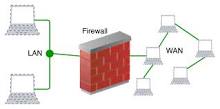
**What is Firewall?**

To revisit, it’s a device used for network security. It monitors network traffic – both incoming and outgoing – to either allow or block data packets based on its security rules.

Its purpose is to create a barrier between your internal network and traffic that flows in from external sources – like the rest of the internet. This blocks hackers, viruses and other malicious traffic.

There are pre-set rules to analyze and filter traffic, rerouting data that comes from suspicious or unsecured sources in order to prevent attacks on your network

****

## **Types of Firewalls**

There are several types of firewalls, and the one you use will depend on your specific needs (single device vs. network or server protection).

### Software vs. Hardware

All firewalls fall into one of two main categories: software or hardware firewalls. It’s best to have both for the utmost protection, but some people may have one or the other. Either way, both types of firewalls provide a barrier between your computer and the rest of the internet.

* **Software:** This type of firewall is a program that’s installed on your computer. It will regulate traffic through applications and ports to do things like monitor and manage users, generate logs and block applications.
* **Hardware:** This physical type of firewall is actual equipment that’s located between the gateway and your network. Your router is a type of hardware firewall, though there are more dedicated devices for larger-scale purposes.

**Types of Firewalls**

A firewall can either be software or hardware. Software firewalls are programs installed on each computer, and they regulate network traffic through applications and port numbers. Meanwhile, hardware firewalls are the equipment established between the gateway and your network. Additionally, you call a firewall delivered by a cloud solution as a cloud firewall.

There are multiple types of firewalls based on their traffic filtering methods, structure, and functionality. A few of the types of firewalls are:

**Packet Filtering**

packet filtering firewall controls data flow to and from a network. It allows or blocks the data transfer based on the packet's source address, the destination address of the packet, the application protocols to transfer the data, and so on.

**Proxy Service Firewall**

This type of firewall protects the network by filtering messages at the application layer. For a specific application, a proxy firewall serves as the gateway from one network to another.

Stateful Inspection

Such a firewall permits or blocks network traffic based on state, port, and protocol. Here, it decides filtering based on administrator-defined rules and context.

Next-Generation Firewall

According to Gartner, Inc.’s definition, the next-generation firewall is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and information from outside the firewall to go beyond port/protocol inspection and blocking.

Unified Threat Management (UTM) Firewall

A UTM device generally integrates the capabilities of a stateful inspection firewall, intrusion prevention, and antivirus in a loosely linked manner. It may include additional services and, in many cases, cloud management. UTMs are designed to be simple and easy to use.

Threat-Focused NGFW

These firewalls provide advanced threat detection and mitigation. With network and endpoint event correlation, they may detect evasive or suspicious behavior.

Application Layer Firewalls

These firewalls can examine application layer (of OSI model) information like an HTTP request. If finds some suspicious application that can be responsible for harming our network or that is not safe for our network then it gets blocked right away.

How Does a Firewall Work?

As mentioned previously, firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer’s entry point which only allows trusted sources, or IP addresses, to enter your network.

A firewall welcomes only that incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rule.

Advantages of Using Firewalls

Now that you have understood the types of firewalls, let us look at the advantages of using firewalls.

* Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.
* It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet. Firewalls provide faster response time and can handle more traffic loads.
* A firewall allows you to easily handle and update the security protocols from a single authorized device.
* It safeguards your network from phishing attacks.

How to Use Firewall Protection?

To keep your network and devices safe, make sure your firewall is set up and maintained correctly. Here are some tips to help you improve your firewall security:

* Constantly update your firewalls as soon as possible: Firmware patches keep your firewall updated against any newly discovered vulnerabilities.
* Use antivirus protection: In addition to firewalls, you need to use antivirus software to protect your system from viruses and other infections.
* Limit accessible ports and host: Limit inbound and outbound connections to a strict whitelist of trusted IP addresses.
* Have active network: To avoid downtime, have active network redundancies. Data backups for network hosts and other critical systems can help you avoid data loss and lost productivity in the case of a disaster.