Chapter VI

Virtual Private Networks: Enhancing the Impact of the Internet

Lance Pickett and Kathy S. Lassila
University of Southern Colorado, USA

INTRODUCTION

Virtual private networks (VPNs) have recently emerged on the forefront of network and Internet development. They combine easy remote access and the low cost of the Internet with the management and security benefits of a private network. VPNs are replacing expensive cabling, leased lines, and proprietary equipment while extending the reach of traditional enterprise networks to individual workers, remote office locations, and business partners. VPNs are the first technology to provide full support, in a cost-effective and secure manner, for the connectivity needed to fulfill the promise of the "virtual organization."

Access to corporate resources from anywhere at any time has become a mission-critical requirement for today's organizations (Tuomenoksa, 1998). VPNs represent a new paradigm for remote access that is destined to replace current fixed wide area network (WAN) technologies within the next decade (LaBorde, 1999). The many advantages of VPNs over private networks make their eventual widespread adoption inevitable. VPNs require less equipment and fewer lines than private networks and are typically less of a management burden. VPNs also provide tremendous flexibility, with a single connection for corporate local area network (LAN) and Internet access. The VPN infrastructure is affordable, has worldwide reach, is easily maintained, and is highly scalable.

VPN development has been driven by the rapid growth of Internet access, the critical mass of companies with a Web presence or conducting some form of e-commerce over the Internet, and the great concern for saving money. The objectives of this chapter are to provide a brief background on the development and technology of VPNs, describe several current VPN implementations and their impacts, and discuss key management issues surrounding the adoption and implementation of VPNs.

VPN DEVELOPMENT AND TECHNOLOGY

A virtual private network, or VPN, refers to "any system that sends encrypted private traffic across public Internet connections" (Gaskin, 1999, p. 23). VPNs, which vary in scope and technology, were initially introduced in the mid-1990s. Their popularity upon introduction was little to none. Organizations could not take full advantage of the Internet due to technical restrictions (i.e., modem speeds of 2400-9600 bps). Speed and efficiency on the VPN platform could not be realized. Eventually, as telephone monopolies vanished, government regulatory policies changed and technology-advanced Internet connections on regular phone lines at speeds as high as 56,600 BPS became possible. This innovation insured high speed and great efficiency for data transmission and, in turn, made VPN technology more attractive. Virtual private networks began to rise in popularity in early 1997. Worldwide expenditures for VPN services could hit $10 billion in 2001 and may be more than $29 billion in 2003 (LaBarba, 1999).

The key word in VPN is "virtual"–meaning the individual packets traversing the network can take any route to get from point A to point B. A packet is a group of fixed-length binary digits that include data and control information (Gaskin, 1999). The encrypted secure channel over which the packet travels is not a fixed pipe, but a dynamic, constantly shifting encrypted communications path that may take various routes to move data from a remote laptop to company headquarters (Schwartau, 1998). The Internet-based VPN consists of five key elements: IP security, tunneling protocols, Network Address Translation, authentication, and firewalls (LaBorde, 1998). These items are illustrated in Figure 1 and described below.

The Internet Engineering Task Force (IETF) created standards for IP (Internet protocol) security, named IPSec, to describe how Internet-based VPNs carry IP traffic securely (LaBorde, 1999). IPSec establishes essential services for protection of network resources, proof of identity, and privacy of information. IPSec provisions are robust and easy to use, offering authentic-