Firewall - A Comprehensive Overview

What is a Firewall ?

A Firewall is a system that is designed to prevent unauthorized access from entering a private network by filtering the information that comes from the internet (i.e. a firewall blocks unwanted traffic and allows wanted traffic). Hence, a firewall creates a safety barrier between a private network and the public internet. The firewall examines each message to make sure it meets a predetermined security criteria before allowing it through.

Firewalls are essentially useful for large organizations and businesses which posses data servers and resources in a private network to protect their network from devious hackers. Firewalls are also used by individuals to secure their stand alone systems.

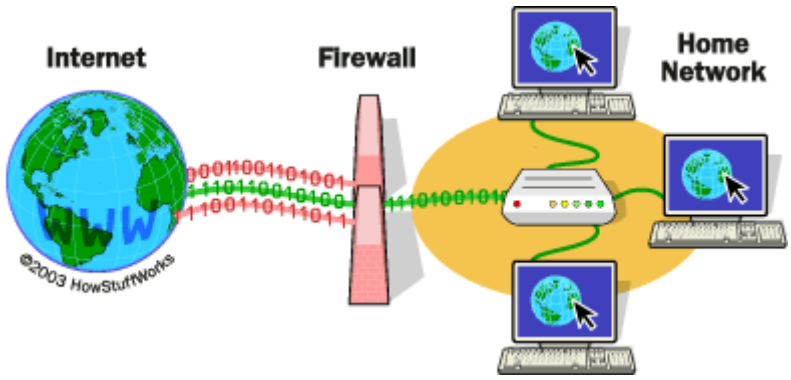

Fig-2: A firewall allowing(green) / blocking(red) IP's according to access control list

Why do we even need firewall ?

Every computer system connected to internet is susceptible to following attacks (courtesy of malicious hackers) :

- *Remote login*
- *Application backdoors*
- *Session Hijacking*
- *Operating System Bugs*
- *Denial of Service*
- *Viruses*
- *Spam*
- *Redirect Bombs*
- *Source routing*

By establishing the right level of security, all these threats can be neutralized using a firewall alone !

How does a firewall know which network data is safe ?

It maintains an **Access Control List** which is just a set of rules that helps the firewall determine whether a network data is allowed to enter the private network or not. It not only contains information about *what can enter a network* but also *what can leave a network*. These rules are customizable and are decided and managed by **Network Administrator**.

Firewall rules can be based on :

- **IP Addresses** - Allow 10.10.20.32 but block 54.21.66.112
- **Domain Names** - Allow www.google.com but deny www.bing.com
- **Protocols** - Allow all TCP traffic but block UDP traffic
- **Programs** - Allow program A but deny access to program B
- **Ports** - Allow data using port 80 but block data using port 94
- **Key Words** - Block data that contains key words in the list {violence, gun, bomb, ...}

Firewalls use the following techniques to regulate network data :

- **Packet Filtering** - Data packets are matched against a a set of rules.
- **Proxy Service** - Network data is sent and receive between internet and host via firewall
- **Stateful Inspection** - Compares the key information of packet with a trusted database

---

Let's take an example !

Consider the following Access Control List :

Permission	IP Address	Protocol	Destination	Port
ALLOW	162.213.214.140	TCP	ANY	80
ALLOW	54.21.66.112	TCP	ANY	80
DENY	40.55.130.66	TCP	ANY	80

