386db66_o and
TS 0.0.0.0/0 === 192.168.200.0/24
Sep 9 16:39:14 rossini charon: 09[KNL] deleting SAD entry with SPI c779dcad  (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] sending XFRM_MSG_DELSA: => 40 bytes @ 0x7f70106157a0
.......
Sep 9 16:39:14 rossini charon: 09[KNL] deleting policy 0.0.0.0/0 === 192.168.200.0/24 out  (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:14 rossini charon: 09[KNL] updating policy 0.0.0.0/0 === 192.168.200.0/24 out  (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] sending XFRM_MSG_UPDPOLICY: => 252 bytes @ 0x7f7010615210
.......
Sep 9 16:39:14 rossini charon: 09[KNL] deleting policy 192.168.200.0/24 === 0.0.0.0/0 in  (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:14 rossini charon: 09[KNL] updating policy 192.168.200.0/24 === 0.0.0.0/0 in (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] sending XFRM_MSG_UPDPOLICY: => 252 bytes @ 0x7f7010615210
Sep 9 16:39:14 rossini charon: 09[KNL] sending XFRM_MSG_UPDPOLICY: => 252 bytes @ 0x7f7010615210
Sep 9 16:39:14 rossini charon: 09[KNL] deleting policy 192.168.200.0/24 === 0.0.0.0/0 fwd (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:14 rossini charon: 09[KNL] updating policy 192.168.200.0/24 === 0.0.0.0/0 in (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] sending XFRM_MSG_UPDPOLICY: => 252 bytes @ 0x7f7010615210
Sep 9 16:39:14 rossini charon: 09[KNL] 208: 32 00 00 00 02 00 00 00 4E 31 E1 28 00 00 00 02 00 00 00 4E 31 E1 28 00 00 00 02 00 00 00 4E 31 E1 28 00 00 00 02 00 00 00 4E 31 E1 28 00 00 00 02 00 00 00

Sep 9 16:39:14 rossini charon: 09[KNL] 224: 00 00 00 00 00 00 00 00 01 00 00 00 01 00 00 00

Sep 9 16:39:14 rossini charon: 09[KNL] 240: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Sep 9 16:39:14 rossini charon: 09[KNL] getting a local address in traffic selector 0.0.0.0/0
Sep 9 16:39:14 rossini charon: 09[KNL] using host %any
Sep 9 16:39:14 rossini charon: 09[KNL] 217.14.X.Y is on interface bond0.11
Sep 9 16:39:14 rossini charon: 09[KNL] deleting policy 0.0.0.0/0 === 192.168.200.0/24 out (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:14 rossini charon: 09[KNL] deleting policy 192.168.200.0/24 === 0.0.0.0/0 in (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:14 rossini charon: 09[KNL] deleting policy 192.168.200.0/24 === 0.0.0.0/0 fwd (mark 0/0x00000000)
Sep 9 16:39:14 rossini charon: 09[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:14 rossini charon: 09[IKE] sending DELETE for ESP CHILD_SA with SPI c779dcad
Sep 9 16:39:28 rossini charon: 05[MGR] checkout IKE_SA by ID
Sep 9 16:39:28 rossini charon: 05[KNL] querying policy 192.168.200.0/24 === 0.0.0.0/0 in (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f7012e198a0
Sep 9 16:39:28 rossini charon: 05[KNL] 0: 50 00 00 00 15 00 01 00 99 9C 01 00 E6 1C 00 00

Sep 9 16:39:28 rossini charon: 05[KNL] querying policy 192.168.200.0/24 === 0.0.0.0/0 fwd (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f7012e198a0
Sep 9 16:39:28 rossini charon: 05[KNL] 0: 50 00 00 00 15 00 01 00 9A 9C 01 00 E6 1C 00 00

Sep 9 16:39:28 rossini charon: 05[KNL] querying policy 0.0.0.0/0 === 192.168.200.0/24 out (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f7012e198a0
Sep 9 16:39:28 rossini charon: 05[KNL] 0: 50 00 00 00 15 00 01 00 9B 9C 01 00 E6 1C 00 00

