# strongSwan - Issue #2684

## kernel_netlink plugin - no traffic through VPN when IPv4 policy on IPv6 ESP tunnel uses IPv6 nexthop when installing IPv4 route

17.06.2018 08:18 - Matthew Grant

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Normal | | |
| **Assignee:** | Tobias Brunner | | |
| **Category:** | kernel-interface | | |
| **Affected version:** | 5.6.3 | **Resolution:** | No feedback |

**Description**

On a dual stack client site with full Ipv6 and IPv4 addressing and full default routing, an IPv4 policy over an IPv6 ESP IPSEC VPN tunnel causes the libcharon kernel_netlink plugin to use the next hop to the IPv6 peer for the IPv4 route locally routing traffic down the VPN tunnel. This results in a route in table 200 saying the remote prefix in the policy is on the local ethernet!  No traffic crosses the tunnel until a correct route is manually installed in the table.

Patch to resolve issue attached. With this applied, VPN works each time it is brought up.

Here are the debug log messages:

Jun 12 19:54:56 en-gedi charon: 11[KNL] adding policy 172.31.8.0/24 === 172.31.28.101/32 in [priority 371327, refcount 1]
Jun 12 19:54:56 en-gedi charon: 11[KNL] adding policy 172.31.8.0/24 === 172.31.28.101/32 fwd [priority 371327, refcount 1]
Jun 12 19:54:56 en-gedi charon: 11[KNL] adding policy 172.31.28.101/32 === 172.31.8.0/24 out [priority 371327, refcount 1]
Jun 12 19:54:56 en-gedi charon: 11[KNL] getting a local address in traffic selector 172.31.28.101/32
Jun 12 19:54:56 en-gedi charon: 11[KNL] using host 172.31.28.101
Jun 12 19:54:56 en-gedi charon: 11[KNL] getting iface name for index 3
Jun 12 19:54:56 en-gedi charon: 11[KNL] using fe80::d6ca:6dff:fed0:71d9 as nexthop and wlan0 as dev to reach 2001:470:f012:1012::1/128
Jun 12 19:54:56 en-gedi charon: 11[KNL] installing route: 172.31.8.0/24 via fe80::d6ca:6dff:fed0:71d9 src 172.31.28.101 dev wlan0
Jun 12 19:54:56 en-gedi charon: 11[KNL] getting iface index for wlan0
Jun 12 19:54:56 en-gedi charon: 11[IKE] CHILD_SA ipsec-vpn{2} established with SPIs c51d9cde_i 08da8ddb_o and TS 172.31.28.101/32 === 172.31.8.0/24
Jun 12 19:54:56 en-gedi charon: 14[KNL] getting iface index for wlan0
Jun 12 19:55:01 en-gedi charon: 16[CFG] received stroke: terminate 'ipsec-vpn'

### History

**#1 - 20.09.2018 18:16 - Tobias Brunner**

*- Tracker changed from Bug to Issue*

*- Category changed from libcharon to kernel-interface*

*- Status changed from New to Feedback*

*- Priority changed from High to Normal*

*- Start date deleted (17.06.2018)*

Hm, I somehow missed this ticket.

Since 4.3.6 (more specifically, since 5be75c2cb189, which added the check that's now at source:src/libcharon/plugins/kernel_netlink/kernel_netlink_net.c#L2615) routes should get installed without a nexthop if it is of a different address family than the source IP. So in your case the actual route that's installed should be 172.31.8.0/24 dev wlan0 src 172.31.28.101 (the log message is printed before the decision is made to ignore the nexthop, so ignore that). This doesn't seem all that wrong.

**#2 - 28.02.2019 16:47 - Tobias Brunner**

*- Status changed from Feedback to Closed*

*- Assignee set to Tobias Brunner*

*- Resolution set to No feedback*

### Files

| | | | |
|---|---|---|---|
| 05_gateway-protocol-tunnel-diff-families.patch | 1.23 KB | 17.06.2018 | Matthew Grant |