02 Expert Quick Start

02 Expert Quick Start

This section assumes that you are very familiar with setting up and running OpenVPN servers and clients. It summarizes those aspects of FEAT VPN that may not be obvious and leaves the rest to your experience. If you prefer more detailed guidance, please skip ahead to the next section **Installing And Running FEAT VPN**.

Initial Setup. FEAT VPN supplies a local L2TP server on your Android device. The basic idea underlying FEAT VPN is to connect the L2TP client built into Android to this local L2TP server. On Android 2.x (i.e., Android phones) FEAT VPN automatically handles this L2TP connection behind the scenes. On Android 3.x (i.e., Android tablets), however, you need to manually configure the L2TP connection with the built-in L2TP client. The name of the L2TP connection needs to be **Feat**, the L2TP server needs to be **localhost**. If you have an Android tablet, push the **Setup** button on the main screen to get to the setup screen, which has further information.

Test Suite. FEAT VPN depends on the correct implementation of the built-in L2TP client. Unfortunately, a few devices have severely broken L2TP clients. This is why FEAT VPN comes with a test suite, which makes sure that it works on your device. If you have an Android phone, pushing the **Setup** button on the main screen starts the test suite. If you have an Android tablet, then push the **Test** button on the setup screen after you have configured the L2TP connection.

If you have an Android tablet, your help is needed after the first four tests have been run. You need to manually establish the L2TP connection to **localhost** that you previously configured. Use a user name of **test** and a password of **x** to establish the connection - as pointed out by the instructions shown by FEAT VPN at this point. Again, on Android phones this happens automatically behind the scenes.

Tunnel Configuration. Push the **Tunnels** button on the main screen to add a VPN tunnel. Push the **Add** button to get to the tunnel edit screen. Here you give your tunnel a name and load your VPN configuration. The two most common configuration formats are supported:

- **ZIP archive.** The ZIP archive must contain one (and only one) VPN configuration file and its accompanying certificate and key files. The file name of the VPN configuration file inside the ZIP archive must end with **.ovpn**. Otherwise FEAT VPN does not recognize it. The file name of the ZIP archive, obviously, must end with **.zip**.
- **Self-contained VPN configuration file**. Instead of referencing external key and certificate files, a VPN configuration file can inline the required certificate and key files. Such a configuration file then has, for example, a `<ca> ... </ca>` section that contains the inlined certificate of the certificate authority instead of a `ca` option that references an external certificate file. The file name of a self-contained VPN configuration file must end with **.ovpn**

Tunnel Establishment. If you have an Android phone, simply push the **Tunnels** button on the main screen and tap on the VPN tunnel that you would like to connect. If you have an Android tablet, you need to manually connect the L2TP connection that you previously configured. Push the **Connect** button on the main screen. This brings up the built-in L2TP client. As the L2TP user name enter the name of the tunnel to be connected, as the L2TP password enter the password that unlocks any password-protected keys in the VPN configuration. If none of your keys are password-protected, simply enter **x** as a dummy password. FEAT VPN will detect the incoming L2TP connection, receive the user name that you entered, and match the user name against the names of the VPN tunnels. The VPN tunnel that matches your entered user name is then connected.

DNS Server. You can push a DNS server from your OpenVPN server to FEAT VPN.

NAT And Battery Life. When you are on mobile data, your phone accesses your OpenVPN server via the operator gateway of your mobile carrier. The operator gateway is essentially a firewall with NAT. This leads to the following problem: When your VPN tunnel is idle for a while, the NAT mapping for your VPN tunnel will time out on the operator gateway. When your VPN tunnel becomes active again, the operator gateway will use a new, different NAT mapping. The OpenVPN server now sees a different source port in your VPN tunnel packets and drops them - your tunnel hangs. You can revive it by pushing the **Reconnect** button on the status screen. You can also keep the NAT mapping from timing out by setting up pings on your OpenVPN server and add, for example, `ping 30` to your server configuration. This, however, can severely drain the battery of your Android device as the pings prevent its radio from going to sleep. So, try to find a ping interval that is as long as possible but still keeps the NAT mapping alive. Also, Wi-Fi routers seem to have longer NAT timeouts than most operator gateways. You may also want to try using OpenVPN via TCP vs. UDP. Different NAT timeouts may apply to different network protocols.

Switching Networks. FEAT VPN detects when you switch from mobile data to Wi-Fi and vice versa and automatically restarts the OpenVPN tunnel on a switch.

FEAT VPN is described in much greater detail in the following sections.

Source URL: http://www.featvpn.com/02-expert-quick-start