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

```plaintext
[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-shal-modp1536
ike=aes128-shal-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]
dns-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,6DC24DE9A76BAC92C3203C662D71BE0
....
-----END RSA PRIVATE KEY-----

• unprotected: ShowHide

-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----

Logs

Apr 25 21:30:15 vbox-test NetworkManager[537]: <info> [1587839415.9416] audit: op="connection-activate" uuid="04f56322-d291-4015-9758-6d54960518c3" name="vpnconnectionid" pid=1392 uid=1000 result="success"
Apr 25 21:30:15 vbox-test NetworkManager[537]: <info> [1587839415.94165] vpn-connection[0x559339da6750,04f56322-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 builders
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[0x559339da6750,04f56322-d291-4015-9758-6d54960518c3,"vpnconnectionid",0]: final secrets request failed to provide 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-activate" uuid="04f56322-d291-4015-9758-6d54960518c3" name="somevpnhost" pid=3622 uid=1000 result="success"
Apr 25 21:20:50 vbox-test NetworkManager[537]: <info> [1587838850.6726] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: Saw the service appear; activating connection
Apr 25 21:20:50 vbox-test NetworkManager[537]: <info> [1587838850.6975] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d54960518c3,"somevpnhost",0]: VPN connection: (ConnectInteractive) reply received
Apr 25 21:20:50 vbox-test charon-nm: 05[CFG] received initiate for NetworkManager connection somevpnhost
Apr 25 21:20:50 vbox-test charon-nm: 05[CFG] using CA certificate, gateway identity 'somevpnhost'
Apr 25 21:20:50 vbox-test NetworkManager[537]: <info> [1587838850.7091] vpn-connection[0x559339da6540,04f56322-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 21:21:00 vbox-test systemd-resolved[495]: Server returned error NXDOMAIN, mitigating potential 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 potential
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
host_ip_here[500] (336 bytes)
Apr 25 21:21:01 vbox-test charon-nm: 12[NET] received packet: from somevpn_host_ip_here[500] to 192
.168.11.137[49412] (361 bytes)
) N(NADT_D_IP) CERTREQ N(FRAG_SUP) N(HASH_ALG) N(MULT_AUTH) ]
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] receiving cert request for "C=RU, O=ORGANIZATION, CN=Ro
otCA"
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
=userid' (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=Staff,
CN=userid"
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(ADD ADDR 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) ]
host_ip_here[4500] (1248 bytes)
host_ip_here[4500] (368 bytes)
2.168.11.137[32967] (544 bytes)
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[ENC] received fragment #2 of 3, waiting for complete IKE m
essage
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(ADD
R ADDR DNS DNS6 DNS) N(IPCOMP_SUP) SA TSI TSr N(MOBIKE_SUP) N(NO_ADD_ADDR) N(MULT_AUTH) N(EAP_O
Ly) N(MSG_ID_SYN_SUP) ]
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] received end entity cert "C=RU, O=ORGANIZATION, OU=Se
rvers, CN=somevpnhost".
rvers, CN=somevpnhost"
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG] using trusted ca certificate "C=RU, O=ORGANIZATION, CN=Ro
otCA"
rvers, CN=somevpnhost".
Apr 25 21:21:02 vbox-test charon-nm: 13[CFG] fetching crl from 'https://CA_HOST_for_crl.der' ... no
able to fetch from https://CA_HOST_for_crl.der, no capable fetcher found
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
rvers, 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 192.168.11.1
37(C=RU, O=ORGANIZATION, OU=Staff, CN=userid)...somevpn_host_ip_here[C=RU, O=ORGANIZATION, OU=Se
rvers, CN=somevpnhost]
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 enp0s3.IPv4.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Joining mDNS multicast group on interface enp0s3.IPv6 with address fe80::df85:df88:9e3b:f87f.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Registering new address record for fd00::2:1 on enp0s3.IPv6 with address fd00::2:1.
Apr 25 21:21:02 vbox-test avahi-daemon[531]: Withdrawing address record for fe80::df85:df88:9e3b:f87f on enp0s3.
Apr 25 21:21:02 vbox-test charon-nm: 13[IKE] CHILD_SA somevpnhost{1} established with SPIs c88d8bc
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info> [1587838862.6882] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d4960518c3,"somevpnhost",0]: VPN connection: (IP Config Get) reply received.
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info> [1587838862.6886] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d4960518c3,"somevpnhost",0]: VPN connection: (IP4 Config Get) reply received
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info> [1587838862.6916] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d4960518c3,"somevpnhost",0]: VPN connection: (IP6 Config Get) reply received
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info> [1587838862.6948] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d4960518c3,"somevpnhost",0]: Data: IPv4 configuration:
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info> [1587838862.6952] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d4960518c3,"somevpnhost",0]: Data: Internal Address: 10.10.0.1
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info> [1587838862.6957] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d4960518c3,"somevpnhost",0]: Data: IPv6 configuration:
Apr 25 21:21:02 vbox-test NetworkManager[537]: <info> [1587838862.6958] vpn-connection[0x559339da6540,04f56322-d291-4015-9758-6d4960518c3,"somevpnhost",0]: Data: Static Route: fd00::2:1 Next Hop: ::
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!

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_20200426-141109.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