Sep 9 16:39:28 rossini charon: 05[KNL] querying policy 0.0.0.0/0 fwd (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f7012e198a0
Sep 9 16:39:28 rossini charon: 05[KNL] 0: 50 00 00 00 15 00 01 00 9A 9C 01 00 E6 1C 00 00

Sep 9 16:39:28 rossini charon: 05[KNL] querying policy 0.0.0.0/0 === 192.168.200.0/24 out (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f7012e198a0
Sep 9 16:39:28 rossini charon: 05[KNL] 0: 50 00 00 00 15 00 01 00 9B 9C 01 00 E6 1C 00 00

Sep 9 16:39:28 rossini charon: 05[KNL] querying policy 0.0.0.0/0 fwd (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f7012e198a0
Sep 9 16:39:28 rossini charon: 05[KNL] 0: 50 00 00 00 15 00 01 00 9A 9C 01 00 E6 1C 00 00

Sep 9 16:39:28 rossini charon: 05[KNL] deleting policy 0.0.0.0/0 === 192.168.200.0/24 out (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:28 rossini charon: 05[KNL] deleting policy 192.168.200.0/24 === 0.0.0.0/0 in (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:28 rossini charon: 05[KNL] deleting policy 192.168.200.0/24 === 0.0.0.0/0 fwd (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] policy still used by another CHILD_SA, not removed
Sep 9 16:39:28 rossini charon: 05[IKE] generating INFORMATIONAL_V1 request 2218840076 [ HASH D ]
Sep 9 16:39:28 rossini charon: 05[IKE] insert payload HASH_V1 into encrypted payload
Sep 9 16:39:28 rossini charon: 05[IKE] insert payload DELETE_V1 into encrypted payload
Sep 9 16:39:28 rossini charon: 05[MGR] checkout IKE_SA by ID
Sep 9 16:39:28 rossini charon: 05[KNL] querying policy 192.168.200.0/24 === 0.0.0.0/0 in (mark 0/0x00000000)
Sep 9 16:39:28 rossini charon: 05[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f7012e198a0
Sep 9 16:39:28 rossini charon: 05[KNL] 0: 50 00 00 00 15 00 01 00 99 9C 01 00 E6 1C 00 00
Sep 9 16:39:28 rossini charon: 05[KNL] 48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:28 rossini charon: 05[KNL] 64: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...


Sep 9 16:39:29 rossini charon: 04[MGR] checkout IKE_SA by ID

Sep 9 16:39:29 rossini charon: 04[KNL] querying policy 192.168.200.0/24 ==> 0.0.0.0/0 in (mark 0 /0x00000000)
Sep 9 16:39:29 rossini charon: 04[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f701381a8a0
Sep 9 16:39:29 rossini charon: 04[KNL] 0: 50 00 00 00 15 00 01 00 9C 9C 01 00 E6 1C 00 00 P...

Sep 9 16:39:29 rossini charon: 04[KNL] 16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 32: C0 A8 C8 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 48: 00 00 00 00 00 00 00 00 02 00 00 18 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 64: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] querying policy 192.168.200.0/24 ==> 0.0.0.0/0 fwd (mark 0 /0x00000000)
Sep 9 16:39:29 rossini charon: 04[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f701381a8a0
Sep 9 16:39:29 rossini charon: 04[KNL] 0: 50 00 00 00 15 00 01 00 9D 9C 01 00 E6 1C 00 00 P...

Sep 9 16:39:29 rossini charon: 04[KNL] 16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 32: C0 A8 C8 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 64: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] querying policy 0.0.0.0/0 ==> 192.168.200.0/24 out (mark 0 /0x00000000)
Sep 9 16:39:29 rossini charon: 04[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f701381a8a0
Sep 9 16:39:29 rossini charon: 04[KNL] 0: 50 00 00 00 15 00 01 00 9E 9C 01 00 E6 1C 00 00 P...

