- **Virtual Private Networks (VPNs) for secure remote access**

Overview of Virtual Private Networks (VPNs) for Secure Remote Access

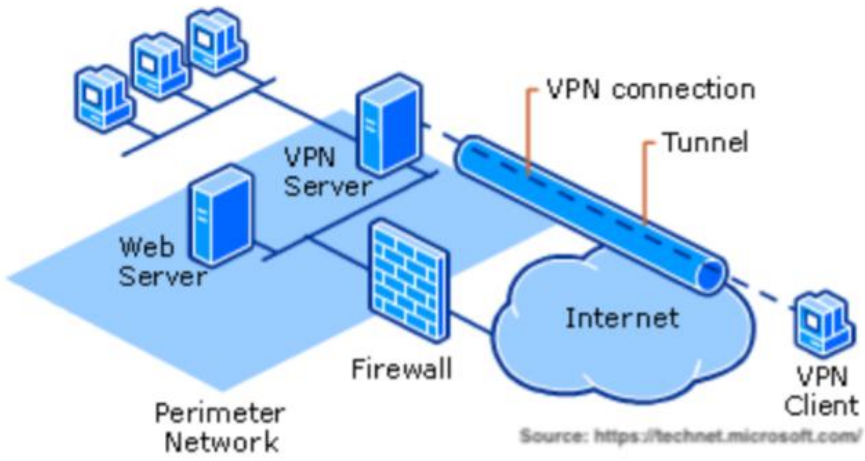
Virtual Private Networks (VPNs) are a foundational technology for enabling secure remote access to corporate networks, especially as remote and hybrid work become standard business practices. They provide encrypted connections, ensuring data confidentiality and integrity even over insecure public networks.

- **What is a Virtual Private Network (VPN)?**

An enterprise can have a private network that connects all their IT infrastructure and employee's computers to form a corporate intranet. This network allows for access to all internal IT services such as payroll, email, etc., at the enterprise's main headquarters. As the enterprise grows, the private network may also need to be extended to additional branch offices.

To establish connectivity between offices for their private network while keeping the network separate from the Internet, dedicated data transport with leased telecommunication circuits are often used. The telecommunication services used to create this connectivity between locations are quite expensive and a more economical alternative was desired.

With advances in cryptography, computing technology, and pervasiveness of the Internet, it became possible to encrypt data traffic and tunnel it over the Internet to a server located in the private network. The secure tunnel creates a virtual link which extends the private network over a public network. This kind of network that makes use of public networks to provide private network connectivity is called Virtual Private Network (VPN).



A VPN can make use of one of many technologies such as Internet Protocol Security (IPsec), Transport Layer Security (SSL/TLS), Datagram Transport Layer Security (DTLS), to securely connect devices or networks, over public networks, in order to extend or form a private network.

The same technology that is used to create virtual connectivity between networks can also be used to connect a user's devices to a private network. A common use of VPNs is to provide remote employees secure access over the Internet to their company's IT services. Employees use VPN clients installed on corporate laptops or mobile devices to connect to a VPN server that is present in the company's private network.

The remote access use case is not limited to access for employees. Any Internet-connected device can use a VPN to be a part of a private network. Devices can range from normal computing devices like laptops to specialized industrial sensors or consumer electronics like smart TVs.

- **Why is a VPN Needed?**

In this section, we explore the various reasons and benefits of using virtual private networks.

1. **Reduces Risk**

A Clark School study is one of the first to quantify the near-constant rate of hacker attacks on computers with Internet access—every 39 seconds on average—and the non-secure usernames and passwords we use that give attackers more chance of success.

As more devices and services are exposed to the Internet the magnitude of cyber attack risk to the overall network and all the devices connected to the network increases. Extending convenient VPN access to the needed devices means that the need of opening up your private services to the Internet, just for internal consumption, is reduced. A properly implemented VPN allows only trusted devices to access your private network and implements strict access controls to enforce least-privilege access. These measures reduce the number of attack vectors available to a hacker to compromise network security.

2. **Secures & Extends Private Network Services**

The main purpose of a VPN is to provide secure access to a private network while not being directly connected to the physical private network. Thus, a VPN extends all the services available on the private network as if the devices are directly connected to the private network even though the device is just connected to the Internet.

To an employee of a large multinational enterprise, this would mean access to the services of the Corporate IT network over the Internet. Corporate IT may be providing services such as file servers, print servers, intranet websites, ERP systems, backup servers, etc. These services are meant for internal use only, but with use of a VPN, the employee is not restricted to physical locations with direct connectivity to the internal IT private network. If the employee is a home-based remote worker or a traveling salesperson, they can still use these internal IT services while connected to the ubiquitous Internet. They continue to get the same IT service experience as being present in their corporate office.

