strongSwan - Bug #852

NetworkManager assumes failure during reauthentication

19.02.2015 21:33 - Grace McGinley

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	networkmanager (charon-nm)		
Target version:	5.8.3		
Affected version:	5.1.2	**Resolution:**	Fixed

Description

After making a connection using strongSwan with NetworkManager, some time after the connection is made, a reauthentication is performed according to the strongSwan configuration. When this occurs, NetworkManager thinks that the VPN failed and assumes that it is no longer present, however, the connection prevails.

Sometimes, the connection will break permanently, and must be re-established via the nm-applet manually.

syslog (local IP is %%%.%%%.%%%.%%%, VPN gateway is ###.###.###.###:

```
13:43 charon-nm: 01[IKE] sending keep alive to ###.###.###.###[4500]
14:03 charon-nm: 12[IKE] sending keep alive to ###.###.###.###[4500]
14:23 charon-nm: 11[IKE] sending keep alive to ###.###.###.###[4500]
14:36 charon-nm: 10[IKE] reauthenticating IKE_SA connection-name[1]
14:36 charon-nm: 10[IKE] deleting IKE_SA connection-name[1] between %%%.%%%.%%%.%%%[C=US, CN=mysel
f]...###.###.###.###[###.###.###.###]
14:36 charon-nm: 10[IKE] sending DELETE for IKE_SA connection-name[1]
14:36 charon-nm: 10[ENC] generating INFORMATIONAL request 7 [ D ]
14:36 charon-nm: 10[NET] sending packet: from %%%.%%%.%%%.%%%[4500] to ###.###.###.###[4500] (76 b
ytes)
14:36 charon-nm: 14[NET] received packet: from ###.###.###.###[4500] to %%%.%%%.%%%.%%%[4500] (76
bytes)
14:36 charon-nm: 14[ENC] parsed INFORMATIONAL response 7 [ ]
14:36 charon-nm: 14[IKE] IKE_SA deleted
14:37 NetworkManager[1026]: <warn> VPN plugin failed: 1
14:37 NetworkManager[1026]: <info> VPN plugin state changed: stopped (6)
14:37 NetworkManager[1026]: <info> VPN plugin state change reason: 0
14:37 charon-nm: 14[IKE] installing new virtual IP 172.16.0.1
14:37 charon-nm: 14[IKE] restarting CHILD_SA connection-name
14:37 charon-nm: 14[IKE] initiating IKE_SA connection-name[2] to ###.###.###.###
14:37 charon-nm: 14[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
14:37 charon-nm: 14[NET] sending packet: from %%%.%%%.%%%.%%%[53518] to ###.###.###.###[500] (1000
 bytes)
14:37 charon-nm: 13[NET] received packet: from ###.###.###.###[500] to %%%.%%%.%%%.%%%[53518] (38
bytes)
14:37 charon-nm: 13[ENC] parsed IKE_SA_INIT response 0 [ N(INVAL_KE) ]
14:37 charon-nm: 13[IKE] peer didn't accept DH group MODP_1024, it requested MODP_2048
14:37 charon-nm: 16[KNL] %%%.%%%.%%%.%%% disappeared from eth0
14:37 charon-nm: 14[KNL] error uninstalling route installed with policy 10.255.255.0/24 === 172.16
.0.1/32 fwd
14:37 charon-nm: 13[IKE] initiating IKE_SA connection-name[2] to ###.###.###.###
14:37 charon-nm: 13[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) ]
14:37 charon-nm: 13[NET] sending packet: from %%%.%%%.%%%.%%%[53518] to ###.###.###.###[500] (1128
 bytes)
