Wired to the World

by *Ralph Lee Scott*

Firewalls

An antivirus program continuously monitors your computer to detect a virus, which is automatically deleted and/or quarantined. Firewall programs, on the other hand, block access to your computer from the Internet and prevent hackers from planting a worm or other type of malicious software in your computer. Firewalls protect your data, your computer, and your name from corruption. Stories are legion about the Internet being used to seize control of a computer identity to do things such as send out fake e-mails in your name canceling final exams, insulting your boss, and ordering merchandise such as ten pizzas to be delivered to your office. A good firewall will prevent such a remote seizure of your computer.

A firewall separates, blocks, and analyzes incoming requests to your computer system, thus acting like a security guard to prevent access to your system by individuals, who are not authorized users. Routers or cable boxes connected to the Internet are often inadvertent open doors for unwanted users. Forcing all Internet traffic coming into your computer through this choke point is the most important function that a firewall provides. The firewall can also enforce your security policy; for example, if there are sensitive personnel or other data records on your computer that you do not want unauthorized users to have access to, the firewall blocks access to these files. If you want patrons or authorized users to pass through your system to access NCLIVE databases, for example, then the firewall will let authorized users through. A firewall can also be used to divide your network into controllable sections so that, if a problem develops on one part of the network, it will not spread to the whole system. A firewall also serves to collect information on system use, including who is accessing your network as an authorized users and who is trying to hack into your computer with malicious intent.

> *Firewall programs … lock access to your computer from the Internet and prevent hackers from planting a worm or other type of malicious software in your computer.*

Firewalls do have their limitations. They are not virus checkers and cannot stop incoming viruses from the Internet. Viruses generally have to be detected on the machine level. You need to scan regularly for viruses and have programs in place that check at the individual e-mail level for infected messages. Firewalls cannot protect against individuals inside your library who want to damage your system. Firewalls only protect your system from people outside the library, who try to access your system through the Internet. Firewalls cannot protect against entry from access points that do not go through the firewall, for example, modem banks and other types of back doors, including entry points to Integrated Library Systems installed by software vendors. It is important to remember that firewalls are not completely safe. Just as soon as methods are devised to protect against a particular threat, hackers discover additional ways to attack.

One type of firewall design is a bastion host—a computer that is highly secured, but very exposed to the Internet. This host must be in a secure location that an attacker does not have physical access to it. The bastion will provide access to the Internet and will allow authorized users to pass through to other parts of your system. For example, if you have an automated ILL system, the bastion host will only allow outside clients access to the public ILL files. Files that the ILL staff use to process requests as well as non-ILL files are not accessible to unauthorized outsiders. Generally user accounts are not allowed on the bastion host. The bastion host is a simple machine that performs only a limited number of functions. When the bastion host starts having a lot of questionable traffic, it sends an alert that your system is under attack, but unauthorized users have not as yet gained access. When this happens often you have to shut down the Internet until you can figure out what is going on. The bastion host lets you know that there is a problem, but does not interfere with the basic functions of your internal non-Internet systems.

Another type of firewall is a proxy system. A proxy server provides access to the Internet for a large number of authorized users to access services such as NCLIVE and serves a firewall to prevent unauthorized users from gaining access to restricted resources such as Science Direct. One of the great advantages of a proxy server is that the users think they are connected to the resource itself, when in point of fact they are not. This system enables you to provide that extra level of security for your systems. Proxy servers do have drawbacks. When a new service is introduced, you have to develop a proxy routine to provide access, which can prove to be a trying experience. Sometimes it is a good idea to have separate proxy servers for major services. That way, if one server gets attacked, the others will remain safe. Many vendors provide redundant backup service by maintaining access to multiple proxy servers so that when one goes down, you are simply transferred to another, usually without your prior knowledge.

Firewalls protect your computer and your files as well as your internal network from attack. There are many different types of firewalls, and setting them up can often be a challenging task. Commercial software is available for home use and small networks, but most large networks build their own firewalls. Commercial firewalls divide your home or small network computer into sections consisting of the two major types of firewalls: bastion servers and proxy servers.

This column is the first in a four-part series on computer security. The next installment will deal with spyware and how you can prevent others from snooping into you computer.