Sep 9 16:39:29 rossini charon: 04[KNL] 16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 32: C0 A8 C8 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 04[KNL] 64: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...


Sep 9 16:39:29 rossini charon: 11[MGR] checkout IKE_SA by ID

Sep 9 16:39:29 rossini charon: 11[KNL] querying policy 192.168.200.0/24 ==> 0.0.0.0/0 in (mark 0 /0x00000000)
Sep 9 16:39:29 rossini charon: 11[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f701f2138a0
Sep 9 16:39:29 rossini charon: 11[KNL] 0: 50 00 00 00 15 00 01 00 9F 9C 01 00 E6 1C 00 00 P...

Sep 9 16:39:29 rossini charon: 11[KNL] 16: C0 A8 C8 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 11[KNL] 32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 11[KNL] 48: 00 00 00 00 00 00 00 00 02 00 00 18 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 11[KNL] 64: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...

Sep 9 16:39:29 rossini charon: 11[KNL] querying policy 192.168.200.0/24 ==> 0.0.0.0/0 fwd (mark 0 /0x00000000)
Sep 9 16:39:29 rossini charon: 11[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f700f2138a0
Sep 9 16:39:29 rossini charon: 11[KNL] 0: 50 00 00 00 15 00 01 00 A0 9C 01 00 E6 1C 00 00 P...
Sep 9 16:39:29 rossini charon: 11[KNL] 32: C0 A8 C8 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
Sep 9 16:39:29 rossini charon: 11[KNL] 48: 00 00 00 00 00 00 00 00 02 00 00 18 00 00 00 00 ...
Sep 9 16:39:29 rossini charon: 11[KNL] querying policy 0.0.0.0/0 === 192.168.200.0/24 out (mark 0/0x00000000)
Sep 9 16:39:29 rossini charon: 11[KNL] sending XFRM_MSG_GETPOLICY: => 80 bytes @ 0x7f700f2138a0
Sep 9 16:39:29 rossini charon: 11[KNL] 0: 50 00 00 00 15 00 01 00 A1 9C 01 00 E6 1C 00 00 P..
Sep 9 16:39:29 rossini charon: 11[KNL] 16: C0 A8 C8 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
Sep 9 16:39:29 rossini charon: 11[KNL] 32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
Sep 9 16:39:29 rossini charon: 11[KNL] 48: 00 00 00 00 00 00 00 00 02 00 00 18 00 00 00 00 ...
Sep 9 16:39:29 rossini charon: 11[KNL] 64: 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 ...
Sep 9 16:39:35 rossini charon: 02[NET] received packet => 92 bytes @ 0x7f7014c1a3e0
Sep 9 16:39:35 rossini charon: 02[NET] 0: 4D AD 7D 9A B6 37 5F 48 12 A8 05 31 3F 7B 87 M.}
Sep 9 16:39:35 rossini charon: 02[ENC] parsing header of message
Sep 9 16:39:35 rossini charon: 02[ENC] parsing HEADER payload, 92 bytes left
Sep 9 16:39:35 rossini charon: 02[ENC] parsing payload from => 92 bytes @ 0x7f7014c1a3e0
Sep 9 16:39:35 rossini charon: 02[ENC] parsing rule 0 IKE_SPI
Sep 9 16:39:35 rossini charon: 02[ENC] => 8 bytes @ 0x7f7014c1a3e0
Sep 9 16:39:35 rossini charon: 02[ENC] parsing rule 1 IKE_SPI
Sep 9 16:39:35 rossini charon: 02[ENC] => 8 bytes @ 0x7f7014c1a3e0
Sep 9 16:39:35 rossini charon: 02[ENC] parsing rule 2 U_INT_8
Sep 9 16:39:35 rossini charon: 02[ENC] => 8
Sep 9 16:39:35 rossini charon: 02[ENC] parsing rule 3 U_INT_4
Sep  9 16:39:35 rossini charon: 02[ENC]  => 1
Sep  9 16:39:35 rossini charon: 02[ENC]  => 5
Sep  9 16:39:35 rossini charon: 02[ENC]  => 0
Sep  9 16:39:35 rossini charon: 02[ENC]  => 0
Sep  9 16:39:35 rossini charon: 02[ENC]  => 0
Sep  9 16:39:35 rossini charon: 02[ENC]  => 1762106169
Sep  9 16:39:35 rossini charon: 02[ENC]  => 92
Sep  9 16:39:35 rossini charon: 14[ENC]  => 64 bytes @ 0x7f6fc0004170

Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 4 U_INT_4
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 5 U_INT_8
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 6 RESERVED_BIT
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 7 RESERVED_BIT
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 8 FLAG
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 9 FLAG
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 10 FLAG
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 11 FLAG
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 12 FLAG
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 13 FLAG
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 14 U_INT_32
Sep  9 16:39:35 rossini charon: 02[ENC]  parsing rule 15 HEADER_LENGTH

Sep  9 16:39:35 rossini charon: 14[ENC] parsing body of message, first payload is HASH_V1
Sep  9 16:39:35 rossini charon: 14[ENC] parsing ENCRYPTED_V1 payload, 64 bytes left
Sep  9 16:39:35 rossini charon: 14[ENC] parsing payload from => 64 bytes @ 0x7f6ff4000f3c
Sep  9 16:39:35 rossini charon: 14[ENC] parsing ENCRYPTED_V1 payload finished

Sep  9 16:39:35 rossini charon: 14[ENC] parsing HEADER payload finished
Sep  9 16:39:35 rossini charon: 02[ENC] parsing message header
Sep  9 16:39:35 rossini charon: 14[NET] waiting for data on sockets
Sep  9 16:39:35 rossini charon: 14[ENC] process payload of type ENCRYPTED_V1
Sep  9 16:39:35 rossini charon: 14[ENC] found an encrypted payload
Sep  9 16:39:35 rossini charon: 14[IKE] next IV for MID 1762106169 => 16 bytes @ 0x7f66fc0004170

Sep  9 16:39:35 rossini charon: 14[ENC] decrypting payloads:
Sep  9 16:39:35 rossini charon: 14[ENC] encrypted => 64 bytes @ 0x7f66fc0004170

Sep  9 16:39:35 rossini charon: 14[ENC] parsing ENCRYPTED_V1 payload finished
Sep  9 16:39:35 rossini charon: 14[ENC] process payload of type ENCRYPTED_V1
Sep  9 16:39:35 rossini charon: 14[ENC] found an encrypted payload
Sep  9 16:39:35 rossini charon: 14[IKE] next IV for MID 1762106169 => 16 bytes @ 0x7f66fc0001190
Sep  9 16:39:35 rossini charon: 14[IKE] 0: 03 1f 88 ef 57 73 7c 23 23 5d 71 31 4f 38 30 a6 ...
This results in an unstable VPN connection if I do not add a rightip to this conn (which may result in strongswan setting up the connection).

Hm, I'm not sure I understand your reasoning here. Why should strongSwan initiate the connection if the only thing you change is right=<ip>? Unless you use ipsec up <name>, auto=start or auto=route strongSwan has no reason to initiate the connection.

And how exactly does setting an IP fix this issue? How are the log or the dumped packets different?

The log you posted shows a DELETE request from strongSwan because the IPsec SA expired:

```
Sep 9 16:39:14 rossini charon: 09[IKE] closing expired CHILD_SA rw-test1{1} with SPIs c779dcad_i 3386db66_o and TS 0.0.0.0/0 === 192.168.200.0/24
```

This is the shorter message you see in the tcpdump output. The FRITZ!Box seems to delete those SAs too:

```
```

It's unclear, though, whether it does so because of the received DELETE payload or because the SA expired locally too. Maybe the box expected a DPD packet and has a problem that it received a DELETE request instead. But from the timings of the captured packets that seems unlikely:
forum messages regarding that error indicated as much). But since we can't be sure, you perhaps should ask AVM what the message means exactly.

