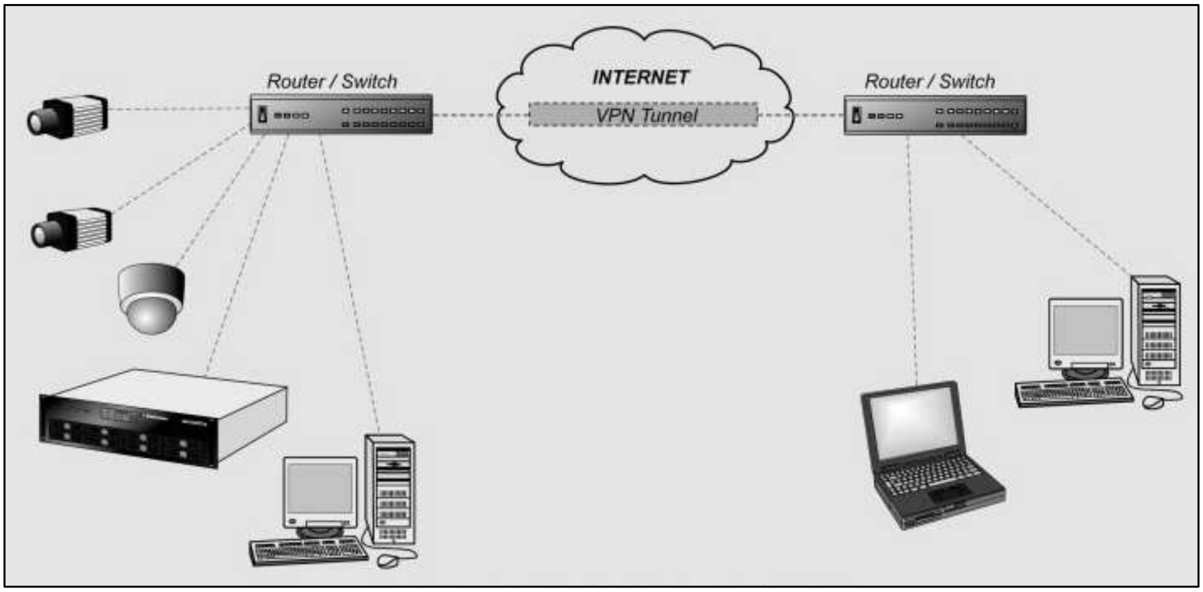
Virtual Private Network (VPN)

VPN stands for the Virtual Private Network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network. A Virtual Private Network is a way to extend a private network using a public network.



A VPN tunnel is an encrypted connection between a device and a VPN server. It's uncrackable without a cryptographic key, so neither hackers nor Internet Service Provider (ISP) could gain access to the data. This protects users from attacks and hides what they're doing online.

Effectively, VPN tunnels are a private route to the internet via intermediary servers. That's why VPNs are popular among privacy-cautious individuals.

In a sense, a VPN acts as a middleman between a device and remote servers, and carries data over existing networks without exposing it to the public Internet.

Let's look at an example of how visiting Amazon would work without a VPN. The user enters the Amazon homepage, it loads, and he/she can do shopping. Here's how it works in more technical terms:

- The user's browser contacts a Domain Name Server (DNS) assigned by his/her ISP, asking it to translate the website domain into an IP address.
- Knowing the Amazon server's IP address, the user's device can now send a request and retrieve the website.
- The user's ISP routes his/her request to the Amazon server and returns a response.

This is very simplified, but that’s essentially how any connection works if VPN is not being used. In this example, the Amazon website is secure and uses HTTPS, so the connection is encrypted. If the user visits an insecure website that doesn’t use HTTPS, his/her data won’t be encrypted. But despite the encryption, this type of session still isn’t completely private. By sending a DNS request to the ISP, the user is telling his/her ISP that he/she wants to visit Amazon.com. Amazon also knows the user’s IP address and can therefore determine the user’s location as well as, potentially, his/her identity.

Now let’s look at an example of how visiting Amazon would work if the user was using a VPN:

- Firstly, the user would connect to a VPN server in a country of choosing, let's say the UK.
- The VPN app uses a tunneling protocol to create an encrypted connection to the VPN server.
- The user heads over to Amazon’s homepage. Yet this time, the DNS query is resolved by the VPN, denying the ISP knowledge of what he/she is doing.
- The VPN establishes a connection between their server and the Amazon.com server.
- Traffic goes from the user to the VPN server, then to Amazon’s server, and back.

Technically, VPN can slow down Internet connection, as there’s an extra step in the process – Internet traffic going through a VPN server. On the bright side, the impact won’t be noticeable.

VPNs can have vulnerabilities. There are no perfect cybersecurity products, and using a VPN comes with some risks as well. Here are some potential VPN vulnerabilities that one should be aware of:

- Some VPN services still use outdated protocols with known vulnerabilities.
- Hackers can impersonate VPN servers and intercept data if the VPN itself is insecure.
- A user’s real IP address can get leaked if a VPN server goes down while he/she is connected and privacy can be compromised. Premium VPNs offer kill switch features to disable the Internet connection when the VPN drops.
- The user’s data is probably being sold if a VPN service is free. The maintenance of server fleets costs money. Hence, when the service is free, the money has to come from somewhere. In many cases, the VPN is collecting the data and selling it off to third parties.
- Some VPNs log user data, even though the logging may not be extensive. There have been instances of several VPN providers handing over user data to governments when asked. That’s why it’s important to make sure that the chosen provider is a no-logs VPN.
- VPN doesn’t protect from malware. For enhanced protection from viruses, malware, trojans, or bots, one should use antivirus software.