Virtual Private Networks Explained

The first virtual private network (VPN) was developed in the early 1990s by Digital Equipment Corporation's (DEC) Field Service organization for the purpose of securely accessing customer's computer environments to provide remote service. The DEC management opted for the no-cost “licensed, bonded and insured” approach, rather than a technical security mechanism. Several years later, DEC's West coast research group needed to demonstrate their value to the company by producing a product. This was the first marketable VPN product. Since then, the technology has improved, processors have become faster and many VPN products are on the market.

There are now standards for VPNs:

High Assurance Internet Protocol Encryptor (HAIPE) specified by National Security Agency

Internet Engineering Task Force (IETF) standards

OpenVPN (www.openvpn.net)

A virtual private network (VPN) is often referred to as a Tunnel. There is no difference.

Threats

Public Charging Stations

Access to a customer's computing platform at public charging stations, such as in airports. For charging at an untrusted location or to keep platforms from communicating with each other on multi-port chargers, the simple and inexpensive solution is a “USB Data Blocker,” a.k.a., “USB Condom.” As the name implies, these allow power to pass to the device being charged, but blocks any data connection.

USB Data Blockers

Unsecured Networks

Connecting to an unsecured network may allow hackers to access you device over the network's data connection and/or monitor your network traffic. The best solution here is a Virtual Private Network, which will encrypt all data to and from your device and prevent any other network connections to the device.

What data can be seen on an unsecured network? Many claim that your usernames and passwords are exposed to anybody monitoring the network. This is generally not true, because almost all web sites now use the Transport Layer Security (TLS) protocol to provide end-to-end encryption between your device and the web site you are accessing.

> Never provide you username or password without verifying that the connection is secure. There will be a padlock and the web address will begin with the letters 'HTTPS" The "S" stands for secure.

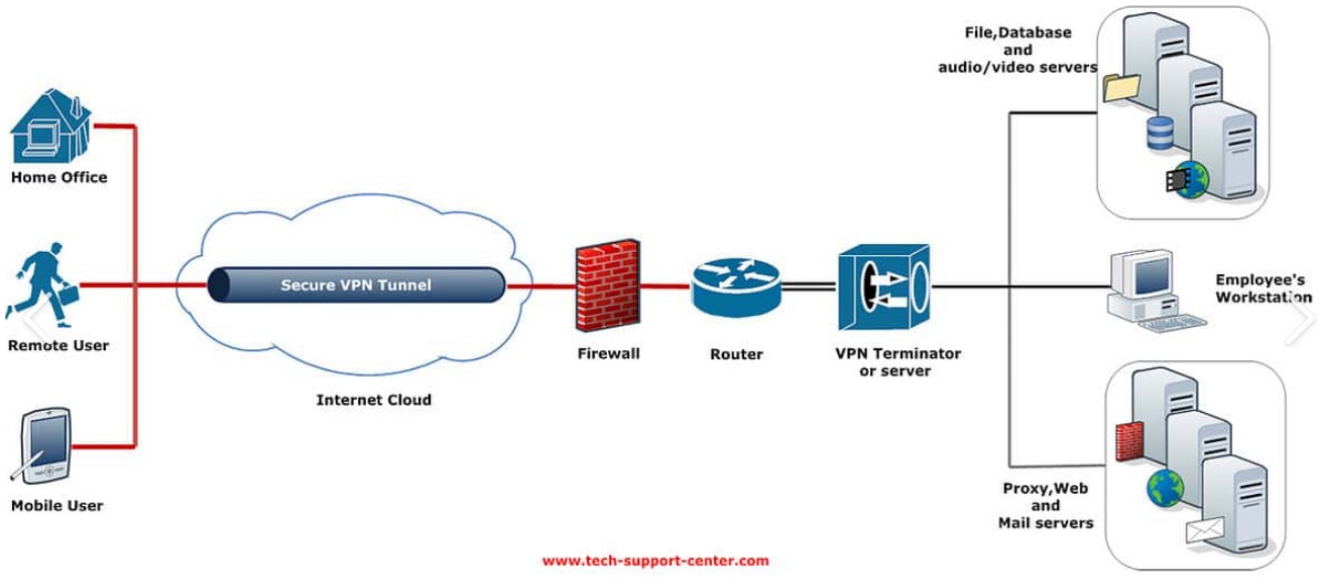
If your TLS-secured connection is being monitored, all that can be seen is what web address you are going to and nothing more. With a VPN, not even that web address is visible.

Typical Users and Uses

Corporate Telecommuting

Corporations frequently use private VPNs for their telecommuting employees for the following reasons.

