strongSwan - Feature #2814

Force Keepalive Packets if There is no NAT

29.10.2018 15:29 - Fabien DE BIASI

Status:	Feedback	**Start date:**	29.10.2018
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:			
Target version:			
Resolution:			

Description

Hello,
I am using a StrongSwan client on Android. This client builds up a tunnel with a Firewall (Stormshield and then Strongswan based).

The Android smartphones are located on a private 4G network where no NAT is done and then, no NATT-keep-alive packet is sent by the Strongswan client. As I have firewalls doing the filtering of the UDP packets in one direction (from Smartphone to the VPN concentrator), then after 40 of inactivity, the communication between the server to the smartphone is not more possible.

Then my request is to have a feature of having the possibility to force the keep-alive packet even if the NATT mechanism is not launched.

I should deploy 6.000 mobiles and I am blocked with that issue up to know. Please tell me if this won't be possible and then I can search another track
Regards
Fabien

History

#1 - 29.10.2018 15:47 - Tobias Brunner

- Subject changed from Keep ALive Packet to Force Keepalive Packets if There is no NAT

- Status changed from New to Feedback

- Priority changed from Urgent to Normal

There is currently no feature in the IKE daemon that forces NAT keepalives if the host is not behind a NAT. So this would involve more than just exposing a configuration option in the Android app (or on the server if that was an option, probably depends on how the firewall behaves).

Using DPDs for this purpose might be an option, but DPDs are currently not enabled in the app (there is no option to change that, other than modifying the source code) and they might have other side-effects. And on servers our recommendation is to use a long DPD interval (just to weed out abandoned SAs) to allow clients to roam between networks or be without network connectivity for a while (but that might not be an issue in your setup, so perhaps enabling DPD on the server is an option for you).