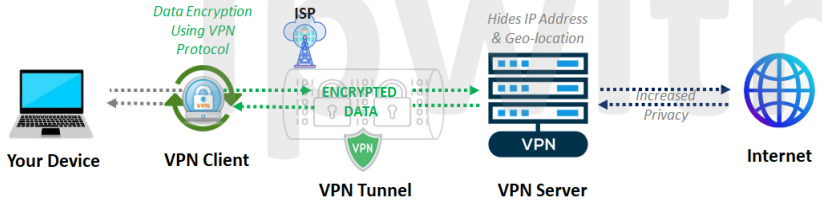
VPN CHEATSHEET – PAGE 1/3

What is a VPN? How does it work?

A VPN or Virtual Private Network is a technology that enables a user to access a private network over the Internet in a secure and private manner. A VPN establishes a secure, encrypted connection known as a VPN tunnel. All online activities and data transmission travel through this protected tunnel.



Is It Legal To Use A VPN?

To learn about the legality of VPN in your country, find the laws of your local government. In general, VPNs seem to be okay to use in most countries, like US, Canada, UK, the rest of Western Europe. VPNs are often not okay in Iraq, UAE, Belarus, Oman, China, Turkey, Russia, Iran, North Korea, and Turkmenistan.

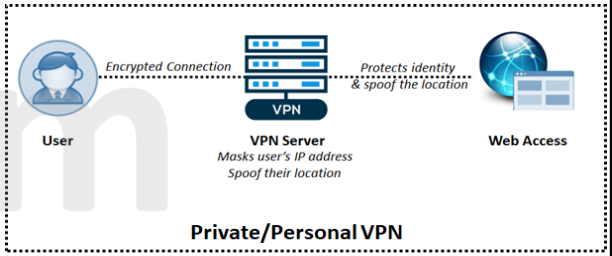
VPN: Which one to choose?

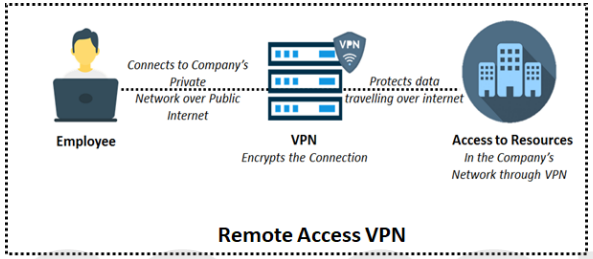
Parameter	Personal VPN	Remote Access VPN	Site-to-Site VPN	Mobile VPN
Type of Connection	User connects the internet via VPN server	User connects to a private network.	Private network connects to another private network	User connects to a private network.
Software Requirement	Web browser VPN, mobile device VPN, router VPN	Software installed on both a private device and the private network	Software on both networks Users do not need apps	App downloaded to mobile device
Use Cases	❑ Protecting personal data ❑ Bypassing geographic restrictions online ❑ Masks IP	Connecting to a private network ❑ from home or ❑ another remote location	Creating a secure tunnel between two private networks	Access the internet securely via ❑ public wifi or ❑ cellular network

Types of VPN

1. Private/Personal VPN

A personal VPN service is VPN that allows users to shield their online activities, ensure confidentiality, and gain access to restricted web content. By hiding your IP address and encrypting the data transmitted, personal VPNs make it impossible for outsiders to intercept communications or gain access to sensitive information.



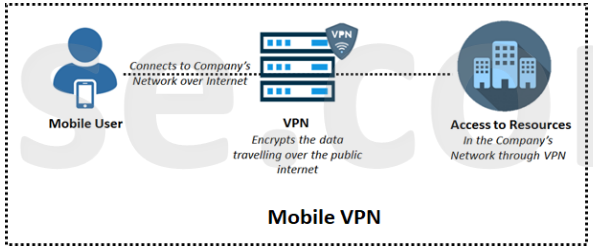


2. Remote Access VPN

It allows users to remotely connect to a private network and access all its services and resources. The Internet serves as the bridge between the user and the private network for a secure and private connection and benefits both home and business users.