> Anyone monitoring the Internet only knows that the employee is connected to the company, not where the employee is connected within the company or what they are doing. Therefore, the VPN is the single, secure gateway into the corporate network.
>
> All other network connections to the employee's computer are disabled, making it impossible for a hacker to gain access to the employee's computer and then to computers within corporate environment.

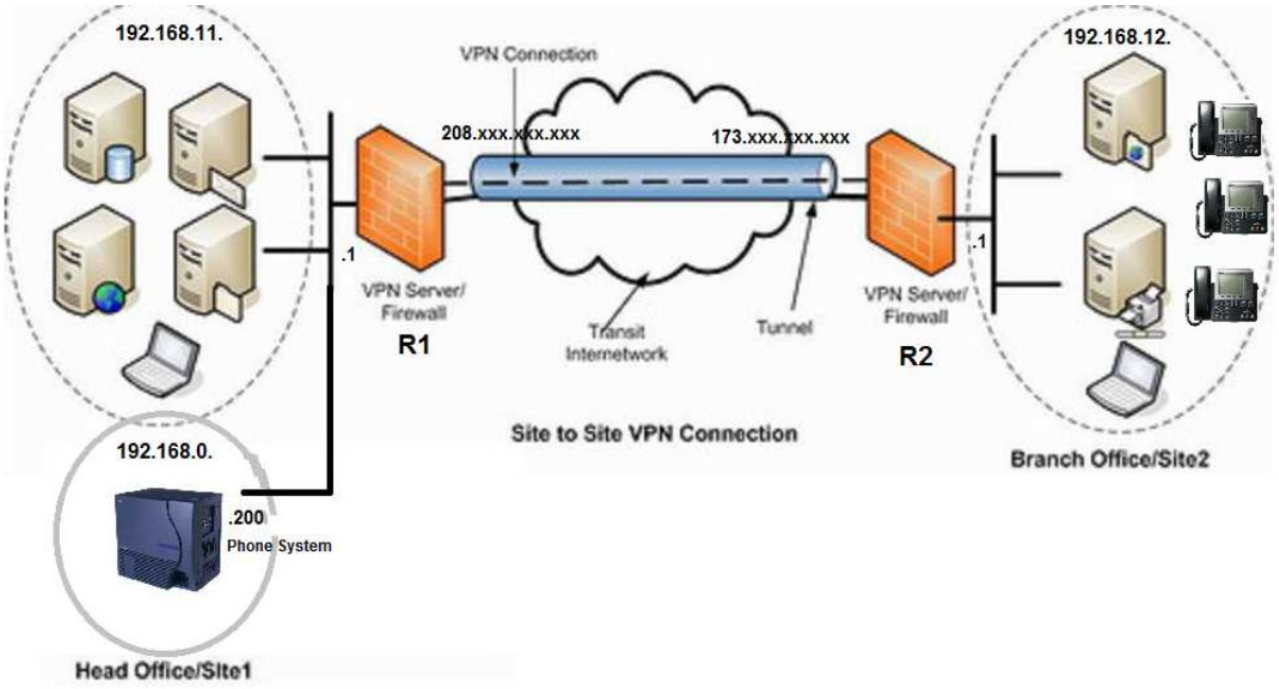


Typical Corporate VPN

Site-to-Site VPN

Corporations also use VPNs for secure site-to-site connections over the public Internet. Here, an observer can only see that one site is communicating with another site, but nothing more. They also can

not access either site.



