Security of Virtual Private Network

D.O.I - 10.51201/Jusst12647
http://doi.org/10.51201/Jusst12647

PARDEEP MEHTA
PG Deptt. of Computer Science, H.M.V. College, Jalandhar(Punjab)

***Abstract*— The world has changed a lot in the last couple of decades. Instead of simply dealing with local or regional concerns, many businesses now have to think about global markets and logistics. Many companies have facilities spread out across the country or around the world, and there is one thing that all of them need a way to maintain fast, secure and reliable communications wherever their offices are.**

Until fairly recently, this has meant the use of leased lines to maintain a wide area network (WAN). A WAN had obvious advantages over a public network like the Internet when it came to reliability, performance and security. But maintaining a WAN, particularly when using leased lines can become quite expensive and often rises in cost as the distance between the offices increases.

As the popularity of the Internet grew, businesses turned to it as a means of extending their own networks. First came Intranets, which are password-protected sites designed for use only by company employees. Now, many companies are creating their own VPN (virtual private network) to accommodate the needs of remote employees and distant offices.

Keywords-VPN, VPN server, VPN client, Tunneling protocols

I. INTRODUCTION

Basically, a VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

It provides remote access to an organization's network via the Internet. VPNs send data over the public Internet through secure "tunnels." Virtual Private Network enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted

The act of configuring and creating a virtual private network is known as virtual private networking.

A well-designed VPN can greatly benefit a company. For example, it can:

- Extend geographic connectivity
- Improve security
- Reduce operational costs versus traditional WAN
- Reduce transit time and transportation costs for remote users
- Improve productivity
- Simplify network topology
- Provide global networking opportunities
- Provide telecommuter support
- Provide broadband networking compatibility
- Provide faster ROI (return on investment) than traditional WAN

II. VPN IS ANYTHINGS BUT VIRTUAL

A).Virtual Private Networking Connections

A Microsoft® Windows® 2000 VPN connection includes the following components as illustrated in Figure 1:

VPN server: A computer that accepts VPN connections from VPN clients. A VPN server can provide a remote access VPN connection or a router-to-router VPN connection

VPN client: A computer that initiates a VPN connection to a VPN server. A VPN client can be an individual computer that obtains a remote access VPN connection or a router that obtains a router-to-router VPN connection. Microsoft® Windows NT® version 4.0, Windows 2000, Microsoft® Windows® 95, and Microsoft® Windows® 98–based computers can create remote access VPN connections to a Windows 2000–based VPN server. Microsoft® Windows® 2000 Server and Microsoft® Windows NT® Server 4.0–based computers running the Routing and Remote Access service (RRAS) can create router-to-router VPN connections to a Windows 2000–based VPN server. VPN clients can also be any non-Microsoft Point-to-Point Tunneling Protocol (PPTP) client or Layer Two Tunneling Protocol (L2TP) client using IPSec.

Tunnel: The portion of the connection in which your data is encapsulated.

VPN connection: The portion of the connection in which your data is encrypted. For secure VPN connections, the data is encrypted and encapsulated along the same portion of the connection.

It is possible to create a tunnel and send the data through the tunnel without encryption. This is not a VPN connection because the private data is sent across a shared or public network in an unencrypted and easily readable form.

Tunneling protocols: Communication standards used to manage tunnels and encapsulate private data. (Data that is tunneled must also be encrypted to be a VPN connection.)

Windows 2000 includes the PPTP and L2TP tunneling protocols.

Tunneled data: Data that is usually sent across a private point-to-point link.

Transit inter-network: The shared or public inter-network crossed by the encapsulated data. For Windows 2000, the transit inter-network is always an IP inter-network. The transit inter-network can be the Internet or a private IP-based intranet.

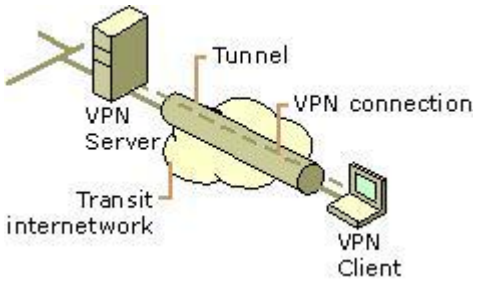

Figure1: Components of a VPN Connection

B). Types of VPN connections

Creating the VPN is very similar to establishing a point-to-point connection using dial-up networking and demand-dial routing procedures. There are two types of VPN connections: the remote access VPN connection and the router-to-router VPN connection.