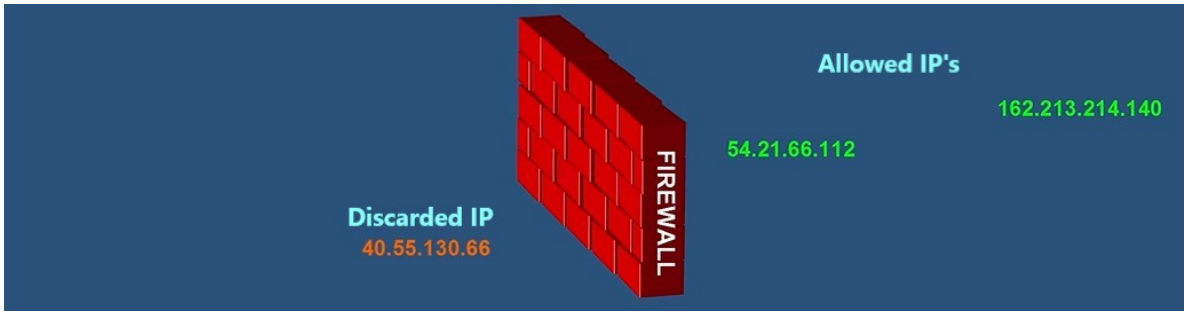

Fig-2: A firewall allowing(green) / blocking(red) IP's according to access control list

---

Types of Firewall

1. **Host-Based Firewall** - It is a **software** firewall that is installed on a computer/host. **It protects the host alone**. For example the built is host based firewall in windows operating system. There are also some 3rd Party host-based firewall in the market such as Zone Alarm etc. A lot of antivirus programs come with a host-based firewall.
2. **Network-Based Firewall** - It is a **combination of hardware and software** and operates at network layer. A network-based firewall is placed between the private network and the public network and it **protects the entire network** unlike host-based firewalls. These can be a stand alone application, a built in software in routers or deployed on a cloud infrastructure.

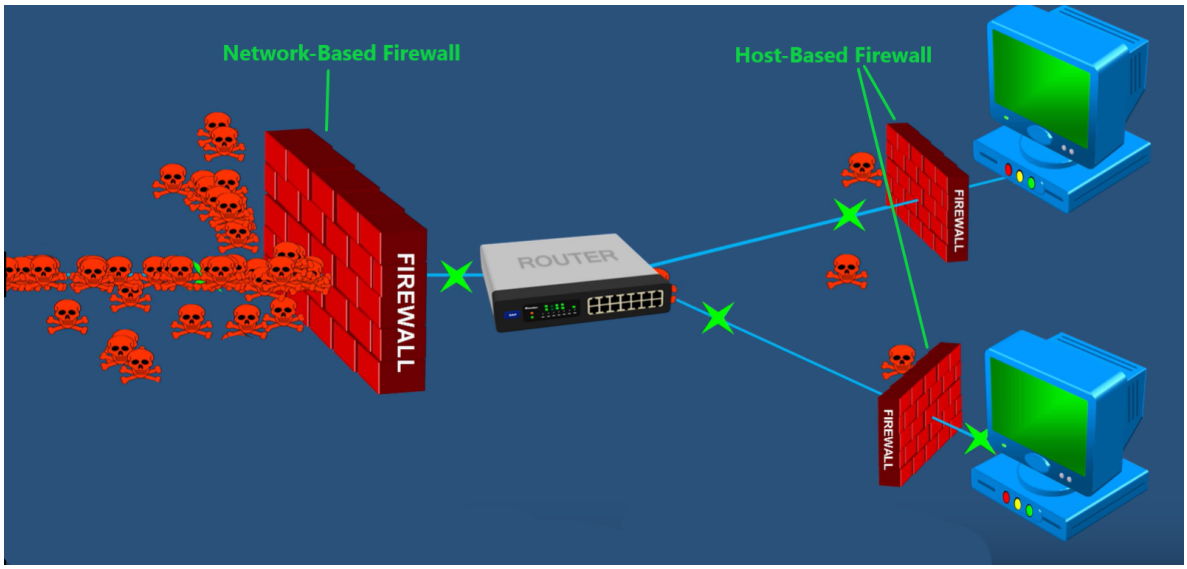

Fig-3: Types of Firewall

NAT (Network Address Translation)[^4]

All private networks are allocated an IP Address by DSL or ISP companies. However, a single private network may contain thousands of hosts. How is this possible ? How can multiple systems be addressed using same IP ? Actually, they don't ! Every private network is allocated 24 million **internal IP addresses**. The **external or actual IP Address** is then converted to internal address and the data packet is forwarded to the specific host. This conversion is done by firewall and is called **Network Address Translation**.

NAT essentially allows a public internet user to send a packet to a private network user using the actual IP address while protecting the internal addresses of the hosts within the private network.
