

# No Bull Guide to Virtual Private Networks (VPNs)



[no/jargon@viatel](mailto:no/jargon@viatel)

No hype, no jargon, just 100% clear and comprehensible advice concerning the most popular business networking technology.

An honest guide to the business benefits of Virtual Private Networks for managers who want a convincing business case to invest in improved communications.

[www.viatel.com](http://www.viatel.com)

Baffled by jargon and afraid to push your business into the technology fast lane? Or are you frustrated by the inability of the Board to grasp the 'obvious' benefits of a CoS guaranteed IP VPN over Broadband?

This No Bull Guide to VPNs reveals the real reasons for investing in improved communication technologies, and is written in a clear and accessible style, to open up an honest dialogue between the IT department and the boardroom.

It has been written to help IT managers and budget holders present a strong business case as to why budget should be invested in a VPN rather than office refurbishment or staff membership to a gym.

## /introduction

Firstly let us explain the benefits of a VPN, and how it can increase business productivity and manage costs.

By improving the effectiveness of your communications, co-operation between employees, customers and business partners will increase. This will enable new, more productive ways of working. The flexibility of the VPN itself means it can change and grow to meet your business needs. The end result is managed costs – both real and hidden. Helping to maximise the return on your investment.

In this booklet we look at:

- 1 Better Co-operation through Communication**
- 2 New Ways of Working**
- 3 Future Proofing**
- 4 Controlling your Costs**
- 5 Return on Investment**
- 6 Supplier Checklist**
- 7 Glossary of Terms**

The following pages assume a basic level of IT awareness, but if you're perplexed by serial ports, and anxious over acronyms, try the glossary for some quick definitions of the most common terms we'll be using.

A virtual Private Network (VPN) enables your office, remote workers, customers and partners to exchange vital information, regardless of their location. It uses a shared infrastructure, so it's cost effective; and the technology it uses gives you your own secure private company network.

## /better co-operation through communication

The average UK worker will come into contact with thousands of people in their working life, but will only ever meet half of these face to face. All the rest are dealt with by phone or via email.

The installation of a VPN creates the framework for a shared network between people who work together, inside and outside the business. It makes for seamless communication between all departments and helps to speed up the time between a query and its resolution. This positions your company to the outside world as an enabling force rather than an obstructive middleman.

Co-operation inside businesses also depends upon timely communications. So, a VPN can make standard business tools such as databases and company directories really come alive. A salesman working remotely could instantly look up stock availability before offering a customer the deal of a lifetime, and a field engineer could check how long he's got to mend Mrs Jones's pipes. In short, a VPN can give remote workers secure access to everything they need to do their jobs faster, smarter and therefore more profitably.

With a VPN, staff from your other offices – perhaps hundreds of miles away – can collaborate effectively,

working with the same information to give a better service to customers. Such co-operation requires more than clever technology, it requires the management of IT infrastructure and trained staff – helping to catalyse better methods of co-operation.

You can also choose to connect your partners and customers to your VPN. The speed and accuracy of your response to queries suddenly becomes as integral to your brand as the quality of your products or the friendliness of your staff. Revealing the inner workings of your business to suppliers, let alone customers, is a daunting prospect for any firm. But if properly managed, sharing key information with your suppliers and customers can really help to improve co-operation and build relationships that drive the business forward.

Enabling a VPN across your business opens up a whole new range of co-operative business tools, from shared applications through to virtual meetings.

### What's in it for you

- Informed, co-operating employees
- A more responsive business
- Distance is no barrier to integration

## /new ways of working

Today's businesses need to take into account the increasingly diverse lifestyles of their employees. At some point in our careers most of us are likely to consider working flexibly. The installation of a VPN can help companies match the needs of their employees with the requirements of business, regulators and legislators. For example, since April 2003, employers have had to give due consideration to the requests for flexible working arrangements from parents of young or disabled children.

This in turn makes you more attractive as an employer – increasing your appeal to the best people. Companies need not view employees' requests to 'work from home' as a coded request for a sneaky lie-in after a night on the town. Instead, they should view it as an opportunity to retain key staff and instigate a more productive business environment. Employees can spend less time travelling to the office and mobile workers can remotely access the information they need. Regional meetings can be done online, rather than on expenses.

A VPN allows staff to access the information they need quickly and securely. Although it cannot stop them watching daytime TV.

A combination of company policies, trust and if necessary, monitoring tools can be used make sure your flexible workforce remain a happy yet productive one.

### What's in it for you

- Business systems compatible with real peoples' lifestyles
- Productivity maximised, regardless of location
- A happy yet flexible work force

## /future proofing

If you are not careful, today's white-hot technology is tomorrow's outdated system. But VPNs are adaptable to future needs, because they use IP technology, which is the standard protocol for the internet. So, almost all future business applications are likely to be compatible, protecting your investment.

