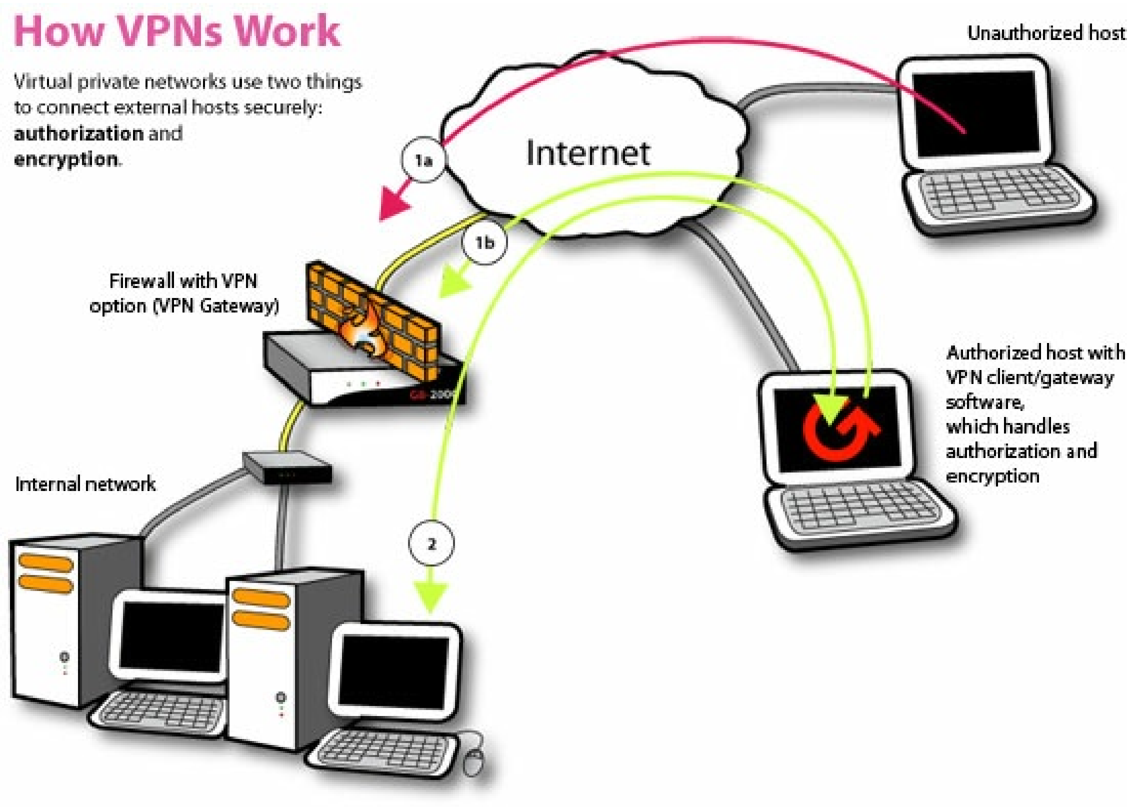
Different Types of VPN Protocols

techpp.com/2010/07/16/different-types-of-vpn-protocols/

What is a VPN?

A VPN (or *Virtual Private Network*) is a way of creating a secure connection 'to' and 'from' a network or a computer. The VPN uses strong encryption and restricted, private data access which keeps the data secure from the other users of the underlying network which could often be a public network like the Internet. VPNs have been used for years, but they have become more robust only in recent years. They are more affordable and also much faster.


How VPNs Work
Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**.
Unauthorized host
Internet
1a
1b
Firewall with VPN option (VPN Gateway)
Authorized host with VPN client/gateway software, which handles authorization and encryption
Internal network
2

Types of VPN

There are many different types of VPNs available. Let's take a look at most common types.

1. PPTP VPN

This is the most common and widely used VPN protocol. They enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication. They don't need extra hardware and the features are often available as inexpensive add-on software. PPTP stands for *Point-to-Point Tunneling Protocol*. The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) to implement security measures.

2. Site-to-Site VPN

Site-to-site is much the same thing as PPTP except there is no "dedicated" line in use. It allows different sites of the same organization, each with its own real network, to connect together to form a VPN. Unlike PPTP, the routing, encryption and decryption is done by the routers on both ends, which could be hardware-based or software-based.

3. L2TP VPN

L2TP or Layer to Tunneling Protocol is similar to PPTP, since it also doesn’t provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the latter provides not only data confidentiality but also data integrity. L2TP was developed by Microsoft and Cisco.

4. IPsec

Tried and trusted protocol which sets up a tunnel from the remote site into your central site. As the name suggests, it’s designed for IP traffic. IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

5. SSL

SSL or Secure Socket Layer is a VPN accessible via https over web browser. SSL creates a secure session from your PC browser to the application server you’re accessing. The major advantage of SSL is that it doesn’t need any software installed because it uses the web browser as the client application.

6. MPLS VPN

MPLS (Multi-Protocol Label Switching) are no good for remote access for individual users, but for site-to-site connectivity, they’re the most flexible and scalable option. These systems are essentially ISP-tuned VPNs, where two or more sites are connected to form a VPN using the same ISP. An MPLS network isn’t as easy to set up or add to as the others, and hence bound to be more expensive.

7. Hybrid VPN

A few companies have managed to combine features of SSL and IPSec & also other types of VPN types. Hybrid VPN servers are able to accept connections from multiple types of VPN clients. They offer higher flexibility at both clienbt and server levels and bound to be expensive.

Conclusion

Deciding which VPN is the best is not easy. It depends on lot of factors like the number of users, bandwidth, security and cost. Remember – cheaper is not always better. For individual users, PP2P VPNs offer the best deal, but for large offices or ones with complex requirements for connectivity MPLS VPNs might be the best option.

It is better to explore the various options available and see which one suits your needs the best.