Firewall

Introduction

- A firewall is a security device that can help protect your internet network by filtering unknown traffic and blocking outsiders from gaining access to your private data.

- We’ve all heard about the dangers of clicking on unknown links or pop-up ads while browsing the internet, but is that really enough to keep your devices and network secure? A firewall should be your first line of defense to protect your network and data.

- Firewalls help filter and block potential hackers from accessing your sensitive data, and there are many types of firewalls that use different strategies to keep your information safe. Read on to learn everything you need to know about firewalls and why they’re so important.

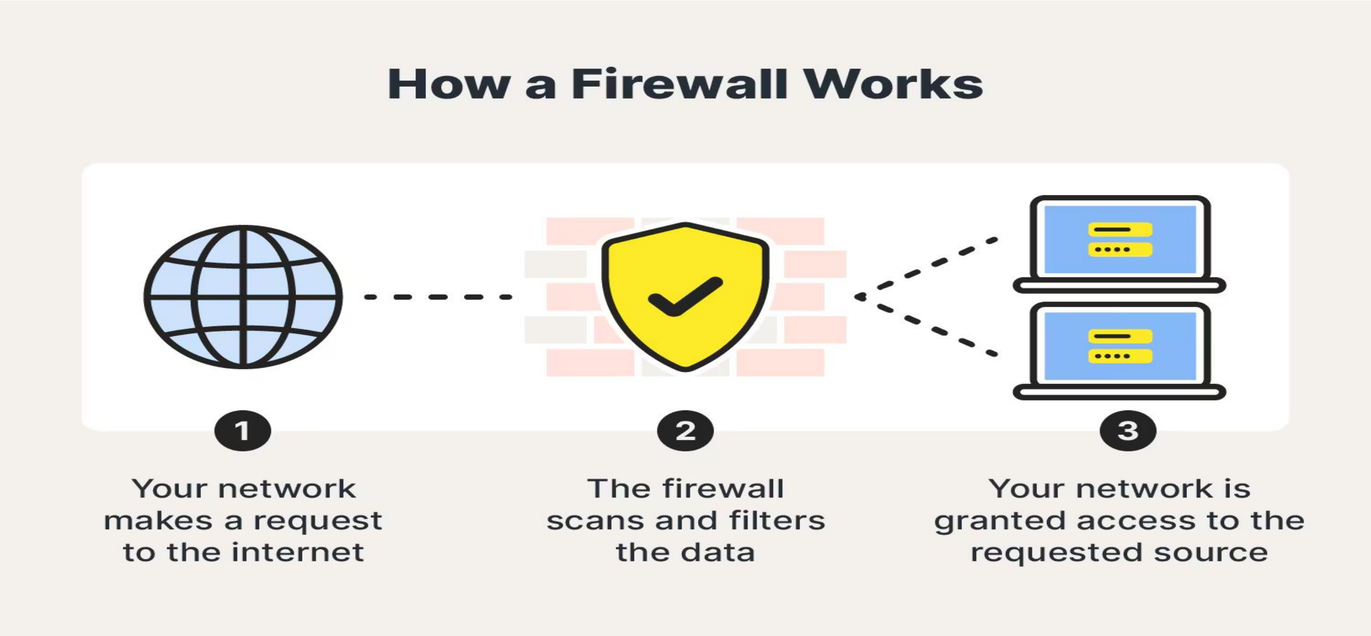
Firewall defined

- A firewall is a security device that can help protect your internet network by filtering unknown traffic and blocking outsiders from gaining access to your private data. Firewalls can provide protection through computer hardware or software

- Firewalls protect your computer from malicious software as well, which can create all sorts of security issues.

- Firewalls can provide different levels of protection. The key is determining how much protection you need.

How does a firewall work?



How a Firewall Works

1. Your network makes a request to the internet

2. The firewall scans and filters the data

3. Your network is granted access to the requested source

- A firewall works at your computer’s entry point, or port. Only trusted sources, or IP addresses, are allowed in. IP addresses are important because they identify a computer or source.