Remote Access VPN Connection : A remote access VPN connection is made by a remote access client, or a single user computer, that connects to a private network. The VPN server provides access to the resources of the VPN server or to the entire network to which the VPN server is attached. The packets sent across the VPN connection originate at the remote access client.

The remote access client (the VPN client) authenticates itself to the remote access server (the VPN server) and, for mutual authentication, the server authenticates itself to the client.

Router-to-Router VPN Connection: A router-to-router VPN connection is made by a router and connects two portions of a private network. The VPN server provides a routed connection to the network to which the VPN server is attached. On a router-to-router VPN connection, the packets sent from either router across the VPN connection typically do not originate at the routers.

The calling router (the VPN client) authenticates itself to the answering router (the VPN server), and, for mutual authentication, the answering router authenticates itself to the calling router.

Typical VPN connections are either Internet-based or intranet-based.

C). Internet-Based VPN Connections

Using an Internet-based VPN connection, you can avoid long-distance and 1-800 telephone charges while taking advantage of the global availability of the Internet.

Remote Access over the Internet

Rather than a remote access client having to make a long distance or 1-800 call to a corporate or outsourced network access server (NAS), the client can call a local ISP. By using the established physical connection to the local ISP, the remote access client initiates a VPN connection across the Internet to the organization's VPN server. When the VPN connection is created, the remote access client can access the resources of the private intranet.

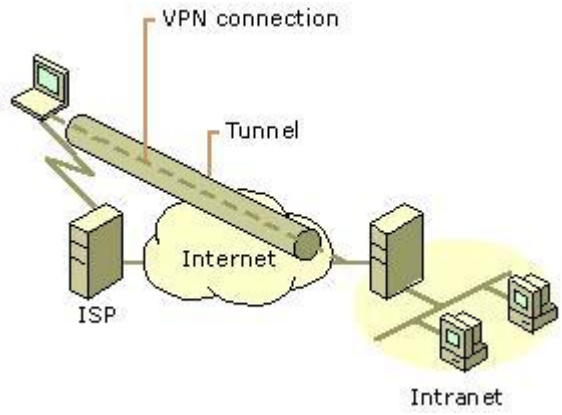

Figure 2: VPN Connection Connecting a Remote Client to a Private Intranet

B). Proposed System

The proposed system provides a better user interface and comprises of a menu driven program.

The proposed system is to be used as a security monitoring system for the organization. The system can be used for exchanging important information between client and administrator without the fear of information leak. The main modules of the proposed system are Admin and Client. We can also reduce the time factor for the internal process with in the development team.

Connecting Networks over the Internet

When networks are connected over the Internet (illustrated in Figure 3), a router forwards packets to another router across a VPN connection. To the routers, the VPN operates as a data-link layer link.

The proposed system starts with the invocation of the password screen. This is a security feature built into the system since all the information stored in the database is confidential and is therefore accessed only by the authorized user.

At any time admin can create a project and allot the project to the particular user. So the team member can get their project assignment through online.

C). System Architecture - Virtual Private Networks

Virtual Private Networks (VPN) can be implemented as an Intranet also and completely replace a private Wide Area Network (WAN). VPN connect both branch offices and tellecommuters into an enterprise-wide corporate network via the Internet, and can eliminate all long distance charges, along with the management and security reponsibilities of maintaining private networks.

VPN differ from ordinary networks in three ways:

There were many reasons for introducing a new system. The existing system was found as 'time-consuming' and 'in-secure', as the Internet or postal services were used to send important folders and any one could easily access information sent through these methods.

- The existing system did not have a secure mechanism for exchanging confidential information between manager and client.
- Leak of information would create unnecessary problems.

The figure below illustrates that VPN software can be used from any location through any existing ISP's dial-in service.

