The Virtual Private Network - VPN

The Virtual Private Network - VPN - has attracted the attention of many organizations looking to both expand their networking capabilities and reduce their costs.

The VPN can be found in workplaces and homes, where they allow employees to safely log into company networks. Telecommuters and those who travel often find a VPN a more convenient way to stay connected to the corporate intranet. No matter your current involvement with VPNs, this is a good technology to know something about. This VPN tutorial involves many interesting aspects of network protocol design, Internet security, network service outsourcing, and technology standards.

What Exactly Is A VPN?

A VPN supplies network connectivity over a possibly long physical distance. In this respect, a VPN is a form of Wide Area Network (WAN).

The key feature of a VPN, however, is its ability to use public networks like the Internet rather than rely on private leased lines. VPN technologies implement restricted-access networks that utilize the same cabling and routers as a public network, and they do so without sacrificing features or basic security.

A VPN supports at least three different modes of use:

- Remote access client connections
- LAN-to-LAN internetworking
- Controlled access within an intranet

Read more - About VPN Applications

VPN Pros and Cons

Like many commercialized network technologies, a significant amount of sales and marketing hype surrounds VPN. In reality, VPNs provide just a few specific potential advantages over more traditional forms of wide-area networking. These advantages can be significant, but they do not come for free.

The potential problems with the VPN outnumber the advantages and are generally more difficult to understand. The disadvantages do not necessarily outweigh the advantages, however. From security and performance concerns, to coping with a wide range of sometimes incompatible vendor products, the decision of whether or not to use a VPN cannot be made without significant planning and preparation.

Read more - Advantages and Disadvantages of VPNs

Technology Behind VPNs

Several network protocols have become popular as a result of VPN developments:

- PPTP
- L2TP
- IPsec
- SOCKS
These protocols emphasize authentication and encryption in VPNs. Authentication allows VPN clients and servers to correctly establish the identity of people on the network. Encryption allows potentially sensitive data to be hidden from the general public.

Many vendors have developed VPN hardware and/or software products. Unfortunately, immature VPN standards mean that some of these products remain incompatible with each other.

Read more - VPN Technologies

**The Future of VPN**

Virtual private networks have grown in popularity as businesses to save money on remote network access for employees. Many corporations have also adopted VPNs as a security solution for private Wi-Fi wireless networks. Expect a continued gradual expansion in use of VPN technology to continue in the coming years.

**What Does A VPN Do?**

A VPN supplies network connectivity over a possibly long physical distance. In this respect, a VPN is a form of Wide Area Network (WAN). VPNs enable file sharing, video conferencing and similar network services. Virtual private networks generally don't provide any new functionality that isn't already offered through alternative mechanisms, but a VPN implements those services more efficiently / cheaply in most cases.

A key feature of a VPN is its ability to work over both private networks as well as public networks like the Internet. Using a method called tunneling, a VPN use the same hardware infrastructure as existing Internet or intranet links. VPN technologies includes various security mechanisms to protect the virtual, private connections.

Specifically, a VPN supports at least three different modes of use:

- Internet remote access client connections
- LAN-to-LAN internetworking
- Controlled access within an intranet

**Internet VPNs for Remote Access**

In recent years, many organizations have increased the mobility of their workers by allowing more employees to telecommute. Employees also continue to travel and face a growing need to stay connected to their company networks.

A VPN can be set up to support remote, protected access to the corporate home offices over the Internet. An Internet VPN solution uses a client/server design works as follows:

1. A remote host (client) wanting to log into the company network first connects to any public Internet Service Provider (ISP).

2. Next, the host initiates a VPN connection to the company VPN server. This connection is made via a VPN client installed on the remote host.

3. Once the connection has been established, the remote client can communicate with the internal company systems over the Internet just as if it were a local host.
Before VPNs, remote workers accessed company networks over private leased lines or through dialup remote access servers. While VPN clients and servers careful require installation of hardware and software, an Internet VPN is a superior solution in many situations.

**VPNs for Internetworking**

Besides using virtual private networks for remote access, a VPN can also bridge two networks together. In this mode of operation, an entire remote network (rather than just a single remote client) can join to a different company network to form an extended intranet. This solution uses a VPN server to VPN server connection.

**Intranet / Local Network VPNs**

Internal networks may also utilize VPN technology to implement controlled access to individual subnets within a private network. In this mode of operation, VPN clients connect to a VPN server that acts as the network gateway.

This type of VPN use does not involve an Internet Service Provider (ISP) or public network cabling. However, it allows the security benefits of VPN to be deployed inside an organization. This approach has become especially popular as a way for businesses to protect their WiFi local networks.