14:37 charon-nm: 14[KNL] error uninstalling route installed with policy 10.10.10.0/24 === 172.16.0
.1/32 fwd
14:37 charon-nm: 14[KNL] received netlink error: Cannot assign requested address (99)
14:37 charon-nm: 11[KNL] %%%.%%%.%%%.%%% appeared on eth0
14:37 charon-nm: 09[NET] error writing to socket: Network is unreachable
14:37 charon-nm: 04[IKE] old path is not available anymore, try to find another
14:37 charon-nm: 04[IKE] looking for a route to ###.###.###.### ...
14:37 charon-nm: 04[IKE] no route found to reach ###.###.###.###, MOBIKE update deferred
```

```
14:37 kernel: [ 9566.854160] userif-3: sent link down event.
14:37 kernel: [ 9566.854166] userif-3: sent link up event.
14:38 charon-nm: 11[IKE] old path is not available anymore, try to find another
14:38 charon-nm: 11[IKE] looking for a route to ###.###.###.### ...
14:38 charon-nm: 11[IKE] no route found to reach ###.###.###.###, MOBIKE update deferred
14:38 NetworkManager[1026]: <info> Policy set 'Wired connection 1' (eth0) as default for IPv4 routing and DNS.
14:38 vmnet-natd: RTM_NEWROUTE: index:2
14:39 dbus[882]: [system] Activating service name='org.freedesktop.nm_dispatcher' (using servicehelper)
14:39 NetworkManager[1026]: <warn> error disconnecting VPN: Could not process the request because no VPN connection was active.
14:39 charon-nm: 14[KNL] interface tun0 deactivated
14:39 charon-nm: 04[KNL] 172.16.0.1 disappeared from tun0
14:40 dbus[882]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
14:41 charon-nm: 11[IKE] retransmit 1 of request with message ID 0
14:41 charon-nm: 11[NET] sending packet: from %%%.%%%.%%%.%%%[53518] to ###.###.###.###[500] (1128 bytes)
14:41 charon-nm: 10[IKE] retransmit 2 of request with message ID 0
14:41 charon-nm: 10[NET] sending packet: from %%%.%%%.%%%.%%%[53518] to ###.###.###.###[500] (1128 bytes)
14:41 charon-nm: 16[NET] received packet: from ###.###.###.###[500] to %%%.%%%.%%%.%%%[53518] (465 bytes)
14:41 charon-nm: 16[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(MULT_AUTH) ]
14:41 charon-nm: 15[MGR] ignoring request with ID 0, already processing
14:41 charon-nm: 16[IKE] local host is behind NAT, sending keep alives
14:41 charon-nm: 16[IKE] received cert request for "C=US, CN=connection-name"
14:41 charon-nm: 16[IKE] sending cert request for "C=US, CN=connection-name"
14:41 charon-nm: 16[IKE] authentication of 'C=US, CN=myself' (myself) with RSA signature successful
14:41 charon-nm: 16[IKE] sending end entity cert "C=US, CN=myself"
14:41 charon-nm: 16[IKE] establishing CHILD_SA connection-name
14:41 charon-nm: 16[ENC] generating IKE_AUTH request 1 [ IDi CERT N(INIT_CONTACT) CERTREQ AUTH CPRQ(ADDR DNS NBNS) SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(MULT_AUTH) N(EAP_ONLY) ]
14:41 charon-nm: 16[NET] sending packet: from %%%.%%%.%%%.%%%[4500] to ###.###.###.###[4500] (1388 bytes)
14:41 charon-nm: 13[NET] received packet: from ###.###.###.###[4500] to %%%.%%%.%%%.%%%[4500] (1308 bytes)
```

