Quick guide to Firewalls & there applications

Introduction

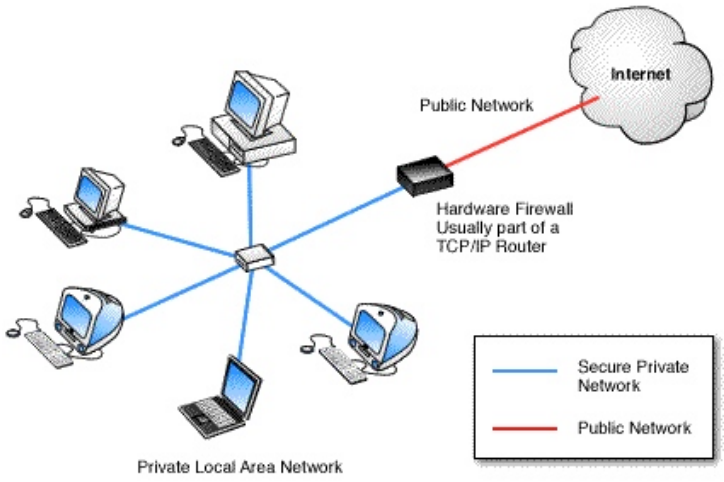
Owing to the expanse of the Internet in general and the fact that more and more users are using an 'always-on' connection like ADSL Broadband, it is now vital that the computers and network in general are protected from Hackers, Internet Worms and other malicious programs. Enter the Firewall!

What is a Firewall?

A Firewall is a general description (first used in the US to describe fire protection in a building) to describe a program that 'sits' between your PC and the Internet which inspects each data 'packet' coming in from the Internet (Inbound) and going out from your computer (Outbound). On Dynamode Router products the Firewall is known as a Hardware Firewall because the Firewall program is programmed directly into a chip in the Router and are generally faster and more secure than the software based Firewalls you might load onto Windows © for example.

Fig. 1

The Dynamode Router (Firewall) sits between the local Network and the Internet



Thus, simplistically, a Firewall performs its duties in the following ways

- Inspects Inbound packets form the Internet and verifies there from a valid source
- Stops any specific Inbound traffic which may cause harm to a Computer. For example, from an unknown IP source which might attack certain TCP/IP Ports (such as Port 80, 21 etc) and cause DoS (Denial of Service) attacks which might crash a Web Server you are running
- Prevents Internet Worms (such as Sasser.B) based on the Port Numbers it tries to enter by. The Firewall will block all unused Inbound ports and only keep open specific ones (like 110 for POP3)
- Outbound traffic on certain TCP/IP ports will also be blocked so to stop the spread of say an Internet Worm from your Computer spreading to others on the Internet. Be careful though, blocking all outbound ports will prevent the usage of applications such as Email, Web, Video Conferencing etc

Nick Beer, Dynamode UK