3. **Leverages Existing Security Investments**

An enterprise needs to give paramount importance to security. No enterprise wants to be in a position to explain the reason for a data breach. To that end, companies invest heavily in people, processes, tools, software and hardware infrastructure for the explicit purpose of strengthening the organization's overall security posture. This includes reducing the attack surface of their internal and private services by employing a variety of safeguards. Use of a private network with public network access protected by firewalls, web proxies, intrusion detection systems form the major bulk of network perimeter security investments.

IT security teams of small and midsize businesses are increasingly using a single appliance or service that provides multiple security features called Unified Threat Management (UTM) service/appliance. This unified service reduces complexity and costs by combining antivirus, anti-spam, content filtering, and web filtering with network security such as firewalls and network intrusion detection and protection. Some UTM implementations also include a VPN server and vice versa.

4. **Increases Employee Productivity**

When employees are out of the office away from direct connectivity to the private network, they still need to use the plethora of services that are only available while connected to the company's network. For any employer that deploys a mobile workforce it is imperative for employees to access their corporate applications from anywhere in the world.

Luckily, high-speed Internet access from cellular data networks and almost omnipresent WiFi hotspots make it nearly impossible to be in a place without access to the Internet. Whether traveling on a train, in an airport, or at a hotel, there is always Internet access to be found. A VPN rides on this Internet access and makes private network access equally ubiquitous. Thus, VPN along with mobile Internet access is a combination that allows employees to access enterprise applications and increase productivity while away from office.

- **How Remote Access VPNs Work**

A remote access VPN establishes an encrypted tunnel between a remote user's device and the corporate network, typically through a VPN client on the user's device and a VPN gateway/server on the company side.

The VPN client authenticates the user, and once authenticated, all data transmitted between the user and the network is encrypted, protecting it from interception or tampering.

This setup allows remote users to access internal company resources-such as file servers, databases, and applications-as if they were physically present in the office.

- **Key Security Features**

Encryption: VPNs use strong encryption protocols (e.g., AES-256) to secure data in transit.

Authentication: Only authorized users can establish VPN connections, often enforced with multi-factor authentication (MFA) for added security.

Access Control: Many VPNs allow administrators to specify which IP addresses or users can access specific resources, supporting zero-trust security models.

Obfuscation: Some VPNs offer obfuscated servers to hide VPN usage in countries where VPNs are restricted.

Dedicated IPs: Certain providers offer dedicated/static IP addresses, which help control and monitor access to sensitive systems

- **Common VPN Protocols for Remote Access**

Protocol	Security Level	Notes
OpenVPN	High	Flexible, open-source, uses SSL/TLS encryption
WireGuard	High	Modern, fast, simple, strong encryption
L2TP/IPsec	High	Robust, combines L2TP with IPsec for encryption
SSTP	High	Uses SSL/TLS, native to Windows
PPTP	Low	Deprecated due to security vulnerabilities

OpenVPN and WireGuard are widely recommended for their strong security and cross-platform compatibility.

Provider	Key Features	Best For
NordVPN	Dedicated IPs, Meshnet virtual LAN, double VPN	Security, flexibility
ExpressVPN	Obfuscation, fast speeds, volume licensing	Teams in restricted regions
Surfshark	Unlimited connections, affordability	Large teams, budget
CyberGhost	Easy to use, always-on protection	Simplicity
Private Internet Access	Budget-friendly, dedicated IPs	Cost-conscious users

NordVPN stands out with advanced features like Meshnet (virtual LAN) and dedicated IPs, making it particularly suitable for businesses needing granular access control and secure file sharing among remote teams.

Modern Alternatives and Enhancements

Zero Trust Network Access (ZTNA): ZTNA solutions build on VPN technology by enforcing strict authentication, network segmentation, and continuous monitoring, often integrating VPN encryption as a component.

Secure Access Service Edge (SASE): SASE frameworks combine VPN, ZTNA, and other security services into a unified, cloud-native solution, offering enhanced scalability and security for larger enterprises.

Remote access VPNs remain a critical tool for enabling secure remote work, providing encrypted tunnels, strong authentication, and access controls to protect sensitive data and resources. Modern solutions like ZTNA and SASE further enhance security by adopting a zero-trust approach and integrating additional security layers. Leading VPN providers such as NordVPN, ExpressVPN, and Surfshark offer robust options tailored to various business needs and sizes.