



Published on *IMUK Mobility Blog* (<http://ukblog.im-mobility.com>)

[Home](#) > [Printer-friendly PDF](#) > Printer-friendly PDF

# What do you need from your mobile operator to set up a VPN connection?

By *admin*

Created 30/01/2010 - 12:49

Created on 30 Jan 2010

I have written before about troubleshooting VPN connections from mobile devices should you experience problems (<http://ukblog.im-mobility.com/troubleshooting-mobile-vpn-connections> <sup>[1]</sup>), but it has cropped up a number of times recently so I thought another post might help to better understand what the options are in terms of operator services and which is right for you based on your VPN infrastructure.

A VPN is a Virtual Private Network. People often believe a VPN is a more secure means of connecting to the Internet. VPN technology can be used to accomplish this, but typically it's actually more basic: the point of a virtual private network is simply to provide remote access. Security is obviously a concern, but this is a feature, not the main objective when used in this scenario. VPNs extend the boundaries of a local network to remote machines by fooling the local network into believing remote machines are connecting locally by creating a virtual network connection over the Internet.

To use a typical example, field workers have a VPN client that when connected effectively puts their laptop on the corporate network regardless of where they are geographically and allows them to connect to the 'Shared' drive (or any network resource) as if they were at their desk. Yes it's much slower, but remember you're having to send your requests over a cellular Internet connection (measured in 100s of Kbps) rather than over the Gigabit LAN infrastructure in the office (measured in 1000s of Mbps).

When a VPN client is installed on a PC, it adds a new network adapter to the PC – a virtual adapter. Network adapters are such things as your Ethernet port (where you plug your network cable) or your WiFi card. A virtual network adapter is a piece of software that acts as a physical device and appears to the operating system as a real device.

When you connect to the VPN, the VPN server will push down a number of 'routes' to your computer, so that the PC knows to send normal traffic to [www.google.com](http://www.google.com) <sup>[2]</sup> over the Internet via either your Ethernet or WiFi device, but to send anything for [xxx.mycompany.com](http://xxx.mycompany.com) over the virtual adapter (and therefore to the VPN server and onward to the internal corporate network). The virtual adapter STILL USES the existing physical adapter to send traffic over your Internet connection, but it does clever stuff in the background to 'wrap up' traffic before sending it over the Internet to the VPN server via the 'real' adapter.

With me so far?

Before I can explain how VPNs work, we need to cover off how the Internet works – very basically. The Internet uses the Internet Protocol: IP.

Currently most of the Internet uses IP version 4 (IPv4). Essentially this means all machines on the Internet are assigned an address, along the lines of 212.58.253.67

In the same way that when you send a letter to 16 Alder Hills, Parkstone, Poole, UK an Internet address can be broken down in the same way, with 67=16 Alder Hills 253=Parkstone, etc etc etc

All that IP does is handle addressing. To actually send stuff to another address from your address, you need a transport protocol: TCP is the most common – that is why you often see TCP/IP written together.

In a nutshell, TCP handles the 'what', IP handles the 'where'.

On a local network, when one machine requests something from another (say you want a document from the file server), the application doing the request (let's say 'Word'), creates a TCP request that says "I want this file". The TCP request is then sent to the network adapter. The network adapter will add 2 IP addresses to the TCP request: the IP address of itself, and the IP address of the target server. You now have a TCP/IP 'packet' that can be sent to the server. At the server, the file is retrieved and sent back to the IP address that was included in the original request.

So far so good.

There are not enough addresses available in IPv4 for all machines to have an address on the Internet.

This means local networks use 'gateways': a single machine 'faces' the Internet and all machines on the local network (behind the gateway) have internal addresses (that cannot be reached from the Internet unless they go through the gateway first).

When a machine on the local network requests something from the Internet, it sends the request to the gateway. At the gateway a process known as NAT (Network Address Translation) happens. THIS IS VERY IMPORTANT.

What this means is that your PC has created a packet with its own address and the address of, say, the BBC web site. If the BBC web site receives this packet it won't be able to send anything back because the source address is an internal address which it doesn't know what to do with. Therefore, at the gateway, what NAT does is to REMOVE the address of your machine and ADD its own Internet address. The BBC sends the web site back to the gateway address. NAT then happens again but in reverse. The gateway's own address is removed and the internal address of your machine added back in again, and the web page is sent back to your machine on the local network.

Now it starts to get a bit tricky.

There are 3 VPN technologies in common use: PPTP, L2TP and IPSec.

PPTP is the simplest and essentially just requires that you enter a username and password to connect. This is weak from a security point of view as anyone who gets your password can log in as you.

L2TP improves on this by requiring that you have a certificate installed on your machine as well as knowing the username and password. Therefore even if someone knows your password, they can only log in as you from a machine that has the correct certificate installed. These are also referred to as SSL-based VPNs. OpenVPN is an example of an SSL-based VPN.

IPSec goes even further and requires both a certificate and a password, but also generates a 'digital hash' based on your IP address. By that I mean that when the VPN TCP/IP packet is created, before it is sent, the IP 'header' (containing both the source and destination addresses) is run through the certificate and a number stored within the packet. At the receiving end, the number is then checked against the IP header information on the received packet. This means that should someone have your password and certificate but try to 'pretend' to be connecting from an IP address other than their own (ie yours), the connection will fail. This is a security measure and is entirely deliberate...but it does have important repercussions on mobile connections.

Mobile networks can be treated as local networks. Yes they are physically huge and cover many geographical miles, but from a logical networking perspective all mobile devices are on a local network behind a gateway. In this case the gateway is the APN – the Access Point Node: the access point to the Internet.

In exactly the same way as an office LAN works, mobile devices are assigned an internal address and NAT occurs at the APN when requests are made to the Internet.

