strongSwan - Issue #3626

"Always On VPN" not available in Fire TV 4k

10.11.2020 16:45 - r2 d2

Status:	Feedback		
Priority:	Low		
Assignee:	Tobias Brunner		
Category:	android		
Affected version:	5.9.0	**Resolution:**	

Description

Hi...
Maybe not an issue byitself more than a new requirement. I have Strongwan sideloaded in Firestick TV device with EAP-mschapv2 working correctly. The problem is this device hasn't VPN native Android features, not sure if hidden or not implemented like the certificate storage, so there is no way to enable "Always On VPN" from Android settings. Would it be possible to enable it via API through StrongSwan android app or include a button to enable VPN connection on system boot like other VPN clients for Android do?.
Regards,

History

#1 - 10.11.2020 17:40 - Tobias Brunner

- Category set to android

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

> Would it be possible to enable it via API through StrongSwan android app

No, AFAIK, the app doesn't have access to this setting (it can't even check if the user enabled Always-On VPN for itself).

> or include a button to enable VPN connection on system boot like other VPN clients for Android do?.

What do you mean by that?

#2 - 10.11.2020 18:28 - r2 d2

Tobias Brunner wrote:

> Would it be possible to enable it via API through StrongSwan android app

> No, AFAIK, the app doesn't have access to this setting (it can't even check if the user enabled Always-On VPN for itself).

I just found in the android doc some workaround maybe would be useful to detect if tunnel has been started/restarted by Always-ON VPN:

https://developer.android.com/guide/topics/connectivity/vpn#:~:text=Android%20can%20start%20a%20VPN,for%20the%20VPN%2Dgateway%20connection.

Android doesn't include APIs to confirm whether the system started your VPN service. But, when your app flags any service instances it starts, you can assume that the system started unflagged services for always-on VPN. Here's an example:

1. Create an Intent instance to start the VPN service.
2. Flag the VPN service by putting an extra into the intent.
3. In the service's onStartCommand() method, look for the flag in the intent argument's extras.

> or include a button to enable VPN connection on system boot like other VPN clients for Android do?.

> What do you mean by that?

For example, to enable some VPN on demand features, like connect automatically to VPN x when android/strongswan service starts or tunnel is disconnected without user intervention, trying to emulate "always-on" feature... or not so important examples like activation on wifi or per ssid connected. I checked automatic reconnection of the tunnel is well managed by Strongswan app when manually trying to restart the server for example, but unfortunately it's quite annoying to connect manually when android reboot itself or double check if it's running because you're having any other kind of problem with the other end discovering it isn't related to strongswan connection itself.

This kind of behaviour can be emulated by third-party solutions like automate from Llama or Tasker and the use of the intents provided by Strongswan, unfortunately practically none of them are adapted or run properly on android tv devices mostly related to their UI not being oriented to be managed with non touchscreen devices, which causes the need to do some nasty tricks like trying to create the "automation workflow" in a mobile device and export this config in tricky ways to the android tv running this same app.

#3 - 10.11.2020 18:57 - Tobias Brunner

I just found in the android doc some workaround maybe would be useful to detect if tunnel has been started/restarted by Always-ON VPN:

The app already handles Always-On service starts

> For example, to enable some VPN on demand features, like connect automatically to VPN x when android/strongswan service starts or tunnel is disconnected without user intervention, trying to emulate "always-on" feature...

That's already the case. Unless manually disconnected, the app keeps the VPN connection up.

> or not so important examples like activation on wifi or per ssid connected.

You can use automation tools for that (no idea about Fire TV, but on regular Android systems that's no problem).

> I checked automatic reconnection of the tunnel is well managed by Strongswan app when manually trying to restart the server for example, but unfortunately it's quite annoying to connect manually when android reboot itself or double check if it's running because you're having any other kind of problem with the other end discovering it isn't related to strongswan connection itself.

On regular Android, you could use shortcuts, automation apps or the Quick Settings tile to quickly initiate connections (but I guess there are some limitations on Fire TV or Android TV in general).

> which causes the need to do some nasty tricks like trying to create the "automation workflow" in a mobile device and export this config in tricky ways to the android tv running this same app.

If that works, I'd go with that.

