

Internet Security

Part 2 of 3: Firewalls

In last month's newsletter (Part 1 of 3: Nature of the Threat), we covered some of the most common internet threats to your system's security. This month, find out all about one of the most critical components of a good internet security strategy: the firewall.



What is a Firewall?

Just like it sounds, a firewall is designed to keep bad stuff out. It prevents hackers and others from gaining access to your computer(s) to deliver damaging malware or obtain personal information. Simply put, it is a checkpoint between cyberspace and your computer(s). Another analogy is to that of a filter, allowing "good" traffic both ways (so you can send and receive the information you want to and from the internet) while still protecting you from unsolicited attacks.

Let's discuss the two different types of firewalls:

Hardware Firewalls

A hardware firewall is a physical device that acts as the "middle-man" between the outside internet and your computer(s).

Chances are, if you share an internet connection among multiple computers, you already have a hardware firewall in place – your Router. Routers use Network Address Translation (NAT) to allow all your computers to share a single internet connection over a single IP address. Conveniently, NAT also provides the firewall protection you need to keep your network secure. It blocks unsolicited requests or probes from outside before they ever reach one of your computers.

Software Firewalls

You may have heard of software packages out there (such as Norton, McAfee, or Trend Micro)* that provide this firewall function. Typically, the firewall software is either included in a total "Internet Security" suite or offered as an individual program.

The "Internet Security" packages contain additional software such as Anti-Virus**, Spam Filters, Parental Controls, etc.

There is also a software firewall available as part of Microsoft's Windows XP (SP2) operating system.

Which kind of firewall do I need?

Because of the physical layer of protection, hardware firewalls are generally more effective than their software counterparts. Software firewalls also take up system resources on each computer, often resulting in decreased speed performing routine tasks.

Therefore, a router that doubles as a hardware firewall is preferred. Installing a software firewall on top of that protection is typically unnecessary and could also cause problems if not configured properly. It is quite common that a software firewall on your server can block one of your Point Of Sale machines from connecting to the server.

Generally, you'll only need a software firewall if you have a computer connected directly to the internet using a DSL or cable modem, **without a router**.

Missed part 1 of this series? Catch up on previous newsletters at www.camcommerce.com under **Customer Resources | Newsletters**.

*CAM does not necessarily endorse or support any software listed as an example.

**Look for more in-depth coverage of Anti-Virus software in next month's newsletter.