

**B**usiness is merciless. If you're not there for your customers, come rain, hail or shine, one of your competitors will be. And yet a recent survey by YouGov found that the heavy snowfall this January caused employees in the UK to miss 124 million hours of work. Those lost hours mean missed deadlines and ultimately, for some, lost clients. The survey also found only 11% of the people who couldn't travel to the office had the option to work remotely.

Many companies don't like the idea of remote working. This is particularly true of smaller businesses that fear remote working is difficult to implement. But smaller companies need all hands on deck if they're to keep functioning – and that's exactly what remote working can deliver. In this feature, we look at ways of safely implementing remote access that will help keep your company working hard even when the rest of the country comes to a standstill.

### The dark art of virtual private networking

Most often, virtual private network (VPN) technology underpins remote access. A VPN is a means of privately and securely sending information over a public network, usually the internet. In a classic VPN, the client uses the IPsec protocol suite to both authenticate itself with the server and then to encrypt the packets that are exchanged between client and server during the communication. Client and server decrypt each other's messages using a pre-shared key.

Although they've been around for years, VPNs are regarded by many IT professionals as something of a dark art: a technology that always requires a lot of tinkering and experimentation to make it work smoothly. This isn't entirely a misconception. Configuring a VPN is rarely as straightforward as its instruction manual, let alone the marketing blarf, would have you believe. That said, in the past few years a number of developments have taken place that have made it easier for even small companies to run VPNs.

# Remote working for small businesses

**KARL WRIGHT** EXPLAINS HOW TO KEEP YOUR WORKERS ON THE JOB  
EVEN WHEN TERRIBLE WEATHER MEANS THE OFFICE IS EMPTY





## Outsourcing

If you don't want to get involved in configuring and managing a VPN, then you can simply outsource. Generally speaking, there are two types of outsource service. With the first option, your workers connect to your LAN through the outsource vendor's VPN gateway. You don't need any hardware on site; you simply install the vendor's client software on your laptops and pay a monthly fee per user. Alternatively, you could choose to have the hardware installed on your network, but then pay a third party, usually the reseller from whom you bought it, to manage it.

The advantages of a managed VPN service are simplicity and predictable costs, but there are pitfalls too. Passing your data through a third party means it's also out of your control, and if something goes wrong with the supplier's service there's nothing you can do about it.

Another downside is agreeing and understanding your security needs. Professor John Walker of Information Systems Audit and Control Association (ISACA) describes the problem: "I've lost count of the number of times I've been to organisations and discovered that they haven't shared their security policies with their managed services vendor. You can't afford to be vague about these things. Unless your vendor knows your precise requirements, you may not be as secure as you think you are."

Over the long-term, you may find a managed service costs more. UTM's and VPN-enabled routers generally cost between £400 and £1,500, depending on its features and the number of remote users required. Managed services start at around £20 per user per month. Clearly, the acquisition cost of a device isn't the same as its total cost of ownership, but with even a moderate number of users it won't take long before you've paid more than you would have to just buy the hardware.

Outsourcing comes into its own is when it adds value above and beyond providing the VPN connection. For instance, iPass provides connection management software that, among other things, dynamically monitors which network a user is connecting to. iPass itself doesn't actually provide a VPN service, but the company's channel partners (see [www3.ipass.com](http://www3.ipass.com) for a list) can provide it with an outsourced VPN service. The software itself monitors and controls how your users connect to the internet. When you're at the office, the client stays dormant. But when the

laptop connects to an unknown network the iPass client will, if so configured, automatically connect to the company VPN. You can even configure iPass to connect to the VPN depending on which application is launched. With a relatively simple addition to your managed service, you greatly simplify asset management and policy enforcement.

Another approach to outsourcing is to use an online service, such as LogMeIn's Hamachi. Hamachi is an online service that provides clients with a VPN that's easy to configure. It costs \$199 (£125) for a 256-user licence. To get it working, simply register on the Hamachi website ([www.pcpco.co.uk/links/187/remote1](http://www.pcpco.co.uk/links/187/remote1)) and create a network. Download the Hamachi client to your PCs, install them and add them to your network using your Hamachi login details.

## Do you already have what it takes?

Before you spend any money, check if you already have hardware or software that can provide remote access to the network. Your current router may already have VPN functions built in; many business models do. It's also possible to add SSL VPN capabilities to some network-edge devices – for instance, some SonicWALL gateways – through a simple firmware update. Note, you'll have to pay for this.