But hold on...

We saw a minute ago that IPSec VPNs create a 'check' value on all packets based on their IP header information.

We also saw that NAT removes the source address of a client request and substitutes it for the gateway's source address.

You guessed it – if an IPSec VPN packet passes through a NAT gateway, when it is received by the VPN server the check value will no longer match the original as the header has been altered, and the VPN connection will fail. Although no intentional foul play has occurred, the VPN server doesn't know this and will reject the packet as having been tampered with (which of course it has been).

IPSec therefore does not play well with NAT. This is the most common reason why mobile VPNs fail.

To address this issue, most network operators offer 2 APNs: one for the public Internet, and one for corporate VPN customers. The only difference between the two is that the VPN APN offers devices public IP addresses, and therefore do not undergo NAT. Sorted. There is no cost to use this APN, but you do have to request it specifically...for all SIMs.

Excellent, we have a solution. BUT – as this is not the standard APN, any device that auto-configures itself (Nokia CS-10, Sierra Wireless 889, etc) will default to the public APN and will need to be reconfigured manually by the user to use the non-standard APN. This may not be acceptable to companies with large numbers of remote workers.

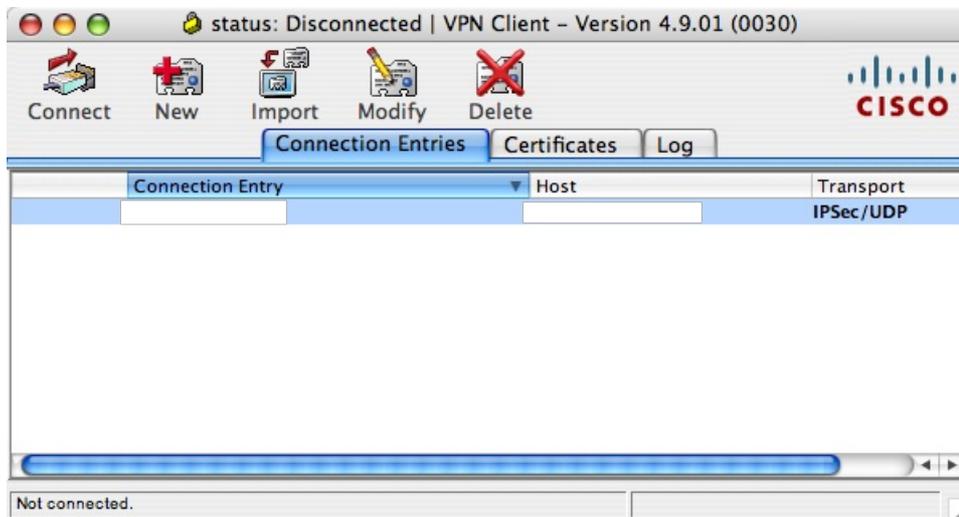
But wait, I know of companies that use an IPSec VPN and they don't have to use a special APN. How come? Now we get REALLY geeky...

We saw earlier that TCP/IP creates packets with 2 IP address: a source and destination address and it is the source address that gets substituted by NAT which breaks IPSec connections. Although TCP is the most common form of transport protocol, there is another.

UDP is another transport protocol that actually pre-dates TCP. An older protocol, the structure of UDP packets is different and does not include the source address in the IP header, only the destination address. Therefore a UDP packet can pass through a NAT gateway without being altered, and therefore can be used successfully for an IPsec VPN from a public APN.

This is a gross simplification, but I sense I'm losing you so we'll leave it at that!

Most decent VPN products offer in their configuration the option to use UDP as a transport mechanism as opposed to TCP, or they may refer to it as 'NAT-T' (for NAT Traversal). This needs to be configured on the server and the client:



### So what have we learnt?

Many mobile operator customer services departments, when they hear the phrase 'VPN' will have a knee-jerk reaction and tell you that you must use the VPN APN – because that is what they have been taught. That is not necessarily true.

The APN you need to use depends entirely on how your VPN server is configured. If NAT-T or UDP Transport is configured (and enabled) then you can connect from ANY Internet connection.

### To summarise

If your VPN does not work over the public APN, the options are (PROVIDED IT IS A PROBLEM WITH THE VPN AND NOT SOMETHING ELSE):

- Use the VPN APN
- Use the public APN but enable UDP or NAT-T on the VPN server appliance
- Use L2TP (or SSL) instead of IPsec – a common example of an SSL-based VPN solution is OpenVPN (<http://ukblog.im-mobility.com/openvpn> [3])

Or there is another option, which is even more geeky: IPsec is basically L2TP with another module bolted on, called 'AH Mode', or 'Authentication Header'. Some IPsec VPN products enable you to turn off the AH mode and just use the L2TP bit, which they may refer to as ESP mode (for Encapsulating Security Protocol). If you have the option to disabling this feature, try that.

This has been an introduction to VPN technologies and the potential pitfalls to be aware of when establishing connections. There is more troubleshooting that can be performed - for more in-depth information about DHCP and network addressing schemes read this article - <http://ukblog.im-mobility.com/troubleshooting-mobile-vpn-connections> [1]

[Reference](#) [4] [VPN](#) [5]

[Reference](#) [VPN](#)

---

Source URL (retrieved on 20/05/2013 - 06:33): <http://ukblog.im-mobility.com/node/230>

#### Links:

- [1] <http://ukblog.im-mobility.com/troubleshooting-mobile-vpn-connections>
- [2] <http://www.google.com>
- [3] <http://ukblog.im-mobility.com/openvpn>
- [4] <http://ukblog.im-mobility.com/category/blog/reference>
- [5] <http://ukblog.im-mobility.com/category/blog/vpn>