When this occurs, the lock icon which appears in the lower right corner of the connection status indicator in nm-applet disappears, but the connection is still present and fully functional.

I attempted to increase verbosity in the logs but was unable to do so no matter the changes made to /etc/ipsec.conf, or /etc/strongswan.d/charon-logging.conf.

When the connection does break (not always), the following messages are reported in syslog:

```
charon-nm: 11[IKE] installing new virtual IP 172.16.0.1
charon-nm: 11[IKE] CHILD_SA connection-name{2} established with SPIs cdcbd95d_i c89a6959_o and TS 172.16.0.1/32 === 10.255.255.0/24 10.10.10.0/24
charon-nm: 11[IKE] received AUTH_LIFETIME of 9839s, scheduling reauthentication in 9239s
charon-nm: 11[IKE] peer supports MOBIKE
charon-nm: 00[DMN] signal of type SIGTERM received. Shutting down
charon-nm: 00[IKE] deleting IKE_SA connection-name[2] between %%%.%%%.%%%.%%%[C=US, CN=myself]...###.###.###.###[###.###.###.###]
charon-nm: 00[IKE] sending DELETE for IKE_SA connection-name[2]
charon-nm: 00[ENC] generating INFORMATIONAL request 2 [ D ]
charon-nm: 00[NET] sending packet: from %%%.%%%.%%%.%%%[4500] to ###.###.###.###[4500] (76 bytes)
vmnet-natd: RTM_DELADDR: index:2, addr:172.16.0.1
NetworkManager[1010]:    SCPlugin-Ifupdown: devices removed (path: /sys/devices/virtual/net/tun0, iface: tun0)
NetworkManager[1010]: <info> VPN service 'strongswan' disappeared
kernel: [ 9696.205768] userif-3: sent link down event.
kernel: [ 9696.205777] userif-3: sent link up event.
```

It's unclear as to where the SIGTERM came from, and due to the inability to increase logging verbosity, I was unable to identify the cause.

Since the command DELETE is sent for IKE_SA the connection is unable to be re-established, and must be connected to via the nm-applet.

It's clear that the connection is working correctly prior to the SIGTERM as no other messages appear which indicate a problem when comparing with a manual connection. It's consistent that the SIGTERM is received after the message peer supports MOBIKE. In a manual connection, further messages are received.

The SIGTERM issue may be a separate issue.

Package information:

```
Package: strongswan-nm
State: installed
Automatically installed: no
Version: 5.1.2-0ubuntu2.2
Priority: optional
Section: universe/net
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Uncompressed Size: 495 k
Depends: libc6 (>= 2.4), libdbus-glib-1-2 (>= 0.78), libglib2.0-0 (>= 2.37.3), libnm-glib-vpn1 (>=
 0.7.999), libnm-util2 (>= 0.7.0), libstrongswan, strongswan-ike
Recommends: network-manager-strongswan
Conflicts: strongswan-nm
Description: strongSwan charon for interaction with NetworkManager
 The strongSwan VPN suite uses the native IPsec stack in the standard Linux kernel. It supports bo
th the IKEv1 and IKEv2 protocols.

 This plugin provides special charon deamon which interfaces with NetworkManager to configure and
control the IKEv2 daemon directly through D-Bus. It is designed to work in conjunction with the
 network-manager-strongswan package, providing a simple graphical frontend to configure IPsec base
d VPNs.
Homepage: http://www.strongswan.org
```

OS: Linux Mint 17.1

Associated revisions

Revision 571769fe - 14.02.2020 13:58 - Tobias Brunner

Merge branch 'nm-reauth'

With these changes, the NM service should be able to handle
reauthentication (and redirection) by switching to the new IKE_SA and
not considering the old SA going down an error.

Fixes #852.

History

#1 - 20.02.2015 13:59 - Tobias Brunner

- Status changed from New to Feedback

> After making a connection using strongSwan with NetworkManager, some time after the connection is made, a reauthentication is performed according to the strongSwan configuration. When this occurs, NetworkManager thinks that the VPN failed and assumes that it is no longer present, however, the connection prevails.

Yes, the strongSwan NM backend does currently not follow re-authentications. So when the old IKE_SA is terminated the backend simply notifies NM that the connection went down.

I added some additional hooks a while ago to better track re-authentication (reestablishing IKE_SAs in general actually), because I needed this for the Android app. So it should be possible to improve the behavior of the NM backend in such situations too.

> I attempted to increase verbosity in the logs but was unable to do so no matter the changes made to /etc/ipsec.conf, or /etc/strongswan.d/charon-logging.conf.

The daemon used by the NM plugin is called *charon-nm*, so you have to add the logger configuration to the *charon-nm* section in strongswan.conf, not the *charon* section. And settings in ipsec.conf have no effect at all on *charon-nm*.

