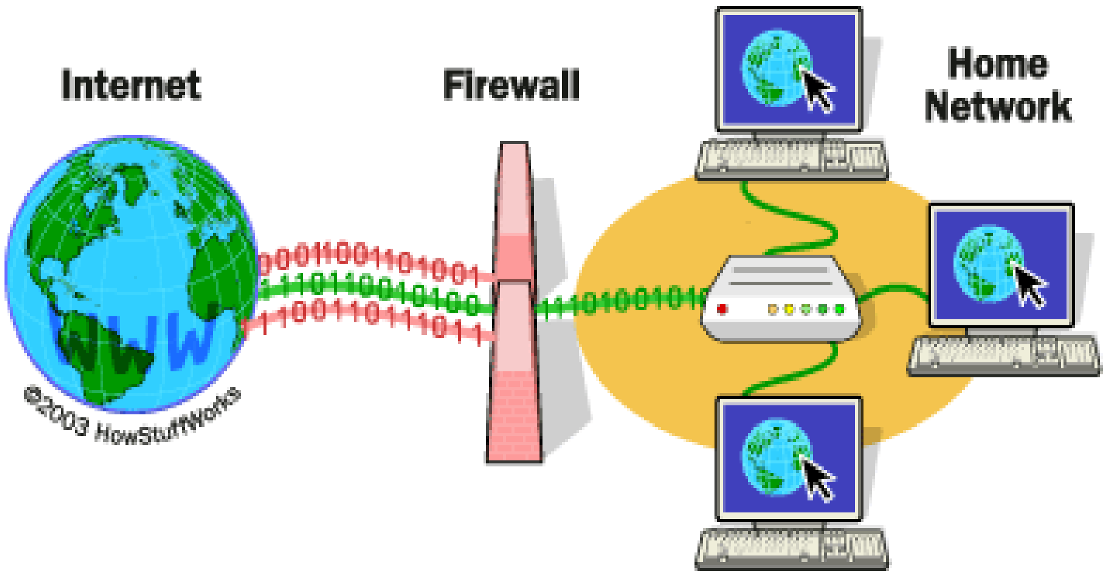
Firewall

Introduction

- A firewall is a utility program (or it can also be a hardware device) that filters the information coming through the Internet connection into your personal computer or into a company's network.

- Its main aim is to safe network from different threats

- For example, a firewall typically exists between a corporate network and a public network like the Internet.
- It can also be used inside a private network to limit access to different parts of the network



- **firewalls work** like a filter between your computer/network and the Internet.

Working

- Firewalls use 3 types of filtering mechanisms:
- **Packet filtering or packet purity**

  Data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets.
- **Proxy**

  Firewalls in this case assume the role of a receiver and in turn sends it to the node that has requested the information & vice versa.
- **Inspection**

  In this case Firewalls instead of examining through all of the information in the packets, mark key features in all outgoing requests & check for the same matching characteristics in the inflow to decide if it relevant information that is coming through.

Firewall Rules

- **IP Addresses**

Blocking off a certain IP address or a range of IP addresses, which you think are destructive.

- **Domain names**

You can only allow certain specific domain names to access your systems/servers or allow access to only some specified types of domain names or domain name extension like .edu or .mil.

- **Protocols**

A firewall can decide which of the systems can allow or have access to common protocols like IP, SMTP, FTP, UDP.

- **Ports**

Blocking or disabling ports of servers that are connected to the internet will help maintain the kind of data flow you want to see it used for.

- **Keywords**
  Firewalls also can filter through the data flow for a match of the keywords or phrases to block out offensive or unwanted data from flowing in.

Examples

- McAfee Internet Security
- Microsoft Windows Firewall
- Norton Personal Firewall
- Trend Micro PC-cillin
- ZoneAlarm Security Suit

Types of firewall

- **Software firewalls**
- New generation Operating systems come with built in firewalls or you can buy a firewall software for the computer that accesses the internet or acts as the gateway to your home network.

- **Hardware firewalls**
- Hardware firewalls are usually routers with a built in Ethernet card and hub. Your computer or computers on your network connect to this router & access the web.

Summary

- Firewalls are a must have for any kind of computer usage that go online. They protect you from all kinds of unauthorized access like trojans that allow taking control of your computers by remote logins or backdoors, virus or use your resources to launch DOS attacks.