

strongSwan - Feature #625

Add option to force the use of NAT-T (or any other) port via charon-nm

25.06.2014 11:45 - Raphael Geissert

Status:	Closed	Start date:	25.06.2014
Priority:	Normal	Due date:	
Assignee:	Tobias Brunner	Estimated time:	0.00 hour
Category:	networkmanager (charon-nm)		
Target version:	5.8.3		
Resolution:	Fixed		
Description			
RFC5996 allows for the initiator to communicate to port 4500, even at the beginning of the connection. Attached patch adds a new "natt" option to charon-nm and nm-strongswan that makes charon-nm create the connection to the gateway on port 4500 - aka "check the box to force NAT-T port".			
This is useful when traffic is blocked or messed around by firewalls and/or too broken NATs.			

Associated revisions

Revision 1157d3e0 - 14.02.2020 13:36 - Tobias Brunner

Merge branch 'nm-server-port'

Adds the option to use a custom server port in the NM plugin.

Fixes #625.

History

#1 - 01.08.2016 16:47 - Raphael Geissert

- File 0001-nm-add-checkbox-for-forcing-use-of-NAT-T-port.patch added

Attached patch has been revisited for version 1.3.1 of the plugin.

#2 - 15.08.2016 11:51 - Tobias Brunner

- Status changed from New to Feedback

Wouldn't it be much more flexible to just make the remote server port configurable? (Default: 500)

And could you please base the patches on the *nm-1.2* branch?

#3 - 16.08.2016 11:37 - Raphael Geissert

Tobias Brunner wrote:

Wouldn't it be much more flexible to just make the remote server port configurable? (Default: 500)

The idea was that from a user perspective she would just mark the checkbox if the connection fails to be established. OTOH, I do see an interest in being able to configure the port.

Perhaps the NAT-T checkbox and a port configuration box could be added, and the logic of the checkbox be handled directly by the GUI. Ex. modifying the value of the port box, and greying it while the checkbox is marked.

What do you think?

#4 - 17.08.2016 11:25 - Tobias Brunner

Perhaps the NAT-T checkbox and a port configuration box could be added, and the logic of the checkbox be handled directly by the GUI. Ex. modifying the value of the port box, and greying it while the checkbox is marked.

What do you think?

I suppose that's a possibility. Using a custom port is not directly related to NAT-T, though. If there is no NAT detected, or randomized NAT-D payloads are used to force it, no UDP encapsulation is used even if a custom port is used (however, messages to that port will usually have to be sent with the non-ESP marker, refer to [this recent response on the mailing list for the reasoning](#), which some implementations will only do/expect on the "NAT-T" port).

#5 - 19.12.2019 14:43 - Tobias Brunner

- Target version set to 5.8.3

I pushed changes to configure a custom server port to the *625-nm-server-port* branch.

#6 - 14.02.2020 13:38 - Tobias Brunner

- Subject changed from *Add option to force the use of NAT-T port via charon-nm* to *Add option to force the use of NAT-T (or any other) port via charon-nm*

- Status changed from *Feedback* to *Closed*

- Assignee set to *Tobias Brunner*

- Resolution set to *Fixed*

Files

0001-nm-add-checkbox-for-forcing-use-of-NAT-T-port.patch	3.51 KB	25.06.2014	Raphael Geissert
0002-charon-nm-add-support-for-forcing-the-use-of-the-NAT.patch	1.66 KB	25.06.2014	Raphael Geissert
0001-nm-add-checkbox-for-forcing-use-of-NAT-T-port.patch	3.62 KB	01.08.2016	Raphael Geissert