

Network Security Basics

**A brief introduction to network security,
IPSec, and Internet Key Exchange**

Scott Nesbitt

Copyright (C) 2000 - 2004 by DMN Communications

Network Security Basics

Without a security framework, the standard Internet Protocol (IP) is far too insecure for transmitting confidential traffic. Information that travels over an unprotected IP channel is vulnerable to numerous attacks, including interception, sniffing, spoofing, etc. As well, there is no mechanism for non-repudiation of transmitted information. These principles apply not only to network connections made with desktop PCs, but also when mobile devices like Personal Digital Assistants (PDAs) are added to networks.

In a world of wired and wireless communication and commerce, efficient network security is vital. One of the best ways to secure network traffic is with a Virtual Private Network.

Virtual Private Networks

A Virtual Private Network (VPN) is a set of individual network sites that sit on top of the Internet. A VPN secures the exchange of data using IP, which ensures that private traffic between the sites in the network is not susceptible to attacks.

The advantages of a VPN include:

- Provides an efficient and inexpensive way of increasing the breadth of a corporate network.
- Ensures the secure exchange of data between corporate headquarters and employees in the field.
- Enables the transmission of confidential data securely using shared links.

Over the last few years, corporate investments in VPNs have grown dramatically. The proliferation of VPNs and mobile devices like PDAs used to access corporate data is forcing the convergence of these two technologies. To leverage the investment in VPNs and to extend sufficient protection to mobile users, network administrators must include mobile devices in their corporate security plans.

The following diagram illustrates a connection to a VPN using mobile and wireless devices:

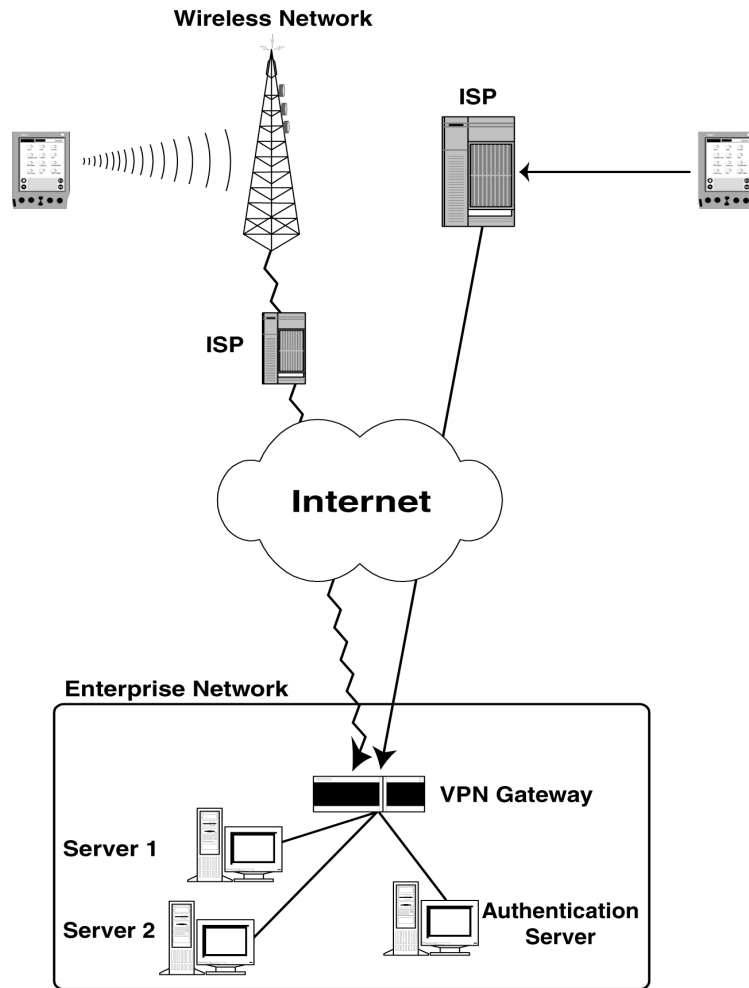


FIGURE 1. Connecting to a VPN with mobile/wireless devices

All data passing through a VPN travels over a secure route called an *encrypted IP tunnel*. A firewall surrounding each site in the network adds further protection. When information leaves a site, the VPN encrypts the data packet. When information comes from a remote user, the VPN decrypts the packet, and then routes the packet to its destination within the network.

The engines used to provide security are *IPSec* and *Internet Key Exchange*.

IPSec

IPSec is an IP security protocol defined by the Internet Engineering Task Force, and is the basis for securing a VPN. IPSec is a set of security standards for online communications that ensures data travelling across a network is secure, confidential, and authentic. An IPSec implementation operates on a host computer, or in a security gateway in conjunction with a network firewall.

Two protocols form the basis of IPSec:

- **Authentication Header (AH)**, which is designed to ensure the integrity of the information being sent, and authenticate its origin. AH only provides authentication. It does not provide privacy.
- **Encapsulating Security Payload (ESP)**, which performs the same functions as the Authentication Header. ESP also provides privacy by encrypting data, and provides protection to the traffic flow.

Central to IPSec is a Security Association (SA). An SA is a simple connection over which security services can travel. The SA is identified by a combination of the IP destination address, and either the Authentication Header or Encapsulated Security Payload. When an SA exists, the sender and receiver hold the algorithm and keys needed to authenticate a message. The algorithm and keys are not included in the authentication header.

Internet Key Exchange

Internet Key Exchange (IKE) is the IPSec security infrastructure. IKE authenticates endpoints and negotiates encryption keys. It also negotiates the security protocols and algorithms between a remote user and a VPN.

When you access a VPN, the system confirms your identity and determines how to encrypt communications. There are two authentication modes.

- **Main mode**, which only reveals your identity once secure communication is established. This is a secure, but slow method of authentication.
- **Aggressive mode**, which reveals your identity before secure communication is established. Aggressive mode is faster than Main mode, and is the preferred mode for IKE.

There are various mechanisms to authenticate users at the VPN gateway. Popular authentication mechanisms include user name and password, digital certificates, SecureID, and smart cards.
