

What is a Hardware Firewall and Which Hardware Firewall is Best?

If you have more than three computers in your home or business that share the same internet connection, a hardware firewall is something you may want to consider. A hardware firewall is a device that sits in between the internet and your network, protecting all computers on the inside from dangerous intruders on the outside.

As opposed to a software firewall (also known as a personal firewall), a hardware firewall is designed to protect ALL the computers on a network instead of just one PC. It is generally more efficient and cost-effective to purchase a hardware firewall (as opposed to several software firewalls) if you have three or more computers you need to protect.

A hardware firewall is a special device that is designed to prevent outside intruders from getting into your network (where they can then easily get into your PC's and servers). Firewalls can be configured to prevent access to certain types of applications that are considered dangerous (like P2P file-sharing programs) by blocking the communication ports that these applications use. A firewall will also provide some protection against hidden spyware infections, as it can help stop outgoing data packets that an infected PC may be sending to a cyber-criminal.

A firewall is considered to be the first line of defense in protecting computers from unwanted "visitors" such as hackers, worms, and remote control applications via hidden spyware. Without firewall protection your network is an "open door" to the internet, and anyone (or anything) can easily come in and out. Even if you don't have any important files to protect, hackers and curious intruders can easily kill all your computers, take control of your network, or damage hardware beyond repair. The small investment in a firewall is nothing compared to the cost of replacing or repairing computer equipment as the result of an intruder's visit.

Hardware firewalls use various techniques to protect your network against intruders and other internet threats. All firewall rules can be configured to apply to outbound or inbound traffic, so giving you a lot of flexibility and control in how the firewall works. Hardware firewalls can be simple or very complex, depending on the size of the network they are designed to protect. High-end corporate firewalls should be installed by a certified technician, but most home office and small business firewalls can be set up by anyone with a general understanding of networking and good technical ability.

Most hardware firewalls use some form of packet filtering, which is somewhat like a "checklist". Certain types of data packets are allowed through, and others may be blocked. If a packet attempting to travel in or out of a network meets the criteria set for "blocked", it is not allowed to pass.

Another technique that is often used with hardware firewalls is called Stateful Packet Inspection, also known as SPI. With SPI, a hardware firewall analyzes additional characteristics of the data packet in order to determine what to do with it. It checks to see where the packet came from, if it was sent as a response to a user request for information, if it just "appeared" out of nowhere, etc... Combined with packet filtering, SPI really makes a firewall appliance "smart", as it can make decisions whether to block or allow data packets based on logical analysis.

Depending on the type of network they are designed for, hardware firewalls can cost anywhere from \$100 for a home firewall appliance up to several thousand dollars for an enterprise-class device. Simple (easy to install and configure) hardware firewalls designed for home use are offered by D-Link, Linksys, and NetGear. SonicWall and HotBrick are very popular hardware firewalls for small and medium businesses.

For more information, see my [Hardware Firewalls](#) page. Another good resource for firewall information is [Virus&Spam at bellonline.com](#)

Article Source: http://EzineArticles.com/?expert=Debbie_Jacobsen