I can reproduce this on Ubuntu 12.04 (but with package backported from 12.10 since 12.04 strongswan is broken) 12.10 and gentoo clients, with version 4.5.2 and 5.0.2. First thing first: server configuration;

Debian wheezy with strongswan 4.5.2-1.5

ipsec.conf

conn %default
  leftid=@<hidden>
  leftsubnet=<some private and public subnet>
  leftauth=pubkey
  leftcert=gwCert.der
  rightsourceip=10.100.44.128/26
  right=%any

conn linux-win7
  keyexchange=ikev2
  esp=aes256-sha1!
  dpdaction=clear
  dpddelay=300s
  left=%any
  # Windows 7 does not like a VPN gateway to take the initiative.
  rekey=no
  rightauth=eap-mschapv2
  rightsendcert=never
  eap_identity=%any
  auto=add

Clients are using networkmanager strongswan plugin to connect. I checked “Request an inner IP address”, otherwise the connection fails.

ip addr show *before* connecting to the VPN

```
root@ubuntults-virt:~# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
   inet6 ::1/128 scope host
   valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 52:54:00:3b:7b:24 brd ff:ff:ff:ff:ff:ff
   inet 192.168.122.187/24 brd 192.168.122.255 scope global eth0
      inet6 fe80::5054:ff:fe3b:7b24/64 scope link
      valid_lft forever preferred_lft forever
```

I connect to the VPN and this is a snippet from the syslog, the part which looks suspect to me.

```
Feb 22 11:30:36 ubuntults-virt NetworkManager[703]: <info> VPN Gateway: 0.0.0.0
Feb 22 11:30:36 ubuntults-virt NetworkManager[703]: <info> Tunnel Device: lo
Feb 22 11:30:36 ubuntults-virt NetworkManager[703]: <info> Internal IP4 Address: 192.168.122.187
Feb 22 11:30:36 ubuntults-virt NetworkManager[703]: <info> Internal IP4 Prefix: 32
Feb 22 11:30:36 ubuntults-virt NetworkManager[703]: <info> Internal IP4 Point-to-Point Address: 0.
```

14.03.2020 1/8
Those 0.0.0.0 looks no less then odd.

ip addr show after the connection

```
root@ubuntults-virt:~# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 192.168.122.187/32 brd 192.168.122.187 scope global lo
   inet6 ::1/128 scope host
     valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 52:54:00:3b:7b:24 brd ff:ff:ff:ff:ff:ff
   inet 192.168.122.187/24 brd 192.168.122.255 scope global eth0
   inet 10.100.44.129/32 scope global eth0
   inet6 fe80::5054:ff:fe3b:7b24/64 scope link
     valid_lft forever preferred_lft forever
```

the loopback interface IP is changed and all the service depending on the loopback interface are gone. This is a very major problem, and on Ubuntu the DNS is from 127.0.0.1 since dnsmasq dynamic dns networkmanager plugin is enabled by default.

When the VPN is disconnected the loopback IP is not restored:

```
root@ubuntults-virt:~# ip addr show
1: lo: <LOOPBACK> mtu 16436 qdisc noqueue state DOWN
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
   link/ether 52:54:00:3b:7b:24 brd ff:ff:ff:ff:ff:ff
   inet 192.168.122.187/24 brd 192.168.122.255 scope global eth0
   inet6 fe80::5054:ff:fe3b:7b24/64 scope link
     valid_lft forever preferred_lft forever
```

If you need more log just ask.

---

**History**

#1 - 22.02.2013 19:17 - Tobias Brunner

- Description updated
- Status changed from New to Feedback
- Assignee set to Tobias Brunner
- Priority changed from High to Normal

This is probably a side-effect of [d12635c7](https://gitlab.gnome.org/GNOME/NetworkManager.git). NetworkManager seems to assume full control over the returned interface.

I tried to work around this by creating a dummy TUN device, which NM can use to do whatever it likes to do. You could try the `nm-dummy-tun` branch in our Git repository. I also fixed the address that is installed on that device (it now uses the virtual IP address, if any - charon will actually install that address too, but that shouldn't really matter). Plus NM doesn't install a default route anymore, our NM backend does that anyway but also respects any narrowing the responder does.

