strongSwan - Issue #3672

ESP connection over IPv6

13.01.2021 16:37 - Boris Tomici

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.6.2	**Resolution:**	

Description

Hello,

I've got any issue trying to establish an ESP connection over IPv6.
Strange that same configuration worked few weeks before and cannot figure it out why is not working now.
Only thing I noticed is "DH group ECP_256 inacceptable, requesting MODP_3072" message.

server log:

```
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[NET] received packet: from 2a02:8100:d1f7:7f48:250:56ff:fe83:d01a[500] to 2a02:8100:c942:801::252[500] (894 bytes)
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG] looking for an ike config for 2a02:8100:c942:801::252...2a02:8100:d1f7:7f48:250:56ff:fe83:d01a
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG]   candidate: %any...%any, prio 28
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG] found matching ike config: %any...%any with prio 28
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[IKE] 2a02:8100:d1f7:7f48:250:56ff:fe83:d01a is initiating an IKE_SA
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[IKE] IKE_SA (unnamed)[5] state change: CREATED => CONNECTING
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG] selecting proposal:
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG]   proposal matches
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG] received proposals: IKE:AES_CBC_128/AES_CBC_192/AES_CBC_256/AES_CTR_128/AES_CTR_192/AES_CTR_256/CAMELLIA_CBC_128/CAMELLIA_CBC_192/CAMELLIA_CBC_256/3DES_CBC/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/AES_XCBC_96/AES_CMAC_96/HMAC_SHA1_96/PRF_AES128_XCBC/PRF_AES128_CMAC/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/PRF_HMAC_SHA1/ECP_256/ECP_384/ECP_521/ECP_256_BP/ECP_384_BP/ECP_512_BP/MODP_3072/MODP_4096/MODP_6144/MODP_8192/MODP_2048, IKE:AES_CCM_16_128/AES_CCM_16_192/AES_CCM_16_256/AES_GCM_16_128/AES_GCM_16_192/AES_GCM_16_256/AES_CCM_8_128/AES_CCM_8_192/AES_CCM_8_256/AES_CCM_12_128/AES_CCM_12_192/AES_CCM_12_256/AES_GCM_8_128/AES_GCM_8_192/AES_GCM_8_256/AES_GCM_12_128/AES_GCM_12_192/AES_GCM_12_256/PRF_AES128_XCBC/PRF_AES128_CMAC/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/PRF_HMAC_SHA1/ECP_256/ECP_384/ECP_521/ECP_256_BP/ECP_384_BP/ECP_512_BP/MODP_3072/MODP_4096/MODP_6144/MODP_8192/MODP_2048
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG] configured proposals: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072, IKE:AES_CBC_128/AES_CBC_192/AES_CBC_256/AES_CTR_128/AES_CTR_192/AES_CTR_256/CAMELLIA_CBC_128/CAMELLIA_CBC_192/CAMELLIA_CBC_256/3DES_CBC/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/AES_XCBC_96/AES_CMAC_96/HMAC_SHA1_96/PRF_AES128_XCBC/PRF_AES128_CMAC/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/PRF_HMAC_SHA1/ECP_256/ECP_384/ECP_521/ECP_256_BP/ECP_384_BP/ECP_512_BP/MODP_3072/MODP_4096/MODP_6144/MODP_8192/MODP_2048, IKE:AES_CCM_16_128/AES_CCM_16_192/AES_CCM_16_256/AES_GCM_16_128/AES_GCM_16_192/AES_GCM_16_256/AES_CCM_8_128/AES_CCM_8_192/AES_CCM_8_256/AES_CCM_12_128/AES_CCM_12_192/AES_CCM_12_256/AES_GCM_8_128/AES_GCM_8_192/AES_GCM_8_256/AES_GCM_12_128/AES_GCM_12_192/AES_GCM_12_256/PRF_AES128_XCBC/PRF_AES128_CMAC/PRF_HMAC_SHA2_256/PRF_HMAC_SHA2_384/PRF_HMAC_SHA2_512/PRF_HMAC_SHA1/ECP_256/ECP_384/ECP_521/ECP_256_BP/ECP_384_BP/ECP_512_BP/MODP_3072/MODP_4096/MODP_6144/MODP_8192/MODP_2048
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_3072
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[CFG] received supported signature hash algorithms: sha256 sha384 sha512
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[IKE] DH group ECP_256 inacceptable, requesting MODP_3072
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[ENC] generating IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[NET] sending packet: from 2a02:8100:c942:801::252[500] to 2a02:8100:d1f7:7f48:250:56ff:fe83:d01a[500] (38 bytes)
```

```
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[MGR] checkin and destroy IKE_SA (unnamed)[5]
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[IKE] IKE_SA (unnamed)[5] state change: CONNECTING => DEST
ROYING
Jan 13 15:42:14 vsrv-bicab-1u charon: 07[MGR] checkin and destroy of IKE_SA successful
```