- Along with screening IP addresses, firewalls have other advanced internal rules they follow to determine whether or not a trusted source is trying to access your computer.

Terminologies

Packet:

- A unit of data transmitted over a network. Firewalls inspect packets to determine if they should be allowed or blocked based on security rules.

IP Address:

- A unique identifier assigned to devices on a network. Firewalls use IP addresses to filter and control traffic.

Port Number:

- A numerical identifier in a network packet used to specify a particular service or application. Firewalls can block or allow traffic based on port numbers.

Protocol:

- A set of rules governing the format and transmission of data. Common protocols include TCP, UDP, HTTP, and FTP. Firewalls can filter traffic based on these protocols.

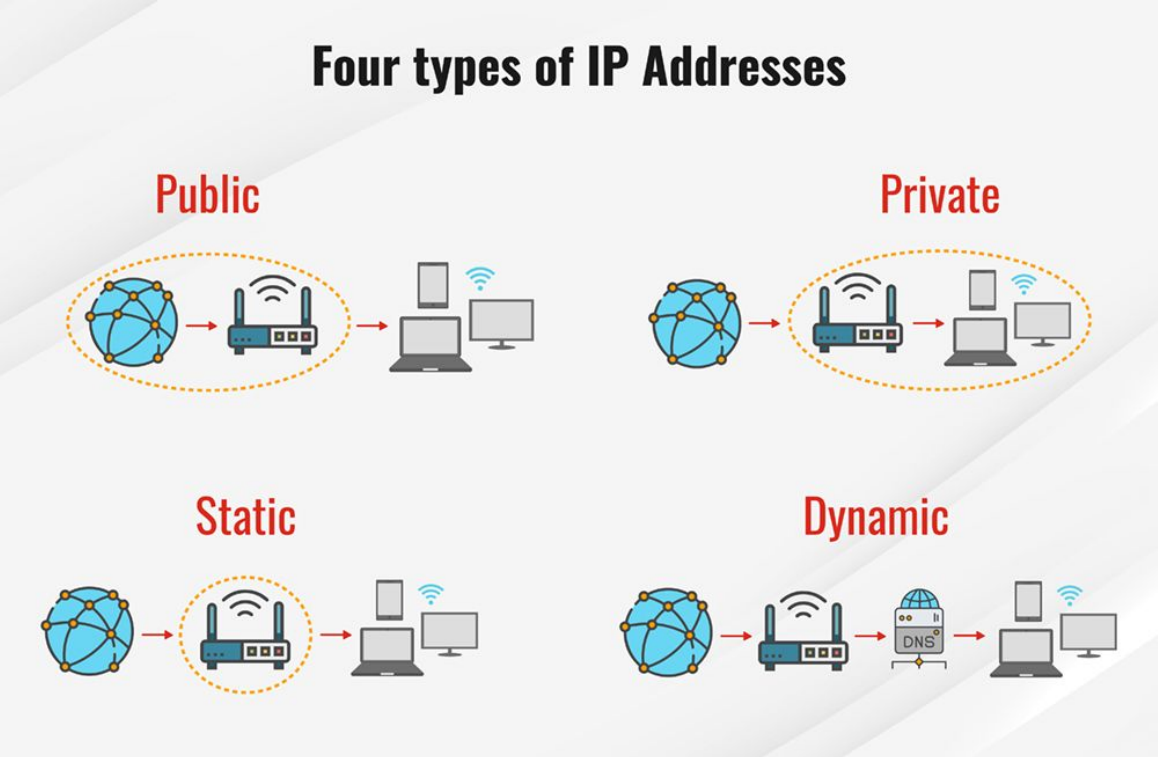
Ip address

- An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate. Computers that communicate over the internet or via local networks share information to a specific location using IP addresses.

IP addresses have two distinct versions or standards.