#2 - 25.02.2013 15:13 - Enrico Tagliavini

Hi Tobias,

I checked out your branch and tested on my gentoo client machine. Seems to work fine! Charon SIGSEV at exit, but that's all. I will attach some log:

Syslog

Feb 25 14:03:50 schroedingerscat NetworkManager[2623]: <info> VPN connection 'ICHEC Dublin Office' (IP Config
Feb 25 14:05:49 schroedingerscat charon-nm: 09[NET] received packet: from 10.100.2.44[4500] to 10.100.2.136[4500] (76 bytes)
Feb 25 14:05:49 schroedingerscat charon-nm: 09[ENC] parsed INFORMATIONAL response 8 [ ]
Feb 25 14:05:49 schroedingerscat charon-nm: 09[IKE] IKE_SA deleted
Feb 25 14:05:49 schroedingerscat charon-nm: 09[KNL] error uninstalling route installed with policy 10.100.2.0/24 == 10.100.44.129/32 fwd
Feb 25 14:05:49 schroedingerscat charon-nm: 09[KNL] error uninstalling route installed with policy 10.100.1.0/24 == 10.100.44.129/32 fwd
# other errors, one for policy
Feb 25 14:05:49 schroedingerscat NetworkManager[2623]: <warn> (7) failed to find interface name for index
Feb 25 14:05:49 schroedingerscat NetworkManager[2623]: nm_system_iface_flush_routes: assertion `iface != NULL'
failed
Feb 25 14:05:49 schroedingerscat NetworkManager[2623]: <warn> (7) failed to find interface name for index
Feb 25 14:05:49 schroedingerscat dbus-daemon[2634]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Feb 25 14:05:49 schroedingerscat nm-dispatcher.action: Script '/etc/NetworkManager/dispatcher.d/10-openrc-stat' could not be executed: not executable by owner.
Feb 25 14:05:49 schroedingerscat nm-dispatcher.action: Script '/etc/NetworkManager/dispatcher.d/per_device_routing_tables.txt' could not be executed: not executable by owner.
Feb 25 14:05:49 schroedingerscat NetworkManager[2623]: <warn> VPN service 'strongswan' died with signal 11
Feb 25 14:05:49 schroedingerscat NetworkManager[2623]: <info> VPN service 'strongswan' disappeared

ip addr and route

# before connecting
schroedingerscat ~ # ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: em1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
link/ether d4:be:d9:6e:cb:f8 brd ff:ff:ff:ff:ff:ff
inet 10.100.2.136/24 brd 10.100.2.255 scope global em1
inet6 fe80::d6be:d9ff:fe6e:cbf8/64 scope link
valid_lft forever preferred_lft forever
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state up qlen 1000
link/ether c4:85:08:8b:00:15:76 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.101/24 brd 192.168.0.255 scope global wlan0
inet6 fe80::c685:8ff:feb0:1576/64 scope link
valid_lft forever preferred_lft forever
4: virbr1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN
link/ether 52:54:00:72:f3:54 brd ff:ff:ff:ff:ff:ff
inet 192.168.124.2/24 brd 192.168.124.255 scope global virbr1
5: virbr1-nic: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN
link/ether 36:a2:82:bb:48:15 brd ff:ff:ff:ff:ff:ff
inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
# while connected
schroedingerscat ~ # ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: em1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
link/ether d4:be:d9:6e:cb:f8 brd ff:ff:ff:ff:ff:ff

int 10.100.2.136/24 brd 10.100.2.255 scope global em1
int 10.100.44.129/32 scope global em1
inet6 fe80::d6be:d9ff:fe6e:cbf8/64 scope link
  valid_lft forever preferred_lft forever
3: wlan0: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
  link/ether c4:85:08:b0:15:76 brd ff:ff:ff:ff:ff:ff
inet 192.168.0.101/24 brd 192.168.0.255 scope global wlan0
inet6 fe80::c685:8ff:feb0:1576/64 scope link
  valid_lft forever preferred_lft forever
4: virbr1: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc noqueue state DOWN
  link/ether 52:54:00:72:63:54 brd ff:ff:ff:ff:ff:ff
inet 192.168.124.1/24 brd 192.168.124.255 scope global virbr1
5: virbr1-nic: <BROADCAST, MULTICAST> mtu 1500 qdisc pfifo_fast master virbr1 state DOWN qlen 500
  link/ether 3e:a2:82:bb:48:15 brd ff:ff:ff:ff:ff:ff
inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
7: tun0: <POINTTOPOINT, MULTICAST, NOARP, UP, LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 500
  link none
inet 10.100.44.129/32 brd 10.100.44.129 scope global tun0

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.100.2.254 0.0.0.0 UG 0 0 0 em1
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan0
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0
192.168.124.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr1

schroedingerscat ~ # route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.100.2.254 0.0.0.0 UG 0 0 0 em1
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan0
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr0
192.168.124.0 0.0.0.0 255.255.255.0 U 0 0 0 virbr1

schroedingerscat ~ # now disconnecting

Keeops good to me except for the, non fatal, SIGSEV. Thank you very much! Hope to see this merged and released soon.

