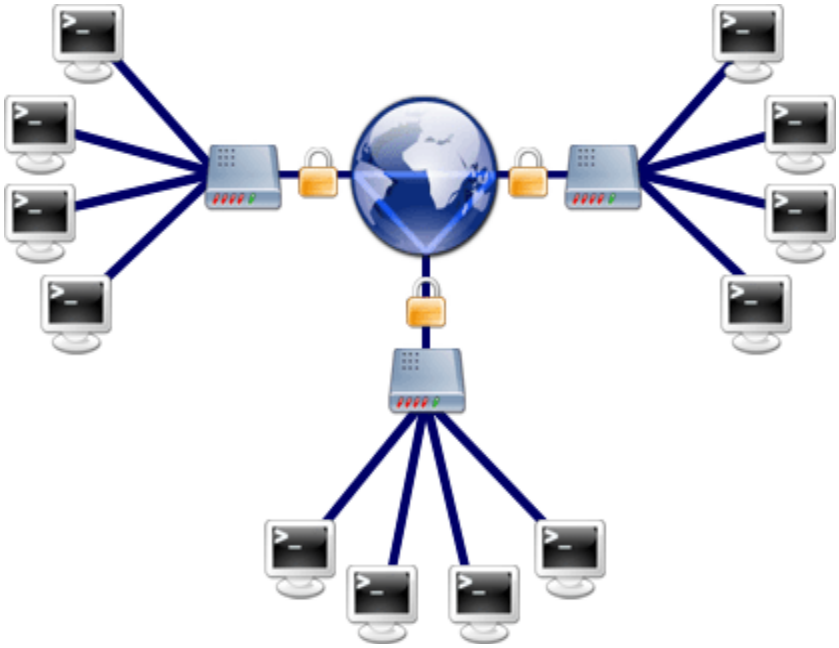
VIRTUAL PRIVATE NETWORK(VPN)



Virtual Private Networking, or VPN, is a technology that lets people access their office's computer network over the Internet while at home or traveling. Accessing a network in this way is referred to as remote access. (For comparison, another common form of remote access is dialing in to the office network over a telephone line.)

But VPN is useful for more than just remote access. It can also be used to link two separate offices over a distance. This is sometimes called a "persistent VPN tunnel", or "site-to-site VPN".

VPN for Remote Access

So why would you want to use VPN for remote access? Let's say you want users to be able to work from home. Or maybe someone needs to retrieve a file while traveling. Without VPN, in order to make resources on the office network available to users, the network administrator would have to weaken the security of your network by opening holes in your firewall — which isn't usually a good idea. Or the remote user would have to dial in over a phone line, sometimes incurring long-distance charges.

With VPN, the integrity of your office network remains intact, but you can allow remote users to act as part of the office network. After connecting over VPN, remote users can

access files, print to printers, and generally do anything with their computers that they would be able to do in the office.

Still, using VPN is not the same as being in the office. Most office networks are pretty fast. Most Internet connections are not. Even the fastest DSL and cable connections are around one-tenth the speed of your average office LAN. This means that accessing resources on the LAN will be much slower over VPN. It would also depend on the "upstream" or upload speed of your office's network connection. As opposed to working on files directly over the VPN connection, it is often more time-efficient to to copy them to your computer over the VPN connection. When you are done working with them you would copy them back to the file server.

How It Works

In a small office network, VPN is most frequently implemented through a router. Just about every small office that shares an Internet connection with more than one computer already has a router of some kind, but most of them don't include VPN. For example, small office/home office (SOHO) routers by Linksys, Netgear, or D-Link are popular choices, offering DHCP, NAT, and basic security features in a single device, but they don't always include VPN support.

Once the VPN router is in place, individual computers can be set up to connect to it from outside the network. Depending on the router and the computers involved, you might need to install software on the computers that will use VPN. Sometimes computers have the ability to connect built-in. Either way, once the hardware and software has been set up, the remote user can initiate a VPN connection.

How a VPN session is initiated depends on how the computer is connected to the Internet. Usually it works something like this: the user double-clicks on a shortcut and the VPN connection window appears. The user enters a username and password and hits "connect." If the computer has an always-on connection like DSL or cable, the VPN connection is immediately established. If the computer dials in to an ISP in order to access the Internet, that connection is established first and then the VPN connection is established on top of that. Once users are connected to the office network over VPN, they can access files and other resources.

When users are done working, they simply disconnect the VPN connection.

VPN As a Persistent Tunnel

VPN technology can also be used to link two separate networks over the Internet so they operate as a single network. This is useful for organizations that have two physical sites. Rather than set up VPN connections on every person's computer, the connection between the two sites can be handled by routers, one at each location. Once configured, the routers maintain a constant tunnel between them that links the two sites. In this scenario, users don't have to do anything to initiate the VPN session because it is always on.

Security and Encryption

There are mainly two kinds of VPN: Point to Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP). Both can link a remote computer to a network, but only L2TP offers strong security. If you must transmit sensitive information, do not use PPTP. Remember that when you set up VPN, you're offering a way into your office network. To minimize the risk of unauthorized parties poking around your network, choose and enforce a strong password policy.

If you allow home users to connect to the office network via VPN, you have to consider viruses or other security threats that could come from the user's home. One way to address this risk is by giving home users a computer that is owned and maintained by the organization, so is certified as up-to-date and virus-free.

Implementing VPN

Before you implement VPN, evaluate the benefits to your organization and weigh it against the costs of equipment, installation time, and staff training. Maybe you're considering VPN because your executive director wants to be able to access files on the server while traveling. Maybe VPN would be a good solution. Or perhaps it would work just as well for your executive director to call the office and ask the receptionist to e-mail the file. Given the plethora of online collaboration tools and web-based technologies available now, VPN may not be the only method to access documents off site. However, VPN remains to be the industry standard that is established, scaleable, and secure. Before deciding on any of these technologies, determine the many risks and rewards first.

Once you have decided to implement VPN, determine whether you need help or not. If someone on your staff understands TCP/ IP networking well and can set up the new router, you might be set. If not, consider finding a trusted consultant to help set it up.

In order to use VPN, your Internet connection should have a static IP address. Most types of Internet connections — dial-up, DSL, and cable — provide you with a numerical address on the Internet that changes from time to time. This is called a dynamic IP address. In order to provide VPN access to remote users it is preferable to have an address that doesn't change, a static IP. Alternately, you can use a dynamic DNS (DDNS) service that can map a domain name to a dynamic IP. There are free services that can map a fixed domain to an account, which your router can update as it obtains different IP addresses. Consult your router or firewall documentation if DDNS is supported

To obtain a static IP address for your Internet connection, talk to your Internet service provider. It may require an additional monthly fee of a few dollars. If you have a friendly ISP, sometimes you can talk it into just giving you a static IP. Occasionally, an ISP will try to sell you much more expensive DSL service, possibly bundled with equipment, when you ask about a static IP. The company might call it a "business class" of service. If the upgrade is too expensive, test the VPN functionality in a pilot phase if DDNS is supported, only then should you decide to pay for the upgrade if necessary.

Source: http://computrnetworking.wordpress.com/2012/02/20/virtual-private-networkvpn/