Chapter 31

FIREWALL TOPOLOGIES

INTRODUCTION

From hardware to software, there are myriad arrays of choice in the realm of security wares that provide the cast of supporting characters on the firewall stage. A firewall is more than just a single piece of equipment; as the authors of this fine book have asserted, a firewall is a policy; it is often a well-documented policy that encapsulates equipment, software, and usage policies. No one piece of equipment should be or could be acting as your entire firewall. For example, having a policy in place of changing your passwords frequently would be part of your firewall. However, where the focus of the previous chapter centered on actual firewalls and the often accompanying softwares bundled with them, this chapter's intent is to focus on independent utilities that may be assembled to provide an in depth defense against intrusion, extrusion, and collusion. Two major areas in this defense involve network topology, especially in terms of the Wide Area Network (WAN). These two areas, how they are handled, how they are managed, and how they are secured, are the measures of success of any firewall security policy. Coincidentally, the implementation and subsequent user leveraging of these security resources greatly improves work force life quality and productivity. It also makes managing remote networks from a central location a very real possibility [1].

VPN – VIRTUAL PRIVATE NETWORK

One of the first areas to cover then becomes one of intentionally opening "holes" in the firewall to allow *desirable* traffic through. One such hole through a firewall is the Virtual Private Network (VPN) as shown in Fig. 31-1 [1].

Often times, when presenting the concept of a VPN as a solution to clients coworkers, customers, there will be some resistance. VPN technology is relatively straightforward and

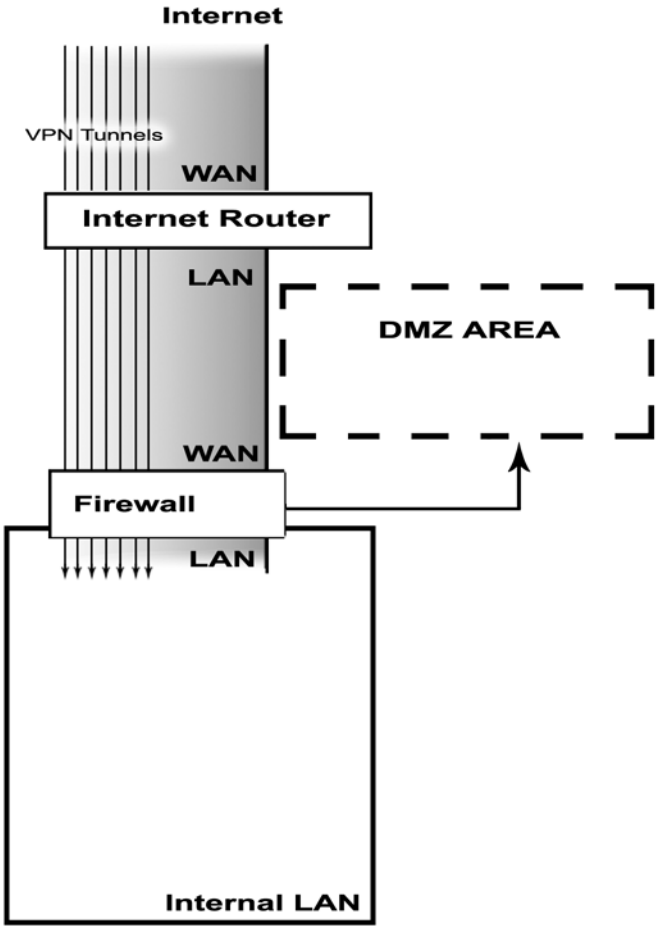

Figure 31-1. With today's high speed connections and advanced encryption algorithms, a possibility of Virtual Private Networking has been created that, traditionally, was accomplished by dial-up servers and modems.

easy to manage – the greatest obstacles to creating a VPN are: The technical abilities of the user, his understanding of the concept; and, Sensitivity of data [1].

Once these obstacles are conquered, and before the actual equipment purchase and integration, policy needs to be established. Questions such as these may arise:

- How sensitive is corporate data?
- How will decisions be made regarding access?
- At the individual server level?
- At the PC level?
- The workgroup or domain level [1]?

This is where the topology of the internal network plays a pivotal role. It can be very time consuming and difficult to arrange servers and information in ways that are particular to one user or even one group of users. Mapping drives is well and good, but can you map drives over a VPN? This is not a book about access control, however, but suffice it to say that yes,