Anyway, since there seems to be another successful DPD exchange later the question is, what exactly is the problem? Does rekeying not work? That is, is there no IPsec SA after this?

Perhaps you should have a look at your lifetime configuration.

#2 - 17.09.2013 21:10 - Andre Valentin

Hi!

Tobias Brunner wrote:

Hm, I'm not sure I understand your reasoning here. Why should strongSwan initiate the connection if the only thing you change is right=<ip>?

Unless you use ipsec up <name>, auto=start or auto=route strongSwan has no reason to initiate the connection.

Okay, I migrated these VPN's from racoon to strongswan. If I use racoon as a responder, I get no errors in the log. Also rekeying always works fine. With strongswan, I get those errors and sometimes rekeying breaks in a way, that there is an SA but no communication is possible, or there is no SA on the strongswan side.

That's why I opened that ticket.

If I use

```
right=%xyz.dyndns
```

everything works because strongswan will setup the tunnel. I took all lifetimes from the working racoon config.

Perhaps you should have a look at your lifetime configuration.

I tried every combination, but after some days there is always a problem.

If it helps, I could recreate the whole setup that worked in racoon as a strongswan config and sniff and log everything.

Here is my current config:

```plaintext
config setup
    uniqueids=no

conn %default
    ike lifetime=1h
    lifetime=1h
    rekeymargin=3m
    keyingtries=1
    authby=secret

conn fritz-base
    left=217.14.X.Y
    leftsubnet=0.0.0.0/0
    leftid=@xxxx.yyyy.ff
    rightallowany=yes
    ike lifetime=1h
    lifetime=20m
    ike=aes256-shal-modp1024
    esp=aes256-shal-modp1024
    # Does not work
    compress=no
    aggressive=no
    authby=secret
    keyingtries=%forever
    keyexchange=ikev1
    fragmentation=no
    dpdaction=restart
    rekey=yes

conn rw-test
    also=fritz-base
    right=test.dyn.org
    rightid=test.dyn.org
    rightsubnet=192.168.200.0/24
    auto=route
```

Thanks for your answer,

André
Hm, I'm not sure I understand your reasoning here. Why should strongSwan initiate the connection if the only thing you change is `right=<ip>`? Unless you use `ipsec up <name>`, `auto=start` or `auto=route` strongSwan has no reason to initiate the connection.

Okay, I migrated these VPN's from racoon to strongswan. If I use racoon as a responder, I get no errors in the log. Also rekeying always works fine. With strongswan, I get those errors and sometimes rekeying breaks in a way, that there is an SA but no communication is possible, or there is no SA on the strongswan side.

There are definitely some interoperability issues with IKEv1 rekeying, for instance #317. Perhaps this is the same issue. Martin just pushed some changes to the `ikev1-reauth` branch you could try.

Since we rarely have access to the actual devices to do interoperability tests, we mostly fly blindly and do the best we can to follow the RFCs (which of course is an issue with IKEv1 as many details are either not described in RFCs, or implemented differently by different vendors).

If it helps, I could recreate the whole setup that worked in racoon as a strongswan config and sniff and log everything.

More data could definitely help. Especially to see in what state the daemon is when this issue seems to hit. But you don't have to change your config for that. Also, the logs don't have to be as detailed as the excerpt you posted above (level 2 or even level 1 should suffice - particularly on low-level groups like `enc` or `asn1`).

I will provide the logs, but it will take some days. Thanks for your support!

André

I just noticed this change:

http://git.strongswan.org/?p=strongswan.git;a=shortlog;h=refs/heads/ikev1-reauth

Perhaps that helps. I will try it before I publish more logs.

Thanks,

André

This patch fixed my problems when only acting as a responder! Please close this ticket.

Thank you very much for your help,

André
That's good to hear, thanks.

#8 - 18.10.2013 10:08 - Tobias Brunner
- Tracker changed from Issue to Bug
- Subject changed from Incompatibility with AVM IKE / Problem with DPD to Incompatibility with AVM IKE / Problem with Reauthentication
- Category set to charon
- Target version set to 5.1.1