

01 Introduction

01 Introduction

FEAT VPN brings OpenVPN to Android versions before Android 4.0, no root required. It is the first layer-3 VPN app that works on any off-the-shelf device with an Android version between 2.1 and 3.2.

Android 4.0 and later break the underlying technology of FEAT VPN. Thus, unfortunately, FEAT VPN cannot be made to work on these Android versions. However, Android 4.0 is also the first release to offer official support for VPN apps. Somebody else will probably come up with a version of OpenVPN for Android 4.0+.

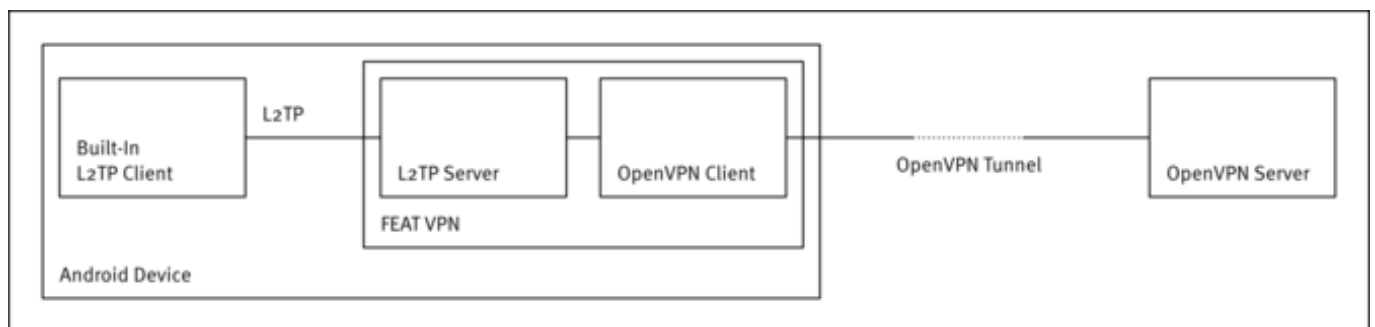
FEAT VPN comes in two versions. The free version, FEAT VPN Lite, is intended for people who connect to a VPN server only occasionally. To check their email a few times each day, for example. Use of FEAT VPN Lite is limited to one hour per day. The commercial version does not have this time limit.

The Underlying Technology

You are probably aware of the built-in Android VPN client. On most devices it is accessible via **Settings > Wireless & networks > VPN settings**. Its supported VPN protocols are PPTP, L2TP, and L2TP/IPsec. Normally, you would use the built-in client to connect to, say, a remote L2TP server. The fundamental idea behind FEAT VPN is to not connect the built-in client to a remote server, but, instead, to connect it locally to the FEAT VPN app on the device. The FEAT VPN app then sits between the built-in L2TP client and the remote OpenVPN server and provides VPN protocol translation:

- **Outbound.** FEAT VPN receives IP packets from the built-in client via an L2TP connection and forwards these IP packets to OpenVPN, which forwards them via an OpenVPN tunnel to a remote OpenVPN server.
- **Inbound.** OpenVPN receives IP packets from the remote OpenVPN server via an OpenVPN tunnel and forwards these IP packets to FEAT VPN, which forwards them via an L2TP connection to the built-in client.

The following diagram illustrates this idea.



Note that the security of L2TP is not relevant here. The L2TP connection is established between two apps on the same device: the built-in L2TP client app and the FEAT VPN app. L2TP packets never traverse a network, because they never leave the device. Security issues of L2TP thus do not apply to FEAT VPN.

01 Introduction

Published on FEAT VPN (<http://www.featvpn.com>)

Limitations Of The Technology

The underlying technology of FEAT VPN has a few drawbacks. In our experience they do not have much of an impact, though.

IPv6. The built-in L2TP client does not support IPv6 and, accordingly, FEAT VPN cannot support IPv6, either.

Network Configuration And Routes. The OpenVPN server pushes network configuration changes to the OpenVPN client when a VPN tunnel is being established, e.g., a DNS server to be used by the client. Just like IP packets, FEAT VPN receives these configuration changes from OpenVPN and forwards them via L2TP to the built-in L2TP client. We are thus limited to network configuration changes that can be transmitted via L2TP, which are:

- Local and remote IP address of the VPN tunnel
- VPN tunnel MTU
- DNS server

In particular, L2TP does not support route modification. The built-in L2TP client generally routes all traffic through the L2TP connection. So, no split tunnels. When the OpenVPN tunnel is up, all traffic always goes to the OpenVPN server.

TUN/TAP. The built-in L2TP client only offers a TUN-like device. FEAT VPN inherits this limitation and, accordingly, only supports TUN configurations.

System Calls. Just like the rest of FEAT VPN, the OpenVPN client does not run with root privileges. This breaks a few OpenVPN options, e.g., `chroot` or `mlock`.

Device-Specific Bugs. Apart from these general limitations, a handful of Android devices comes with a broken built-in L2TP client. On startup, FEAT VPN detects and notifies you of any known problems with your device. The section **Installing And Running FEAT VPN** contains more details.

Open Source Components

The source code of our versions of OpenVPN is available at the following URLs:

Version 8 - <http://www.featvpn.com/sites/default/files/v08.tgz>

Version 10 - <http://www.featvpn.com/sites/default/files/v10.tgz>

Version 20 - <http://www.featvpn.com/sites/default/files/v20.tgz>

The archive includes the OpenSSL and LZO libraries as well as the build files that are required to recompile OpenVPN. Note that we use Linux to develop FEAT VPN and it has been brought to our attention that at least on Windows the build process does not work out of the box. On Linux, simply install the Android NDK, unpack the archive, and run **ndk-build**.

The licenses of the open source components used by FEAT VPN are available at the following URL:

<http://www.featvpn.com/r/licenses>

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

[Print Section](#)

[Print All Sections](#)

[Export Section](#)

[Export All Sections](#)

01 Introduction

Published on FEAT VPN (<http://www.featvpn.com>)

Source URL: <http://www.featvpn.com/1-introduction-0>