strongSwan - Bug #3428

Ubuntu 20.04, NetworkManager, Encrypted (protected) private key

27.04.2020 17:35 - Alex Mfl

Status:	Closed	**Start date:**	
Priority:	Low	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	networkmanager (charon-nm)		
Target version:	5.9.0		
Affected version:	5.8.2	**Resolution:**	Fixed

Description

Hello! I'm not sure whether this is the right place for this request. Anyway, I'm trying to describe the problem in detail.

- OS: Ubuntu 20.04
- Installed packages: network-manager-strongswan + dependencies
- VPN auth mode: Cert+Key

The main problem

The keyfile is encrypted, and NetworkManager asks a password for the keyfile. I suppose the password for keyfile is not used. There are no problems with an unprotected keyfile.

NetworkManager connection config

```
[connection]
id=vpnconnectionid
uuid=04f56322-d291-4015-9758-6d54960518c3
type=vpn
autoconnect=false
permissions=user:someuser:;

[vpn]
address=somevpnhost
certificate=/home/someuser/vpnkeys/caCert.pem
encap=no
esp=aes128-sha1-modp1536
ike=aes128-sha1-modp1024
ipcomp=yes
method=key
proposal=yes
usercert=/home/someuser/vpnkeys/client-cert.pem
userkey=/home/someuser/vpnkeys/client-key.pem
virtual=yes
service-type=org.freedesktop.NetworkManager.strongswan

[ipv4]
dns=10.10.10.10;
dns-search=somedomain
method=auto

[ipv6]
addr-gen-mode=stable-privacy
dns-search=
method=ignore

[proxy]
```

Diff between protected and unprotected keyfiles

I think it's obvious, but may be usefull:

- protected: ShowHide

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,6DC24DE9A76BAC92C3203C662D71BEB0
....
-----END RSA PRIVATE KEY-----
```

- unprotected: ShowHide

```
-----BEGIN RSA PRIVATE KEY-----
...
-----BEGIN RSA PRIVATE KEY-----
```

Logs

```
Apr 25 21:30:15 vbox-test NetworkManager[537]: <info>  [1587839415.9416] audit: op="connection-act
ivate" uuid="04f56322-d291-4015-9758-6d54960518c3" name="vpnconnectionid" pid=1392 uid=1000 result
="success"
Apr 25 21:30:15 vbox-test NetworkManager[537]: <info>  [1587839415.9465] vpn-connection[0x559339da
6750,04f56322-d291-4015-9758-6d54960518c3,"vpnconnectionid",0]: Saw the service appear; activating
 connection
Apr 25 21:30:15 vbox-test charon-nm: 05[LIB] building CRED_PRIVATE_KEY - ANY failed, tried 6 build
ers
Apr 25 21:30:17 vbox-test charon-nm: message repeated 2 times: [ 05[LIB] building CRED_PRIVATE_KEY
 - ANY failed, tried 6 builders]
Apr 25 21:30:17 vbox-test NetworkManager[537]: <error> [1587839417.6588] vpn-connection[0x559339da
6750,04f56322-d291-4015-9758-6d54960518c3,"vpnconnectionid",0]: final secrets request failed to pr
ovide sufficient secrets
```

Additional problem with unprotected keyfile

I think this is not strongSwan's problem, but maybe somebody here knows the correct solution. The problem is repeatable avahi-daemon errors: ShowHide

```
Apr 25 21:20:50 vbox-test NetworkManager[537]: <info>  [1587838850.6662] audit: op="connection-act
ivate" uuid="04f56322-d291-4015-9758-6d54960518c3" name="somevpnhost" pid=3622 uid=1000 result="su
ccess"
Apr 25 21:20:50 vbox-test NetworkManager[537]: <info>  [1587838850.6726] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Saw the service appear; activating con
nection
Apr 25 21:20:50 vbox-test NetworkManager[537]: <info>  [1587838850.6975] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN connection: (ConnectInteractive) r
eply received
Apr 25 21:20:50 vbox-test charon-nm: 05[CFG] received initiate for NetworkManager connection somev
pnhost
Apr 25 21:20:50 vbox-test charon-nm: 05[CFG] using CA certificate, gateway identity 'somevpnhost'
Apr 25 21:20:50 vbox-test charon-nm: 05[IKE] initiating IKE_SA somevpnhost[2] to somevpnhost_ip_he
re
Apr 25 21:20:50 vbox-test charon-nm: 05[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) ]
Apr 25 21:20:50 vbox-test charon-nm: 05[NET] sending packet: from 192.168.11.137[49412] to somevpn
host_ip_here[500] (336 bytes)
Apr 25 21:20:50 vbox-test NetworkManager[537]: <info>  [1587838850.7091] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN plugin: state changed: starting (3
)
Apr 25 21:20:54 vbox-test charon-nm: 10[IKE] retransmit 1 of request with message ID 0
Apr 25 21:20:54 vbox-test charon-nm: 10[NET] sending packet: from 192.168.11.137[49412] to somevpn
host_ip_here[500] (336 bytes)
Apr 25 21:21:01 vbox-test systemd-resolved[495]: Server returned error NXDOMAIN, mitigating potent
ial DNS violation DVE-2018-0001, retrying transaction with reduced feature level UDP.
```