Current ipsec.conf file:

1. ipsec.conf - strongSwan IPsec configuration file

```
config setup
charondebug="ike 2, knl 2, cfg 2, net 2, esp 2, dmn 2,  mgr 2, lib 2"

conn %default
keyexchange=ikev2
ike=aes128-sha256-modp3072!
dpdaction=clear
dpddelay=300s
authby=pubkey
rightdns=2a02:8100:c942:801::53
fragmentation=yes

conn IPSec-IKEv2-ESP
esp=aes128-sha256
keyexchange=ikev2
auto=add
left=%any
leftid=100.80.1.252
leftsubnet=2a02:8100:d102:1::0/64
leftcert=vpnHostCert_100.80.1.252.der
leftsendcert=always
right=%any
rightcert=VPNclientCert.der
rightsourceip=2a02:8100:d102:2::2
rightsubnet=2a02:8100:d102:2::0/64
mobike=no
```

History

#1 - 13.01.2021 18:03 - Tobias Brunner

- Status changed from New to Feedback

I don't see what this has to do with IPv6 or ESP.

Anyway, what does the initiator say when it receives the INVALID_KE_PAYLOAD notify? Why does it not retry with MODP_3072?

#2 - 14.01.2021 08:40 - Boris Tomici

Client seems to send back the response:

```
Jan 14 07:18:35 vsrv-bicab-2u charon: 06[CFG]   loaded certificate "C=DE, O=CPE Engineering, CN=VPN Client" fr
om 'VPNclientCert.der'
Jan 14 07:18:35 vsrv-bicab-2u charon: 06[CFG]   id '%any' not confirmed by certificate, defaulting to 'C=DE, O
=CPE Engineering, CN=VPN Client'
Jan 14 07:18:35 vsrv-bicab-2u charon: 06[CFG] added configuration 'ikev2-rw-esp'
Jan 14 07:18:35 vsrv-bicab-2u charon: 07[CFG] received stroke: initiate 'ikev2-rw-esp'
Jan 14 07:18:35 vsrv-bicab-2u charon: 07[IKE] initiating IKE_SA ikev2-rw-esp[1] to 2a02:8100:c942:801::252
Jan 14 07:18:35 vsrv-bicab-2u charon: 07[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_
S_IP) N(NATD_S_IP) N(NATD_S_IP) N(NATD_S_IP) N(NATD_S_IP) N(NATD_S_IP) N(NATD_S_IP) N(NATD_S_IP) N(NATD_S_IP)
N(NATD_S_IP) N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jan 14 07:18:35 vsrv-bicab-2u charon: 07[NET] sending packet: from ::[500] to 2a02:8100:c942:801::252[500] (12
02 bytes)
Jan 14 07:18:35 vsrv-bicab-2u charon: 09[NET] received packet: from 2a02:8100:c942:801::252[500] to 2a02:8100:
d1f7:7f30::41f7[500] (38 bytes)
Jan 14 07:18:35 vsrv-bicab-2u charon: 09[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
Jan 14 07:18:35 vsrv-bicab-2u charon: 09[IKE] peer didn't accept DH group ECP_256, it requested MODP_3072
Jan 14 07:18:35 vsrv-bicab-2u charon: 09[IKE] initiating IKE_SA ikev2-rw-esp[1] to 2a02:8100:c942:801::252
Jan 14 07:18:35 vsrv-bicab-2u charon: 09[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_
```

```
D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
Jan 14 07:18:35 vsrv-bicab-2u charon: 09[NET] sending packet: from 2a02:8100:d1f7:7f30::41f7[500] to 2a02:8100
:c942:801::252[500] (1214 bytes)
Jan 14 07:18:39 vsrv-bicab-2u charon: 11[IKE] retransmit 1 of request with message ID 0
Jan 14 07:18:39 vsrv-bicab-2u charon: 11[NET] sending packet: from 2a02:8100:d1f7:7f30::41f7[500] to 2a02:8100
:c942:801::252[500] (1214 bytes)
Jan 14 07:18:39 vsrv-bicab-2u charon: 12[IKE] retransmit 2 of request with message ID 0
Jan 14 07:18:39 vsrv-bicab-2u charon: 12[NET] sending packet: from 2a02:8100:d1f7:7f30::41f7[500] to 2a02:8100
:c942:801::252[500] (1214 bytes)
Jan 14 07:18:46 vsrv-bicab-2u charon: 16[IKE] retransmit 3 of request with message ID 0
Jan 14 07:18:46 vsrv-bicab-2u charon: 16[NET] sending packet: from 2a02:8100:d1f7:7f30::41f7[500] to 2a02:8100
:c942:801::252[500] (1214 bytes)
Jan 14 07:18:52 vsrv-bicab-2u charon: 07[IKE] retransmit 4 of request with message ID 0
Jan 14 07:18:52 vsrv-bicab-2u charon: 07[NET] sending packet: from 2a02:8100:d1f7:7f30::41f7[500] to 2a02:8100
:c942:801::252[500] (1214 bytes)
```

But on server side I got same logs everytime, I am also thinking that there might be a network issue looking at those retransmit messages.

