strongSwan - Feature #2365

Make Android client NAT keep alive interval configurable

21.06.2017 20:50 - Hans Muster

Status:	Closed	**Start date:**	21.06.2017
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	android		
Target version:	5.6.0		
Resolution:	Fixed		

Description

There are NAT devices "in wild" with a default NAT timeout of only 20 seconds. For example LANCOM devices with LCOS v9.24:

https://www.lancom-systems.de/docs/LCOS-Menu/9.24-Rel/EN/topics/2_8_9_2.html

My IKEv2/IPSec-VPN Server has a Dead Peer Detection (DPD) interval of 30 seconds. My VPN server detects the broken connection and close (correct) the IKE channel/connection.

Could you please reopen ticket #1326 and set the default NAT keep alive interval to **15** seconds.

=> The native vpn client of windows 10 (Agile VPN Client) use a NAT keep alive interval of 15 seconds.

Thank you.

Es sind NAT-Geräte im Umlauf, die standardmässig mit einer NAT-Timeout-Zeit von nur 20 Sekunden konfiguriert sind. Zum Beispiel LANCOM-Geräte mit LCOS v9.24:

https://www.lancom-systems.de/docs/LCOS-Menu/9.24-Rel/DE/topics/2_8_9_2.html

Mein IKEv2/IPSec-VPN-Server verwendet eine "Dead Peer Detection" (DPD) mit einem Intervall von 30 Sekunden. Dadurch erkennt der VPN Server die unterbrochene Verbindung und schliesst (korrekterweise) die IKE-Verbindung.

Könnten Sie bitte Ticket #1326 wieder eröffnen und die voreingestellte Zeit für das NAT-Keep Alive-Intervall auf **15** Sekunden setzen?

=> Der in Windows 10 integrierte (native) VPN-Client (Agile VPN Client) verwendet eine NAT-Keep Alive-Intervallzeit von 15 Sekunden.

Besten Dank.

Associated revisions

Revision 6f0888c8 - 03.07.2017 10:33 - Tobias Brunner

Merge branch '2365-android-nat-keepalive'

This makes the NAT-T keepalive interval configurable per connection.

Fixes #2365.

History

#1 - 22.06.2017 08:40 - Tobias Brunner

- Tracker changed from Bug to Feature

- Subject changed from Android client NAT keep alive interval (Reopen request #1326) to Make Android client NAT keep alive interval configurable

- Category set to android

- Status changed from New to Feedback

I guess the whole point of #1326 was to **increase** the interval from its default of 20 seconds to avoid sending packets too often if there is no other traffic and thus save some battery power. So the current default probably won't change (this is the first time I've heard that it's a problem since I've increased the value). But we could perhaps make it configurable in a future release.

> For example LANCOM devices with LCOS v9.24

But as you point out, it's configurable and could easily be set to e.g. 60 seconds. 20 seconds timeout is very low for NAT entries of established UDP connections, even the actual default value used by strongSwan (20 seconds) might be too low when you are behind such a router in its default configuration.

> My IKEv2/IPSec-VPN Server has a Dead Peer Detection (DPD) interval of 30 seconds

That's quite short. What if you are roaming and don't have any network connection for a while? I'd configure a relative high DPD interval on the server (hours) just to clean out old SAs if they get abandoned by the clients (if you use uniqueness checks, the default, then a reconnect from a client will remove any old SA anyway).

#2 - 22.06.2017 20:16 - Hans Muster

Could you please **decrease** the **default** NAT-T keep alive interval to 15 seconds in the next android app version?

The increase of NAT-T keep alive interval (# 1326) breaks VPN connections in foreign enviroments where i don't have any access or possiblity to increase the UDP NAT time out of foreign NAT devices. For example Hotel Wifi/WLAN in german speaking regions:

https://www.lancom-systems.com/references/

Battery power saving is not a reason to break VPN connections!

Is there any way to escalate this bug?

Thank you.

#3 - 23.06.2017 09:06 - Tobias Brunner

> Could you please **decrease** the **default** NAT-T keep alive interval to 15 seconds in the next android app version?

No. That's even lower than our (and the recommended) default of 20 seconds.

> The increase of NAT-T keep alive interval (# 1326) breaks VPN connections in foreign enviroments where i don't have any access or possiblity to increase the UDP NAT time out of foreign NAT devices.

As I said we might make this configurable in an upcoming release. Then you can set it to 15 seconds if you think it's necessary.

> For example Hotel Wifi/WLAN in german speaking regions:
>
> https://www.lancom-systems.com/references/

And you just assume they all use it with the default settings without modifying them to some more sensible values? Why not complain to them and LANCOM directly? (Refer to RFC 3948 if you need a good argument why 20 seconds might be too low a timeout for established UDP mappings.)

> Battery power saving is not a reason to break VPN connections!

If it helps a huge majority of users, why not? You are the first and, so far, only one complaining about this since the interval was increased over a year ago.

> Is there any way to escalate this bug?

What do you have in mind?

#4 - 24.06.2017 20:46 - Hans Muster

RFC 3948 chaptre 4:

*A peer SHOULD send a NAT-keepalive packet if a need for it is detected according to [RFC3947] and if no other packet to the peer has been sent in M seconds. M is a **locally configurable** parameter with a default value of **20** seconds.*

Revision 73a6bec3 (ticket #1326) is not conform to RFC 3948!

=> According RFC 3948 chaptre 4 LANCOM devices are conform to RFC 3948.

=> According RFC 3948 chaptre 4 StrongSwan Android App is **not** conform to RFC 3948.

#5 - 26.06.2017 10:02 - Tobias Brunner

> Revision 73a6bec3 (ticket #1326) is not conform to RFC 3948!

You read that ticket and the comments and what I wrote above, right? That change was deliberate because it looked like it will work fine and might save some battery life.

> => According RFC 3948 chaptre 4 LANCOM devices are conform to RFC 3948.

20 seconds is too low, it is prone to races if the client uses 20 seconds as interval as well.

#6 - 03.07.2017 10:34 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.6.0

- Resolution set to Fixed

#7 - 14.07.2017 14:26 - Hans Muster

Your solution in StrongSwan Android App v1.9.2 works fine. Thank you very much for your effort.