3. Site to Site VPN

It can be *Intranet based or Extranet based*. It is intended to establish a secure connection between two sites located in different geographical locations. When networks that belong to the same company are linked together, it is called an intranet-based VPN. When two networks owned by separate companies are linked together, the resulting VPN is referred to as an extranet-based VPN.

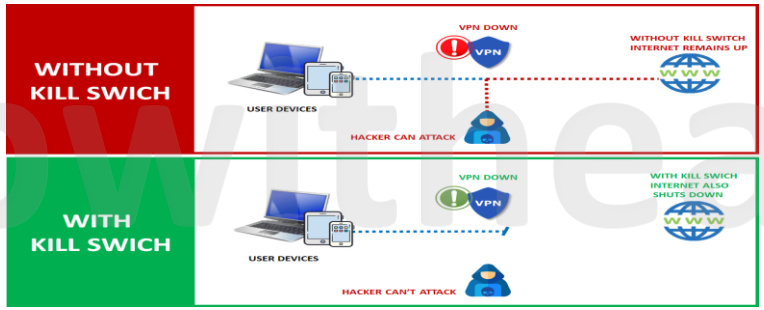


4. Mobile VPN

This enables mobile users to establish a secure connection with a private network using a cellular network. It creates a secure & encrypted tunnel between the mobile device & the VPN server, protecting the data transmitted over the connection.

What is a Kill switch in VPN?

A VPN kill switch ensures you that your real IP address would not be exposed online if there is a drop in VPN connection. It is important for those who use the BitTorrent and are the users of torrent downloaders. This is because no one would prefer to expose there IP address and location to the torrent swarm.



Benefits of VPN

- Data Encryption
- Anonymity
- Online Privacy:
- Bypass Geo-restrictions
- Hide Online Activities
- Protection on Public Wi-Fi (which are often vulnerable to hacking and snooping)
- Bypass Internet Censorship
- Prevent Bandwidth Throttling
- Protection from Cyber Threats
- Secure File Sharing
- Multi-Network Access
- Torrenting Safely

Parameter	VPN	Firewall
Purpose	Secure and encrypt data in transit	Control network traffic and access
Security Focus	Data encryption and privacy	Traffic filtering, access control
Access Control	Limited, usually by user or device	Extensive, can be highly granular
Deployment	Client and server-based	Network device or software
Traffic Control	Encrypts data for privacy	Filters traffic based on rules
Protocols	OpenVPN, IPsec, L2TP, PPTP, etc.	Stateful, Stateless, NGFW, etc.
Protection Scope	Data in transit	Network security
Use Cases	▪ Remote access ▪ Bypass geo-restrictions Privacy and anonymity	▪ Protecting networks from threats ▪ Intrusion detection/prevention ▪ Access control and filtering

VPN Protocols

Some commonly used protocols in VPNs are:

PPTP (Point to Point tunnelling protocol)
It is the most widely used VPN protocol, but it has the weakest security encryption as compared to its other counterparts. However, it is easy to set up and used for decades and used by many cheap VPN providers to minimize the cost of running their virtual network businesses. It gives faster access and access to various blocked sites and can be used on all platforms.

Open VPN
It is an open-source VPN technology which makes it possible to establish a highly secure private connection for devices. It has 256-bit encryption and high configuration on many platforms. Very stable in protecting against threats. OpenVPN is for mobile devices.

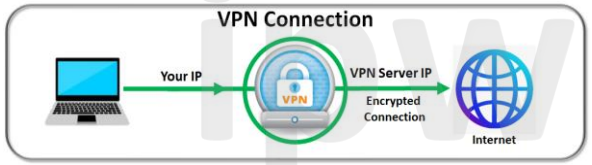
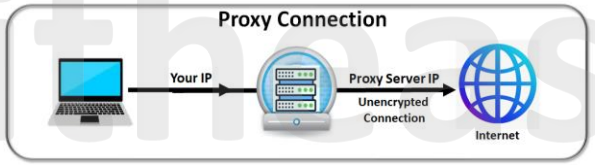
L2TP (Layer 2 tunnelling protocol)
This is similar to PPTP but it is more secure than PPTP and less secure than OpenVPN. It is also slower then OpenVPN however it is considered easy to setup and compatible to all modern devices and operating systems.

