



## Virtual Private Networks - VPNs

July 2007

**You may have heard the term “VPN” - but be unclear about what it is and how this form of long-distance networking could benefit your business.**

**Our E-Business Advisers explain:**

### 1. What is a VPN?

A Virtual Private Network (VPN) is a secure means to allow you to give remote access to your main office computer network to other branch offices, or individuals working at home or in other locations (e.g. sales staff on the road).

Unlike linking your branch offices back to the head office through leased phone lines, a VPN uses the Internet, and secure encryption technology.

This means that VPNs are extremely secure, and comparatively cheap and easy to set up. Because of these advantages, VPNs have fast become a major networking technology over the last few years.

### 2. How does it work?

With a VPN, you can send data, via the (publicly-shared) Internet in the same secure way as you would in a point-to-point private link.

This could be between two networks in offices in different locations, between two servers, or between a “client” (an individual PC) and the main office server.

The most common setup for a VPN in small and medium sized firms is that between a client and a server.

The remote client PC (installed with special VPN client software) uses its Internet connectivity (e.g. a broadband connection) to set up a secure “tunnel” through the Internet.

This “tunnel” uses special encryption and user authentication techniques to only allow authorised users to access the server at the other end of the tunnel.

Your office VPN server allows this remote user, via this secure tunnel, to access resources inside your network, as if the user was physically in the office.

After the client computer has been successfully connected to the office server, the secure tunnel between it and the VPN server will then encrypt all the data which passes along it.

As such good encryption is used, the tunnel between the client and server is considered very secure.

Because of this security, the remote client computer can be trusted by local computers on the office network that the server runs. The client PC effectively becomes part of the network, as if it was in the same office

### 3. What are the benefits of using a VPN?

- By using a VPN, business can use a secure “tunnel” through the Internet without the need for expensive private communication links - with as good a level of security as if the user was in the office.

This can bring considerable levels of cost savings - a recent client of the authors’ found that implementing a VPN between their main



# Fact Sheet

base and two small external offices had a “return on investment” period of 3 MONTHS!

As private leased telephone lines can be very expensive - several thousand pounds per year as compared to a broadband business connectivity package of circa £600 per year, it is easy to see how benefits can quickly accrue.

- As the popularity of broadband increases, more and more staff will have broadband at home. VPN technology makes teleworking much more practical (See “Teleworking” Fact Sheet in this series).
- A connection to the Internet is all that is needed for VPNs to work.

This means that staff who travel as part of their jobs could use Wi-Fi to connect in their hotel rooms or at the airport, then use their VPN to work as if they were actually in the office. (See “Wi-Fi - Wireless Fidelity” Fact Sheet)

## 4. Useful Links

<http://computer.howstuffworks.com/vpn.htm> - Easy to understand explanation of the different types of VPNs

[www.intranetjournal.com/foundation/vpn-1.shtml](http://www.intranetjournal.com/foundation/vpn-1.shtml)  
Overview of a range of VPNs and technical issues