strongSwan - Issue #3345

NetworkManager-strongswan failed to detect EAP-GTC method

20.02.2020 21:18 - Xinzhe Wang

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	networkmanager (charon-nm)		
Affected version:	5.8.2	**Resolution:**	No change required

Description

Hi,
I tried NetworkManager-strongswan recently to connect to a IKEv2 VPN, it works well when I use the config file and commands to manually connect, but failed when I tried NetworkManager GUI.

Here are my environment:

- manjaro KDE
- strongswan 5.8.2
- NetworkManager-strongswan 1.4.5

The VPN use EAP-GTC method to connect and **I can connect without any problem in Windows and MacOS**

```
journalctl -u NetworkManager |tail -n 1000 > log.txt

00[DMN] Starting charon NetworkManager backend (strongSwan 5.8.2)
<info>  [1582228337.3121] vpn-connection[0x560404b34150,b9c45984-eaab-4af5-82ef-bc15b752d72e,"New
vpn connection",0]: Saw the service appear; activating connection
00[LIB] loaded plugins: nm-backend charon-nm ldap pkcs11 aesni aes des rc2 sha2 sha3 sha1 md5 mgf1
 random nonce x509 revocation constraints pkcs1 pkcs7 pkcs8 sshkey pem openssl fips-prf gmp curve2
5519 agent chapoly xcbc cmac hmac ntru drbg newhope bliss curl kernel-netlink socket-default bypas
s-lan eap-identity eap-md5 eap-gtc eap-mschapv2 eap-tls eap-ttls eap-peap
00[LIB] dropped capabilities, running as uid 0, gid 0
00[JOB] spawning 16 worker threads
06[IKE] installed bypass policy for 172.17.0.0/16
06[IKE] installed bypass policy for 192.168.1.0/24
06[IKE] installed bypass policy for 192.168.56.0/24
06[KNL] received netlink error: Invalid argument (22)
06[KNL] unable to install source route for %any6
06[IKE] installed bypass policy for ::1/128
06[IKE] installed bypass policy for fe80::/64
06[IKE] interface change for bypass policy for fe80::/64 (from vboxnet0 to wlp58s0)
<info>  [1582228337.6028] audit: op="statistics" arg="refresh-rate-ms" pid=1361 uid=1000 result="s
uccess"
05[CFG] received initiate for NetworkManager connection New vpn connection
05[LIB]   file coded in unknown format, discarded
05[LIB] building CRED_CERTIFICATE - X509 failed, tried 5 builders
05[CFG] loading CA certificate '/etc/ssl/certs/java/cacerts' failed
05[CFG] using CA certificate, gateway identity '<DELETED>'
05[IKE] initiating IKE_SA New vpn connection[1] to <DELETED>
05[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_A
LG) N(REDIR_SUP) ]
05[NET] sending packet: from 192.168.1.100[56354] to <DELETED>[500] (1000 bytes)
<info>  [1582228341.6634] vpn-connection[0x560404b34150,b9c45984-eaab-4af5-82ef-bc15b752d72e,"New
vpn connection",0]: VPN plugin: state changed: starting (3)
10[NET] received packet: from <DELETED>[500] to 192.168.1.100[56354] (280 bytes)
10[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG)
 N(CHDLESS_SUP) N(MULT_AUTH) ]
10[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA2_256_128/PRF_AES128_XCBC/ECP_256
10[IKE] local host is behind NAT, sending keep alives
10[IKE] sending cert request for "C=NL, O=Staat der Nederlanden, CN=Staat der Nederlanden Root CA
- G3"
...
```

```
10[IKE] sending cert request for "C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Ro
ot G2"
10[IKE] establishing CHILD_SA New vpn connection{1}
10[ENC] generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) CERTREQ CPRQ(ADDR ADDR6 DNS NBNS DNS6)
 SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
10[ENC] splitting IKE message (8688 bytes) into 8 fragments
10[ENC] generating IKE_AUTH request 1 [ EF(1/8) ]
10[ENC] generating IKE_AUTH request 1 [ EF(2/8) ]
10[ENC] generating IKE_AUTH request 1 [ EF(3/8) ]
10[ENC] generating IKE_AUTH request 1 [ EF(4/8) ]
10[ENC] generating IKE_AUTH request 1 [ EF(5/8) ]
10[ENC] generating IKE_AUTH request 1 [ EF(6/8) ]
10[ENC] generating IKE_AUTH request 1 [ EF(7/8) ]
10[ENC] generating IKE_AUTH request 1 [ EF(8/8) ]
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (1236 bytes)
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (1236 bytes)
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (1236 bytes)
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (1236 bytes)
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (1236 bytes)
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (1236 bytes)
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (1236 bytes)
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (532 bytes)
11[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (1236 bytes)
11[ENC] parsed IKE_AUTH response 1 [ EF(1/3) ]
11[ENC] received fragment #1 of 3, waiting for complete IKE message
12[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (1236 bytes)