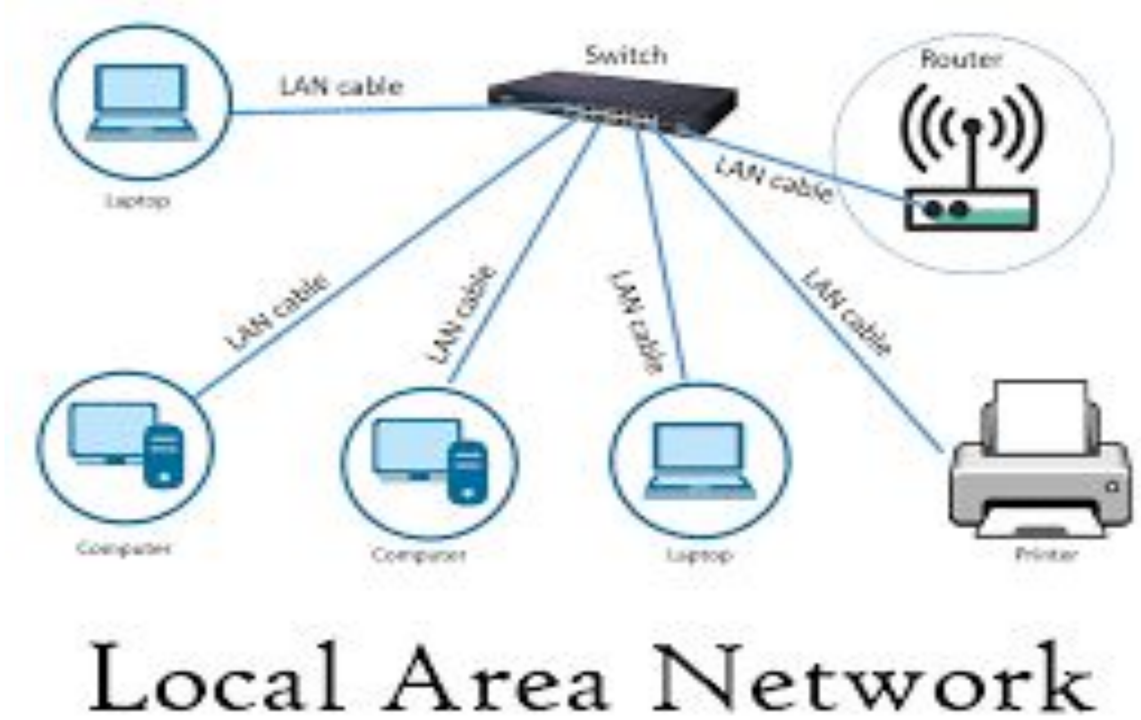
- **The Internet Protocol version 4 (IPv4)** address is the older of the two, which has space for up to 4 billion IP addresses and is assigned to all computers.
- **Recent Internet Protocol version 6 (IPv6)** has space for trillions of IP addresses, which accounts for the new breed of devices in addition to computers.

