strongSwan - Issue #965

Windows 8.1 cannot connect to strongSwan on IKEv2 error 809

23.05.2015 11:17 - malfoy john

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	interoperability		
Affected version:	5.3.0	**Resolution:**	No change required

Description

I followed this tutorial:
https://www.zeitgeist.se/2013/11/22/strongswan-howto-create-your-own-vpn/
on a cloud ubuntu instance built a VPN server using IKEv2.
The weird part is, under the same wifi network, my Windows Phone8.1 can connect to it easily,
but my windows 8.1 laptop still refuses to connect, saying error 809.

I tried both auth options (used client-cert / eap-mschapv2), still no help.

Syslog on the server side (ubuntu) when try to connect from win8.1:

```
May 23 09:04:08 netlink charon: 03[CFG] selecting proposal:
May 23 09:04:08 netlink charon: 03[CFG]   no acceptable PSEUDO_RANDOM_FUNCTION found
May 23 09:04:08 netlink charon: 03[CFG] selecting proposal:
May 23 09:04:08 netlink charon: 03[CFG]   proposal matches
May 23 09:04:08 netlink charon: 03[CFG] received proposals: IKE:3DES_CBC/HMAC_SHA1_96/PRF_HMAC_SHA
1/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:3DES_CBC/HMAC_SHA2_38
4_192/PRF_HMAC_SHA2_384/MODP_1024, IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:AES_C
BC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:AES_CBC_128/HMAC_SHA2_384_192/PRF_HMAC_S
HA2_384/MODP_1024, IKE:AES_CBC_192/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:AES_CBC_192/HMAC_SHA2
_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:AES_CBC_192/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_102
4, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMA
C_SHA2_256/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1024
May 23 09:04:08 netlink charon: 03[CFG] configured proposals: IKE:AES_CBC_128/HMAC_SHA2_256_128/PR
F_HMAC_SHA2_256/ECP_256, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/ECP_384, IKE:AES_CBC_
128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_2048, IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP
_2048, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_4096, IKE:AES_CBC_256/HMAC_SHA2_25
6_128/PRF_HMAC_SHA2_256/MODP_4096, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_4096, IKE:AES_C
BC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1536, IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/M
ODP_1536, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_2048, IKE:AES_CBC_256/HMAC_SHA2
_256_128/PRF_HMAC_SHA2_256/MODP_2048, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048, IKE:AE
S_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024, IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA
1/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1536, IKE:AES_CBC_256/HMAC_S
HA2_256_128/PRF_HMAC_SHA2_256/MODP_1536, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536, IKE
:AES_CBC_256/HMAC_SHA2_384_192/PRF_HMAC_SHA2_384/MODP_1024, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_
HMAC_SHA2_256/MODP_1024, IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
May 23 09:04:08 netlink charon: 03[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_H
MAC_SHA2_256/MODP_1024
May 23 09:04:08 netlink charon: 03[IKE] local host is behind NAT, sending keep alives
May 23 09:04:08 netlink charon: 03[IKE] remote host is behind NAT
May 23 09:04:08 netlink charon: 03[IKE] sending cert request for "C=CH, O=MockyTech, CN=MockyTech
Root CA"
May 23 09:04:08 netlink charon: 03[ENC] generating IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP)
N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
May 23 09:04:08 netlink charon: 03[NET] sending packet: from 100.68.156.125[500] to 50.197.66.210[
49850] (337 bytes)
May 23 09:04:08 netlink charon: 09[NET] sending packet: from 100.68.156.125[500] to 50.197.66.210[
49850]
May 23 09:04:28 netlink charon: 05[IKE] sending keep alive to 50.197.66.210[49850]
May 23 09:04:28 netlink charon: 09[NET] sending packet: from 100.68.156.125[500] to 50.197.66.210[
49850]
May 23 09:04:38 netlink charon: 01[JOB] deleting half open IKE_SA after timeout
May 23 09:04:38 netlink charon: 01[IKE] IKE_SA (unnamed)[39] state change: CONNECTING => DESTROYIN
```

G

Wireshark Capture on the client side (Win8.1) when trying to connect:

```
Time           Source                Destination           Src.Prt Dst.Prt Protocol Length Info
9.423422000    192.168.1.2           23.99.92.105          500     500     ISAKMP   922    IKE_SA_
INIT MID=00 Initiator Request
9.931315000    23.99.92.105          192.168.1.2           500     500     ISAKMP   379    IKE_SA_
INIT MID=00 Responder Response
9.977419000    192.168.1.2           23.99.92.105          4500    4500    ISAKMP   1238   IKE_AUT
H MID=01 Initiator Request
10.965163000   192.168.1.2           23.99.92.105          4500    4500    ISAKMP   1238   IKE_AUT
H MID=01 Initiator Request
11.980558000   192.168.1.2           23.99.92.105          4500    4500    ISAKMP   1238   IKE_AUT
H MID=01 Initiator Request
```

Thanks.

Related issues:

Has duplicate Issue #1026: IKEv2 VPN fails when connecting via WAN	**Closed**	**09.07.2015**
Has duplicate Issue #3152: Problem connecting from Windows 7 but not from mobile	**Closed**	

History

#1 - 27.05.2015 15:22 - Tobias Brunner

- Description updated

- Category changed from windows to interoperability

- Status changed from New to Feedback

Windows sends the IKE_AUTH request but strongSwan apparently does not receive it. The reason for this is often IP fragmentation. Due to the certificate sent in the message, and even with EAP-MSCHAPv2 because of certificate requests sent for each installed CA certificate, it can get larger than the MTU. So the message gets fragmented on the IP layer. Some firewalls/routers might drop such fragments and prevent the responder from receiving the IKE_AUTH requests. Depending on the number of installed CA certificates (Windows automatically installs them as needed when surfing the Web) the size of the IKE_AUTH message may vary between clients.

strongSwan supports IKE fragmentation for IKEv1 and since 5.2.1 for IKEv2, but the latter is pretty new and not yet supported by most clients. Windows does still support IKEv1 (including fragmentation) but I think only in combination with L2TP for roadwarrior scenarios (you'll probably find tutorials for that online).

#2 - 08.06.2015 23:09 - Conrad Kostecki

Hm, at least, it seems, I have the same problem here. My Linux and Windows Phone can connect fine on the same network. But Windows 8.1 can't. I've the same captures, as malfoy john.

#3 - 09.07.2015 19:08 - Tobias Brunner

- Has duplicate Issue #1026: IKEv2 VPN fails when connecting via WAN added

#4 - 21.12.2017 23:09 - Noel Kuntze

- Status changed from Feedback to Closed

- Resolution set to No change required

#5 - 20.08.2019 09:32 - Tobias Brunner

- Has duplicate Issue #3152: Problem connecting from Windows 7 but not from mobile added