```
Apr 25 21:21:01 vbox-test systemd-resolved[495]: Server returned error NXDOMAIN, mitigating potent
ial DNS violation DVE-2018-0001, retrying transaction with reduced feature level UDP.
Apr 25 21:21:01 vbox-test charon-nm: 11[IKE] retransmit 2 of request with message ID 0
Apr 25 21:21:01 vbox-test charon-nm: 11[NET] sending packet: from 192.168.11.137[49412] to somevpn
host_ip_here[500] (336 bytes)
Apr 25 21:21:01 vbox-test charon-nm: 12[NET] received packet: from somevpnhost_ip_here[500] to 192
.168.11.137[49412] (361 bytes)
Apr 25 21:21:01 vbox-test charon-nm: 12[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP)
 N(NATD_D_IP) CERTREQ N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Apr 25 21:21:01 vbox-test charon-nm: 12[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_H
MAC_SHA1/MODP_1024
Apr 25 21:21:01 vbox-test charon-nm: 12[IKE] local host is behind NAT, sending keep alives
Apr 25 21:21:01 vbox-test charon-nm: 12[IKE] received cert request for "C=RU, O=ORGANIZATION, CN=R
ootCA"
Apr 25 21:21:01 vbox-test charon-nm: 12[IKE] sending cert request for "C=RU, O=ORGANIZATION, CN=Ro
otCA"
Apr 25 21:21:01 vbox-test charon-nm: 12[IKE] authentication of 'C=RU, O=ORGANIZATION, OU=Staff, CN
=username' (myself) with RSA_EMSA_PKCS1_SHA2_256 successful
Apr 25 21:21:01 vbox-test charon-nm: 12[IKE] sending end entity cert "C=RU, O=ORGANIZATION, OU=Sta
ff, CN=username"
Apr 25 21:21:01 vbox-test charon-nm: 12[IKE] establishing CHILD_SA somevpnhost{1}
Apr 25 21:21:01 vbox-test charon-nm: 12[ENC] generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTA
CT) CERTREQ AUTH CPRQ(ADDR ADDR6 DNS NBNS DNS6) N(IPCOMP_SUP) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_AD
DR) N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
Apr 25 21:21:01 vbox-test charon-nm: 12[ENC] splitting IKE message (1548 bytes) into 2 fragments
Apr 25 21:21:01 vbox-test charon-nm: 12[ENC] generating IKE_AUTH request 1 [ EF(1/2) ]
Apr 25 21:21:01 vbox-test charon-nm: 12[ENC] generating IKE_AUTH request 1 [ EF(2/2) ]
Apr 25 21:21:01 vbox-test charon-nm: 12[NET] sending packet: from 192.168.11.137[32967] to somevpn
host_ip_here[4500] (1248 bytes)
Apr 25 21:21:01 vbox-test charon-nm: 12[NET] sending packet: from 192.168.11.137[32967] to somevpn
host_ip_here[4500] (368 bytes)
Apr 25 21:21:02 vbox-test charon-nm: 13[NET] received packet: from somevpnhost_ip_here[4500] to 19
2.168.11.137[32967] (544 bytes)
Apr 25 21:21:02 vbox-test charon-nm: 13[ENC] parsed IKE_AUTH response 1 [ EF(1/3) ]
Apr 25 21:21:02 vbox-test charon-nm: 13[ENC] received fragment #1 of 3, waiting for complete IKE m
essage
Apr 25 21:21:02 vbox-test charon-nm: 13[NET] received packet: from somevpnhost_ip_here[4500] to 19
2.168.11.137[32967] (544 bytes)
Apr 25 21:21:02 vbox-test charon-nm: 13[ENC] parsed IKE_AUTH response 1 [ EF(2/3) ]
Apr 25 21:21:02 vbox-test charon-nm: 13[ENC] received fragment #2 of 3, waiting for complete IKE m
essage
Apr 25 21:21:02 vbox-test charon-nm: 13[NET] received packet: from somevpnhost_ip_here[4500] to 19
2.168.11.137[32967] (416 bytes)
Apr 25 21:21:02 vbox-test charon-nm: 13[ENC] parsed IKE_AUTH response 1 [ EF(3/3) ]
Apr 25 21:21:02 vbox-test charon-nm: 13[ENC] received fragment #3 of 3, reassembled fragmented IKE
 message (1372 bytes)
Apr 25 21:21:02 vbox-test charon-nm: 13[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR
ADDR6 DNS6 DNS DNS) N(IPCOMP_SUP) SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADD
R) N(ADD_6_ADDR) N(ADD_6_ADDR) ]
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] received end entity cert "C=RU, O=ORGANIZATION, OU=Se
rvers, CN=somevpnhost"
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG]   using certificate "C=RU, O=ORGANIZATION, OU=Servers
, CN=somevpnhost"
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG]   using trusted ca certificate "C=RU, O=ORGANIZATION,
 CN=RootCA"
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG] checking certificate status of "C=RU, O=ORGANIZATION,
 OU=Servers, CN=somevpnhost"
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG]   fetching crl from 'https://CA_HOST_for_crl.der' ...
Apr 25 21:21:02 vbox-test charon-nm: 13[LIB] unable to fetch from https://CA_HOST_for_crl.der, no
capable fetcher found
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG] crl fetching failed
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG] certificate status is not available
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG]   reached self-signed root ca with a path length of 0
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] authentication of 'C=RU, O=ORGANIZATION, OU=Servers,
CN=somevpnhost' with ECDSA_WITH_SHA384_DER successful
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] IKE_SA somevpnhost[2] established between 192.168.11.
137[C=RU, O=ORGANIZATION, OU=Staff, CN=username]...somevpnhost_ip_here[C=RU, O=ORGANIZATION, OU=Se
```

```
rvers, CN=somevpnhost]
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] scheduling rekeying in 35691s
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] maximum IKE_SA lifetime 36291s
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] installing new virtual IP 10.10.0.1
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for 10.10.0.1 on enp0s
3.IPv4.
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] installing new virtual IP fd00::2:1
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Leaving mDNS multicast group on interface enp0s3.IPv6
 with address fe80::df85:df88:9e3b:f87f.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Joining mDNS multicast group on interface enp0s3.IPv6
 with address fd00::2:1.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for fd00::2:1 on enp0s
3.*.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Withdrawing address record for fe80::df85:df88:9e3b:f
87f on enp0s3.
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EX
T_SEQ
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] CHILD_SA somevpnhost{1} established with SPIs c88d8bc
d_i c4ea9adf_o and TS 10.10.0.1/32 fd00::2:1/128 === 0.0.0.0/0 ::/0
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] peer supports MOBIKE
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6882] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN connection: (IP Config Get) reply
 received.
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6886] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN connection: (IP4 Config Get) reply
 received
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6916] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN connection: (IP6 Config Get) reply
 received
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6943] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data: VPN Gateway: somevpnhost_ip_here
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6945] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data: Tunnel Device: (null)
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6946] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data: IPv4 configuration:
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6948] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal Address: 10.10.0.1
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6949] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal Prefix: 32
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6950] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal Point-to-Point Addres
s: 10.10.0.1
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6952] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal DNS: 10.10.10.10
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6953] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal DNS: 8.8.8.8
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6954] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   DNS Domain: '(none)'
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6956] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data: IPv6 configuration:
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6957] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal Address: fd00::2:1
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6960] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal Prefix: 128
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6962] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal Point-to-Point Addres
s: ::
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6963] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Static Route: fd00::2:1/128
Next Hop: ::
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6965] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   Internal DNS: fd00::1:1
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.6981] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Data:   DNS Domain: '(none)'
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.7018] vpn-connection[0x559339da
6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN connection: (IP Config Get) comple
te
```