Site-to-Site VPN

Personal Use

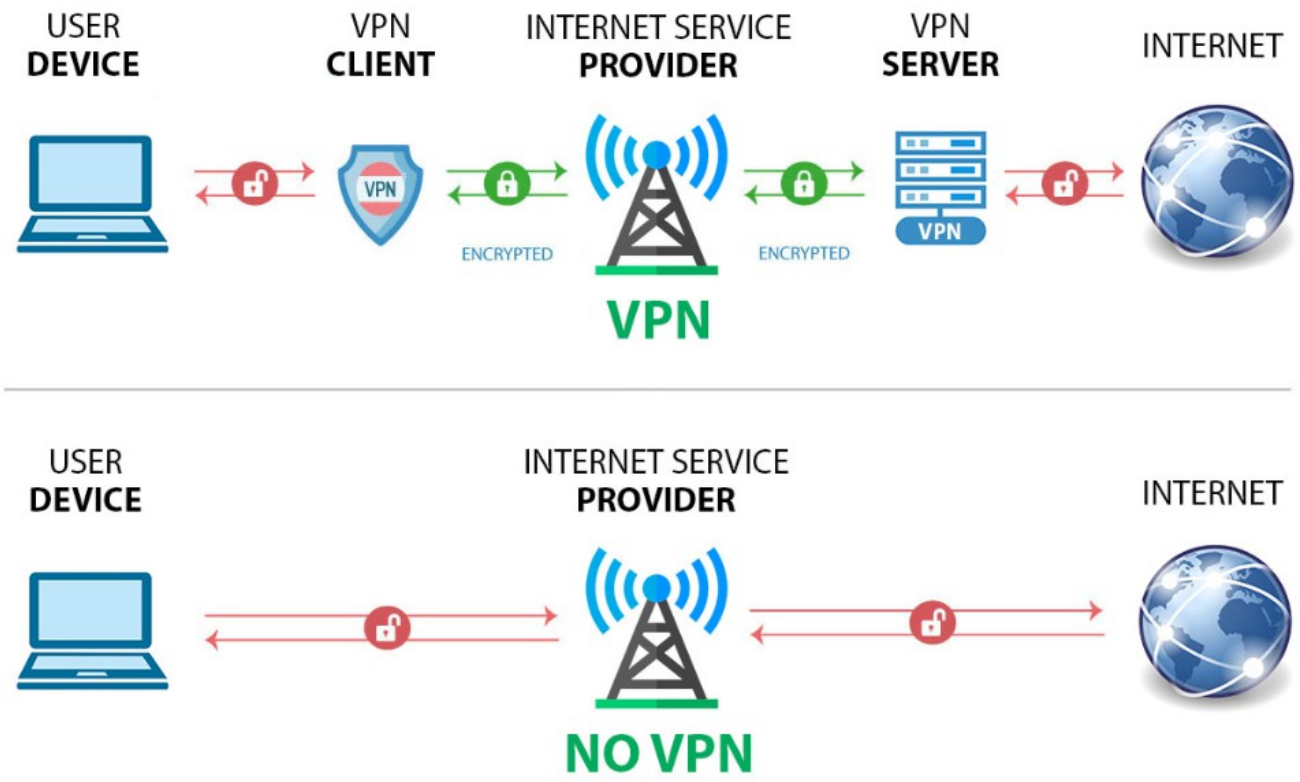
Personal use of VPN services is quite different for the following reasons. Here, the user relies on the fact that many users are connected to the VPN and the VPN is connected to many web site on behalf of those users. Therefore, it is not possible for a monitoring entity to correlate which users are connected to which web sites.

Your browsing history is kept private, from governments and your Internet Service Provider (ISP).

You will not receive targeted advertising, based on your browsing history, because advertisers don't know who you are..

You may be able to access geo-restricted services, such as movies, that are not available in your physical location. This is done by using a VPN server where such services can be accessed. For example, a bank may not allow on-line access from outside the country, but can be accessed through on in-country VPN server.

Get better hotel prices by going through a foreign VPN server and appearing to be in another country.



Typical Personal VPN versus No VPN

In the above diagrams, the red open padlocks represent network traffic in which the source and destination addresses are transmitted in the clear and, therefore, can be seen by anyone monitoring the network. The actual data being transmitted is very likely encrypted by the TLS protocol in the user device. The green closed padlocks represent traffic in which the source and destination addresses are also encrypted and not visible to anyone monitoring the network.

The VPN client may reside within the user device and operate within the protocol stack of the device's communication services or it may reside within the router on the user's premises and provide VPN services to all of the user's devices.

