**What Firewall Does**

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private [network](https://computer.howstuffworks.com/home-network.htm) or [computer system](https://computer.howstuffworks.com/). If an incoming packet of information is flagged by the filters, it is not allowed through.

A firewall helps protect computers inside a large company. Let's say that you work at a company with 500 employees. The company will therefore have hundreds of computers that all have network cards connecting them together. In addition, the company will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall in place, all of those hundreds of computers are directly accessible to anyone on the Internet. A person who knows what he or she is doing can probe those computers, try to make FTP connections to them, try to make telnet connections to them and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit the hole.

With a firewall in place, the landscape is much different. A company will place a firewall at every connection to the Internet. The firewall can implement security rules.

A company can set up rules like this for FTP servers, Web Servers, Telnet servers and so on. In Addition, the company can control how employees connect to web sites, Whether files are allowed to leave the company over the network and so on. A firewall gives a company tremendous control over how people use the network.

Firewalls use 3 methods to control traffic flow over network:

**Packet Filtering**- Packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.

**Proxy Service** – Information from the Internet is retrieved by the firewall and then sent tio the requesting system.

**Stateful inspection** – A newer method that doesn’t examine the content of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to outside is monitored for specific defining characteristics, then the incoming information is compared to these characteristics