```
Apr 25 21:21:02 vbox-test dbus-daemon[536]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.11' (uid=0 pid=537 comm="/usr/sbin/NetworkManager --no-daemon " label="unconfined")
Apr 25 21:21:02 vbox-test systemd[1]: Starting Network Manager Script Dispatcher Service...
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info>  [1587838862.7172] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN plugin: state changed: started (4)
Apr 25 21:21:02 vbox-test dbus-daemon[536]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Apr 25 21:21:02 vbox-test systemd[1]: Started Network Manager Script Dispatcher Service.
Apr 25 21:21:02 vbox-test charon-nm: 09[KNL] received netlink error: Invalid argument (22)
Apr 25 21:21:02 vbox-test charon-nm: 09[KNL] unable to install source route for fd00::2:1
Apr 25 21:21:02 vbox-test charon-nm: 09[IKE] installed bypass policy for fd00::2:1/128
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Withdrawing address record for fd00::2:1 on enp0s3.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Withdrawing address record for 192.168.11.137 on enp0s3.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Withdrawing address record for ::1 on lo.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Withdrawing address record for 127.0.0.1 on lo.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Host name conflict, retrying with vbox-test-2
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for fd00::2:1 on enp0s3.*.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for 10.10.0.1 on enp0s3.IPv4.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for 192.168.11.137 on enp0s3.IPv4.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for ::1 on lo.*.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for 127.0.0.1 on lo.IPv4.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Withdrawing address record for fd00::2:1 on enp0s3.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Withdrawing address record for 192.168.11.137 on enp0s3.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Withdrawing address record for ::1 on lo.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Withdrawing address record for 127.0.0.1 on lo.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Host name conflict, retrying with vbox-test-3
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Registering new address record for fd00::2:1 on enp0s3.*.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Registering new address record for 10.10.0.1 on enp0s3.IPv4.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Registering new address record for 192.168.11.137 on enp0s3.IPv4.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Registering new address record for ::1 on lo.*.
Apr 25 21:21:03 vbox-test avahi-daemon[531]: Registering new address record for 127.0.0.1 on lo.IPv4.
Apr 25 21:21:04 vbox-test avahi-daemon[531]: Withdrawing address record for fd00::2:1 on enp0s3.
Apr 25 21:21:04 vbox-test avahi-daemon[531]: Withdrawing address record for 192.168.11.137 on enp0s3.
Apr 25 21:21:04 vbox-test avahi-daemon[531]: Withdrawing address record for ::1 on lo.
Apr 25 21:21:04 vbox-test avahi-daemon[531]: Withdrawing address record for 127.0.0.1 on lo.
...
```

One of possible workarounds is to disable avahi-daemon service.

Questions

1. Is it possible to make VPN connection with a protected keyfile? If "yes", then "how"?)
2. If more information or tests needed, then I'm ready to provide them.

Thank you in advance!

Associated revisions

Revision 532d5fc8 - 08.05.2020 18:11 - Tobias Brunner

nm: Fix password entry for private keys and allow saving it

On newer desktops the auth dialog is called with --external-ui-mode and

it seems that the password flag has to be set, otherwise the password is not stored temporarily in the profile and passed to charon-nm (not sure how this works exactly as need_secrets() is called multiple times even after the password was already entered, only before doing so the last time is the password available in that callback, but only if the flag was set). This now also allows storing the password for the private key with the profile.

Fixes #3428.

Revision d5d83756 - 08.05.2020 18:12 - Tobias Brunner

charon-nm: Clear secrets when disconnecting

The need_secrets() method is called before connect() (where we clear the previous secrets too), so e.g. a password-protected private could be decrypted with the cached password from earlier but if the password was not stored with the connection, it would later fail as no password was requested from the user that could be passed to connect().

References #3428.

History

#1 - 28.04.2020 09:53 - Tobias Brunner

- Status changed from New to Feedback

> I think this is not strongSwan's problem, but maybe somebody here knows the correct solution.

No idea.

> ## Questions
>
> 1. Is it possible to make VPN connection with a protected keyfile? If "yes", then "how"?)

It should.

> 2. If more information or tests needed, then I'm ready to provide them.

Could you please try the current versions of charon-nm and the NM plugin (see 5.8.3 but use 5.8.4).

#2 - 28.04.2020 13:47 - Alex Mfl

- File src_20200428-141109.png added

Tobias Brunner wrote:

> Could you please try the current versions of charon-nm and the NM plugin (see 5.8.3 but use 5.8.4).

Thanks for your reply. Yes, I can.

Installation from source

Required packages

```
apt install gcc make libnm-dev libssl-dev libglib2.0-dev network-manager-dev intltool libgtk-3-dev libsecret-1
-dev libnma-dev
```

strongSwan installation

```
wget http://download.strongswan.org/strongswan-5.8.4.tar.bz2
tar xjf strongswan-5.8.4.tar.bz2
cd strongswan-5.8.4

./configure --sysconfdir=/etc --prefix=/usr --libexecdir=/usr/lib \
   --disable-des --disable-md5 --disable-fips-prf --disable-gmp --enable-openssl \
```

```
   --enable-nm --enable-agent --enable-eap-gtc --enable-eap-md5 --enable-eap-identity

make
make install
```

NetworkManager-strongswan

```
cd
wget http://download.strongswan.org/NetworkManager/NetworkManager-strongswan-1.5.0.tar.bz2
tar xjf NetworkManager-strongswan-1.5.0.tar.bz2
cd NetworkManager-strongswan-1.5.0

./configure --sysconfdir=/etc --prefix=/usr --with-charon=/usr/lib/ipsec/charon-nm --without-libnm-glib

make
make install
```

Tests

Connection config

```
[connection]
id=vpnconnectionid
uuid=da5217f7-41a3-4e20-a5bd-520afe76c09e
type=vpn
autoconnect=false
permissions=user:someuser:;

[vpn]
address=somevpnhost
cert-source=file
certificate=/home/someuser/vpnkeys/caCert.pem
encap=no
esp=aes128-sha1-modp1536
ike=aes128-sha1-modp1024
ipcomp=yes
method=cert
proposal=yes
usercert=/home/someuser/vpnkeys/client-cert.pem
userkey=/home/someuser/vpnkeys/client-key.pem
virtual=yes
service-type=org.freedesktop.NetworkManager.strongswan

[ipv4]
dns=10.10.10.10;
dns-search=somedomain
method=auto

[ipv6]
addr-gen-mode=stable-privacy
dns-search=
method=ignore

[proxy]
```

ScreenshotScreenshot

src_20200428-141109.png

Protected keyfile. Same errors.

Logs:

```
Apr 28 13:43:16 vbox-test NetworkManager[98300]: <info>  [1588070596.0773] audit: op="connection-activate" uui
d="da5217f7-41a3-4e20-a5bd-520afe76c09e" name="vpnconnectionid" pid=1405 uid=1000 result="success"
Apr 28 13:43:16 vbox-test NetworkManager[98300]: <info>  [1588070596.1010] vpn-connection[0x562ca12c4330,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Started the VPN service, PID 103389
Apr 28 13:43:16 vbox-test charon-nm: 00[DMN] Starting charon NetworkManager backend (strongSwan 5.8.4)
Apr 28 13:43:16 vbox-test kernel: [ 5695.398172] Initializing XFRM netlink socket
Apr 28 13:43:16 vbox-test NetworkManager[98300]: <info>  [1588070596.1811] vpn-connection[0x562ca12c4330,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Saw the service appear; activating connection
Apr 28 13:43:16 vbox-test charon-nm: 00[LIB] loaded plugins: nm-backend charon-nm aes rc2 sha2 sha1 random non
ce x509 revocation constraints pkcs1 pkcs7 pkcs8 sshkey pem openssl curve25519 agent xcbc cmac hmac drbg kerne
l-netlink socket-default eap-identity eap-md5 eap-gtc
```

