6.5 VPN Solutions

Regardless of which protocols you use for VPN, you must implement your choice in some software/hardware configuration. Many operating systems have built-in VPN server and client connections. These are generally fine for small office or home situations. However, they might not be adequate for larger scale operations in which multiple users connect via VPN. For those situations, a dedicated VPN solution might be necessary.

6.5.1 Cisco Solutions

Cisco offers VPN solutions, including a module that can be added to many of their switches and routers to implement VPN services. It also offers client-side hardware that is designed to provide an easy-to-implement yet secure client side for the VPN.

The main advantage of this solution is that it incorporates seamlessly with other Cisco products. Administrators using a Cisco firewall or Cisco router might find this solution to be preferable. However, this solution might not be the correct one for those not using other Cisco products and those who are not familiar with the Cisco systems. However, many attractive specifications for this product include the following:

- It can use 3DES encryption (an improved version of DES). But AES is preferred and strongly recommended.
- It can handle packets larger than 500 bytes.
- It can create up to 60 new virtual tunnels per second, a good feature if a lot of users might be logging on or off.

6.5.2 Openswan

The Openswan product (www.openswan.org/) is an open source VPN solution available for Linux operating systems. As an open source product, one of its biggest advantages is that it is free. Openswan uses IPSec, making it a highly secure VPN solution.

Openswan supports either remote users logging on via VPN, or site-to-site connections. It also supports wireless connections. However, it does not support NAT (network address translation, the new alternative to proxy servers).