12[ENC] parsed IKE_AUTH response 1 [ EF(2/3) ]
12[ENC] received fragment #2 of 3, waiting for complete IKE message
13[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (628 bytes)
13[ENC] parsed IKE_AUTH response 1 [ EF(3/3) ]
13[ENC] received fragment #3 of 3, reassembled fragmented IKE message (2960 bytes)
13[ENC] parsed IKE_AUTH response 1 [ IDr CERT CERT AUTH EAP/REQ/ID ]
13[IKE] received end entity cert "CN=<DELETED>"
13[IKE] received issuer cert "C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3"
13[CFG]   using certificate "CN=<DELETED>"
13[CFG]   using untrusted intermediate certificate "C=US, O=Let's Encrypt, CN=Let's Encrypt Author
ity X3"
13[CFG] checking certificate status of "CN=<DELETED>"
13[CFG]   requesting ocsp status from 'http://ocsp.int-x3.letsencrypt.org' ...
13[LIB] libcurl request failed [28]: Connection timed out after 10000 milliseconds
13[CFG] ocsp request to http://ocsp.int-x3.letsencrypt.org failed
13[CFG] ocsp check failed, fallback to crl
13[CFG] certificate status is not available
13[CFG]   using trusted ca certificate "O=Digital Signature Trust Co., CN=DST Root CA X3"
13[CFG] checking certificate status of "C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3"
13[CFG]   requesting ocsp status from 'http://isrg.trustid.ocsp.identrust.com' ...
13[LIB] libcurl request failed [28]: Connection timed out after 10000 milliseconds
13[CFG] ocsp request to http://isrg.trustid.ocsp.identrust.com failed
13[CFG] ocsp check failed, fallback to crl
13[CFG]   fetching crl from 'http://crl.identrust.com/DSTROOTCAX3CRL.crl' ...
13[CFG]   using trusted certificate "O=Digital Signature Trust Co., CN=DST Root CA X3"
13[CFG]   crl correctly signed by "O=Digital Signature Trust Co., CN=DST Root CA X3"
13[CFG]   crl is valid: until Mar 07 01:46:18 2020
13[CFG] certificate status is good
13[CFG] certificate policy 2.23.140.1.2.1 for 'CN=<DELETED>' not allowed by trustchain, ignored
13[CFG] certificate policy 1.3.6.1.4.1.44947.1.1.1 for 'CN=<DELETED>' not allowed by trustchain, i
gnored
13[CFG]   reached self-signed root ca with a path length of 1
13[IKE] authentication of 'CN=<DELETED>' with RSA_EMSA_PKCS1_SHA2_256 successful
13[IKE] server requested EAP_IDENTITY (id 0x00), sending '<DELETED>'
13[ENC] generating IKE_AUTH request 2 [ EAP/RES/ID ]
13[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (96 bytes)
16[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (80 bytes)
16[ENC] parsed IKE_AUTH response 2 [ EAP/REQ/PEAP ]
16[IKE] server requested EAP_PEAP authentication (id 0x01)
16[TLS] EAP_PEAP version is v0
16[ENC] generating IKE_AUTH request 3 [ EAP/RES/PEAP ]
```

```
16[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (256 bytes)
08[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (1104 bytes)
08[ENC] parsed IKE_AUTH response 3 [ EAP/REQ/PEAP ]
08[TLS] negotiated TLS 1.2 using suite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
08[ENC] generating IKE_AUTH request 4 [ EAP/RES/PEAP ]
08[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (80 bytes)
07[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (1104 bytes)
07[ENC] parsed IKE_AUTH response 4 [ EAP/REQ/PEAP ]
07[ENC] generating IKE_AUTH request 5 [ EAP/RES/PEAP ]
07[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (80 bytes)
10[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (1072 bytes)
10[ENC] parsed IKE_AUTH response 5 [ EAP/REQ/PEAP ]
10[TLS] server certificate does not match to 'CN=<DELETED>'
10[TLS] sending fatal TLS alert 'access denied'
10[ENC] generating IKE_AUTH request 6 [ EAP/RES/PEAP ]
10[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (96 bytes)
12[NET] received packet: from <DELETED>[4500] to 192.168.1.100[50376] (80 bytes)
12[ENC] parsed IKE_AUTH response 6 [ EAP/FAIL ]
12[IKE] received EAP_FAILURE, EAP authentication failed
12[ENC] generating INFORMATIONAL request 7 [ N(AUTH_FAILED) ]
12[NET] sending packet: from 192.168.1.100[50376] to <DELETED>[4500] (80 bytes)
<warn>  [1582228364.8063] vpn-connection[0x560404b34150,b9c45984-eaab-4af5-82ef-bc15b752d72e,"New
vpn connection",0]: VPN plugin: failed: connect-failed (1)
<warn>  [1582228364.8065] vpn-connection[0x560404b34150,b9c45984-eaab-4af5-82ef-bc15b752d72e,"New
vpn connection",0]: VPN plugin: failed: connect-failed (1)
<info>  [1582228364.8068] vpn-connection[0x560404b34150,b9c45984-eaab-4af5-82ef-bc15b752d72e,"New
vpn connection",0]: VPN plugin: state changed: stopping (5)
<info>  [1582228364.8073] vpn-connection[0x560404b34150,b9c45984-eaab-4af5-82ef-bc15b752d72e,"New
vpn connection",0]: VPN plugin: state changed: stopped (6)
```

