Middle-East Journal of Scientific Research 19 (9): 1175-1178, 2014
ISSN 1990-9233
© IDOSI Publications, 2014
DOI: 10.5829/idosi.mejsr.2014.19.9.11229

Remote Access Virtual Private Network

B. Sundarraj

Department of CSE, Bharath University, India

Abstract: The term "VPN," or Virtual Private Network, has become almost as recklessly used in the networking industry as has "QoS" (Quality of Service) to describe a broad set of problems and "solutions," when the objectives themselves have not been properly articulated. This confusion has resulted in a situation where the popular trade press, industry pundits and vendors and consumers of networking technologies alike, generally use the term "VPN" as an offhand reference for a set of different technologies. This paper attempts to provide a common sense definition of a VPN and an overview of different approaches to building them. 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. In this article, you will gain a fundamental understanding of VPNs and learn about basic VPN components, technologies, tunneling and security.

Key words: Been properly · Definition of a VPN · Usually the Internet

INTRODUCTION

The purpose of VPN is to establish the major requirements and Specification necessary to transfer the file from one end to another end in a client server technology [1-3]. The overall objective of the VPN is to establish a System based utility having high security. The goal of this document is the same as any requirements document, to lay out all requirements of the application in order to have both the developers and the end users maintaining the same understanding and expectations from the application.

While transferring a file from one point to another through Intranet and Internet we need more file secure concepts. Instead of simply dealing with local or regional concerns, many businesses now have to think about global markets and logistics. 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 [4]. Now, many companies are creating their own VPN (virtual private network) to accommodate the needs of remote employees and distant offices. In this, we encrypt the data and then it is send using the UDP. The receiver can view the data only after decrypting. And while chatting to some other client or employee in the VPN, it will be also encrypted and sent. So it is highly secured.

VPN Motivation: There are several motivations for building VPN's, but a common thread in each is that they all share the requirement to "virtualize" some portion of an organization's communications-in other words, make some portion (or perhaps all) of the communications essentially "invisible" to external observers, while taking advantage of the efficiencies of a common communications infrastructure [5].

The base motivation for VPN's lies in the economics of communications. Communications systems today typically exhibit the characteristic of a high fixed-cost component and smaller variable cost components which vary with the transport capacity, or bandwidth, of the system. Within this economic environment, it is generally financially attractive to bundle a number of discrete communications services onto a common high capacity communications platform, allowing the high fixed-cost components associated with the platform to be amortized over a larger number of clients. Accordingly, a collection

Corrseponding Author: B. Sundarraj, Department of CSE, Bharath University, India.

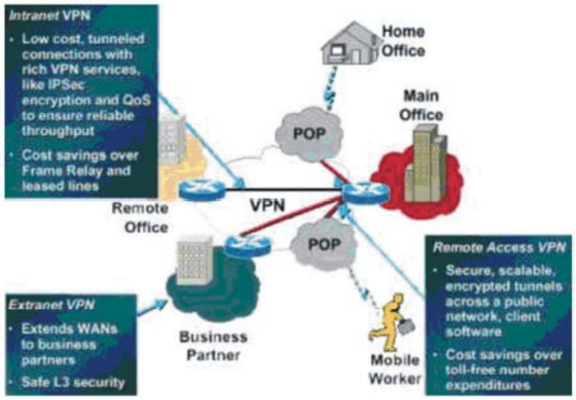
of virtual networks implemented on a single common physical communications plant is cheaper to operate than the equivalent collection of smaller physically discrete communications plants, each servicing a single network client [6].

Features of VPN:

- Security
- Reliability
- Scalability
- Network management
- Policy management

Remote Access VPN: There are two common types of VPN. Remote-access, also called a virtual private dial-up network (VPDN), is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN will outsource to an enterprise service provider (ESP). The ESP sets up a network access server (NAS) and provides the remote users with desktop client software for their computers. The telecommuters can then dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network.

A good example of a company that needs a remote-access VPN would be a large firm with hundreds of sales people in the field. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.


Intranet VPN
• Low cost, tunneled connections with rich VPN services, like IPSec encryption and QoS to ensure reliable throughput
• Cost savings over Frame Relay and leased lines
Home Office
Main Office
POP
VPN
Remote Office
POP
Remote Access VPN
• Secure, scalable, encrypted tunnels across a public network, client software
• Cost savings over toll-free number expenditures
Extranet VPN
• Extends WANs to business partners
• Safe L3 security
Business Partner
Mobile Worker

Site-to-Site VPN: Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Site-to-site VPNs can be one of two types:

Intranet-based

If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN connect to LAN.

Extranet-Based: When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN and that allows all of the various companies to work in a shared environment.

Virtual Private Network-Encryption Technology: Computers must know in order to decode the information. The code provides the key to decoding the message. Think of it like this: You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So "A" becomes "C," and "B" becomes "D". You have already told a trusted friend that the code is "Shift by 2". Your friend gets the message and decodes it. Anyone else who sees the message will see only nonsense. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.