If you grow from 2 sites to 10, you can add new sites and users to your VPN without increasing your IT overheads. A VPN supports all manner of business applications including email, shared files, voice, video, CRM and billing. In fact, whatever business you run, and however much you think it'll change, a VPN will continue to give you access to the information you need.

VPNs are based on a wide range of technologies including MPLS and IPSec. With MPLS you get Class of Service, which allows you to prioritise one type of network traffic over another. So, you can tell it to deliver voice calls faster than email. IPSec gives you data encryption and traffic tunnelling for even greater security.

A supplier should offer total flexibility in their choice of VPN, supporting hybrid solutions with

a mix of MPLS and IPSec technologies, and accommodating any kind of network access: broadband; dial-up; leased lines and Ethernet. Remote access for mobile workers can be supported either via direct dial into the MPLS VPN or access via the internet over standard IPSec VPN.

A VPN service should be available as a 'wires only' option if you have the internal IT resource available, but it becomes even more flexible when you get someone to manage it for you. Most good providers will offer a managed service – meaning they'll design the VPN to your exact requirements and then install and support it in line with service guarantees.

### What's in it for you

- A solution that grows with you
- Managed service option allows you to focus on core business
- Works with your existing infrastructure

## /controlling your costs

The reality of business is that there are always more opportunities to invest than there is money in the pot. Building an effective business plan that demonstrates the cost savings and business benefits of a VPN will provide the best edge to securing budget.

VPNs are one of the best value networking technologies available to businesses today. They have the ability to use existing network infrastructures – which reduces your upfront capital expenditure – and you can connect a VPN using a wide range of options. So, whether you just need to connect 2 small offices using broadband, or link 25 sites via high capacity leased lines or Ethernet connections, a VPN will still be cost effective to install and manage. The knock-on effect of increased business efficiency can lead to greater cost savings.

When evaluating a managed VPN service, you should begin by calculating what you're already spending or what you would spend on an in-house solution.

### Real costs to consider include:

- Hardware equipment – cost to buy, configure and install
- Connectivity costs – installation costs, monthly charges, cost of back-up services
- Call charges
- IT staff to manage your network equipment

### Hidden costs to consider include:

- Lost productivity of employees if service unavailable
- Lost sales and damage to company reputation if service unavailable
- Expensive IT specialists
- Core work not completed by IT staff spending time troubleshooting
- Cost of IT staff supporting multiple sites round-the-clock
- High and unpredictable cost of external consultants to fix service
- Cost of investing in equipment which may quickly become obsolete

### What's in it for you

- Improves communications without increasing IT overheads
- Add new sites and users easily and economically
- Wide range of cost-effective connectivity options

## /ROI

In order to understand the Return on Investment (ROI) for a managed VPN service, you should compare the costs of your current solution with the cost of a managed VPN service from a provider such as Viatel. We can help calculate the savings you could expect from a managed service, and help you to prepare a business case for a VPN.

Typical metrics we can help to calculate include:

- Monthly cost savings of managed v in-house service
- Payback period for investment in managed service
- Potential £ cost savings over period of contract
- Potential % cost savings over period of contract

As well as cost savings, we can help to measure the business benefits that a VPN can deliver. Whilst these benefits are not always easy to quantify, they are key to consider e.g. increased employee and network efficiency.

**ROI Example** (All values are indicative based on typical market prices)

Cost savings and increased network performance can be gained by moving to an up-to-date IP VPN with broadband access.

IP VPN purchased 2 years ago, based on leased line local access tails:

	Main Site Access	Access for 9 branch sites	Annual Charge	% saving 1st year	% saving subsequent years
Existing Solution	2Mbps	256kbps	£64,000		
New Solution	2 Mbps leased line access	512kbps uncontended ADSL	£40,000 including installation	37.5%	Over 40%

If existing internet access is a separate service at the main site you could save more:

	Main Site Access	Annual Charge	% Annual savings
Existing Solution	2Mbps internet access via separate service	£10,000	
New Solution	2 Mbps direct access to internet via IP VPN	£3,000	70%

## /supplier checklist

In order to design, install, support and manage your VPN service properly, your provider should meet the following technical and operational requirements:

### Technical Requirements

- UK-wide and international coverage
- On-site configuration, installation, monitoring and maintenance of routers
- Full range of site access options and speeds to suit all sizes of sites
- Secure access options for remote workers
- Resilient and reliable core service provider network
- Broad range of back-up options
- Fully managed or 'wires only' option if you want to supply and manage your own site equipment
- Classes of Service available to prioritise traffic by type of application
- Traffic separation for full security
- Choice of encryption options including DES, 3DES and AES
- Network design that allows simple addition of new sites
- Online management tool to add and remove remote access users
- Access to the internet with appropriate security capabilities (e.g. firewall)

