strongSwan - Bug #3615

DNS resolution not via VPN when using systemd-resolved and the NetworkManager plugin

31.10.2020 06:21 - Peter Beurle

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	networkmanager (charon-nm)		
Target version:	5.9.2		
Affected version:	5.9.0	**Resolution:**	Fixed

Description

I am using a Fedora 33 road warrior laptop that connects to a pfsense strongSwan based ipsec VPN implementation. On the laptop the strongSwan NetworkManager packages are installed and it I use the gnome gui to turn VPN on and off. Since the upgrade to 33 VPN DNS names will not resolve. This is the same for a couple of years with Ubuntu [[https://bugs.launchpad.net/ubuntu/+source/systemd/+bug/1783377]]

After some reading it seems that the resolver (systemd-resolved) will select any DNS server, not the VPN one. Restarting resolved after connecting to the VPN puts the VPN DNS at the top of the list and it works. Poettering believes all DNS servers should be equal.

You can have different DNS per interface and this seems to be done to stop dns leaks.

It seems to me that we need to create a XFRM interface and associate the VPN domain to that interface so DNS works again?

Associated revisions

Revision aa3d5bf7 - 19.01.2021 14:49 - Tobias Brunner

Revert "nm: Remove dummy TUN device"

This reverts commit a28c6269a4aeb5369fed8933fa1baf0cd8847622.

We add a dummy TUN device again because systemd-resolved insists on
managing DNS servers per interface.

Fixes #3615.

History

#1 - 02.11.2020 09:19 - Tobias Brunner

- Category set to networkmanager (charon-nm)

- Status changed from New to Feedback

While some aspects of systemd-resolved are OK, associating DNS servers with interfaces make no sense, you need a destination IP to select a route/interface in the first place.

From my experience, configuring ~. in "Additional search domains" in the IPv4 settings of the VPN connection (e.g. via nmcli connection modify <name> ipv4.dns-search '~.') and restarting systemd-resolved when the VPN is established via script in /etc/NetworkManager/dispatcher.d/pre-up.d e.g.

```
#!/bin/bash
if [ "$2" == "vpn-pre-up" ]; then
   echo "Restart systemd-resolved to fix VPN DNS lookups"
   /bin/systemctl restart systemd-resolved
fi
```

seems to work.

#2 - 30.11.2020 15:40 - Tobias Brunner

I pushed a commit to the *3615-nm-interface* branch that reintroduces the dummy TUN device in our NM plugin that was removed with 5.5.2 (after being added with 5.0.3 as a workaround for NM issues). At least older NM versions still need manually setting search domains to ~., but then it seems to work fine without script and systemd-resolved associates the DNS servers with the TUN device and uses them as expected.

#3 - 19.01.2021 14:52 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from systemd resolved to DNS resolution not via VPN when using systemd-resolved and the NetworkManager plugin

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.9.2

- Resolution set to Fixed

#4 - 19.03.2021 02:11 - Mirek Svoboda

Another workaround for this issue in Fedora 33 is to bypass systemd-resolved resolver, while still letting it set DNS servers.
It is done with the following command:

```
sudo ln -sfv /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

Explanation from

```
man systemd-resolved
```

is this:

```
systemd-resolved maintains the /run/systemd/resolve/resolv.conf file for compatibility with traditional Linux programs. This
           file may be symlinked from /etc/resolv.conf and is always kept up-to-date, containing information about all known DNS
           servers. Note the file format's limitations: it does not know a concept of per-interface DNS servers and hence only contains
           system-wide DNS server definitions. Note that /run/systemd/resolve/resolv.conf should not be used directly by applications,
           but only through a symlink from /etc/resolv.conf. If this mode of operation is used local clients that bypass any local DNS
           API will also bypass systemd-resolved and will talk directly to the known DNS servers.
```

#5 - 06.06.2021 14:46 - Peter Beurle

Fedora finally got strongswan 5.9.2 into the testing repository in the last few days and I can confirm everything works with VPN name resolution again (without any workarounds).

Thanks for getting this fixed.