**What Are the Advantages and Benefits of a VPN**

A Virtual Private Network is one solution to establishing long-distance and/or secured network connections. VPNs are normally implemented (deployed) by businesses or organizations rather than by individuals, but virtual networks can be reached from inside a home network. Compared to other technologies, VPNs offers several advantages, particularly benefits for wireless local area networking.

**Answer:** For an organization looking to provide a secured network infrastructure for its client base, a VPN offers two main advantages over alternative technologies: cost savings, and network scalability. To the clients accessing these networks, VPNs also bring some benefits of ease of use.

**Cost Savings with a VPN**

A VPN can save an organization money in several situations:

- eliminating the need for expensive long-distance leased lines
- reducing long-distance telephone charges
- offloading support costs

**VPNs vs leased lines** - Organizations historically needed to rent network capacity such as T1 lines to achieve full, secured connectivity between their office locations. With a VPN, you use public network infrastructure including the Internet to make these connections and tap into that virtual network through much cheaper local leased lines or even just broadband connections to a nearby Internet Service Provider (ISP).

**Long distance phone charges** - A VPN also can replace remote access servers and long-distance dialup network connections commonly used in the past by business travelers needing to access to their company intranet. For example, with an Internet VPN, clients need only connect to the nearest service provider's access point that is usually local.
Support costs - With VPNs, the cost of maintaining servers tends to be less than other approaches because organizations can outsource the needed support from professional third-party service providers. These providers enjoy a much lower cost structure through economy of scale by servicing many business clients.

VPN Network Scalability

The cost to an organization of building a dedicated private network may be reasonable at first but increases exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations, but 4 branch offices require 6 lines to directly connect them to each other, 6 branch offices need 15 lines, and so on.

Internet based VPNs avoid this scalability problem by simply tapping into the the public lines and network capability readily available. Particularly for remote and international locations, an Internet VPN offers superior reach and quality of service.

Using a VPN

To use a VPN, each client must possess the appropriate networking software or hardware support on their local network and computers. When set up properly, VPN solutions are easy to use and sometimes can be made to work automatically as part of network sign on.

VPN technology also works well with WiFi local area networking. Some organizations use VPNs to secure wireless connections to their local access points when working inside the office. These solutions provide strong protection without affecting performance excessively.

Limitations of a VPN

Despite their popularity, VPNs are not perfect and limitations exist as is true for any technology. Organizations should consider issues like the below when deploying and using virtual private networks in their operations:

1. VPNs require detailed understanding of network security issues and careful installation / configuration to ensure sufficient protection on a public network like the Internet.

2. The reliability and performance of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.

3. Historically, VPN products and solutions from different vendors have not always been compatible due to issues with VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give as great a cost savings.

VPN Tunneling

Virtual private network technology is based on the idea of tunneling. **VPN tunneling** involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.
For Internet-based VPNs, packets in one of several VPN protocols are encapsulated within Internet Protocol (IP) packets. VPN protocols also support authentication and encryption to keep the tunnels secure.

**Types of VPN Tunneling**

VPN supports two types of tunneling - voluntary and compulsory. Both types of tunneling are commonly used.

In voluntary tunneling, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection.

In compulsory tunneling, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.

Compulsory VPN tunneling authenticates clients and associates them with specific VPN servers using logic built into the broker device. This network device is sometimes called the VPN Front End Processor (FEP), Network Access Server (NAS) or Point of Presence Server (POS). Compulsory tunneling hides the details of VPN server connectivity from the VPN clients and effectively transfers management control over the tunnels from clients to the ISP. In return, service providers must take on the additional burden of installing and maintaining FEP devices.

**VPN Tunneling Protocols**

Several computer network protocols have been implemented specifically for use with VPN tunnels. The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

**Point-to-Point Tunneling Protocol (PPTP)**

Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

More - [About PPTP](#)

**Layer Two Tunneling Protocol (L2TP)**

The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create a new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model -- thus the origin of its name.

**Internet Protocol Security (IPsec)**

IPsec is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (Layer Three) of the OSI model.
Introduction to PPTP - Point-to-Point Tunneling Protocol

PPTP - Point-to-Point Tunneling Protocol - extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking. PPTP operates at Layer 2 of the OSI model. (See below)

Using PPTP

PPTP packages data within PPP packets, then encapsulates the PPP packets within IP packets (datagrams) for transmission through an Internet-based VPN tunnel. PPTP supports data encryption and compression of these packets. PPTP also uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination.

PPTP-based Internet remote access VPNs are by far the most common form of PPTP VPN. In this environment, VPN tunnels are created via the following two-step process:

1. The PPTP client connects to their ISP using PPP dial-up networking (traditional modem or ISDN).
2. Via the broker device (described earlier), PPTP creates a TCP control connection between the VPN client and VPN server to establish a tunnel. PPTP uses TCP port 1723 for these connections.