```
Apr 28 13:43:16 vbox-test charon-nm: 00[JOB] spawning 16 worker threads
Apr 28 13:43:16 vbox-test charon-nm: 05[LIB] building CRED_PRIVATE_KEY - ANY failed, tried 6 builders
Apr 28 13:43:19 vbox-test charon-nm: message repeated 2 times: [ 05[LIB] building CRED_PRIVATE_KEY - ANY faile
d, tried 6 builders]
Apr 28 13:43:19 vbox-test NetworkManager[98300]: <error> [1588070599.9164] vpn-connection[0x562ca12c4330,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: final secrets request failed to provide sufficient secre
ts
Apr 28 13:43:19 vbox-test NetworkManager[98300]: <info>  [1588070599.9277] vpn-connection[0x562ca12c4330,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN plugin: state changed: stopped (6)
```

Unprotected keyfile. No problems (except fetching crl.der and avahi-daemon)

Prepare keyfile:

```
openssl rsa -in client-key.pem -out client-key.pem
```

Logs: ShowHide

```
Apr 28 14:35:19 vbox-test systemd-resolved[492]: Server returned error NXDOMAIN, mitigating potential DNS viol
ation DVE-2018-0001, retrying transaction with reduced feature level UDP.
Apr 28 14:35:25 vbox-test NetworkManager[98300]: <info>  [1588073725.6481] audit: op="connection-activate" uui
d="da5217f7-41a3-4e20-a5bd-520afe76c09e" name="vpnconnectionid" pid=1405 uid=1000 result="success"
Apr 28 14:35:25 vbox-test NetworkManager[98300]: <info>  [1588073725.6532] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Saw the service appear; activating connection
Apr 28 14:35:25 vbox-test NetworkManager[98300]: <info>  [1588073725.6956] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN connection: (ConnectInteractive) reply received
Apr 28 14:35:25 vbox-test charon-nm: 05[CFG] received initiate for NetworkManager connection vpnconnectionid
Apr 28 14:35:25 vbox-test charon-nm: 05[CFG] using gateway identity 'somevpnhost'
Apr 28 14:35:25 vbox-test charon-nm: 05[IKE] initiating IKE_SA vpnconnectionid[3] to somevpnhost_ip_here
Apr 28 14:35:25 vbox-test charon-nm: 05[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) ]
Apr 28 14:35:25 vbox-test charon-nm: 05[NET] sending packet: from 192.168.11.137[41402] to somevpnhost_ip_here
[500] (336 bytes)
Apr 28 14:35:25 vbox-test NetworkManager[98300]: <info>  [1588073725.7683] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN plugin: state changed: starting (3)
Apr 28 14:35:25 vbox-test charon-nm: 06[NET] received packet: from somevpnhost_ip_here[500] to 192.168.11.137[
41402] (361 bytes)
Apr 28 14:35:25 vbox-test charon-nm: 06[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP
) CERTREQ N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
Apr 28 14:35:25 vbox-test charon-nm: 06[CFG] selected proposal: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MOD
P_1024
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] local host is behind NAT, sending keep alives
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] received cert request for "C=RU, O=ORGANIZATION, CN=RootCA"
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] sending cert request for "C=RU, O=ORGANIZATION, CN=RootCA"
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] authentication of 'C=RU, O=ORGANIZATION, OU=Staff, CN=mindfl' (my
self) with RSA_EMSA_PKCS1_SHA2_256 successful
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] sending end entity cert "C=RU, O=ORGANIZATION, OU=Staff, CN=mindf
l"
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] establishing CHILD_SA vpnconnectionid{3}
Apr 28 14:35:25 vbox-test charon-nm: 06[ENC] generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ
AUTH CPRQ(ADDR ADDR6 DNS NBNS DNS6) N(IPCOMP_SUP) SA TSi TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_O
NLY) N(MSG_ID_SYN_SUP) ]
Apr 28 14:35:25 vbox-test charon-nm: 06[ENC] splitting IKE message (1548 bytes) into 2 fragments
Apr 28 14:35:25 vbox-test charon-nm: 06[ENC] generating IKE_AUTH request 1 [ EF(1/2) ]
Apr 28 14:35:25 vbox-test charon-nm: 06[ENC] generating IKE_AUTH request 1 [ EF(2/2) ]
Apr 28 14:35:25 vbox-test charon-nm: 06[NET] sending packet: from 192.168.11.137[37660] to somevpnhost_ip_here
[4500] (1248 bytes)
Apr 28 14:35:25 vbox-test charon-nm: 06[NET] sending packet: from 192.168.11.137[37660] to somevpnhost_ip_here
[4500] (368 bytes)
Apr 28 14:35:26 vbox-test charon-nm: 11[NET] received packet: from somevpnhost_ip_here[4500] to 192.168.11.137
[37660] (544 bytes)
Apr 28 14:35:26 vbox-test charon-nm: 11[ENC] parsed IKE_AUTH response 1 [ EF(1/3) ]
Apr 28 14:35:26 vbox-test charon-nm: 11[ENC] received fragment #1 of 3, waiting for complete IKE message
Apr 28 14:35:26 vbox-test charon-nm: 11[NET] received packet: from somevpnhost_ip_here[4500] to 192.168.11.137
[37660] (544 bytes)
Apr 28 14:35:26 vbox-test charon-nm: 11[ENC] parsed IKE_AUTH response 1 [ EF(2/3) ]
Apr 28 14:35:26 vbox-test charon-nm: 11[ENC] received fragment #2 of 3, waiting for complete IKE message
Apr 28 14:35:26 vbox-test charon-nm: 11[NET] received packet: from somevpnhost_ip_here[4500] to 192.168.11.137
[37660] (416 bytes)
Apr 28 14:35:26 vbox-test charon-nm: 11[ENC] parsed IKE_AUTH response 1 [ EF(3/3) ]
Apr 28 14:35:26 vbox-test charon-nm: 11[ENC] received fragment #3 of 3, reassembled fragmented IKE message (13
72 bytes)
Apr 28 14:35:26 vbox-test charon-nm: 11[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR ADDR6 DNS6 D
NS DNS) N(IPCOMP_SUP) SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6
_ADDR) ]
```

