strongSwan - Issue #3282

Android VPN client keeps retrying in airplane mode

29.11.2019 08:04 - Erik T

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	android		
Affected version:	5.8.1	**Resolution:**	

Description

First of all thank you for this wonderful software :-) It keeps our whole family surfing safe and ad-free via the VPN in our home router.

I am trying to upgrade from the native Android VPN client (IKEv1) to the strongSwan Android VPN client (IKEv2). I am using the "Always-on VPN" feature of both. I noticed a difference in behaviour between the native Android client and the strongSwan client.

The difference is when the phone is put into airplane mode (I do this every night to save on battery). The native Android client has no issue with this. But the strongSwan client, after a few hours, starts to try to "reconnect" to the server. This is shown on the screen as notification with a red progress bar indicating after how many seconds it will retry. Needless to say, trying to reconnect is pointless when the phone is in airplane mode.

Also the other apps still think there is a network connection, and start to show notifications about their failure to connect/sync/whatever. This is also something that does not happen when using the native Android VPN client. So apparently the native Android client removes its tunnel network interface so that the apps know that there is no connection. The strongSwan client seems to keep on offering a tunnel network interface even in airplane mode.

Would it be possible for the strongSwan VPN client to show the same "airplane mode" behaviour as the native Android client?

This is the server version (on OpenWrt):

1. ipsec --version
   Linux strongSwan U5.8.0/K4.14.151

The client version is 2.2.1. I have the option "Block connections without VPN" turned on.

Phone is on Android 9, Kernel 4.4.153-perf+ .

History

#1 - 29.11.2019 11:40 - Tobias Brunner

- Status changed from New to Feedback

> So apparently the native Android client removes its tunnel network interface so that the apps know that there is no connection.

No, that works completely differently. The native client uses the kernel's IPsec stack, so if there is no connectivity, there is simply isn't any. It doesn't create any virtual tunnel interfaces like apps have to.

> The strongSwan client seems to keep on offering a tunnel network interface even in airplane mode.

It does. And even if we'd stop retrying in airplane mode (which would probably be a good idea, but not sure when I'll have time to look into it), we'd probably keep a virtual blocking interface to avoid that any plaintext traffic leaks into the network once airplane mode is turned off (until the VPN can be reestablished). Unless, there is a way to somehow detect if the user enabled the Android system option "Block connections without VPN" (not sure if there is a way, in particular detecting changes to it).

#2 - 29.11.2019 12:24 - Erik T

Thanks Tobias.

> which would probably be a good idea, but not sure when I'll have time to look into it

Sure, understood. A quick fix might be (in my specific use case) to start retrying only after let's say 12 hours. Usually I wake up before that :-) It seems the retry currently also starts after a few hours (but less than 12).

> Unless, there is a way to somehow detect if the user enabled the Android system option "Block connections without VPN"

Does that option affect the retrying behaviour in the strongSwan client then? Or do you mean that unchecking that option can be used as a criterion to remove the tunnel network interface when no connection to the VPN server can be made?

Just for information: the native VPN client does not offer the "Block connections without VPN" option. I have seen quite some leaked packets, e.g. to 'connectivitycheck.gstatic.com' and 'www.google.com' (duh...) Which might be Google's way to determine whether or not it is sensible to retry.

#3 - 29.11.2019 16:06 - Tobias Brunner

> A quick fix might be (in my specific use case) to start retrying only after let's say 12 hours. Usually I wake up before that :-) It seems the retry currently also starts after a few hours (but less than 12).

What most likely breaks the connection and causes the retries are the scheduled rekeyings (in the Android app CHILD_SAs are rekeyed every hour, IKE_SAs every 10 hours). Check the app's log for details.

> > Unless, there is a way to somehow detect if the user enabled the Android system option "Block connections without VPN"

> Does that option affect the retrying behaviour in the strongSwan client then? Or do you mean that unchecking that option can be used as a criterion to remove the tunnel network interface when no connection to the VPN server can be made?

The latter. If that option is enabled it's possible that we don't have to explicitly create a tunnel device to block traffic because Android already blocks all traffic if no such device exists (I don't know what that would mean regarding how other apps perceive the connectivity state).

> Just for information: the native VPN client does not offer the "Block connections without VPN" option. I have seen quite some leaked packets, e.g. to 'connectivitycheck.gstatic.com' and 'www.google.com' (duh...) Which might be Google's way to determine whether or not it is sensible to retry.

That's probably just normal stuff Android does to determine whether it has connectivity.

Files

Screenshot_20191129-072354.png	1.19 MB	29.11.2019	Erik T