strongSwan - Feature #2135

Support automatic passthrough for local subnets

07.10.2016 09:27 - Chen-Yu Tsai

Status:	Closed	**Start date:**	07.10.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.5.2		
Resolution:	Fixed		

Description

Hi,

With normal strongswan/charon users can set passthrough connections to be able to access local IPs, albeit the settings are somewhat static, meaning one has to edit the config file to update the local IP.

With the network manager plugin, such possibilities aren't available, and all traffic is routed through the VPN tunnel, due to how the routing is setup.

It would be nice to have the option of being able to still access local resources when the VPN is up, which is the case for other types of VPN, and also the behavior of IKEv2 on Microsoft Windows. This could be done by automatically adding a route for the local subnet using the local IP address as the source IP. Not sure if passthrough policies are needed. Doing

```
ip route add table 220 LOCALNET dev LOCALIF src LOCALIP
```

did the trick for me.

Thank you.

History

#1 - 07.10.2016 09:52 - Tobias Brunner

- Status changed from New to Feedback

Yes, if virtual IPs are used you only need one or more routes that prevent that the virtual IP is used for specific subnets (without the route installed by strongSwan everything would bypass the tunnel as the local traffic selector is for the virtual IP only). When the daemon installs passthrough policies it also adds such routes.

The tricky part is probably determining the local subnet, interface and IP. I think instead of writing a new plugin that adds passthrough policies or extending the NM plugin it might be easier to just write a script that's e.g. run by NM when the network config changes (e.g. in /etc/NetworkManager/dispatcher.d). This could also be used to write config snippets that are included by the regular daemon (if installation of passthrough policies is needed e.g. when NM is not used).

#2 - 10.03.2017 13:49 - Tobias Brunner

- Category changed from networkmanager (charon-nm) to libcharon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.5.2

- Resolution set to Fixed

The upcoming 5.5.2 release will include a new optional plugin (*bypass-lan*) that automatically installs and updates passthrough policies for locally attached subnets.