(Approx. 1171 words)

## Firewalls

By Dick Maybach, Member, Brookdale Computer User Group, NJ

www.bcug.com

n2nd (at) att.net

A firewall is a program that monitors traffic on a network and rejects any data that violate its security rules. One way to classify a firewall is by its location: it can be host-based, where it resides on a computer and controls all the data transferred through its data port, or it can be network-based where it resides on a modem or router that connects a local area network (LAN) to the Internet. The latter is sometimes inaccurately called a “hardware firewall,” although it is actually software, but running on a router, a modem, or a dedicated processor rather than a general-purpose PC.



Figure 1. Network-based Firewall.

The primary purpose of a network-based firewall is to isolate your home network from the Internet. Without one, your networked printers, PCs without host-based firewalls, and shared storage devices would be available to the world. A host-based firewall is very similar to a network-based one; the major difference is its location. It isolates the data on your PC, primarily on its disk, from other computers on the network. If you use your laptop to access the Internet through a wireless (Wi-Fi) hotspot, only its firewall protects you. Some firewalls, e.g. that included with Windows, allow increasing the protection when connected to such unprotected networks.



Figure 2. Host-based Firewall.

There are multiple types of firewalls, each using a different approach to traffic filtering.

* First-generation firewalls were *packet filters*, comparing basic information, such as the original source and destination of the packet, the port being used, and the protocol, against a list of rules.
* Second-generation firewalls were the so-called *stateful* firewalls, which added another connection state to the filtering criteria. Based on this information, the technology could determine if the packet was starting the connection, was a part of an existing connection, or wasn’t involved at all.
* *Third-generation* firewalls understand applications as well as some widely-used protocols such as File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). Based on this information, the firewall can detect attacks trying to circumvent it by misusing a protocol or violating application procedures.

Third-generation firewalls control traffic flow in several ways.

* Service control determines what types of services are accessed.
* Direction control determines in which direction particular service requests are initiated.
* User control determines if a user is allowed access to the service.
* Behavior control determines how particular services are used.

A firewall protects your computer from Internet hacking, where someone gains remote access to it over a network, and against worms, malware that spreads over a network. However, it provides little or no protection against many other threats.

* If you give permission for other computers to connect to yours, e.g. enable remote access.
* Switching off the firewall or adding many exceptions to its rules reduces the protection.
* It is not effective against malware, including viruses, spyware, ransomware, etc. This is most commonly acquired through clicking on email attachments and email links, downloading pirated media, and visiting rouge or infected Websites.
* It does nothing about spam.
* People with physical access to your computer or network are not monitored.
* Data introduced to the computer other than online, e.g. via USB connected devices, CD/DVD etc. are not checked.
* If your laptop acquires malware while connected to a Wi-Fi hotspot, and you later connect it to your home LAN, your other PCs can become compromised since you are behind the firewall.
* Traffic that appears to be legitimate passes freely.
* A firewall protects only information on your home LAN; once you send it to the Internet it’s accessible to anybody.
* Only you can prevent phishing, where you are tricked by e-mail, a Website, or a phone call into installing malware, bypassing the firewall, or disclosing sensitive information, such as your bank passwords or credit card details.

If you run a server from home, perhaps to host a Website or exchange files, you need two firewalls, one between the Internet and the network called a Demilitarized Zone (DMZ), and a second one between the DMZ and your home network; see Figure 3. The firewall between the DMZ and the Internet is less secure, because it allows incoming requests to the servers on the DMZ network. Such requests are not allowed through to the home network. Other DMZ architectures may be preferable depending on your requirements. You will need to do some research before implementing one, but fortunately, few home computer users need this complexity.



Figure 3. DMZ

Because firewalls are software running on small dedicated processors and are exposed to the Internet, they are subject to hacking, and they are attractive targets. Most home users rely on firewalls included in the cable modems and routers supplied by their Internet Service Providers (ISPs). Unfortunately, ISPs are not diligent in installing patches to correct the security flaws that are frequently uncovered. If the only devices on your home network are PCs with their own host-based firewalls and you haven’t enabled file sharing among them, the risk isn’t large. However, if you have network-shared storage or other devices without firewalls, you should add your own firewall between your network and the ISP’s interface. Many routers include firewalls and these are convenient to use here. Most security experts say that keeping your software up-to-date is the most important security measure, more so even than installing anti-virus software. This applies to any firewalls you install.

Most operating system include a host-based firewall, which is probably adequate for most home users with a network-based firewall between their LAN and the Internet. However, aftermarket software is available from many anti-virus vendors, and you may wish to consider one of these, especially if you have a laptop with sensitive information and use it at public Wi-Fi hot spots. Regardless of how you use it, check your firewall’s documentation to be sure it’s properly configured for you situation.

You can implement a network-based firewall in three different ways:

* purchase purpose-built hardware, probably with an integrated router,
* install firewall software on a compact PC such as a Raspberry Pi, and
* install firewall software on a standard PC.

The first is the easiest and by far the most preferable, as it’s ready to use right out of the box after minimal configuration. The second requires more work and expertise but can result in a unit that is at least as effective, but few users have the expertise needed to insure the security that this application requires. The third is unlikely to be satisfactory, as PCs have hard disks, monitors, and keyboards which aren’t needed here, and you will be tempted to use a surplus one that probably has an old operating system with many known vulnerabilities. You will also have to remove many programs that were needed in its former role as a general-purpose PC but may have security risks. For firewall duty you want simple hardware and software and the latest version of the latter.

A good firewall tutorial is available at http://computer.howstuffworks.com/firewall.htm and a more technical one at <http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf> .