> It's unclear as to where the SIGTERM came from, and due to the inability to increase logging verbosity, I was unable to identify the cause.

I think this signal is sent by NM after the connection has been "down" for a while, that is, when it seems down from NM's point of view because there was a status update that said so when the old IKE_SA was terminated.

The configuration used by the NM backend does not explicitly enable re-authentication, but if the server is configured with *reauth=yes* it will request the client to re-authenticate after a while. So a workaround would be to set *reauth=no* on the server.

#2 - 20.02.2015 17:19 - Grace McGinley

Tobias Brunner wrote:

> > I attempted to increase verbosity in the logs but was unable to do so no matter the changes made to /etc/ipsec.conf, or /etc/strongswan.d/charon-logging.conf.
>
> The daemon used by the NM plugin is called *charon-nm*, so you have to add the logger configuration to the *charon-nm* section in strongswan.conf, not the *charon* section. And settings in ipsec.conf have no effect at all on *charon-nm*.

Ah, I had overlooked the section which stated this:

```
Note: Many of the options in this section also apply to charon-cmd, charon-systemd and other charon derivative
s. Just use their respective name (e.g. charon-cmd instead of charon).
```

After renaming the charon section to charon-nm, the logging is working as expected. Thanks for the clarification.

> > It's unclear as to where the SIGTERM came from, and due to the inability to increase logging verbosity, I was unable to identify the cause.
>
> I think this signal is sent by NM after the connection has been "down" for a while, that is, when it seems down from NM's point of view because there was a status update that said so when the old IKE_SA was terminated.
>
> The configuration used by the NM backend does not explicitly enable re-authentication, but if the server is configured with *reauth=yes* it will request the client to re-authenticate after a while. So a workaround would be to set *reauth=no* on the server.

I've configured the connection on the server as described above (explicit reauth=no, since the default is reauth=yes) and I believe this is a fine workaround for the issue. If there are further issues, I think that additional logging will be helpful.

#3 - 09.07.2015 21:01 - Olaf Martens

Good to know how any hangs can be mitigated - however, is there anything planned on fixing this so that charon-nm becomes aware of reauthentication? This problem can be annoying at times, especially when you are working on an NFS that has been exported through an IPsec tunnel.

#4 - 10.07.2015 11:49 - Tobias Brunner

> however, is there anything planned on fixing this so that charon-nm becomes aware of reauthentication?

There are no immediate plans to do so.

> This problem can be annoying at times, especially when you are working on an NFS that has been exported through an IPsec tunnel.

Didn't the *reauth=no* workaround work for you?

#5 - 10.07.2015 15:41 - Grace McGinley

Something to consider in this is if a connecting user doesn't have the authority to change the settings on the server to disable reauth. Also reauth may be a requirement due to security policy, or some other requirement. Sometimes disabling reauth may not be an option.

#6 - 12.07.2015 10:38 - Olaf Martens

Tobias Brunner wrote:

> Didn't the *reauth=no* workaround work for you?

Sorry - my fault. I seem to have confused two things here (I wrongly thought that disabling reauthentication would kill the connection once the rekey threshold was reached).
Actually this woraround works perfectly, and the connection stays open without any problems.

#7 - 29.03.2016 17:09 - Lauri Võsandi

This bug makes NetworkManager plugin rather useless for high security applications where disabling reauth is not acceptable. I'm interested in donating to fix this issue :)

#8 - 31.05.2017 00:21 - Noel Kuntze

- Priority changed from Low to Normal

- Affected version deleted (5.1.2)

If the behaviour of the plugin did not change, then this is pretty bad.
Did it change? Otherwise, it goes on my lengthy TO-DO list for strongSwan additions/fixes.

#9 - 07.02.2020 17:18 - Tobias Brunner

- Tracker changed from Issue to Bug

- Target version set to 5.8.3

I pushed a fix for this to the *852-nm-reauth* branch.

#10 - 14.02.2020 14:01 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Affected version set to 5.1.2

- Resolution set to Fixed