The only other option I see is trying to initiate the connection when the system triggers ACTION_BOOT_COMPLETED, but that requires a new permission and broadcast receiver, and it obviously conflicts with the Always-On behavior, which is not ideal (the latter might actually be triggered already when ACTION_LOCKED_BOOT_COMPLETED is sent, but that could depend on the Android version, on some the VPN is definitely not initiated until the device has been unlocked, which makes sense as e.g. client keys won't be accessible before). I'd rather try to avoid using this and rely on the system's Always-On functionality and maybe automation apps.

#4 - 10.11.2020 19:57 - r2 d2

Tobias Brunner wrote:

> > which causes the need to do some nasty tricks like trying to create the "automation workflow" in a mobile device and export this config in tricky ways to the android tv running this same app.
>
> If that works, I'd go with that.

Without entering in the user-friendly discussion (android tv here...), saying it works it's something I can't confirm with these tv devices so far. Until now, I've tested the following top automation apps:
- Easer - Can't do anything due to the issues with UI not being adapted to non touchscreen devices.
- Macrdroid - Worse than the previous one, you can't bypass the welcome screen because it isn't possible to click the next button.
- Automate - Unfortunately it isn't possible to click the edit workflow button due to these problems. With StrongSwan receiver intent you have to forward the VPN profile ID (Ouch!!!!... Where is the copy-paste in these devices?) and this is unique per tunnel/device. When you try to export the workflow created from a mobile to android tv device due to these limitations, you can't change the profile ID within for the new Device... Game Over!. Maybe a simpler approach would be to use VPN name, like Wireguard does with its start/stop intents in Android, in that way would be A LOT simpler to remember/type it for the end user and reuse these workflows created with other devices like in this case.
- Tasker - I gave up here, after the previous experiences not willing to pay for something without guarantees that it would works in these environments.

Appart from it, StrongSwan is miles ahead of any other Android TV VPN apps not comercially oriented to sell you a subscription model. Unfortunately without the possibility to maintain a automatic persistent connection from start it's a no go for me.

I agree with you about the potential conflicts with Always-On VPN features that justify why this kind of automated integration doesn't work for you. Maybe the improvement of how intents are managed is something you can evaluate.

Regards,

#5 - 11.11.2020 12:41 - Tobias Brunner

> - Automate - Unfortunately it isn't possible to click the edit workflow button due to these problems. With StrongSwan receiver intent you have to forward the VPN profile ID (Ouch!!!!... Where is the copy-paste in these devices?) and this is unique per tunnel/device. When you try to export the workflow created from a mobile to android tv device due to these limitations, you can't change the profile ID within for the new Device... Game Over!.

Is it possible to import [VPN profile files](#) on the Fire TV? If so, the ID would be constant if the same profile is used on all devices. Mainly due to how keys are stored (in that the app has no access to them), there is currently no option to export profiles. But it's quite easy to write one from scratch. However, if the Fire TV has the same limitation as the stock Android TV image (i.e. the [SAF is not available](#)), this won't be an option.

> Maybe a simpler approach would be to use VPN name, like Wireguard does with its start/stop intents in Android, in that way would be A LOT simpler to rembember/type it for the end user and reuse these workflows created with other devices like in this case.

That's on purpose to make it harder for other apps to disconnect connections via Intent (since they must be public, they can't otherwise be protected).

> Appart from it, StrongSwan is miles ahead of any other Android TV VPN apps not comercially oriented to sell you a subscription model. Unfortunately without the possibility to maintain a automatic persistent connection from start it's a no go for me.

My only experience with Android TV is from the emulator and there the main issue is that the app is not listed in the "Apps" menu. Not sure if that's different on the Fire TV. Looks like that's because we don't have any Activity with CATEGORY_LEANBACK_LAUNCHER Intent filter. Adding that to the MainActivity, seems to work and it e.g. allows adding the app to the favorites so it could be started relatively quickly from the home screen (it would look a bit nicer if we'd also define a banner image). The app itself seems to work reasonably well inside the emulator (except for the mentioned SAF issue). For the app to appear in the Google Play store on Android TV there are some [other requirements too](#), but since the app is not optimized for the Leanback UI Google might have issues if we'd do that (I guess that's not really an issue on the Fire TV, or is the Play store available there too?). However, perhaps it's not a problem as long as we don't actually request the features so it won't appear in the store. With the filter added it would at least show up when side-loaded.

Something like [this](#) might also be interesting, as it could allow you to create a shortcut to initiate a specific profile by building and installing a proxy app that only issues that Intent.