```
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] received end entity cert "C=RU, O=ORGANIZATION, OU=Servers, CN=so
mevpnhost"
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG]   using certificate "C=RU, O=ORGANIZATION, OU=Servers, CN=somevpn
host"
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG]   using trusted ca certificate "C=RU, O=ORGANIZATION, CN=RootCA"
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG] checking certificate status of "C=RU, O=ORGANIZATION, OU=Servers,
 CN=somevpnhost"
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG]   fetching crl from 'https://CA_HOST_for_crl.der' ...
Apr 28 14:35:26 vbox-test charon-nm: 11[LIB] unable to fetch from https://CA_HOST_for_crl.der, no capable fetc
her found
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG] crl fetching failed
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG] certificate status is not available
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG]   reached self-signed root ca with a path length of 0
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] authentication of 'C=RU, O=ORGANIZATION, OU=Servers, CN=somevpnho
st' with ECDSA_WITH_SHA384_DER successful
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] IKE_SA vpnconnectionid[3] established between 192.168.11.137[C=RU
, O=ORGANIZATION, OU=Staff, CN=mindfl]...somevpnhost_ip_here[C=RU, O=ORGANIZATION, OU=Servers, CN=somevpnhost]
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] scheduling rekeying in 35524s
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] maximum IKE_SA lifetime 36124s
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] installing new virtual IP 10.10.0.1
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Registering new address record for 10.10.0.1 on enp0s3.IPv4.
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] installing new virtual IP fd00::2:1
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Leaving mDNS multicast group on interface enp0s3.IPv6 with add
ress fe80::df85:df88:9e3b:f87f.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Joining mDNS multicast group on interface enp0s3.IPv6 with add
ress fd00::2:1.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Registering new address record for fd00::2:1 on enp0s3.*.
Apr 28 14:35:26 vbox-test charon-nm: 11[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] CHILD_SA vpnconnectionid{3} established with SPIs c3bd1b45_i c411
a325_o and TS 10.10.0.1/32 fd00::2:1/128 === 0.0.0.0/0 ::/0
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1151] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN connection: (IP Config Get) reply received.
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1188] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN plugin: state changed: started (4)
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1196] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN connection: (IP4 Config Get) reply received
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1259] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN connection: (IP6 Config Get) reply received
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1281] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data: VPN Gateway: somevpnhost_ip_here
Apr 28 14:35:26 vbox-test charon-nm: 11[IKE] peer supports MOBIKE
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1296] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data: Tunnel Device: (null)
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1301] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data: IPv4 configuration:
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1304] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal Address: 10.10.0.1
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1306] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal Prefix: 32
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1308] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal Point-to-Point Address: 10.10.0.1
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1310] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal DNS: 10.10.10.10
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1312] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal DNS: 8.8.8.8
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1314] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   DNS Domain: '(none)'
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1316] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data: IPv6 configuration:
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1319] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal Address: fd00::2:1
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1321] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal Prefix: 128
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1323] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal Point-to-Point Address: ::
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1326] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Static Route: fd00::2:1/128   Next Hop: ::
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1328] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   Internal DNS: fd00::1:1
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1333] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Data:   DNS Domain: '(none)'
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Withdrawing address record for fe80::df85:df88:9e3b:f87f on en
p0s3.
Apr 28 14:35:26 vbox-test NetworkManager[98300]: <info>  [1588073726.1426] vpn-connection[0x562ca12c4540,da521
7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN connection: (IP Config Get) complete
```

```
Apr 28 14:35:26 vbox-test dbus-daemon[533]: [system] Activating via systemd: service name='org.freedesktop.nm_
dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.171' (uid=0 pid=98300 comm="/us
r/sbin/NetworkManager --no-daemon " label="unconfined")
Apr 28 14:35:26 vbox-test systemd[1]: Starting Network Manager Script Dispatcher Service...
Apr 28 14:35:26 vbox-test dbus-daemon[533]: [system] Successfully activated service 'org.freedesktop.nm_dispat
cher'
Apr 28 14:35:26 vbox-test systemd[1]: Started Network Manager Script Dispatcher Service.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Withdrawing address record for fd00::2:1 on enp0s3.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Withdrawing address record for 192.168.11.137 on enp0s3.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Withdrawing address record for ::1 on lo.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Withdrawing address record for 127.0.0.1 on lo.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Host name conflict, retrying with vbox-test-2
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Registering new address record for fd00::2:1 on enp0s3.*.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Registering new address record for 10.10.0.1 on enp0s3.IPv4.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Registering new address record for 192.168.11.137 on enp0s3.IP
v4.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Registering new address record for ::1 on lo.*.
Apr 28 14:35:26 vbox-test avahi-daemon[104283]: Registering new address record for 127.0.0.1 on lo.IPv4.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Withdrawing address record for fd00::2:1 on enp0s3.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Withdrawing address record for 192.168.11.137 on enp0s3.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Withdrawing address record for ::1 on lo.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Withdrawing address record for 127.0.0.1 on lo.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Host name conflict, retrying with vbox-test-3
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Registering new address record for fd00::2:1 on enp0s3.*.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Registering new address record for 10.10.0.1 on enp0s3.IPv4.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Registering new address record for 192.168.11.137 on enp0s3.IP
v4.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Registering new address record for ::1 on lo.*.
Apr 28 14:35:27 vbox-test avahi-daemon[104283]: Registering new address record for 127.0.0.1 on lo.IPv4.
Apr 28 14:35:28 vbox-test avahi-daemon[104283]: Withdrawing address record for fd00::2:1 on enp0s3.
Apr 28 14:35:28 vbox-test avahi-daemon[104283]: Withdrawing address record for 192.168.11.137 on enp0s3.
Apr 28 14:35:28 vbox-test avahi-daemon[104283]: Withdrawing address record for ::1 on lo.
Apr 28 14:35:28 vbox-test avahi-daemon[104283]: Withdrawing address record for 127.0.0.1 on lo.
Apr 28 14:35:28 vbox-test avahi-daemon[104283]: Host name conflict, retrying with vbox-test-4
```

Any ideas?

#3 - 28.04.2020 14:39 - Tobias Brunner

Sorry, I can't reproduce this. Maybe the password you entered is simply wrong, or the encrypted key file is invalid somehow. Did you uninstall all strongSwan packages before installing from source?

There will always be one such error message when the plugin determines if it requires a password, but if the password is provided and correct, there shouldn't be any more afterwards. I guess it's also possible that it's a problem with newer versions of NM (the final secrets request failed to provide sufficient secrets message sounds suspicious), I'll have to try on Ubuntu 20.04 some time.

#4 - 28.04.2020 16:23 - Alex Mfl

Tobias Brunner wrote:

> Sorry, I can't reproduce this. Maybe the password you entered is simply wrong

The password is 100% correct (copy+paste). I've used the same password to decrypt keyfile by command:

