Firewalls

In the simplest terms, a firewall is a device or program that restricts computers from communicating with each other, and allows only certain methods of communication. Practically speaking, a firewall is a good step towards preventing malicious users from attempting to attack your computer. As we discuss in other sections, a firewall is not a perfect solution, and should be augmented with good security practices including antivirus software.

Firewalls come in two flavors: Hardware and Software. Hardware firewalls are devices which connect between your home computers and your DSL modem. They are available from a wide variety of manufacturers. Software firewalls are included with recent versions of Microsoft Windows, Apple OS X, and Linux. Software firewalls can also be purchased or downloaded for many different operating systems.

A software firewall is a good choice if you have a single computer. It does not require the purchase of any new hardware. If your operating system does not come with a built-in software firewall, you will need to download or purchase one.

- Information on configuring the firewall included with Windows XP can be found at Micros oft's Security site

.

- To learn how to set up the firewall in Apple OS X, visit Apple .
- Linux users can consult this site for an introduction to the iptables firewall.
- Reviews and information about other software firewalls can be found here .

If you have multiple computers networked together, you should seriously consider the use of a hardware firewall. These devices are readily available for well under $100, and are generally marketed with names like "residential gateway", "broadband router" or "cable/dsl router". Most of these units contain a hardware firewall, a multi-port switch to connect multiple computers, and are easily set up and configured using a web browser.

Hardware firewalls sold to home and small business users typically use a procotol called "Network Address Translation" (NAT). NAT enables each of the connected computers to have their own "private" IP address, which is different from the "public" static IP address that is assigned to the router. By assigning private IP addresses to each computer connected to the router, other computers are not able to directly see these IP addresses. This helps to protect these computers by essentially making them "invisible" to everyone on the Internet.

A good model that MCN recommends is the Linksys BEFSR41 . It will allow you to connect up to four computers, and connects seamlessly to your DSL bridge, providing security for your home network. This model can be purchased online for around $60.

Since the purpose of a firewall is to restrict communications with other computers, sometimes it may block communications that you want. In order to understand how this occurs, you should understand the concept of *ports*. Ports are numbers that a program on one computer uses to identify programs on another computer when communication is required. For example:

- A web browser uses port 80 when making requests to a web server.
- A mail program uses port 25 when sending mail to a mail server.

If you experience problems using a particular program, you'll need to know what ports that program requires before you can configure your firewall to allow those ports through. There are many websites that detail this information. For specific configuration instructions on your particular firewall, consult the documentation. We have provided several links below that will get you started.

- How To Open Ports In The Windows XP Firewall