Configuring IP Addresses for VPNs: This describes IP address assignment methods IP addresses make internetwork connections possible. They are like telephone numbers: both the sender and receiver must have an assigned number to connect. But with VPNs, there are actually two sets of addresses: the first set connects client and server on the public network. Once that connection is made, the second set connects client and server through the VPN tunnel.

In security appliance address management, we are dealing with the second set of IP addresses: those private IP addresses that connect a client with a resource on the private network, through the tunnel and let the client function as if it were directly connected to the private network. Furthermore, we are dealing only with the private IP addresses that get assigned to clients. The IP addresses assigned to other resources on your private network are part of your network administration responsibilities, not part of VPN management [7]. Therefore, when we discuss IP addresses here, we mean those IP addresses available in your private network addressing scheme that let the client function as a tunnel endpoint.

This includes the following sections:

- Configuring an IP Address Assignment Method,
- Configuring Local IP Address Pools,
- Configuring AAA Addressing,
- Configuring DHCP Addressing.

Advantages of VPN: 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
- Policy management

Future of VPN

Built on Standards: Based technologies, GET VPN easily integrates routing and security in the network fabric, delivering a rich functionality set [8].

Group Domain of Interpretation: The key management protocol that establishes security associations among authorized group member routers.

IP Header Preservation: Preserves the original IP header inside the IP sec packet.

Centralized Key and Policy Management: Responsible for pushing keys and re-key messages as well as security policies to authorized group member routers.

Key Server High Availability: Synchronizes keys and the policy Database with a secondary key server.

Support for Anti-Replay: Protects against “man-in-the-middle” attacks.

Encryption Support: Data Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES). Impressive benefits.

CONCLUSION

So what is a Virtual Private Network? As we have discussed, a VPN can take several forms. A VPN can be between two end-systems, or it can be between two or more networks. A VPN can be built using tunnels or encryption (at essentially any layer of the protocol stack), or both, or alternatively constructed using MPLS or one of the “virtual router” methods. A VPN can consist of networks connected to a service provider’s network by leased lines, Frame Relay, or ATM, or a VPN can consist of dial-up subscribers connecting to centralized services, or other dial-up subscribers [9-13].

REFERENCES

1. Wired Magazine, 1998. Wired's Hype List - Deflating this month's overblown memes, pp: 80. Ironically, number 1 on the Hype List is Virtual Private Networks with a life expectancy of 18 months.
2. The New Hacker’s Dictionary, Third Edition. Compiled by Eric S. Raymond, published by MIT Press, 1993. The Jargon File online: http:// www.ccil.org/jargon/
3. Webster’s Revised Unabridged Dictionary, 1913. Hypertext Webster Gateway: http:// work.ucsd.edu:5141/cgi-bin/http_webster.
4. Kumaravel, A., 2013. An application of non-uniform cellular automata for Efficient Cryptography, Xplore, pp: 1200-1205.
5. Kumaravel, A., 2013. Routing Algorithm over Semi-regular Tessellations, Xplore, pp: 1180-1184.
6. Kumaravel, A., 2013. Algorithm for Automaton Specification for Exploring Dynamic Labyrinths, Indian Journal of Science and Technology, 6(5).
7. Kumaravel, A., 2013. Application of Non-uniform Cellular Efficient Cryptography Automata, Indian Journal of Science and Technology, 6(5S): 4561-4566.
8. Kumaravel, A., 2013. Introducing an Efficient Programming Paradigm for Object-oriented Distributed Systems, Indian Journal of Science and Technology, 6(5S): 4597-4603.
9. Shafaq Sherazi and Habib Ahmad, 2014. Volatility of Stock Market and Capital Flow Middle-East Journal of Scientific Research, 19(5): 688-692.
10. Kishwar Sultana, Najm ul Hassan Khan and Khadija Shahid, 2013. Efficient Solvent Free Synthesis and X Ray Crystal Structure of Some Cyclic Moieties Containing N-Aryl Imide and Amide, Middle-East Journal of Scientific Research, 18(4): 438-443.

11. Pattanayak, Monalisa and P.L. Nayak, 2013. Green Synthesis of Gold Nanoparticles Using Elettaria cardamomum (ELAICHI) Aqueous Extract World Journal of Nano Science & Technology, 2(1): 01-05.
12. Chahataray, Rajashree and P.L. Nayak, 2013. Synthesis and Characterization of Conducting Polymers Multi Walled Carbon Nanotube-Chitosan Composites Coupled with Poly (P-Aminophenol) World Journal of Nano Science and Technology, 2(1): 18-25.
13. Parida, Umesh Kumar, S.K. Biswal, P.L. Nayak and B.K. Bindhani, 2013. Gold Nano Particles for Biomedical Applications World Journal of Nano Science & Technology, 2(1): 47-57.