

Remote Access

An open network with closed access



Giving your staff, suppliers, business partners and customers remote access to your information has become a business necessity. It helps to increase productivity, enables more flexible working and improves communication between all key players. We can help you do all this while keeping you firmly in control.

Our managed Virtual Private Network (VPN) solutions provide easy-to-use and completely secure access through our national Next Generation Network. So you can connect people across multiple locations, ensure all information transmitted stays private, and be sure that all users are welcome. And everything is configured to meet the exact needs of your business.

What is a Remote Access VPN?

Our Remote Access VPN solutions combine internet, intranet and extranet connectivity in a single, powerful network. One that helps you to:

- Reduce both costs and complexity, while freeing up your IT staff to focus on other tasks.
- Boost operational efficiency by securely connecting staff, wherever they're based.
- Share information more freely across your organisation.
- Offer employees more flexible working, which in turn creates a happy workforce and improves productivity.

- Add to your business continuity strategy, by ensuring staff can still get the information they need and communicate with customers (and each other) should the worst happen.

And as the service is managed by us, you don't need to worry about the overheads associated with maintaining it. Once you've chosen which solution is right for you, we'll be there 24/7 to take care of the rest. It's really that simple.

Keeping your business secure. IPSec or SSL?

An **IPSec – or network layer – VPN** uses a shared network to transmit sensitive, multi-protocol traffic, using a combination of encryption and tunnelling technology. Your people can enjoy the same full and continuous access to your network as if they were at their desks, but they can do so from any location 'known' to the system.

Choose IPSec VPN if you want to:

- Establish permanent tunnels and connections between sites – for example, connecting branch offices to headquarters.
- Grant access to ‘authorised’ hardware such as company PCs or laptops.
- Ensure an ‘always-on’ connection that enables automated file transfer of data to be sent between programmes – such as a retail POS system that constantly needs to keep head office up to date with transaction data.



A SSL – or application layer – VPN

offers your staff the ability to connect to your network from *any* web-enabled device, in *any* location. So home or mobile workers can always access the information they need, wherever they are, without putting your network at risk.

Choose SSL VPN if you want to:

- Provide secure remote access to workers both inside and outside corporate locations.
- Enable access to your network from any web-enabled device (be it an employee’s home computer, a public internet kiosk or their smartphone).
- Reduce the cost and complexity of installing, configuring and supporting corporate software or hardware devices.
- Control users’ access at a granular level, including their identity, the network they’re connecting from, and even how secure their device is.
- Ensure your business can continue to operate in the event of a disaster.

Combining connectivity and security

Both our IPSec and SSL VPN solutions meet a wide range of connectivity demands – from the lower bandwidth needs of people working from home, to the high bandwidth, high availability requirements of a corporate enterprise.

Plus, in the event of a disaster or unplanned disruption to your business, a Managed VPN enables remote workers to continue with their day-to-day activities unaffected. And it can quickly and easily be increased to accommodate everyone.

If you’re looking for tightly integrated connectivity and remote access solutions with just one point of accountability, just speak to us. All our solutions also include business class Service Level Agreements (SLAs) for extra peace of mind. As well as:

- Configuration and installation.
- Service availability and performance monitoring.
- Device configuration, integrity checking, back-up and restore.
- Access to skilled security specialists.
- Hardware and software maintenance.
- Change management.

Enjoy total protection

Opening up your network to enable remote access no longer means putting it at risk. Our Managed VPN solutions use industry-leading, award-winning security appliances from Juniper Networks. These not only integrate with the VPN to provide superior levels of protection, but also combine with proactive management to create complete peace of mind.

IPSec VPN solutions are based on robust encryption. This not only maintains the integrity of your data while it’s being transmitted, but also ensures the device to which it’s going is authentic. Plus, you can configure dedicated tunnels to the appropriate security you need.

SSL VPN solutions provide an unmatched level of protection. Administrators have visibility of the actual content of data, not just network ports and IP addresses, so they can grant or deny access to resources at a very granular level. Plus, detailed logging of actions at the precise time they occur.

In addition, our **Managed Authentication Service** takes your security a step further. It uses CRYPTOCARD's award-winning authentication technology to positively identify end users before granting access to resources. Put simply: No token, no access.

Key Remote Access facts

- A Managed VPN provides a secure, cost-effective way to share sensitive information across your organisation – and beyond.
- An IPSec VPN gives you a secure, private tunnel between corporate devices or PCs, making it ideal for connecting branch offices to other sites or head offices.
- A SSL VPN uses familiar, browser-based technology that connects both internal and external users to your organisation's data and applications.
- Industry-leading, award-winning security appliances from Juniper Networks ensure your network is always protected.
- Our strong, two-way Managed Authentication Service ensures you can always identify end users before allowing access to any information.

Quick comparison table

	IPSec VPN	SSL VPN
Device	Managed corporate device	Various devices
Software	Managed client software required	No additional client software needed
Installation	Requires client-side software or hardware	Plug and play – no additional client-side software or hardware installation
Authentication	Two-way authentication, digital certificates	Two-way authentication, digital certificates
Encryption	Depends on implementation	Browser based
Security	Edge-to-client	End-to-end
User constituency	Limited to a predefined and controlled user base	Anytime, anywhere access for distributed user base
Ease of use	Non-technical users may require some instruction	Based on familiar web browsers, user friendly, no training required
Supported applications	All IP-based services	All IP-based services
User base	Internal use, site-to-site communications	Employees, remote workers, contractors, suppliers, customers, business partners
Scalability	Harder to scale clients	Easily deployed and highly scalable
Reporting	Limited to connection only information	Very detailed auditing requests including user, application, resource, time and event information



For more information about how our Remote Access can help boost productivity across your business, call 0800 052 0845 or visit www.virginmediabusiness.co.uk



We've worked hard to ensure that the information in this document is correct and fairly stated. We can't, however, accept liability for any error or omission. Our products and services are under continuous development, so the information published here may not be up to date. It's important that you check the current position with your local Virgin Media Business office. This document is not part of a contract or licence unless expressly agreed in writing. Virgin Media Business, Media House, Bartley Wood Business Park, Hook, Hampshire, RG27 9UP.

