3.4 Proxy Servers

A proxy server is often used with a firewall to hide the internal network's IP address and to present a single IP address (its own) to the outside world. A proxy server is a server that sits between a client application, such as a web browser, and a real server. Proxy servers prevent hackers from seeing the IP addresses of internal machines, knowing how many machines are behind the proxy server, or learning anything about the network configuration.

Proxy servers also provide a valuable control mechanism because most proxy servers log all outgoing traffic. This enables network administrators to see where employees go on the Internet. A proxy server normally runs as software on the same machine as your firewall.

The proxy server is configured to redirect certain traffic. For example, incoming traffic using the HTTP protocol is usually allowed through the proxy server but is redirected to the web server. That means that all outgoing and incoming HTTP traffic first goes through the proxy server. A proxy server can be configured to redirect any traffic you want. If an e-mail server or FTP server is on the network, all incoming and outgoing traffic for that network will run through the proxy server.

Using a proxy server means that when a machine inside the network visits a website, the website will only detect that the proxy server visited it. In fact, if dozens of different machines on the network visit a site that logs the IP addresses of incoming connections, they will all be logged with the same IP address—that of the proxy server.

For the most part, this sort of proxy server has been supplanted by network address translation. However, the term proxy server is still used, but with a different application. Now proxy servers work with the firewall in order to filter things such as web content. They allow a network administrator to block certain sites and to also record all websites a given user visits.

This hiding of the network is a very valuable service because knowledge of internal IP addresses can be used to execute certain forms of attack. For example, IP spoofing is contingent upon knowing the IP address of an internal server. Hiding those IP addresses is an important step in network security. It can also be very useful to know where employees go on the Internet.

Proxy servers track such information, and many network administrators use this to restrict employees from using the company Internet connection for illicit purposes. This can also be a useful tool for stopping attacks. An employee who visits hacker websites might be a potential security risk. They may return some of the techniques that they read about on the network. Administrators can also detect potential industrial espionage. An employee who spends a lot of time on a competitor’s website might be considering a job change and might consider taking valuable data with him.

3.4.1 NAT (Network Address Translation)

For many organisations, proxy servers have been superseded by a newer technology known as network address translation (NAT). Proxy servers today do not carry out the purpose they once did (i.e., translate a private IP address into a public IP address). Primarily, NAT translates internal addresses and external addresses to allow communication between network computers and outside computers. The outside sees only the address of the machine running NAT (often the firewall). From this perspective, it functions exactly like a proxy server.

NAT also provides significant security because, by default, it allows only connections that are originated on the inside network. This means that a computer inside the network can connect to an outside web server, but an outside computer cannot connect to a web server inside the network. You can make some internal servers available to the outside world via inbound mapping, which maps certain well-known TCP ports (80 for HTTP, 21 for FTP, etc.) to specific internal addresses, thus making services such as FTP or websites available to the outside world. However, this inbound mapping must be done explicitly; it is not present by default.