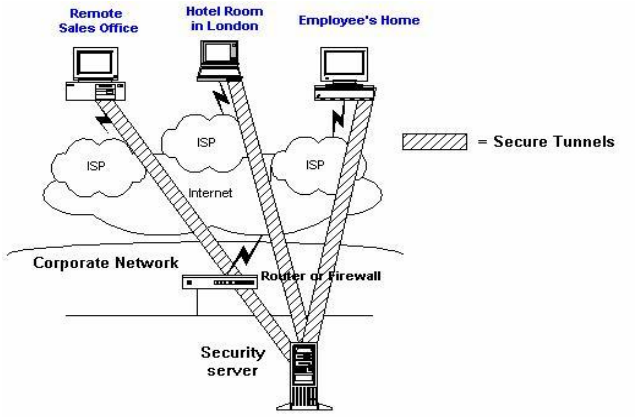

Fig – 4: Illustrates of VPN

IV. ANALYSIS AND DESIGN OF VPN

A). System Analysis and Design

In this phase, the software's overall structure and its nuances are defined. In terms of the client/server technology, the number of tiers needed for the package architecture, the database design, the data structure design etc are all defined in this phase. A software development model is created. Analysis and Design are very crucial in the whole development cycle. Any glitch in the design phase could be very expensive to solve in the later stage of the software development. The logical system of the product is developed in this phase.

As the Internet was used to send important folders, the existing system was found to be 'time-consuming' and 'in-secure', and any one could easily access information sent through these methods.

1. Virtual Private Networks allow any valid remote user to become part of a corporate central network, using the same network scheme and addressing as users on this central network.

2. Each Corporate's central network can also be responsible for validating their own users, despite the fact that they are actually dialling into a public network.

3. The Internet Service Provider can give each of their customer's a unique dial-up telephone number which will distinguish their service from any other. But this is depend on the software that will be used by the remote user.

Benefits:

- Secure data transmission with Tunneling Protocol through Internet
- Cost effectiveness with eliminate long distance charges

exchanging information between client and administrator. The main modules of the proposed system are Admin and Client. The proposed system is helpful in sending the important folders to the Admin without the fear of information leak. We can also reduce the time factor for the internal process with in the development team.

The proposed system starts with the invocation of the password screen. This is a security feature built into the system since all the information stored in the database is confidential and is therefore accessed only by the authorized user. Password screen includes the username and password. On being entered, the password is evaluated and the entry is given only to the correct password entry.

At any time admin can create a project and allot the project to the particular user. So the team member can get their project assignment through online.

B). Preliminary Investigation

The first and foremost strategy for development of a project starts from the preliminary investigation begins. The activity has three parts:

•Request Clarification

- The existing system did not have a secure mechanism for exchanging confidential information between manager and client.
- Leak of information would create unnecessary problems.
- Considerable time was taken to retrieve field data.

The system studies phase studies the problem, identifies the alternate solution, evaluates these solutions and finally recommends best solution. A detailed system study is essential for developing an efficient system. The proposed system provides a better user interface. The system comprise of a menu driven program.

The proposed system is to be used as a security monitoring system for the organization. The system can be used for

- Feasibility Study

- Request Approval

After the approval of the request to the organization and project guide, with an investigation being considered, the project request must be examined to determine precisely what the system requires.

Here our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network (LAN).

C). Feasibility Analysis

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are

- Operational Feasibility
- Economic Feasibility
- Technical Feasibility

Operational Feasibility: Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible.

Economic Feasibility: Economic Feasibility or Cost-benefit is an assessment of the economic justification for a computer-based project. As hardware was installed from the beginning & for lots of purposes thus the cost of project on hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at anytime. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

Technical Feasibility: According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independent environment. Java Server Pages, JavaScript, HTML, MS Access and WebLogic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing facility.

CONCLUSION

The performance of any software product can be measured by the ability to satisfy the customer needs, the speed at which it is done, its ability to integrate the various functions, its ability to capture the errors and conveying the same to the user for appropriate corrective actions. In this connection the performance of this software is upon the satisfactory.

REFERENCES

[1] Feilner, Markus. "Chapter 1 - VPN—Virtual Private Network". OpenVPN: Building and Integrating Virtual Private Networks: Learn How to Build Secure VPNs Using this Powerful Open Source Application. Packt Publishing.
[2] Trademark Applications and Registrations Retrieval (TARR)
[3] OpenBSD ssh manual page, VPN section
[4] E. Rosen & Y. Rekhter
[5] Ethernet Bridging (OpenVPN), http://openvpn.net/index.php/access-server/howto-openvpn-as/214-how-to-setup-layer-2-ethernet-bridging.html
[6] Address Allocation for Private Internets
[7] RFC 2917, A Core MPLS IP VPN Architecture