Cheers

#3 - 25.02.2013 19:03 - Tobias Brunner
Thanks for testing.

Charon SIGSEV at exit, but that's all.

I can't reproduce this. Would it be possible for you to attach gdb to charon-nm before disconnecting in order to provide us with a backtrace? (Or even provide a core dump?)
By the way, the errors you see in the log regarding the route deinstallation are due to the tun0 device being removed before terminating the SAs. The routes installed by charon seem to get removed by the kernel when the interface disappears (probably because it features the virtual IP, even though the routes won't actually feature the tun0 interface). There are also some warnings issued by NM regarding the TUN device (<warn> (7) failed to find interface name for index etc.). It seems NM assumes the interface exists until the child-process is terminated. Therefore, I moved the creation/destruction of the TUN device to the initialization/deinitialization phases of the NM plugin instead of doing so together with the connection, this should fix both warnings.

Please note that I rebased the branch, so you'll have to delete your local copy and check it out anew.

#4 - 26.02.2013 11:32 - Enrico Tagliavini
- File charon-nm5.bt added
- File charon-nm4.bt added
- File charon-nm3.bt added

It seems easier said then done. Probably I'm just doing the wrong thing, if so forgive me and just point me to the right procedure. The command I'm using is:

gdb /usr/libexec/ipsec/charon-nm $(pgrep charon-nm) & tee charon-nm5.bt

and the result is pretty random, as you can see from the gdb outputs attached.

Since the /proc/pid/maps file is empty (!!!) after the segfault I did one try copying it before the segfault. this is the result:

Program received signal SIGSEGV, Segmentation fault.
0x00007fb6b097c500 in ?? ()
(gdb) bt
#0  0x00007fb6b097c500 in ?? ()
Cannot access memory at address 0x7fff3c86c4c8

and in maps
151 7fb6b0777000-7fb6b0976000 ---p 00003000 fe:00 7301 /usr/lib64/ipsec/plugins/libstrongswan-revocation.so
152 7fb6b0976000-7fb6b0977000 r--p 00002000 fe:00 7301 /usr/lib64/ipsec/plugins/libstrongswan-revocation.so
153 7fb6b0977000-7fb6b0978000 rw-p 00003000 fe:00 7301 /usr/lib64/ipsec/plugins/libstrongswan-revocation.so
154 7fb6b0978000-7fb6b098c000 r-xp 00000000 fe:00 8817 /usr/lib64/ipsec/plugins/libstrongswan-x509.so
155 7fb6b098c000-7fb6b0b8000 ---p 00014000 fe:00 8817 /usr/lib64/ipsec/plugins/libstrongswan-x509.so
156 7fb6b0b8000-7fb6b0bb8000 r-p 00013000 fe:00 8817 /usr/lib64/ipsec/plugins/libstrongswan-x509.so
7fff3c84d000-7fff3c86e000 rw-p 00000000 00:00 0 [stack]

Which means not much to me, but may be it does to you :). Note: addresses are randomized, so they are different upon every execution.

#5 - 26.02.2013 15:54 - Tobias Brunner

Thanks for the backtraces.

charon-nm4.bt indicates that it is the order in which plugins are unloaded. In nm_backend_deinit() the NM-specific credential set is destroyed, which destroys any loaded certificate and private key objects. If the plugin that provides the implementation for such an object is already unloaded this will cause a segmentation fault.

Since the nm-backend plugin is one of the first that is loaded and because it has no explicit dependencies on plugins providing certificates/keys it is also one of the last being unloaded (plugins are unloaded in reverse order, but their dependencies are considered). Nevertheless, in some plugin configurations this crash will not be triggered, e.g. when enabling the pkcs11 plugin it doesn't crash.

To avoid all this I added additional dependencies to the nm-backend plugin and updated the branch.