```
openssl rsa -in client-key.pem -out client-key.pem
```

> or the encrypted key file is invalid somehow.

I thought about it, and I tried to decrypt/encrypt keyfile with same password.

> Did you uninstall all strongSwan packages before installing from source?

Yes, I did. I restored the test VM from snapshot with clean Ubuntu 20.04 (no strongSwan installed). After that I installed strongSwan + NetworkManager-strongswan from source with above mentioned commands.

> There will always be one such error message when the plugin determines if it requires a password, but if the password is provided and correct, there shouldn't be any more afterwards. I guess it's also possible that it's a problem with newer versions of NM (the final secrets request failed to provide sufficient secrets message sounds suspicious), I'll have to try on Ubuntu 20.04 some time.

Thank you. I'll try to do without a protected keyfile for now.

#5 - 28.04.2020 17:01 - Alex Mfl

Additional debug information

I enabled tracing for NetworkManager:

```
nmcli general logging level TRACE
```

and I tried to establish vpn connection: Full logFull log

```
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.3998] active-connection[0x55c1ed4c2790]: cr
eating
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4016] active-connection[0x55c1ed4c2790]: se
t device "enp0s3" [0x55c1ed456e10]
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4018] device[48acd2f8b5127c5e] (enp0s3): ad
d_pending_action (1): 'activation-5'
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4022] active-connection[0x55c1ed4c2790]: co
nstructed (NMVpnConnection, version-id 5, type managed)
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.4023] auth: call[573]: CheckAuthorization(o
rg.freedesktop.NetworkManager.network-control), subject=unix-process[pid=1397, uid=1000, start=1576]
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.4251] auth: call[573]: completed: authorize
d=1, challenge=0
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.4252] dbus-object[5c1192e366042f88]: export
: "/org/freedesktop/NetworkManager/ActiveConnection/5"
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4270] active-connection[0x55c1ed4c2790]: se
t state activating (was unknown)
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4288] active-connection[0x55c1ed4c2790]: ch
eck-master-ready: not signalling (state activating, no master)
Apr 28 17:45:42 vbox-test NetworkManager[534]: <info>  [1588085142.4358] audit: op="connection-activate" uuid=
"da5217f7-41a3-4e20-a5bd-520afe76c09e" name="vpnconnectionid" pid=1397 uid=1000 result="success"
Apr 28 17:45:42 vbox-test NetworkManager[534]: <info>  [1588085142.4468] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: Saw the service appear; activating connection
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4526] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: requesting VPN secrets pass #1
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4537] Secrets requested for connection /org
/freedesktop/NetworkManager/Settings/1 (vpnconnectionid/vpn)
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4641] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x55c1ed461810) secrets requested flags 0x80000004 hints '(none)'
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4650] agent-manager: ([8febf694f4a04ca0/"vp
nconnectionid"/"vpn"]) system settings secrets sufficient
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4663] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff37c014a30) existing secrets returned
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4671] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff37c014a30) secrets request completed
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4691] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff37c014a30) new agent secrets processed
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.4695] settings: update[da5217f7-41a3-4e20-a
5bd-520afe76c09e]: get-new-secrets: update profile "vpnconnectionid" (not persisted)
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.4699] settings: storage[da5217f7-41a3-4e20-
a5bd-520afe76c09e,49aa8fc499f5a953/keyfile]: change event with connection "vpnconnectionid" (file "/etc/Networ
kManager/system-connections/vpnconnectionid.nmconnection")
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.4704] settings: update[da5217f7-41a3-4e20-a
5bd-520afe76c09e]: updating connection "vpnconnectionid" (49aa8fc499f5a953/keyfile)
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.4718] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: update agent secrets: secrets set
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4792] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: asking service if additional secrets are required
Apr 28 17:45:42 vbox-test charon-nm: 05[LIB] building CRED_PRIVATE_KEY - ANY failed, tried 6 builders
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4958] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: service indicated additional secrets required
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4966] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: requesting VPN secrets pass #2
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4977] Secrets requested for connection /org
/freedesktop/NetworkManager/Settings/1 (vpnconnectionid/vpn)
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4996] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent allowed for secrets request [6c2b2ba12295b99b/"vpnconnectioni
d"/"vpn"]
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.5005] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x55c1ed461bd0) secrets requested flags 0x4 hints '(none)'
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.5020] agent-manager: ([6c2b2ba12295b99b/"vp
nconnectionid"/"vpn"]) system settings secrets insufficient, asking agents
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.5042] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent getting secrets for request [6c2b2ba12295b99b/"vpnconnectioni
```

```
d"/"vpn"]
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.5048] agent-manager: ([6c2b2ba12295b99b/"vp
nconnectionid"/"vpn"]) request has system secrets; checking agent :1.82 for MODIFY
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.5053] auth: call[574]: CheckAuthorization(o
rg.freedesktop.NetworkManager.settings.modify.own), subject=unix-process[pid=1397, uid=1000, start=1576]
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.5109] auth: call[574]: completed: authorize
d=1, challenge=0
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.5122] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent [6c2b2ba12295b99b/"vpnconnectionid"/"vpn"] MODIFY check resul
t YES
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.5136] secret-agent[d797243476a38cb4] reques
t [d1ed8aa28dbacaec,GetSecrets,"/org/freedesktop/NetworkManager/Settings/1"]: new request...
Apr 28 17:45:43 vbox-test NetworkManager[534]: <trace> [1588085143.1782] secret-agent[d797243476a38cb4] reques
t [d1ed8aa28dbacaec,GetSecrets,"/org/freedesktop/NetworkManager/Settings/1"]: completed successfully
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1783] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent returned no secrets for request [6c2b2ba12295b99b/"vpnconnect
ionid"/"vpn"]
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1783] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff37c014a30) secrets request error: No agents were available fo
r this request.
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1786] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: asking service if additional secrets are required
Apr 28 17:45:43 vbox-test charon-nm: 05[LIB] building CRED_PRIVATE_KEY - ANY failed, tried 6 builders
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1816] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: service indicated additional secrets required
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1820] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: requesting VPN secrets pass #3
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1831] Secrets requested for connection /org
/freedesktop/NetworkManager/Settings/1 (vpnconnectionid/vpn)
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1836] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent allowed for secrets request [6c2b2ba12295b99b/"vpnconnectioni
d"/"vpn"]
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1840] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x55c1ed461bd0) secrets requested flags 0x5 hints '(none)'
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1846] agent-manager: ([6c2b2ba12295b99b/"vp
nconnectionid"/"vpn"]) system settings secrets insufficient, asking agents
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1868] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent getting secrets for request [6c2b2ba12295b99b/"vpnconnectioni
d"/"vpn"]
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1872] agent-manager: ([6c2b2ba12295b99b/"vp
nconnectionid"/"vpn"]) request has system secrets; checking agent :1.82 for MODIFY
Apr 28 17:45:43 vbox-test NetworkManager[534]: <trace> [1588085143.1876] auth: call[575]: CheckAuthorization(o
rg.freedesktop.NetworkManager.settings.modify.own), subject=unix-process[pid=1397, uid=1000, start=1576]
Apr 28 17:45:43 vbox-test NetworkManager[534]: <trace> [1588085143.1913] auth: call[575]: completed: authorize
d=1, challenge=0
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1950] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent [6c2b2ba12295b99b/"vpnconnectionid"/"vpn"] MODIFY check resul
t YES
Apr 28 17:45:43 vbox-test NetworkManager[534]: <trace> [1588085143.1959] secret-agent[d797243476a38cb4] reques
t [d9dd0d0ca754d55a,GetSecrets,"/org/freedesktop/NetworkManager/Settings/1"]: new request...
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.2784] secret-agent[d797243476a38cb4] reques
t [d9dd0d0ca754d55a,GetSecrets,"/org/freedesktop/NetworkManager/Settings/1"]: completed successfully
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.2785] agent-manager: agent[d797243476a38cb4
,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent returned secrets for request [6c2b2ba12295b99b/"vpnconnection
id"/"vpn"]
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.2792] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff380004ed0) secrets returned from agent :1.82
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.2792] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff380004ed0) secrets request completed
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.2796] settings-connection[645641685f016c99,
da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff380004ed0) new agent secrets processed
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.2796] settings: update[da5217f7-41a3-4e20-a
5bd-520afe76c09e]: get-new-secrets: update profile "vpnconnectionid" (not persisted)
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.2797] settings: storage[da5217f7-41a3-4e20-
a5bd-520afe76c09e,49aa8fc499f5a953/keyfile]: change event with connection "vpnconnectionid" (file "/etc/Networ
kManager/system-connections/vpnconnectionid.nmconnection")
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.2797] settings: update[da5217f7-41a3-4e20-a
5bd-520afe76c09e]: updating connection "vpnconnectionid" (49aa8fc499f5a953/keyfile)
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.2958] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: asking service if additional secrets are required
Apr 28 17:45:46 vbox-test charon-nm: 05[LIB] building CRED_PRIVATE_KEY - ANY failed, tried 6 builders
Apr 28 17:45:46 vbox-test NetworkManager[534]: <error> [1588085146.3157] vpn-connection[0x55c1ed4c2790,da5217f
7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: final secrets request failed to provide sufficient secrets
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.3160] active-connection[0x55c1ed4c2790]: se
t state deactivated (was activating)
```

