Chapter 3
Virtual Private Networks

Alok Vishwakarma
Sysbiz Technologies Pvt. Ltd., India

ABSTRACT

Virtual Private Network, Its ‘Virtual’, Its ‘Private’ and it’s a ‘Network’. A virtual private network (VPN) provides a secure connection between a sender and a receiver over a public non-secure network such as the Internet. A secure connection is generally associated with private networks. (A private network is a network that is owned, or at least controlled via leased lines, by an organization.). We can define a VPN by the following relationship: VPN = Tunneling + Security + QoS Parameters. This Chapter deals with Advantages of VPNs, Types of VPNs, VPN Architectures, VPN Models, VPN Devices, Technologies and Protocols Used to Enable Remote Access VPNs.

INTRODUCTION

What Makes a VPN?

A well-designed VPN can greatly benefit a company (see Figure 1). 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

DOI: 10.4018/978-1-4666-8761-5.ch003
Background

A VPN can transform the characteristics of a public non-secure network into those of a private secure network. VPNs reduce remote access costs by using public network resources. Compared to other solutions, including private networks, a VPN is inexpensive. VPNs are not new. In fact, they have been used in telephone networks for years and have become more prevalent since the development of the intelligent network (Web ProForum Tutorials, n.d.). Frame relay networks, which have been around for some time, are VPNs. Virtual private networks are only new to IP networks such as the Internet. Therefore, some authors use the terms Internet VPN and virtual private data network to distinguish the VPN described in this chapter from other VPNs. In this book, the term VPN refers to Internet VPN. The goal of a VPN is to provide a secure passage for users’ data over the non-secure Internet. It enables companies to use the Internet as the virtual backbone for their corporate networks by allowing them to create secure virtual links between their corporate office and branch or remote offices via the Internet. The cost benefits of VPN service have prompted corporations to move more of their data from private WANs to Internet-based VPNs.

Technologies and Protocols Used to Enable Remote Access VPNs

- The Layer Two Forwarding (L2F) Protocol—L2F
- The Point-to-Point Tunneling Protocol (PPTP)
- The Layer 2 Tunneling Protocol versions 2 and 3 (L2TPv2/L2TPv3)
- IPsec
- The Secure Sockets Layer (SSL)
Related Content

**Modified DP-Q and MGF BER**  
[www.igi-global.com/chapter/modified-dp-q-and-mgf-ber/117823?camid=4v1a](www.igi-global.com/chapter/modified-dp-q-and-mgf-ber/117823?camid=4v1a)

**Internet of Things (IoT) Security and Privacy**  
*Powering the Internet of Things With 5G Networks* (pp. 247-267).  
[www.igi-global.com/chapter/internet-of-things-iot-security-and-privacy/185929?camid=4v1a](www.igi-global.com/chapter/internet-of-things-iot-security-and-privacy/185929?camid=4v1a)

**Opportunistic Networking in Delay Tolerant Vehicular Ad Hoc Networks**  
(pp. 282-300).  
[www.igi-global.com/chapter/opportunistic-networking-delay-tolerant-vehicular/43175?camid=4v1a](www.igi-global.com/chapter/opportunistic-networking-delay-tolerant-vehicular/43175?camid=4v1a)

**The Internet of Things: Enabling Artificial Intelligence**  
[www.igi-global.com/article/the-internet-of-things/210624?camid=4v1a](www.igi-global.com/article/the-internet-of-things/210624?camid=4v1a)