

Next-Gen Business VPN Solution

Evolve your security beyond encryption with a more powerful business VPN.

Perimeter 81 provides a unified array of additional security features and networking tools that together offer a better solution to the problems facing modern enterprises.

Why Legacy VPNs Aren't Enough

- Reshaped Networks Need Visibility

Legacy VPNs provide zero additional visibility to IT teams as their users go remote, and local and cloud access occurs increasingly from the network's edge.

- Diversity Required for Access Privileges

Enterprises rely on a diverse variety of resources with varying sensitivity, yet traditional VPN solutions can only grant "one-size-fits-all" access to users.

- Multi-Layered Security is Bare Minimum

Singular VPNs do one thing well, while business VPNs streamline security and deliver a holistic solution with 2FA, SSO, and much more.

Business VPN: Realigning IT with Business Goals

What is a Business VPN?

A business VPN, unlike a retail or personal VPN, brings both strong encryption and easy management features to better suit organizational IT teams, which need to orchestrate traffic security for multiple people at once. Business VPNs evolve beyond standard VPNs by incorporating tools to solve the pains of low scalability, little variety in access policies, and difficult security management which occur with large scale VPN deployments. This saves time and money and also improves security.

How Do I Compare a VPN with a Business VPN?

The simplest way to compare a regular VPN with a VPN for business is by lining up the various security and admin tools available with each. Security commoditization has meant that VPN is rarely a standalone product except in the consumer space, while business VPNs support encryption as one of many complementary networking and security features. For instance, a business VPN can encrypt traffic, but it might also allow the deployment of private gateways, enforce 2FA and SSO, support custom Zero Trust network access, monitoring, and more. For companies that are considering a standard VPN solution and want to see how it might serve their needs versus a business VPN, the basic arena in which two products compete is in how they encrypt traffic. When it comes down to brass tacks, many legacy VPNs support only one or two tunneling protocols, and just the common examples such as IPSec or OpenVPN, while business focused VPNs are able to offer more protocols including newer, better ones like WireGuard.

Why Your Organization Needs a Business VPN

1. **Variety of Protocols:** A greater selection of encryption protocols ensures security that suits individual users' devices and habits, as do the other tools bundled within a business VPN.
2. **Custom Access Management:** Additional tools like identity Providers and network segmentation provide a way for IT to automatically qualify users and assign them relevant security and access profiles.
3. **Streamline Logins:** User password hygiene is a quiet yet looming risk for networks. Business VPNs rely on Single Sign-On to give all users an easy password manager and auto login tool.
4. **Improve Remote Work:** Business VPNs boost remote work productivity, with full network integration and access through local gateways rather than on-site hardware, resulting in lower latency.

Perimeter 81's Business VPN

Our SaaS solution is a holistic business security suite. More sophisticated than standard VPNs, it features: Multi-Regional Deployment With just a few clicks you can deploy private gateways to different locations, offering secure and low-latency network access to your employees around the world. Policy-Based Segmentation Segment your network with granular detail, and assign access to user groups based on Google, Okta, Microsoft Azure AD and Active Directory/LDAP Identity Provider integration. 2FA Made Easier Add an additional layer of security and reinforce user authentication with SMS notifications, Google Authenticator and Duo Security authentication. Flexible, Cost Effective Consume networking and security without expensive hardware or maintenance, make security processes scalable and cut IT overheads. Interconnected Resources Integrate security across your cloud environments, including AWS, Azure, and Google Cloud, and between your networks at various branch offices. Thorough Traffic Monitoring Get a closer look at your network's health, activity and security, including visibility into group and server creation, authentication, password habits and more.

[FAQ] Business VPN Questions and Answers

What are the different types of business VPNs?

There are many different types of business VPNs, but they can generally be categorized into two groups: remote access VPNs and site-to-site VPNs. While a remote access VPN can help individual people remotely connect to a local area network, a site-to-site VPN connects two of these networks together. The latter version helps companies more so than the former, as a business is more easily able to extend its resources across multiple locations and offices. Additionally, there are different types of encryption protocols in use across the same type of VPN - for example, there is SSL and IPSec, but WireGuard is a faster and newer protocol now gaining steam.

How are business VPNs different from consumer VPNs?

A business VPN differs from a consumer VPN largely in the functions it has that serve an organizational purpose rather than a retail one. For example, business VPNs can come with an array of extra tools that are designed to help orchestrate access to multiple resources from multiple users - static IP addresses, traffic monitoring, and network segmentation - but keep in

mind that these benefits only come when the VPN is packaged in unified fashion alongside other networking and security solutions, much like in a Network as a Service. Consumer VPNs, on the other hand, are standalone pieces of software that help individuals mask the origin of their traffic over the web. Why is a VPN for teams important for business? VPNs are crucial for businesses that want their employees to be able to safely connect to resources - local server storage, cloud SaaS applications, and more - but from afar. Remote work is the single biggest use case for a VPN for business, because connections to internal resources that aren't secure are easy to exploit, and put invaluable proprietary data at risk. With a VPN, each employee is required to encrypt his or her traffic before connecting to sensitive resources, meaning that IT can assume anyone who is connected is also protected.

How do I set up a business VPN for remote access?

After finding a VPN provider and signing up, you'll need to enter your VPN credentials into the computer or mobile device you plan on using. Next, you'll need to ensure that the VPN settings are recognized in your network, which means adding the correct details like the server address, remote ID, and authentication login details. This can be done in bulk by IT for managed devices. Next, once the client is installed, the admin can choose which encryption protocol to use with employee devices and configure other options according to the needs of the network.

Can a business VPN help my company become compliant with HIPAA?

Yes. A quality business VPN solution can prove beyond a reasonable doubt that your data is secure and compliant with common regulatory guidelines such as HIPAA and HITRUST, through mandatory encryption and traffic privacy for all who are authorized to access your network. Business VPNs are the most simple solution for compliance's lowest-hanging fruit.

The Industry's Best Business VPN: Perimeter 81

Chosen by multiple security experts and trusted industry voices, including Tech Radar and Tom's Guide, Perimeter 81 is widely recognized as the best VPN for business available right now.

Our business VPN offers:

- Complete network visibility
 - Precise segmentation
 - A user-centric experience
 - Increased network security
 - A highly scalable solution
- Simpler encryption across the cloud Secure all employees' access to local and cloud resources with a single click.