### Operational Requirements

- Design, configuration and implementation driven by dedicated project manager
- 24x7x365 service monitoring and technical support
- Guaranteed minimum on-site fix time
- Timely response to configuration change requests
- Dedicated service management
- Clearly defined and documented escalation process and contacts
- Web-based service reporting capability
- Comprehensive Service Level Agreements (SLAs)
- Simple billing process
- Easy upgrade process

## /glossary of terms

**Bandwidth** – A measure of the data capacity of your connection, or how much information can be squeezed down your line. The most common bandwidths are 512k, 1Mb and 2Mb for standard broadband connections.

**Broadband** – An ‘always-on’ internet connection with speeds ranging from 256kbps up to 2Mbps for most standard offerings. To tailor the speed and cost you can choose how many other companies share your line (the contention ratio).

**CoS - Class of Service** – This allows you to assign different priorities to different types of data, rather like slapping a first class stamp on them, except they’ll arrive on time. This is very useful for streams of data you want to arrive on time, voice or video for example, where delay affects the quality.

**Contention ratio** – The number of other organisations sharing your bandwidth. Normally expressed as a ratio, 20:1 means you might have to share your bandwidth with up to 19 other companies, whereas 1:1 (uncontended) means it is your own dedicated line.

**Dial-up** – The most basic type of connection to the internet. In today’s terms these connections are very low speed and it is still important to check your VPN is able to support such connections.

**DSL** – The most common type of broadband connection. This runs over standard phone lines rather than a costly leased line. Quality and availability will vary widely across the UK, so check your supplier is able to offer all levels of speed and contention across the nation.

**Ethernet** – A high speed connection originally used to connect IT resources, such as PCs, within a local area network or LAN (network of PCs confined to a small area, usually an office). The most common protocol to transmit data over a LAN is Ethernet, which can now be used outside of a building to connect into VPN services.

**IP – Internet Protocol** – The digital equivalent of the postal service, though more reliable. It allows you to address individual packets of data (discrete chunks of information) and send them off across the internet without establishing a physical connection with the receiving computer.

**IPSec – IP Security** – A type of encryption applied to data sent over a VPN to keep it safe from prying eyes. Generally used to secure confidential company information.

**ISDN – Integrated Services Digital Network** – Is a technology that sits half way between DSL broadband lines and standard dial-up. Whilst it is available nationally it can prove expensive as it is charged on a per minute basis.

**Local Access Tail** – A Point-to-Point connection from the customer's site to the nearest access point in the service provider's network.

**Managed Service** – Outsourcing is an increasingly attractive option for businesses requiring highly skilled 24 hour support but are unable to recruit IT staff with so few social skills that staying in on Friday night to watch server lights flash is an attractive vocation.

**MPLS – Multi Protocol Label Switching** – Essentially means that certain types of data can be prioritised over others, allowing both Class and Quality of Service. Only operators with their own network such as Viatel are able to offer such services directly.

**Protocol** – Set of rules by which various internet devices communicate between themselves to transmit data.

**Router** – A device that forwards data to the correct destination. Effectively a set of railway points across two or more networks, forwarding data off one and onto another and ensuring your data stays on track. Routers communicate amongst themselves to determine the best path for forwarding the data.

**VoIP – Voice over IP** – A term applied to both the hardware and software that allows you to make phone calls over the internet. The advantages include cheaper calls, and the ability to integrate telephone calls with your PC applications.

**VPN – Virtual Private Network** – Provides cost-effective communication between company sites, remote workers and business partners over a shared network, but gives you the security of a private corporate network.

**'Wires Only' VPN** – The customer installs and manages their own site equipment, leaving the provider to manage the connections to the VPN.

A dictionary of common 'technobabble' terms is available free of charge from [www.viatel.com/technobabble](http://www.viatel.com/technobabble)

**/clarity guaranteed**

The No Bull Guide to Virtual Private Networks (VPNs) reveals the real reasons for investing in improved communications technologies, and is written in a clear and accessible style, to open up an honest dialogue between the IT department and the boardroom table.

Since 1991, Viatel has been providing communications services to companies of all sizes across Europe. At Viatel we think business information is best kept safely inside your business. We provide secure communications between offices and employees, whatever the size of your company, wherever your people may be.

We think differently at Viatel. We listen to our customers, make a point of understanding their needs, and deliver a service that is right for them, not most convenient for us.

Find out how Viatel can help to connect and secure your business.

Call 0870 166 2269 or visit  
[www.viatel.com](http://www.viatel.com)

**Vi@tel** // simply different