Even if your network-edge hardware doesn't have a built-in VPN, chances are that your server does. The server versions of all new Linux distros have their own VPN implementations. Ubuntu Server, for example, comes bundled with OpenVPN, while Red Hat has applications that allow you to create VPNs based on both the standard IPsec protocol suite and the CIPE protocol, an encryption protocol developed mainly for use with Linux. Doing things in this way, you can save money by turning an old server into a Linux box and configuring it as a VPN. Or, if you don't want to configure a Linux box from scratch, you could download a pre-configured virtual machine from a company such as Astaro: hardware costs are still nil (or close to nil), but there's a lot less work to do.

Microsoft Small Business Server also has an integrated VPN. In the 2008 version this has been simplified so that it can be set up with only a few clicks using the Configure a Virtual Private Network wizard. To run this, open the Windows SBS Console and in the



↑ As well as simple network browsing, you can configure Hamachi to allow applications to run over your secure channel, just as you would with a normal VPN.

Network tab select "Connect to a VPN". The wizard will configure Routing and Remote Access (RRAS) to accept VPN connections, the DHCP to work with remote clients and, if your external firewall supports UPnP, will even open port 1723 for you. As long as you already have the SBS and CALs for the affected users, setting up your VPN this way

is free and allows up to 250 users to connect simultaneously. The client software is already a part of Windows.

Alternatively, using Windows Server 2008 R2 and Windows 7 clients allows you to avoid VPNs altogether, and connect via a new technology called DirectAccess.

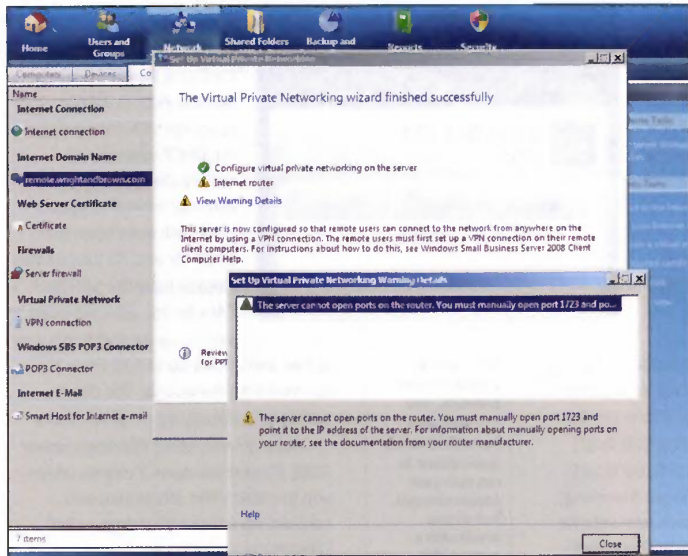
Finally, SoThin ([www.sothin.net](http://www.sothin.net)) has just released Thin Package. This lets employees use their work PCs and network remotely. Its chief attraction is its price: £99 exc VAT for the software (with no limit on users) plus £49 exc VAT for the Upgrade Protection package, which is mandatory for the first year.

## Routers and UTMs

Most manufacturers of business routers make a product that's also a VPN gateway. These devices range in price from the £50 Cisco WRV210 to the £140 Netgear FVS338. The cheaper devices tend to offer basic IPsec VPN networking for anything up to ten users. You simply create user accounts on the router itself, enable the VPN function and enter a pre-shared passkey: and that's the VPN up and running. Your users can connect using either the router's client software or the Windows VPN client.

Although limited in comparison with more expensive devices, it's still surprising what you can achieve with these relatively simple built-in VPN gateways. Take, for instance, the case of Swift Technology Group, a small engineering technology company with offices around the country and a small but growing number of remote workers. Currently, the remote users, who are often transferring many gigabytes worth of CAD data, all dial into a single £90 router with support for eight simultaneous VPN connections.

But as more remote workers come online, the company's needs are quickly outstripping its infrastructure. Sam Dickinson, the company's IT manager, who also doubles as design manager, isn't daunted. He's already experimenting with a site-to-site tunnel



← The VPN wizard in Windows Small Business Server 2008 configures the server's VPN function in a few steps; here it's warning us that the router must be configured manually.

between the two main offices using another router of the same model. Doubling the number of remote connections available will solve the company's remote working limitations, and also allow it to synchronise backup between the two sites over the VPN using an IDSbox (web ID: 351127). "I like to push the kit and see what it's capable of," Sam explains. "If I can get everything I need for £180, so much the better."