PPTP also supports VPN connectivity via a LAN. ISP connections are not required in this case, so tunnels can be created directly as in Step 2 above.

Once the VPN tunnel is established, PPTP supports two types of information flow:

- **control** messages for managing and eventually tearing down the VPN connection. Control messages pass directly between VPN client and server.
- **data** packets that pass through the tunnel, to or from the VPN client

**PPTP Control Connection**

Once the TCP connection is established in Step 2 above, PPTP utilizes a series of **control messages** to maintain VPN connections. These messages are listed below.

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>StartControlConnectionRequest</td>
<td>Initiates setup of the VPN session; can be sent by either client or server.</td>
</tr>
<tr>
<td>2</td>
<td>StartControlConnectionReply</td>
<td>Sent in reply to the start connection request (1); contains result code indicating success or failure of the setup operation, and also the protocol version number.</td>
</tr>
<tr>
<td>3</td>
<td>StopControlConnectionRequest</td>
<td>Request to close the control connection.</td>
</tr>
<tr>
<td>4</td>
<td>StopControlConnectionReply</td>
<td>Sent in reply to the stop connection request (3); contains result code indicating success or failure of the close operation.</td>
</tr>
<tr>
<td>5</td>
<td>EchoRequest</td>
<td>Sent periodically by either client or server to &quot;ping&quot; the connection (keep alive).</td>
</tr>
<tr>
<td>6</td>
<td>EchoReply</td>
<td>Sent in response to the echo request (5) to keep the connection active.</td>
</tr>
<tr>
<td>7</td>
<td>OutgoingCallRequest</td>
<td>Request to create a VPN tunnel sent by the client.</td>
</tr>
<tr>
<td>8</td>
<td>OutgoingCallReply</td>
<td>Response to the call request (7); contains a unique identifier for that tunnel.</td>
</tr>
<tr>
<td></td>
<td>Control Message</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9</td>
<td>IncomingCallRequest</td>
<td>Request from a VPN client to receive an incoming call from the server.</td>
</tr>
<tr>
<td>10</td>
<td>IncomingCallReply</td>
<td>Response to the incoming call request (9), indicating whether the incoming call should be answered.</td>
</tr>
<tr>
<td>11</td>
<td>IncomingCallConnected</td>
<td>Response to the incoming call reply (10); provides additional call parameters to the VPN server.</td>
</tr>
<tr>
<td>12</td>
<td>CallClearRequest</td>
<td>Request to disconnect either an incoming or outgoing call, sent from the server to a client.</td>
</tr>
<tr>
<td>13</td>
<td>CallDisconnectNotify</td>
<td>Response to the disconnect request (12); sent back to the server.</td>
</tr>
<tr>
<td>14</td>
<td>WANErrorNotify</td>
<td>Notification periodically sent to the server of CRC, framing, hardware and buffer overruns, timeout and byte alignment errors.</td>
</tr>
<tr>
<td>15</td>
<td>SetLinkInfo</td>
<td>Notification of changes in the underlying PPP options.</td>
</tr>
</tbody>
</table>

With control messages, PPTP utilizes a so-called **magic cookie**. The PPTP magic cookie is hardwired to the hexadecimal number 0x1A2B3C4D. The purpose of this cookie is to ensure the receiver interprets the incoming data on the correct byte boundaries.

**PPTP Security**

PPTP supports **authentication**, **encryption**, and **packet filtering**. PPTP authentication uses PPP-based protocols like EAP, CHAP, and PAP. PPTP supports packet filtering on VPN servers. Intermediate routers and other firewalls can also be configured to selectively filter PPTP traffic.

**PPTP and PPP**

In general, PPTP relies on the functionality of PPP for these aspects of virtual private networking.

- authenticating users and maintaining the remote dial-up connection
- encapsulating and encrypting IP, IPX, or NetBEUI packets

PPTP directly handles maintaining the VPN tunnel and transmitting data through the tunnel. PPTP also supports some additional security features for VPN data beyond what PPP provides.

**PPTP Pros and Cons**

PPTP remains a popular choice for VPNs thanks to Microsoft. PPTP clients are freely available in all popular versions of Microsoft Windows. Windows servers also can function as PPTP-based VPN servers.

One drawback of PPTP is its failure to choose a single standard for authentication and encryption. Two products that both fully comply with the PPTP specification may be totally incompatible with each other if they encrypt data differently, for example. Concerns also persist over the questionable level of security PPTP provides compared to alternatives.