```bash
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

```bash
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

```bash
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

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

08.05.2020
address=somevpnhost
cert-source=file
certificate=/home/someuser/vpnkeys/caCert.pem
enca=no
esp=aes128-shal-modp1536
ike=aes128-shal-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]

Logs:
Apr 28 13:43:16 vbox-test NetworkManager[98300]: <info> [1588070596.0773] audit: op="connection-activate" uuid=\"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-vpn 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-vpn 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 NetworkManager[98300]: <error> [1588070599.9164] vpn-connection[0x562ca12c4330,da521 7f7-41a3-4e20-a5bd-520afe76c09e,"vpnconnectionid",0]: final secrets request failed to provide sufficient secre
Apr 28 13:43:16 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:
oppenssl rsa -in client-key.pem -out client-key.pem

Logs:
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
A
Apr 28 14:35:25 vbox-test NetworkManager[98300]: <info> [1588073725.7683] vpn-connection[0x562ca12c4540,da5217f7-4f1a-3e20-a5bd-520afe76c09e,"vpnconnectionid",0]: VPN plugin: state changed: starting (3)
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] local host is behind NAT, sending keep alive
Apr 28 14:35:25 vbox-test charon-nm: 06[IKE] received fragment #1 of 3, waiting for complete IKE message
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) ]
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 Mi

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 Mi

Additional debug information

I enabled tracing for NetworkManager:

```
nmcli general logging level TRACE
```

and I tried to establish vpn connection: Full log

```
Apr 28 17:45:42 vbox-test NetworkManager[534]: <trace> [1588085142.3998] active-connection[0x55c1ed4c2790]: creating
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4016] active-connection[0x55c1ed4c2790]: set device "enp0s3" [0x55c1ed456e10]
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4018] device[48acd2f8b5127c5e] (enp0s3): ad
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4022] active-connection[0x55c1ed4c2790]: co
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4022] active-connection[0x55c1ed4c2790]: co
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4023] auth: call[573]: CheckAuthorization(o
Apr 28 17:45:42 vbox-test NetworkManager[534]: <debug> [1588085142.4251] auth: call[573]: completed: authorize
eck-master-ready: not signalling (state activating, no master)
```

08.05.2020
nnectivity: [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-d-resolved)
Apr 28 17:47:55 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 17:47:55 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 17:47:57 vbox-test NetworkManager[534]: <debug> [1588085217.2467] connectivity: (enp0s3,IPv4,26) check completed: FULL; status header found

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"*/"]
Apr 28 17:45:43 vbox-test NetworkManager[534]: <debug> [1588085143.1785] settings-connection[645641685f016c99,da5217f7-41a3-4e20-a5bd-520afed6c09e]: (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-520afed6c09e,"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 networkmanager-dev intltool libgtk-3-dev libsecret-1-dev libnma-dev libcurl4-openssl-dev
```

git clone https://github.com/strongswan/strongswan

cd strongswan
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-shal-modp1536
ike=aes128-shal-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!
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.

Files

```
<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>src_20200428-141109.png</td>
<td>70.3 KB</td>
<td>28.04.2020</td>
<td>Alex Mfl</td>
</tr>
</tbody>
</table>
```