Types of Ip address



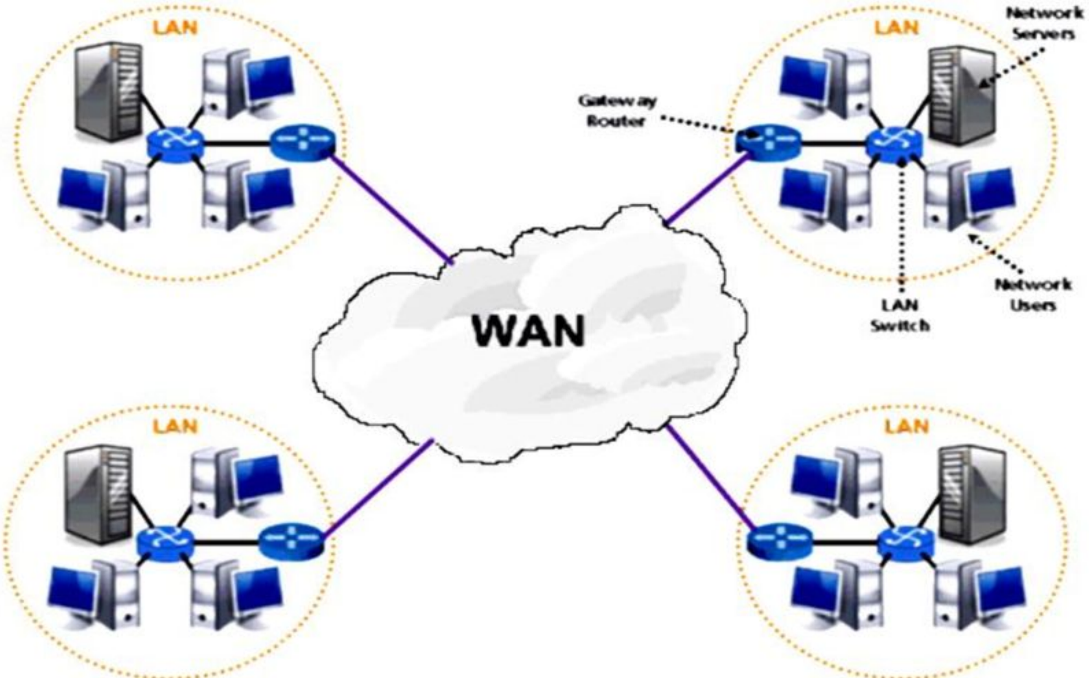
LAN

- A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.



WAN

- A wide-area network (WAN) is the technology that connects your offices, data centers, cloud applications, and cloud storage together.
- The world’s largest WAN is the internet because it is a collection of many international networks that connect to each other.



Internet traffic

- Network traffic is the amount of data moving across a computer network at any given time. Network traffic, also called data traffic, is broken down into data packets and sent over a network before being reassembled by the receiving device or computer.
- **Web Traffic**:
  - **HTTP/HTTPS**: Traffic generated by web browsers and servers using the Hypertext Transfer Protocol (HTTP) and its secure version (HTTPS) to access websites and web applications.
- **Email Traffic**:
  - **SMTP, IMAP, POP3**: Traffic generated by email services. Simple Mail Transfer Protocol (SMTP) is used for sending emails, while Internet Message Access Protocol (IMAP) and Post Office Protocol version 3 (POP3) are used for retrieving emails from servers.
- **File Transfer Traffic**:
  - **FTP, SFTP**: Traffic generated by file transfer services. File Transfer Protocol (FTP) and its secure version (SFTP) are used to upload and download files between clients and servers.

Ip header

- An IP header is header information at the beginning of an Internet Protocol (IP) packet. An IP packet is the smallest message entity exchanged via the Internet Protocol across an IP network.
- IP packets consist of a header for addressing and routing, and a payload for user data.
- The header contains information about IP version, source IP address, destination IP address, time-to-live, etc.

Key Components of an IP Header:

- **Version**: Specifies the IP version (IPv4 or IPv6).
- **Header Length (IHL)**: Indicates the length of the IP header.
- **Type of Service (ToS)**: Defines the quality of service and priority of the packet.
- **Total Length**: The total length of the packet, including header and data.
- **Identification**: Used for uniquely identifying fragments of an original IP packet.

TCP header

The transmission control protocol (TCP) is the internet standard ensuring the successful exchange of data packets between devices over a network. TCP is the underlying communication protocol for a wide variety of applications, including web servers and websites, email applications, FTP and peer-to-peer apps.

The 10 TCP header fields are as follows:

- Source port – The sending device’s port.
- Destination port – The receiving device’s port.
- Sequence number – A device initiating a TCP connection must choose a random initial sequence number, which is then incremented according to the number of transmitted bytes.
- Acknowledgment number – The receiving device maintains an acknowledgment number starting with zero. It increments this number according to the number of bytes received.
- TCP data offset – This specifies the size of the TCP header, expressed in 32-bit words. One word represents four bytes.