richline wordshop
DIVISION OF RICHLINE SERVICES

Feature product report for a monthly computer journal

Considering a Firewall? Hardware or Software or Both?

For most home users, except for the built-in protection of routers, hardware-style firewalls have been too expensive, thereby yielding the market to software utilities—until now.

Over the past few years, in escalating strides, seeking protection against Internet demons has become a primary consideration among computer users in both the business and home sectors. From being an issue of only moderate concern to the average consumer, e-mail viruses (joined by website spyware and "Trojan horses") are the downside of computing. And we aren't even touching on the out-of-hand spam phenomenon that has become the Black Plague of communicating today.

As with any popular event, good or evil, vendors rush to smother the market with an array of me-too products to combat the foe—software, hardware, reference books—accompanied by rash promises, quickly joined by rebates and upgrades. In time, everyone becomes familiar with the existence of the unfriendly e-mail intruders even though diligence in keeping them at bay often falters. It would make for an interesting news clip to learn what percentage of product buyers regularly maintain the integrity of their defensive utilities through new purchases, upgrades, and patches. Chances are that the vendors accurately guessed and found that automatic downloading was the practical solution. And a profitable one at that. But all of that deals essentially with virus-laden and, more recently, spam-dominated e-mail transmissions. With the rapid expansion of faster broadband connections (both cable and phone-based DSL) replacing dial-up service, the spotlight now turns to yet another Internet enemy action—successful intrusion of your computer via any port that is always open, or nearly so.

The time to adopt a firewall is already here

For those who are unfamiliar with the concept, firewall technology is something like a gatekeeper. It's a way to establish patterns of control and apply them to allow or stop movement through a designated opening. For computers, that translates to opening or closing a port to Internet data going out or coming in. The port is simply an address that identifies the specific application associated with the data being sent or received. Without some way to close any open "door" while still being connected to the Internet, you are providing a means for stealth entry by others. How's that, you say? Indeed, you've read of taking over command of a computer by unknown outsiders as well as the insertion of programming code that can disrupt the settings established by the owner. Simply by scanning the Internet (much as is done by those using radio or wireless telephone equipment scanning the broadcast bands), open ports resulting from "always on" service that show no activity can be detected and therefore are vulnerable to whoever has the technology to gain entrance.

If your connection to the Internet is via a cable or (especially) a DSL modem, you may have either a *static* or *dynamic* address furnished by your provider. The latter will be automatically assigned each time you start accessing the Internet, which does offer somewhat more protection against invasion, or "hacking," but this shouldn't be counted on as making for a secure setup. Similarly, dial-up modem connections, which also use dynamic-assigned addresses , have a quasi-protected environment, but their chief defense is the much shorter duration of most Internet sessions.

Software firewalls prevail because of cost or customized controls

If you are beginning to feel convinced that firewall protection is a necessary partner to your anti-virus and spam utilities, then the next step is to select the means for doing it. By far, the popular choice today is using a dedicated software program either alone or in combination with a broadband router. The two major producers of anti-virus utilities, *Symantec* and *McAfee*, both have added firewall products to their line that are available as stand-alone purchases or as part of inclusive "security" suites. Even Microsoft has gotten into the act with the addition of a basic firewall program to its Windows XP operating system. As pre-eminent as these vendors are, the most highly-rated software in this category comes from a trio of independents: *Zone Alarm* (Std. and Pro), *Sygate Firewall* (Std. and Pro), and *Black Ice PC Protection.* No question that the popularity of these programs partly can be attributed to their lower cost—the "standard" versions being free downloads —but all have the added advantage of having been around for some time, proving their solid understanding of the strategies of combat.

While any firewall can be enhanced by a number of features (especially the paid versions), the basic functions are similar among the various players. You install the utility from a disk or download and then configure the operating settings to your computer's complement of Internet programs, such as browsers, e-mail, search engines, etc. The firewall options permit you to select complete, restricted, or denial of Internet connection for each program. Guidance by default choices can be a good start, allowing you to alter the classifications after using the settings. Furthermore, it's usually possible to override any of the choices while the computer is connected to the Internet. When intrusions of unauthorized data packets are detected, screen messages advise you of the action and either deny the connection or ask your approval. When possible, the source address is given and the activity can be logged for reference. Differences in operation among the leading titles are of less importance than the similarities, in that all of the best-known products employ up-to-date artificial intelligence technology. And, like most other software programs, there are the customary upgrades and patches that will be offered to users.

Isn't a router sufficient for broadband protection?

Study the issue of firewalls and you'll soon encounter the claim that a cable or DSL modem gains Internet safety through the use of a router. But that's not the principal purpose of these devices. During the past few years much of the growth of high-speed connection usage relates to the ease by which multiple computers in a home or business network can be served by just one Internet subscription through using a router. This external piece of hardware connected between the computer and the modem quickly moved from being a somewhat costly connection distribution accessory to an inexpensive necessity. With its ability to hide or disguise the identity of multiple port addresses, users found the router to be an automatic defensive weapon. In fact, manufacturers such as *Linksys* even sold models with just one-port capability for a single computer "network" for the protection value in its ability to monitor and filter data . Yet, typical routers have at least one address for connection to the server. This provides for distribution of the data packets coming to or being sent from the modem in conjunction with the hidden or disguised addresses for each of the user computers connected to the router. So, "hacking" is still possible.

Routers, then, don't qualify as being the one-and-only line of firewall defense. Noting that this contribution actually is a plus value to their primary function, there really should be no objection to adding a complementary product to enhance the level of protection. This is why software firewall utilities often become their partners, adding another layer of defense through their capability for more specialized transmission control. Suppose, though, that you don't want to bother with configurations for approval and denial of data transmissions? The option is there in the form of dedicated *hardware* firewalls. This and other significant advantages are covered in a product review that follows, coupled with some disadvantages. Unquestionably, the chief deterrent has been the high purchase cost—at least until now**.**

[Approximately half of the complete article reproduced. Balance available upon request.]