IPSec (Internet protocol security)
This is quite similar to L2TP; it has similar security and vulnerabilities to L2TP. This is usually used to encrypt the IP network which you use so all data packets are encrypted during transmission. When combined with other security protocols it can provide security enhancements for those protocols.

SSL VPN
This secure socket layer VPN is a security used for encrypting network communications. SSL VPNs prevent unauthorized 3rd parties from spying and eavesdropping on communications and also provide protection against Man in the Middle attacks which are not new and quite common.

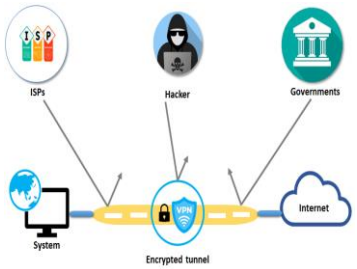
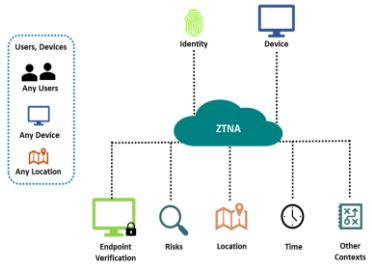
WireGuard
Considered highly secure and efficient, with a minimal attack surface. It's gaining popularity for its simplicity and speed. Known for its excellent performance and low overhead, making it suitable for both mobile and desktop use. While relatively new, WireGuard is being adopted as a modern VPN protocol due to its advantages.

VPN vs Proxy

Parameter	VPN	Proxy
		
Philosophy	A virtual private network (VPN) is a computer network that uses public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their organization's network.	a proxy server is a server or an application that acts as an intermediary for requests from clients seeking resources from other servers
Level of Security	High level of security with encryption up to 256 bits for both SSL and non-SSL connections	Low level of security compared to VPN for both SSL and non-SSL connections
Data Privacy	VPN makes sure that user data is totally encrypted and therefore threats to data privacy, in fact ISP can monitor VPN user activities.	Private data is vulnerable and can be intercepted.
Speed & Performance impact	VPN does not compromise the internet speed of user	Proxy server may reduce the speed and user experience like when proxy server is overloaded with requests , the response time slows down etc.
Cost	High on cost	Low on cost especially when high number of clients/users.
Setup	Complex setup and require skilled resource to setup.	Easy to deploy
Browser compatibility	Compatible with all Operating system and devices	Limited to certain browsers only
Deployment type	VPN connections are configured on system-by-system basis	proxy server connections are configured on an application-by-application basis
Principle of working	A VPN just encapsulates the traffic before sending to target	A proxy server modifies your traffic before it gets to the target.

VPN vs ZTNA

While VPNs provided remote users a secure way of connecting over public networks for many years, recently a new concept of Zero trust networks emerged in the age of cloud computing and questions started arising which is better a VPN an age oldest trusted way to connect to networks or newly found Zero trust network access.

Parameter	VPN	ZTNA
		
Management	No central network policies	Centralized management of network policies
Concept	Once user authenticated at VPN entry point, they can access entire network	Zero trust, least privilege access to remote users
Access Management	no granular access rules	context based access rules and segmentation
Security measures	Lacks device posture security	several security measures at device and network levels
Identity management	Does not integrate with identity providers	Supports multifactor authentication and seamless identification
Audit and reporting	Limited network traffic visibility, no network activity reports	audit and reporting supported
Product flavours	Cisco, NordVPN, Express.VPN etc	Akamai, Broadcom, Cisco, Google, Palo Alto networks, Verizon etc.