

Firewalls: Very Necessary Protection

By Bill Hely

For most "average" computer users the word "firewall" evokes one of three responses:

- "Oh, that's complex big-business stuff – it's not something I need or could afford".
- The Windows Firewall built-in to Windows XP and Vista.
- A software brand such as *ZoneAlarm*.

Those who think a firewall is just a software program have the edge. At least they know that a firewall can be a consumer item they could purchase and install if they were so inclined.

Now, the nature and purpose of this article dictates that I don't tell all of the story all of the time. For example, I am now telling you there are two types of firewall to consider. In actual fact the number of "types" depends entirely on how you choose to categorize them. For our purposes a simplistic breakdown is more than adequate.

The two types we'll discuss are *software firewalls* and *hardware firewalls*.

Hardware firewalls usually take the form of a small "black box" that plugs into your Internet connectivity device (cable, ADSL or dial-up modem) and also into your PC or into some network component such as a Hub or Switch. By the way, "black boxes" are almost never black; the term simply denotes a device whose exact inner workings are irrelevant to the discussion. It's only what goes in and what comes out that matters.

Dedicated hardware firewall devices are expensive, complex to configure and maintain, and thus rarely found in the home or very small business. What is often referred to as a "hardware firewall" at the domestic/small-business level is more often a router with some firewall capability built-in. Such devices are very inexpensive and more than adequate protection for the home or small business. In this article all references to "firewall" mean a NAT Router.

The software firewall (often called a "personal firewall" because it protects only the one PC on which it is installed) is, as the name suggests, simply a computer program.

What software and hardware firewalls have in common is that they both receive, inspect and make decisions about all incoming data before passing it on to the computers protected by the firewall.

However a most important difference between the two types is that the hardware firewall doesn't control *outbound* communications (i.e. from the computer to the Internet) to any really useful degree. It's effectiveness is mainly over data from the Internet to the computer—*incoming* data. This is a significant deficiency when some scumware program gets into your hard drive that has the ability to communicate back out to someone on the Internet.

On the other hand, the software firewall offers strong control over both incoming and outgoing data.

You would thus be justified in wondering why you need to use two different types of firewall that both control incoming connections. If the software firewall controls data traffic in both directions why not just go for that option?

There are several reasons but, from the point of view of a computer user, as good a reason as any is "much improved usability".

Firewalls: Necessary Protection

The software firewall's control over incoming connection requests is quite powerful. Using its programmed "intelligence", it can analyze incoming data streams. However it cannot make final "block or allow" decisions without your help, until you have "taught" it how to respond to different situations. It needs to learn as it goes. In short, the software firewall will frequently ask you to make decisions on what to do about certain incoming data it encounters—whether to allow them in or not.

That's fine, until the frequency of the alarms becomes distracting to the point of being annoying. While you are trying to concentrate on other things in the face of these interruptions, there is a very real risk that you will take the easy way out and command the software firewall to "always allow" or "always deny" such data packets, without giving careful thought to the consequences, which could be significant either way.

The hardware firewall, on the other hand, enforces a very simple policy on incoming connections: if the connection wasn't requested by a PC from within its "walls"—that is a PC under its protection—the connection is refused or ignored.

In most situations such simplistic decision making by the hardware firewall is quite OK. You will appreciate that the stubborn inflexibility of the hardware firewall makes the software firewall's job much easier.

You may have also noticed from its positioning that the hardware device is a "perimeter" firewall placed between your PC (or your network) and the Internet, so it gets first look at any incoming data.

On the other hand, the software firewall is on a local PC and thus inside the perimeter, so it only gets to see incoming data that has survived the hardware firewall. And the only incoming data that does survive is that requested by an internal PC in the first place.

With a hardware firewall in place there will be less questionable incoming traffic for the software firewall to analyze, thus fewer excuses for it to bother you with a request for a decision. And therefore fewer chances for you to respond with a dangerous answer.

This improvement in usability is not a minor matter. The difference can be so pronounced that many people who install a hardware firewall, after having a software type in place for a while, begin to wonder if the latter is still working, so reduced are the "alarms" they have to respond to.

Another very important reason for using both hardware and software firewalls is that software is ... well, software. And software, any software, can be compromised. Conversely the hardware firewall, with very few exceptions, can only be "got at" physically. That is, a bad guy has to have physical hands-on access to the firewall to do anything nefarious with it.

Finally, both software and hardware can fail for any number of reasons. If a **good** software firewall encounters a problem it should be designed to fall back to some sort of safe mode, blocking all Internet traffic until the problem is dealt with.

But if something should occur that forces the software firewall to shut down, or that prevents it from loading at all (something many trojans attempt to do), it is no longer an impediment to unauthorized data. You could well be vulnerable to attack and remain blissfully unaware of the fact that your firewall isn't operating.

On the other hand, if the hardware firewall fails it will do so in such a way that access to and from the Internet is cut off altogether. The hardware firewall, by its very nature, can

Firewalls: Necessary Protection

only fail on the side of complete safety. If it's "not there", neither is the Internet connection.

Well ... does that make the software firewall too much trouble?

No way !!!

As already described, a good software firewall that does its job properly is positively invaluable for its management of outgoing connections, which is where one of the biggest threats to your security lies.

At the very least you should install a good software firewall on each PC for which you are responsible. My personal choice is an excellent, fully supported, and yet free program called Comodo.

<http://HackersNightmare.com/Comodo-Firewall>

Before installing Comodo firewall you should be sure to disable the built-in Windows XP Firewall which, while better than nothing, is really not good enough to stake your data security on. The click sequence to disable the Windows XP Firewall is:

Start button → Settings → Control Panel → Security Center → Windows Firewall

Do not, under any circumstances, attempt to run both the Windows XP Firewall and a 3rd party firewall such as Comodo at the same time.

A very strong case can be made for having both firewall types (hardware and software) in place. I do, as do most professionals with an understanding of, and a respect for, data security. Given the parlous state of the World Wide Web today, running both firewall types simultaneously is a necessity, not a luxury and certainly not over-kill. Fortunately the cost to do so is negligible.

There is no space here to discuss hardware firewall recommendations, as the most suitable type will depend on a number of factors. Seek advice from a reputable computer dealer or, better still, consult a more detailed resource such as *The Hacker's Nightmare*[™], wherein I make specific recommendations and discuss the wireless variety as well.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity. He is the author of several books on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*[™].

To comment on this article please use the "Support" link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation
— and especially testimonials —
are most welcome.