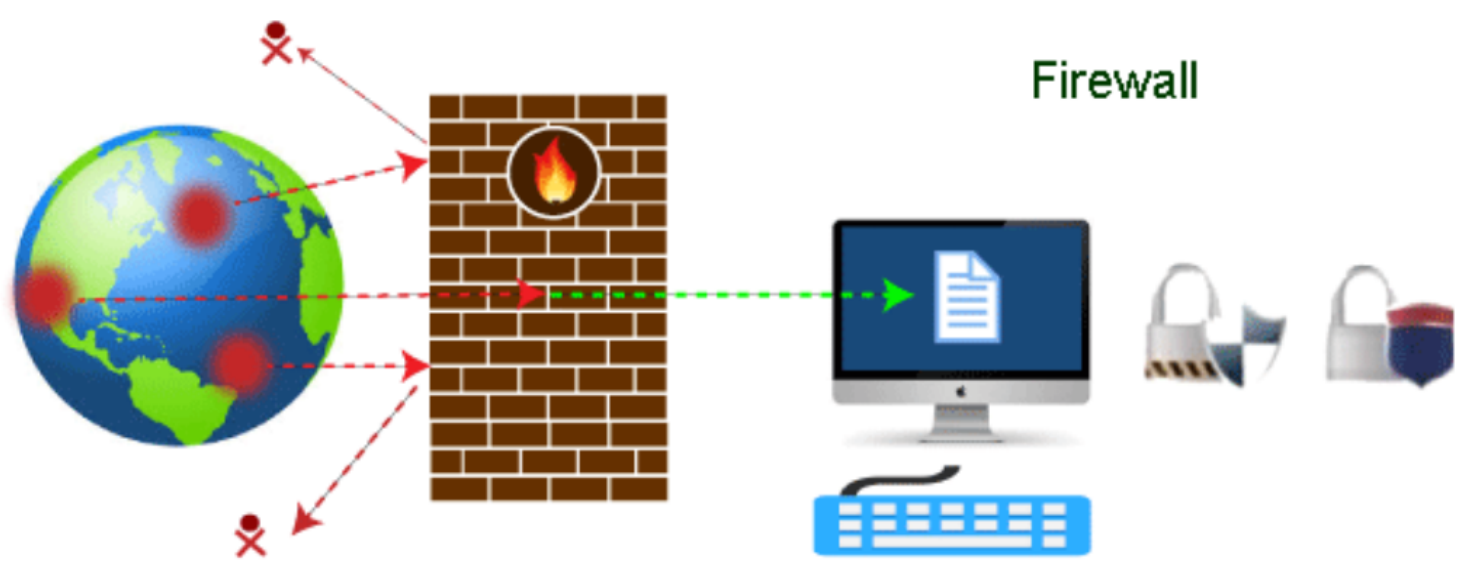


What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.



Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., **hardware** and **software**, though it's best to have both.

Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a **computer network** and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