```
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.3181] active-connection[0x55c1ed4c2790]: check-master-ready: not signalling (state deactivated, no master)
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.3183] device[48acd2f8b5127c5e] (enp0s3): remove_pending_action (0): 'activation-5'
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.3220] settings: update[da5217f7-41a3-4e20-a5bd-520afe76c09e]: clear-secrets: update profile "vpnconnectionid" (not persisted)
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.3230] settings: storage[da5217f7-41a3-4e20-a5bd-520afe76c09e,49aa8fc499f5a953/keyfile]: change event with connection "vpnconnectionid" (file "/etc/NetworkManager/system-connections/vpnconnectionid.nmconnection")
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.3232] settings: update[da5217f7-41a3-4e20-a5bd-520afe76c09e]: updating connection "vpnconnectionid" (49aa8fc499f5a953/keyfile)
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.3236] settings-connection[645641685f016c99,da5217f7-41a3-4e20-a5bd-520afe76c09e]: update agent secrets: secrets cleared
Apr 28 17:45:46 vbox-test NetworkManager[534]: <trace> [1588085146.3280] dbus-object[5c1192e366042f88]: unexport: "/org/freedesktop/NetworkManager/ActiveConnection/5"
Apr 28 17:45:46 vbox-test NetworkManager[534]: <debug> [1588085146.3338] active-connection[0x55c1ed4c2790]: disposing
Apr 28 17:45:56 vbox-test systemd-resolved[493]: Server returned error NXDOMAIN, mitigating potential DNS violation DVE-2018-0001, retrying transaction with reduced feature level UDP.
Apr 28 17:45:56 vbox-test systemd-resolved[493]: Server returned error NXDOMAIN, mitigating potential DNS violation DVE-2018-0001, retrying transaction with reduced feature level UDP.
Apr 28 17:46:55 vbox-test NetworkManager[534]: <trace> [1588085215.2261] settings: [timestamps-keyfile]: updated entry for timestamps.db635ae3-2a95-3229-b647-9e25606e2037
Apr 28 17:46:55 vbox-test NetworkManager[534]: <trace> [1588085215.2262] settings: [timestamps-keyfile]: schedule flushing changes to disk
Apr 28 17:46:55 vbox-test NetworkManager[534]: <trace> [1588085215.2487] settings: [timestamps-keyfile]: write keyfile: "/var/lib/NetworkManager/timestamps"
Apr 28 17:46:55 vbox-test NetworkManager[534]: <trace> [1588085215.8608] device[48acd2f8b5127c5e] (enp0s3): connectivity: [IPv4] periodic-check: re-scheduled in 299999 milliseconds (300 seconds interval)
Apr 28 17:46:55 vbox-test NetworkManager[534]: <trace> [1588085215.8609] device[48acd2f8b5127c5e] (enp0s3): connectivity: [IPv4] start check (seq:26, periodic-check)
Apr 28 17:46:55 vbox-test NetworkManager[534]: <debug> [1588085215.8613] connectivity: (enp0s3,IPv4,26) start request to 'http://connectivity-check.ubuntu.com/' (try resolving 'connectivity-check.ubuntu.com' using systemd-resolved)
Apr 28 17:46:55 vbox-test NetworkManager[534]: <trace> [1588085215.8654] connectivity: (enp0s3,IPv4,26) adding 'connectivity-check.ubuntu.com:80:35.224.99.156' to curl resolve list
Apr 28 17:46:55 vbox-test NetworkManager[534]: <trace> [1588085215.8655] connectivity: (enp0s3,IPv4,26) adding 'connectivity-check.ubuntu.com:80:35.222.85.5' to curl resolve list
Apr 28 17:46:57 vbox-test NetworkManager[534]: <debug> [1588085217.2467] connectivity: (enp0s3,IPv4,26) check completed: FULL; status header found
Apr 28 17:46:57 vbox-test NetworkManager[534]: <trace> [1588085217.2482] device[48acd2f8b5127c5e] (enp0s3): connectivity: [Ipv4] complete check (seq:26, state:FULL)
Apr 28 17:46:57 vbox-test NetworkManager[534]: <trace> [1588085217.2493] device[48acd2f8b5127c5e] (enp0s3): connectivity: [IPv4] periodic-check: re-scheduled in 298610 milliseconds (300 seconds interval)
```

I think interesting here is:

```
...
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1783] agent-manager: agent[d797243476a38cb4,:1.82/org.gnome.Shell.NetworkAgent/1000]: agent returned no secrets for request [6c2b2ba12295b99b/"vpnconnectionid"/"vpn"]
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1783] settings-connection[645641685f016c99,da5217f7-41a3-4e20-a5bd-520afe76c09e]: (vpn:0x7ff37c014a30) secrets request error: No agents were available for this request.
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1786] vpn-connection[0x55c1ed4c2790,da5217f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: asking service if additional secrets are required
Apr 28 17:45:43 vbox-test charon-nm: 05[LIB] building CRED_PRIVATE_KEY - ANY failed, tried 6 builders
...
```

Establishing vpn connection from console

Hmm. It's works o_O

```
$ nmcli --ask connection up vpnconnectionid
Private key decryption password required to establish VPN connection 'vpnconnectionid'.
Password: (vpn.secrets.password): ••••••••••••
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
```

It looks like GUI problem only.

#6 - 28.04.2020 19:22 - Tobias Brunner

OK, I was able to reproduce this on Ubuntu 20.04. It seems that if NM (or whoever) calls the auth dialog with --external-ui-mode (not the case on older versions) it somehow does not make the password available to the VPN plugin afterwards if the password flags are not set beforehand, so that's

different from older NM versions. How this works exactly I don't really understand, the need_secrets() method is called several times even after the password was requested but we can't retrieve the password there. So maybe there is something else missing.

Anyway, I pushed a possible fix to the *3428-nm-cert-pw* branch (you need to edit the profile so the password flag is set).

#7 - 29.04.2020 11:09 - Alex Mfl

Tobias Brunner wrote:

> OK, I was able to reproduce this on Ubuntu 20.04. It seems that if NM (or whoever) calls the auth dialog with --external-ui-mode (not the case on older versions) it somehow does not make the password available to the VPN plugin afterwards if the password flags are not set beforehand, so that's different from older NM versions. How this works exactly I don't really understand, the need_secrets() method is called several times even after the password was requested but we can't retrieve the password there. So maybe there is something else missing.
>
> Anyway, I pushed a possible fix to the *3428-nm-cert-pw* branch (you need to edit the profile so the password flag is set).

Thank you! I'll try to check it in the next couple of days.

#8 - 08.05.2020 03:42 - Alex Mfl

3428-nm-cert-pw branch

I have tested version from the new branch. Nothing changed. Build commands (for history):

```
apt install git autogen autoconf libtool gperf bison flex gcc make libnm-dev libssl-dev libglib2.0-dev network
-manager-dev intltool libgtk-3-dev libsecret-1-dev libnma-dev libcurl4-openssl-dev
git clone https://github.com/strongswan/strongswan
cd strongswan
git checkout 3428-nm-cert-pw
./autogen.sh
./configure --sysconfdir=/etc --prefix=/usr --libexecdir=/usr/lib --enable-curl \
   --disable-des --disable-md5 --disable-fips-prf --disable-gmp --enable-openssl \
   --enable-nm --enable-agent --enable-eap-gtc --enable-eap-md5 --enable-eap-identity
make
make install
```

password-flags option

But password-flags in NetworkManager connection config works! I have tested:

- Ubuntu 20.04 repo version
- latest stable version
- new 3428-nm-cert-pw branch version

It works like expected and needed: asks password, but doesn't save it.

NetworkManager connection config: ShowHide

```
[connection]
id=vpnconnectionid
uuid=da5217f7-41a3-4e20-a5bd-520afe76c09e
type=vpn
autoconnect=false
permissions=user:someuser:;


[vpn]
address=somevpnhost
cert-source=file
certificate=/home/someuser/vpnkeys/caCert.pem
encap=no
esp=aes128-sha1-modp1536
ike=aes128-sha1-modp1024
ipcomp=yes
method=cert
password-flags=2
proposal=yes
usercert=/home/someuser/vpnkeys/client-cert.pem
userkey=/home/someuser/vpnkeys/client-key.pem
virtual=yes
service-type=org.freedesktop.NetworkManager.strongswan
```

```
[ipv4]
dns=10.10.10.10;
dns-search=somedomain
method=auto

[ipv6]
addr-gen-mode=stable-privacy
dns-search=
method=ignore

[proxy]
```

What next

The password-flags workaround it is enough for me. But it would be nice add a checkbox/menu/or_something_else into NetworkManager plugin for connection config generation with a password-flags option.

I think the issue is solved. Thank you!

#9 - 08.05.2020 10:42 - Tobias Brunner

> Build commands (for history):

But incomplete. That doesn't build/install the new version of the NM plugin (in source:src/frontends/gnome), only the D-Bus service (charon-nm), which hasn't changed in that branch (I did push a commit now, though, that fixes an issue when reconnecting with a password-protected private key while charon-nm is still running).

> But it would be nice add a checkbox/menu/or_something_else into NetworkManager plugin for connection config generation with a password-flags option.

There is, it's built into the password field. With the changes to the plugin in the mentioned branch, just open the connection in the editor and save it again, the password flag should be set.

#10 - 08.05.2020 14:39 - Alex Mfl

Tobias Brunner wrote:

> But incomplete. That doesn't build/install the new version of the NM plugin (in source:src/frontends/gnome), only the D-Bus service (charon-nm), which hasn't changed in that branch (I did push a commit now, though, that fixes an issue when reconnecting with a password-protected private key while charon-nm is still running).

Yes, looks like I missed it.

Cloned git repo state (for proof)

```
root@vbox-test:~/strongswan# git branch
* 3428-nm-cert-pw
  master

root@vbox-test:~/strongswan# git rev-parse HEAD
20264da08de4e2cc0853ff8c3c0d3dfc9607195d

root@vbox-test:~/strongswan# git pull
Already up to date.
```

Full rebuild

```
make clean
./autogen.sh
./configure --sysconfdir=/etc --prefix=/usr --libexecdir=/usr/lib --enable-curl \
   --disable-des --disable-md5 --disable-fips-prf --disable-gmp --enable-openssl \
```

```
   --enable-nm --enable-agent --enable-eap-gtc --enable-eap-md5 --enable-eap-identity
make
make install

cd src/frontends/gnome
apt install gnome-common
./autogen.sh --without-libnm-glib
./configure --sysconfdir=/etc --prefix=/usr --with-charon=/usr/lib/ipsec/charon-nm --without-libnm-glib
make
make install
rm /etc/NetworkManager/system-connections/*
reboot  # not necessary. I think systemctl restart NetworkManager is enough too.
```

Test

1. New connection added (without edits by hands in /etc/NetworkManager/system-connections)
2. Established VPN connection (password asked, but didn't save in /etc/NetworkManager/system-connections)

The password-flags=2 option exists in generated connection config file. So It works perfectly well! Thank you.

#11 - 08.05.2020 18:18 - Tobias Brunner

- Tracker changed from Issue to Bug

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.9.0

- Resolution set to Fixed

Thanks for testing. I've released a new version of the NM plugin (1.5.1) that includes the GUI fix. The fix for charon-nm will be included in version:5.8.5.

Files

src_20200428-141109.png	70.3 KB	28.04.2020	Alex Mfl