#6 - 27.02.2013 11:19 - Enrico Tagliavini

First attempt: no SIGSEGV

Feb 27 10:12:51 schroedingherscat charon-nm: 03[KNL] 10.100.2.136 disappeared from em1

dns stuff

Feb 27 10:12:51 schroedingherscat charon-nm: 03[KNL] 10.100.2.136 appeared on em1

Feb 27 10:12:51 schroedingherscat dnsmasq[2068] using local addresses only for unqualified names

Feb 27 10:12:51 schroedingherscat charon-nm: 16[IKE] sending address list update using MOBIKE


Feb 27 10:12:51 schroedingherscat charon-nm: 16[NET] sending packet: from 10.100.2.136 to 10.100.2.44 (124 bytes)

Feb 27 10:12:51 schroedingherscat charon-nm: 05[NET] received packet: from 10.100.2.44 to 10.100.2.136 (76 bytes)
Feb 27 10:12:51 schroedingherscat charon-nm: 05[ENC] parsed INFORMATIONAL response 7 [ ]
Feb 27 10:12:52 schroedingherscat NetworkManager[2622]: <info> Policy set 'eth0' (em1) as default for IPv4 routing and DNS.
Feb 27 10:12:52 schroedingherscat NetworkManager[2622]: <info> Clearing nscd hosts cache.
Feb 27 10:12:52 schroedingherscat dbus-daemon[2648]: dbus[2648]: [system] Activating service name='org.freedesktop.nm_dispatcher' (using servicehelper)
Feb 27 10:12:52 schroedingherscat dbus[2648]: [system] Activating service name='org.freedesktop.nm_dispatcher' (using servicehelper)
Feb 27 10:12:52 schroedingherscat charon-nm: 09[IKE] deleting IKE_SA ICHEC Dublin Office
between 10.100.2.136[enrico]...10.100.2.44[forbin.ichec.ie]
Feb 27 10:12:52 schroedingherscat charon-nm: 09[IKE] sending DELETE for IKE_SA ICHEC Dublin Office
Feb 27 10:12:52 schroedingherscat charon-nm: 09[ENC] generating INFORMATIONAL request 8 [ D ]
Feb 27 10:12:52 schroedingherscat charon-nm: 09[NET] sending packet: from 10.100.2.136 to 10.100.2.44 (76 bytes)
Feb 27 10:12:52 schroedingherscat charon-nm: 10[NET] received packet: from 10.100.2.44 to 10.100.2.136 (76 bytes)
Feb 27 10:12:52 schroedingherscat charon-nm: 10[ENC] parsed INFORMATIONAL response 8 [ ]
Feb 27 10:12:52 schroedingherscat dbus-daemon[2648]: dbus[2648]: [system] IKE_SA deleted
Feb 27 10:12:52 schroedingherscat dbus-daemon[2648]: dbus[2648]: [system] IKE_SA deleted
Feb 27 10:12:52 schroedingherscat charon-nm: 03[KNL] interface tun0 deactivated
Feb 27 10:12:52 schroedingherscat charon-nm: 03[KNL] 10.100.44.129 disappeared from tun0
Feb 27 10:12:52 schroedingherscat dbus-daemon[2648]: dbus[2648]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Feb 27 10:12:52 schroedingherscat dbus[2648]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Feb 27 10:12:52 schroedingherscat charon-nm: 03[KNL] interface tun0 deactivated
Feb 27 10:12:52 schroedingherscat charon-nm: 03[KNL] 10.100.44.129 disappeared from tun0
Feb 27 10:12:52 schroedingherscat dbus-daemon[2648]: dbus[2648]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Feb 27 10:12:52 schroedingherscat dbus-daemon[2648]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Feb 27 10:12:52 schroedingherscat charon-nm: 00[DMN] signal of type SIGTERM received. Shutting down
Tried to connect and disconnect some time, no SIGTERM, seems to work good for me.

Thank you very much.

#7 - 21.03.2013 18:47 - Tobias Brunner
- Status changed from Feedback to Closed
- Target version set to 5.0.3
- Resolution set to Fixed

#8 - 07.08.2013 03:58 - Марк Коренберг
Linux Mint 14,

```
1. dpkg -l | fgrep strong
   i libstrongwan 4.5.2-1.5ubuntu2
   i network-manager-strongwan 1.3.0-0ubuntu1
   i strongswan-ikev1 4.5.2-1.5ubuntu2
   i strongswan-ikev2 4.5.2-1.5ubuntu2
   i strongswan-nm 4.5.2-1.5ubuntu2
   i strongswan-starter 4.5.2-1.5ubuntu2
```

still the same issue. Why all ubuntu packges have 4.x version, and no one 5.x ?
How I can fast-fix that?
Should I run

```
1. ip tuntap add
```

#9 - 07.08.2013 09:22 - Tobias Brunner

strongswan-nm 4.5.2-1.5ubuntu2
...

still the same issue.

Why would you expect anything else? The fixes were included in 5.0.3, so unless someone ports them back to 4.5.2 you really have to update to a newer release.

How I can fast-fix that?

You could build strongSwan from sources yourself. There is also a 5.x package in Debian experimental, which you might be able to use on Linux Mint.

Files