More expensive devices come with a broader range of features. They may offer a variety of means of authentication, including integration with Active Directory. They even support one-time passwords, which are texted to the user's mobile phone when they request a connection. Many dedicated VPN devices also support connections for mobile devices. Cisco ASA 5500 Security Appliances, for instance, come with their own iPhone client. Alternatively, look for a device that supports IPsec with IKE Extended Authentication, as used by the iPhone's IPsec client.

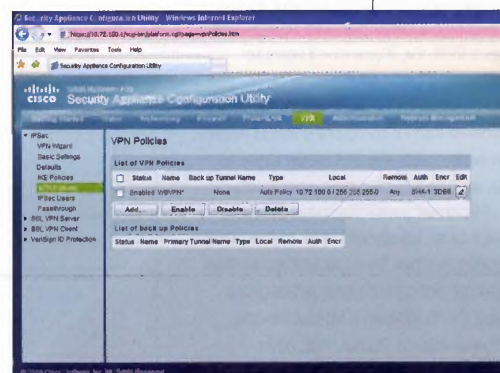
Another function that many pricier VPN gateways offer is the ability to host an SSL VPN. But don't be scared by the word "pricier". For instance, you can buy the SonicWALL SSL-VPN 200 for around £400 exc VAT. Secured with the SSL browser encryption protocol, these VPNs are supposedly easier to use than conventional IPsec VPNs. Instead of using special software to log in, users simply browse to your organisation's VPN homepage, log in and a secure connection is established. The first SSL VPNs only provided access to browser-based applications and to simple file browsing. Most of the current crop, however, support

port-forwarding to specific applications: so your business software can use the secure connection and operate as it normally would, without the user having to do any special configuration.

In practice, installing the JavaScript applets that most SSL VPNs use to connect can be tricky, often requiring fiddling with Internet Explorer security settings to get them working. It's worth bearing this in mind when you first let your users loose on your new VPN. More seriously, in November 2009 the American government security agency US-Cert reported a potential security flaw in clientless SSL VPNs (see [www.pcpco.co.uk/links/187remote2](http://www.pcpco.co.uk/links/187remote2)). Sites open in the same browser as an SSL VPN can potentially run scripts on the VPN pages to extract confidential information. Before choosing a product with SSL VPN capabilities, you should ask the vendor how its technology will protect you against this vulnerability.

A final word on hardware devices: marketing brochures often claim things such as "this device can be up and running in less than an hour". This

↓ This Cisco SA540 router has assigned client PCs addresses starting with 10.72.100.0 to avoid conflict with remote networks.



assumes you're already familiar with VPNs and will know things such as not to assign your virtual adapters' IP addresses from the same range as those of their local network, and lots of other small details that will prevent your VPN working if you don't get them right.

### Support and asset management

Another challenge is how to maintain and support machines that are remote for long periods of time. Locking down the PC to prevent remote users installing their own software can be easily achieved using Group Policy. What's trickier is educating users that they have a clear pipe into your company's IT infrastructure: any nasty stuff they accidentally install on their PC can and will attack the company. To this end, make sure that internet usage policies are followed. If you're using a managed service, your provider's client may force the users to connect through the VPN whenever they want to go online. Client software from some routers also supports this function.

Support is perhaps the easiest of these problems to solve. There are several remote solutions on the market – for instance, LogMeIn Rescue and NetSupport Manager – that allow your IT staff to securely take control of and troubleshoot remote clients. If you're running a Windows network, you can also configure Windows Server Update Services (WSUS) to validate only updates (according to your policies), leaving the client machine to download from the Microsoft servers. Making sure that clients only get validated updates can greatly simplify support.

### Conclusion

Rob Bamforth, principal analyst in communication, collaboration and convergence Quocirca, sees remote working as something that can help SMBs compete with their larger rivals. "In the same way that the internet empowered SMBs by giving them a virtual presence that belied their size, remote working allows SMBs and SoHos to become mini-enterprises, competing in an ad hoc needs-driven way with... larger organisations."

More than ever before, there's now a range of competing technologies designed to keep small businesses connected and working, no matter what. Not only can this technology protect your company against natural disaster, it can also help you be everywhere, all the time – and in doing so, level the playing field between SMB and enterprise. ■