#3 - 14.01.2021 10:24 - Tobias Brunner

> But on server side I got same logs everytime, I am also thinking that there might be a network issue looking at those retransmit messages.

Yes, could be an IP fragmentation issue due to the larger DH public value. The IKE_SA_INIT message can't be fragmented on the IKE layer, so it gets fragmented on the IP layer if necessary. Make sure these fragments are not blocked by any firewall. Note that the minimum MTU for IPv6 should actually be 1280 bytes (and the difference between the two requests is also only 12 bytes).

#4 - 14.01.2021 16:52 - Boris Tomici

- File server_syslog.log added

Tobias Brunner wrote:

> > But on server side I got same logs everytime, I am also thinking that there might be a network issue looking at those retransmit messages.
>
> Yes, could be an IP fragmentation issue due to the larger DH public value. The IKE_SA_INIT message can't be fragmented on the IKE layer, so it gets fragmented on the IP layer if necessary. Make sure these fragments are not blocked by any firewall. Note that the minimum MTU for IPv6 should actually be 1280 bytes (and the difference between the two requests is also only 12 bytes).

In the end the issue was related to the modem where client is connected, for some reasons the built-in firewall was dropping the packets.
Disabling the firewall the connection is established but I have run into another issue.
While generating traffic between peers, client sends DELETE CHILD_SA after rekey event.

Client log

```
Jan 14 15:45:09 vsrv-bicab-2u charon: 05[KNL] creating rekey job for CHILD_SA ESP/0xc09af837/2a02:8100:c942:80
1::252
Jan 14 15:45:09 vsrv-bicab-2u charon: 06[IKE] establishing CHILD_SA ikev2-rw-esp{2} reqid 1
Jan 14 15:45:09 vsrv-bicab-2u charon: 06[ENC] generating CREATE_CHILD_SA request 2 [ N(REKEY_SA) SA No TSi TSr
 ]
Jan 14 15:45:09 vsrv-bicab-2u charon: 06[NET] sending packet: from 2a02:8100:d1f7:7f48:250:56ff:fe83:ccdc[4500
] to 2a02:8100:c942:801::252[4500] (320 bytes)
Jan 14 15:45:09 vsrv-bicab-2u charon: 08[NET] received packet: from 2a02:8100:c942:801::252[4500] to 2a02:8100
:d1f7:7f48:250:56ff:fe83:ccdc[4500] (256 bytes)
Jan 14 15:45:09 vsrv-bicab-2u charon: 08[ENC] parsed CREATE_CHILD_SA response 2 [ SA No TSi TSr ]
Jan 14 15:45:09 vsrv-bicab-2u charon: 08[IKE] inbound CHILD_SA ikev2-rw-esp{2} established with SPIs c4a5e027_
i c4950f79_o and TS 2a02:8100:d102:2::/64 === 2a02:8100:d102:1::/64
Jan 14 15:45:09 vsrv-bicab-2u charon: 08[IKE] outbound CHILD_SA ikev2-rw-esp{2} established with SPIs c4a5e027
_i c4950f79_o and TS 2a02:8100:d102:2::/64 === 2a02:8100:d102:1::/64
Jan 14 15:45:09 vsrv-bicab-2u charon: 08[IKE] closing CHILD_SA ikev2-rw-esp{1} with SPIs ceb60050_i (370140712
 bytes) c09af837_o (370142794 bytes) and TS 2a02:8100:d102:2::/64 === 2a02:8100:d102:1::/64
Jan 14 15:45:09 vsrv-bicab-2u charon: 08[IKE] sending DELETE for ESP CHILD_SA with SPI ceb60050
```

On the server I noticed
Jan 14 15:45:11 vsrv-bicab-1u charon: 14[IKE] detected CHILD_REKEY collision with CHILD_REKEY

Attached the full server log during the test.

#5 - 14.01.2021 17:04 - Tobias Brunner

While generating traffic between peers, client sends DELETE CHILD_SA after rekey event.

There will obviously be a delete for the old CHILD_SA after a rekeying. Your problem is that when the server tries to rekey the CHILD_SA (at 15:42:55), its packets don't reach the client, so it eventually deletes the IKE_SA after 5 retransmits (at 15:45:40, the last retransmit was sent at 15:44:24). So there seems still something weird happening on the network because the response to the client's rekey request (sent at 15:45:11) is apparently received fine. Maybe there is still some firewall rule that blocks inbound traffic if there is no traffic for a while.

Files

server_syslog.log	45.7 KB	14.01.2021	Boris Tomici