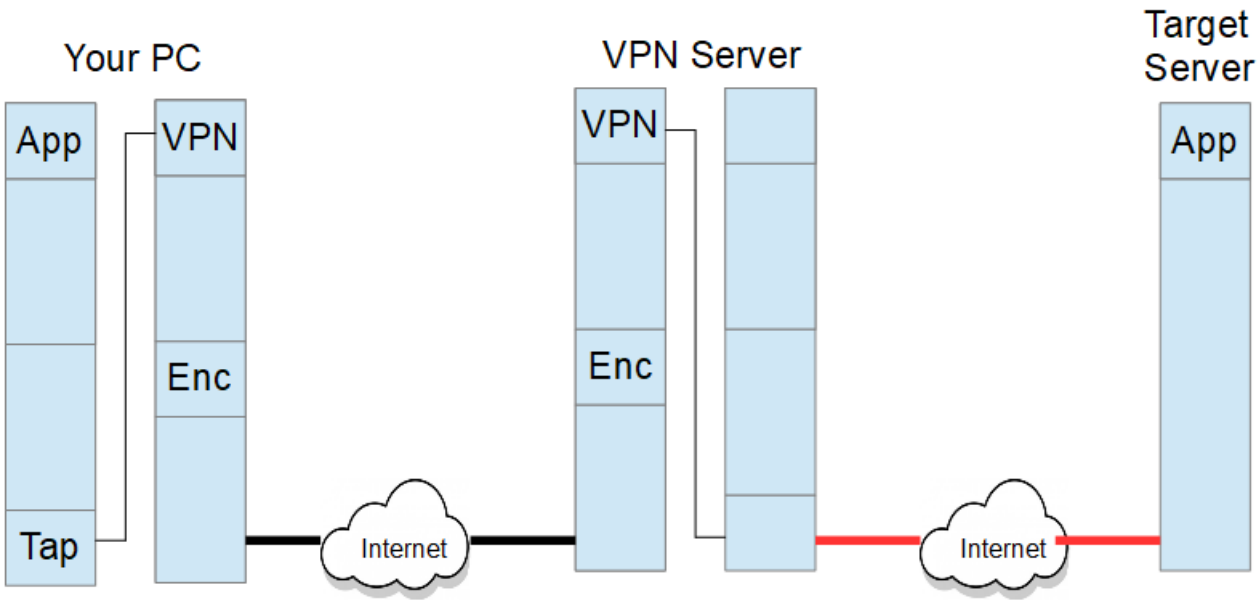
How VPNs Work

At their heart, both the TLS protocol and VPNs provide cryptographic services to both authenticate the communicates to each other and to provide confidentiality. You might think of the nested Russian Doll model. In lectures, I use envelopes of different sizes, putting a message into the smallest envelope and then putting that envelope into a larger envelope and so on. This process is generally called **encapsulation.**

At the source end, as data flows downward through the protocol stack, each layer encapsulates the data from the layer above. At the destination, as data flows upward through the protocol stack, each layer removes the encapsulates from the layer below. Therefore, each layer has a peer-to-peer relationship.

The VPN client at the source end captures the data near the bottom of the stack and passes it up to a new application layer, where it is encapsulated and passed back down. The process is reversed to the

VPN server. The VPN's encryption is shown in the diagram below, but any other encryption is omitted for simplicity.



Protocol Stack and VPN Encapsulation

Inner doll/envelope: The TLS protocol encrypts the data end-to-end, between the client and the remote web server. While the data is secure, the source and destinations addresses are in the clear. (This is omitted from the diagram above for simplicity)

VPN doll/envelope: At the source end, the VPN encapsulates the entire message, including the source and destinations addresses, encrypts the result and adds a new set of source and destinations addresses. One of these addresses is now the VPN server, rather than the web site being visited. At the destination end of he VPN tunnel, the original message is removed from the encapsulation. Note that the VPN may also use the TLS protocol between the VPN client and VPN server.

WiFi doll/envelope: Finally, a secure WiFi connection provides another layer of encryption between the user device and the WiFi router. This is not strong encryption and mainly provides protection from casual snooping and theft of Internet services. (This is also omitted from the diagram above for simplicity)

Choosing a Good VPN Provider

Consider the following criteria when choosing a VPN provider.

Performance: bandwidth or latency
Large service with many world-wide locations of VPN servers
Platforms supported: Windows, Android, Apple, etc.
Protocols supported
Ease of use

Customer support
Price: affordable, but not free (Free means they spy or sell your data.)
Robustness & reputation
A “no logs” policy
Cryptography explained
Update frequency & hack recovery

Cautions

Beware of a lot of hype by VPN service providers.

Some VPN providers may provide your browsing history to government or third parties, the latter being for targeted marking purposes. Be sure to read the VPN providers policy before signing up. Regardless of the policy, governments can obtain court orders and use threats to force VPN providers to hand over your browsing history.

In mid-2025, it has been reported that Chinese firms are buying VPN providers, with the possibility that customers' browsing history might be provided to the Chinese government, without disclosure in the VPN provider's policy.

The cryptography that a VPN uses is seldom fully disclosed, although there will be some marketing fluff to make it sound secure. There are usually several algorithms used for varying purposes that, when used in concert, provide good cryptographic security.

Frequently, politicians make noise about outlawing cryptography for national; security or law enforcement reasons. Between WW-II and the 1990s, cryptography was limited and export controlled to keep it out of the hands of terrorists and drug trafficers. More recently there was noise about outlawing cryptography, because child pornographers might use it. In reality, we all use it, every day. Technology is amoral, neither good nor bad, but the good uses far outweigh the bad uses. Cryptography keeps us safe on-line, enables e-commerce, and protects intellectual property. Besides, even if banned, the bad actors can also get the technology from another country and have some kid (or retired cryptographer) implement it. The art is very mature and published by such entities as the U.S. National Institute of Standards and Technology (NIST) and Internet Engineering Task Force (IETF)