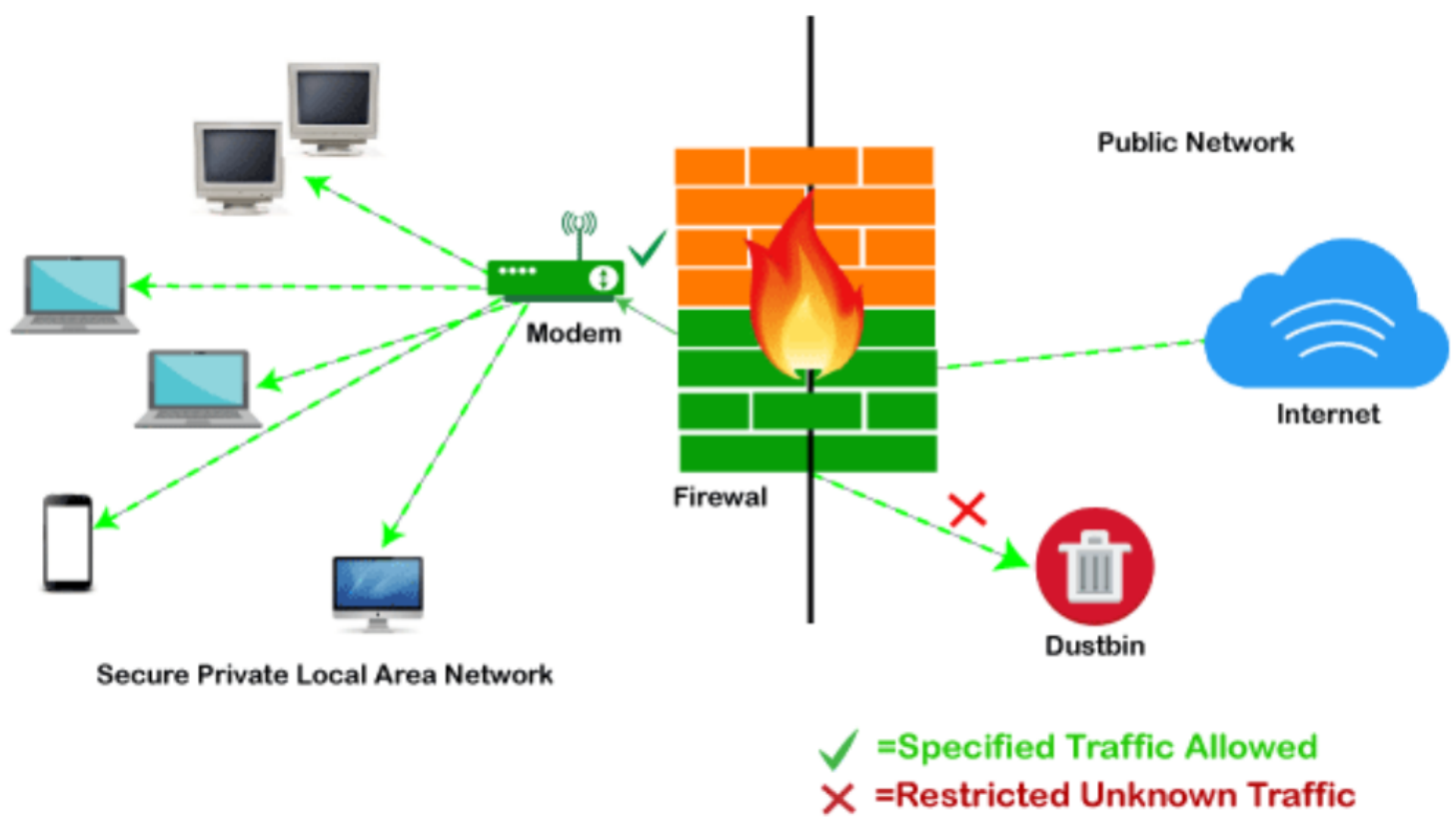
Why Firewall

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

How does a firewall work?

A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.

Typically, firewalls intercept network traffic at a computer's entry point, known as a port. Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules. Incoming traffic is allowed only through trusted IP addresses, or sources.



As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.

Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller. Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

The importance of using firewalls as a security system is obvious; however, firewalls have some limitations:

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.

Difference between a Firewall and Anti-virus

Attributes	Firewall	Anti-virus
Definition	A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.	Anti-virus is defined as the special type of software that acts as a cyber-security mechanism. The primary function of Anti-virus is to monitor, detect, and remove any apprehensive or distrustful file or software from the device.
Structure	Firewalls can be hardware and software both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall.	Anti-virus can only be used as software. Anti-virus is a program that is installed on the device, just like the other programs.

Implementation	Because firewalls come in the form of hardware and software, a firewall can be implemented either way.	Because Anti-virus comes in the form of software, therefore, Anti-virus can be implemented only at the software level. There is no possibility of implementing Anti-virus at the hardware level.
----------------	--------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Responsibility	A firewall is usually defined as a network controlling system. It means that firewalls are primarily responsible for monitoring and filtering network traffic.	Anti-viruses are primarily responsible for detecting and removing viruses from computer systems or other devices. These viruses can be in the form of infected files or software.
Scalability	Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.	Anti-viruses are generally considered less-scalable than firewalls. This is because anti-virus can only be implemented at the software level. They don't support hardware-level implementation.

Threats	<p>A firewall is mainly used to prevent network related attacks. It mainly includes external network threats?for example- Routing attacks</p>	<p>Anti-virus is mainly used to scan, find, and remove viruses, malware, and Trojans, which can harm system files and software and share personal information (such as login credentials, credit card details, etc.) with hackers.</p>
---------	-----------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------