

# Firewalls

A firewall is basically a barrier that keeps destructive forces away from the computer. The name *firewall* is derived from the real firewalls in buildings that keep fires from spreading to other parts of a building.

Firewalls are used in schools and companies to control how students and employees connect to websites. Network managers define the rules for the firewalls and determine which sites users may access. Firewalls give network administrators tremendous control over how people use their networks.

## The four basic types of firewalls:

1. **Packet Filtering** – packets (small chunks of data) are checked against a list of filters set up by the network administrator. If the packets do not meet the filters, they are discarded or blocked.
2. **Circuit level gateways** – data is only allowed into the network based on requests that were sent out of the network. The firewall remembers the requests, and matches them with the incoming data.
3. **Application level gateways** – Proxies – information from the Internet is retrieved by the firewall and then sent to the requesting computer and vice versa.
4. **Stateful inspection** – A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Data traveling out is monitored for specific characteristics, and then the data coming in is compared to those characteristics.

## **Firewalls can protect against:**

1. **Remote logins** – when someone can connect to a user's computer and control it in some form.
2. **Application backdoors** – some programs have hidden features that allow for remote access.
3. **Operating system bugs** – some operating systems have backdoors as well.
4. **Email bombs** – when someone sends a user thousands of emails to fill up and block the account.
5. **Macros** – these are programming code scripts created to make a task shorter. Hackers have created macros that can destroy all data or crash a computer.
6. **Viruses** – firewalls help to keep viruses from spreading in a network.
7. **Spam** – firewalls often protect emails from junk email messages.
8. **Source routing** – hackers can specify which ports and routers they want the data to take through a network. Most firewalls disable this.