I deleted a lot of the certificate try(I think it wont help a lot) in the middle and replace the IP and username with <DELETED>

I can make sure the password is correct, I can connect by console with it. It seems that the plugin use the wrong method to authenticate, when I use the config file and console I can see

```
server requested EAP_IDENTITY (id 0x00), sending '<DELETED>'
generating IKE_AUTH request 2 [ EAP/RES/ID ]
sending packet: from 192.168.1.100[4500] to <DELETED>[4500] (96 bytes)
received packet: from <DELETED>[4500] to 192.168.1.100[4500] (80 bytes)
parsed IKE_AUTH response 2 [ EAP/REQ/PEAP ]
server requested EAP_PEAP authentication (id 0x01)
requesting EAP_GTC authentication, sending EAP_NAK
generating IKE_AUTH request 3 [ EAP/RES/NAK ]
sending packet: from 192.168.1.100[4500] to <DELETED>[4500] (80 bytes)
received packet: from <DELETED>[4500] to 192.168.1.100[4500] (96 bytes)
parsed IKE_AUTH response 3 [ EAP/REQ/GTC ]
server requested EAP_GTC authentication (id 0x02)
generating IKE_AUTH request 4 [ EAP/RES/GTC ]
sending packet: from 192.168.1.100[4500] to <DELETED>[4500] (96 bytes)
received packet: from <DELETED>[4500] to 192.168.1.100[4500] (80 bytes)
parsed IKE_AUTH response 4 [ EAP/SUCC ]
EAP method EAP_GTC succeeded, no MSK established
authentication of 'config' (myself) with EAP
generating IKE_AUTH request 5 [ AUTH ]
sending packet: from 192.168.1.100[4500] to <DELETED>[4500] (96 bytes)
received packet: from <DELETED>[4500] to 192.168.1.100[4500] (256 bytes)
parsed IKE_AUTH response 5 [ AUTH CPRP(ADDR DNS DNS) SA TSi TSr N(MOBIKE_SUP) N(ADD_6_ADDR) ]
authentication of '<DELETED>' with EAP successful@
```

in the end.

I find that the plugin claims to support EAP-GTC(https://wiki.strongswan.org/projects/strongswan/wiki/NetworkManager).
So is it a bug in the plugin(I cant find the settings in NetworkManager to manually change the method to EAP-GTC, only the EAP, perhaps it is auto-detected?) or there is something wrong in the server settings(But Windows and MacOS can connect automatically).

Any suggestions?

History

#1 - 21.02.2020 09:25 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

> The VPN use EAP-GTC method to connect and I can connect without any problem in Windows and MacOS

These two things can't be related, because neither of the latter platforms actually supports EAP-GTC.

As you can see in the log, the problem is that the server requests EAP-PEAP and that the AAA server certificate validation fails:

```
16[IKE] server requested EAP_PEAP authentication (id 0x01)
...
10[TLS] server certificate does not match to 'CN=<DELETED>'
10[TLS] sending fatal TLS alert 'access denied'
```

If you don't want to use EAP-PEAP, but EAP-GTC, don't load the *eap-peap* plugin in *charon-nm* (see PluginLoad). Or configure the server to not request EAP-PEAP first.

#2 - 21.02.2020 13:50 - Xinzhe Wang

Thanks for reply.
I think this is the problem but I have no access to server.
So I tried to disable the plugin with *load_modular*, make *load=no* in */etc/strongswan.d/charon/eap-peap.conf* and *load_modular = yes* in */etc/strongswan.d/charon.conf*

From swanctl --stats or ipsec statusall I can see the eap-peap is not loaded. But the log file in NetworkManager shows that charon-nm still load eap-peap plugin.

What else shall I configure or the only way is to recompile the strongswan.

#3 - 21.02.2020 14:05 - Tobias Brunner

> So I tried to disable the plugin with *load_modular*, make *load=no* in */etc/strongswan.d/charon/eap-peap.conf* and *load_modular = yes* in */etc/strongswan.d/charon.conf*

You need to change this for *charon-nm* (the NM backend) not *charon* (the regular IKE daemon). So you can't use the snippets in /etc/strongswan.d.

But you also don't need to use modular plugin loading to disable a specific plugin. Just add the following to strongswan.conf:

```
charon-nm {
  plugins {
    eap-peap {
      load = no
    }
  }
}
```

> From swanctl --stats or ipsec statusall

Both of these tools have no relation to *charon-nm*, which is configured by the NM plugin.

#4 - 21.02.2020 15:50 - Xinzhe Wang

OK, I see.
Thanks a lot, after making eap-peap and eap-md5 disabled, I can connect successfully. Cheers!

#5 - 21.02.2020 16:00 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required