# PANDIT DEENDAYAL ENERGY UNIVERSITY

## SCHOOL OF TECHNOLOGY

**Course: Cyber security**

**Course Code: 20CP316P**

**LAB MANUAL**

**B.Tech. (Computer Science and Engineering)**

**Semester 6**

**Submitted To:**

Dr. Kaushal Shah

**Submitted By:**

Dhruv Bhanderi(20BCP025-G1G2)
Meet Mehta(20BCP126-G1G2)
Arpit Dobariya(20BCP022-G1G2)

# What is firewall?

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules and policies. It is a software or hardware solution that helps to protect a computer or network from unauthorized access, attacks, and malicious activity. Firewalls can be used to block unwanted traffic and allow only authorized traffic to pass through, and they are often the first line of defense in a network security strategy.

# Why to use firewall?

Firewalls are used to protect networks and devices from unauthorized access and malicious activity. They can help to prevent hackers from gaining access to sensitive information, block malware and viruses from entering a network, and protect against denial-of-service (DoS) attacks. Firewalls can also be used to control access to specific resources, such as websites or applications, and to limit the types of network traffic that are allowed through. Additionally, firewalls can be used to monitor network activity and generate logs that can be used to detect and troubleshoot security incidents. Overall the main reasons to use a firewall are:

1. To block unauthorized access to your network and devices
2. To protect against malware and viruses
3. To prevent denial-of-service (DoS) attacks
4. To control access to specific resources
5. To monitor network activity and detect security incidents

# Hardware firewall vs Software firewall:

A hardware firewall and a software firewall are both types of firewalls that are used to protect networks and devices from unauthorized access and malicious activity. However, they work in slightly different ways.

A hardware firewall is a physical device that is installed on a network and is responsible for monitoring and controlling incoming and outgoing network traffic. Hardware firewalls are typically placed at the perimeter of a network and are responsible for protecting the entire network from unauthorized access. They are usually easy to set up and manage, and can be used to control access to specific resources, such as websites or applications.

A software firewall, on the other hand, is a program that runs on a computer or other device and is responsible for monitoring and controlling incoming and outgoing network traffic. Software firewalls are typically installed on individual host devices, such as computers or servers, and are responsible for protecting those specific devices from unauthorized access. They can be more flexible and configurable than hardware firewalls, as they can be tailored to the specific needs of a device or network.

Both hardware and software firewalls have their own benefits and limitations, depending on the specific use case. Hardware firewalls are generally more powerful and can provide more comprehensive protection for large networks, while software firewalls are more flexible and can provide more targeted protection for individual devices.

# Types of firewall:

There are several types of firewalls, each with its own strengths and weaknesses. Some of the most common types of firewalls include:

1. Network firewalls: These are the most common type of firewall and are used to protect a network from unauthorized access. Network firewalls can be hardware-based or software-based and are typically placed at the perimeter of a network to control incoming and outgoing traffic.

2. Host-based firewalls: These firewalls are installed on individual host devices, such as computers or servers, and protect those specific devices from unauthorized access.
3. Application firewalls: These firewalls are used to control access to specific applications or services. They can be used to block unwanted traffic and allow only authorized traffic to pass through.
4. Next-generation firewalls (NGFWs): These are advanced firewalls that combine traditional firewall features with additional capabilities such as intrusion prevention, application control, and advanced threat protection.
5. Stateful Inspection firewalls: These firewalls keep track of the state of network connections and use that information to make decisions about whether or not to allow traffic through.
6. Packet filtering firewalls: These firewalls inspect the headers of packets passing through the network and make decisions about whether or not to allow those packets through based on predefined rules.
7. Proxy firewalls: These firewalls act as intermediaries between a device and the internet, and all incoming and outgoing traffic must pass through the firewall. This allows the firewall to inspect and control all traffic.

## How does firewall works?

Firewalls work by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules and policies. They can be used to block unwanted traffic and allow only authorized traffic to pass through.

When network traffic attempts to pass through a firewall, the firewall inspects the traffic to determine if it meets the security rules and policies that have been set up. Depending on the type of firewall, this inspection process may involve looking at the headers of packets, analyzing the contents of the packets, or checking the state of network connections.

If the traffic meets the security rules and policies, the firewall allows it to pass through to the intended destination. If the traffic does not meet the security rules and policies, the firewall blocks it, preventing it from reaching its destination.

Firewalls can also be used to control access to specific resources, such as websites or applications, and to limit the types of network traffic that are allowed through. They can also be used to monitor network activity and generate logs that can be used to detect and troubleshoot security incidents.

In summary, a firewall's main job is to inspect the network traffic and based on the predefined security rules and policies, it either allows the traffic to pass through or blocks it.

# Functions of firewall:

A firewall has several key functions that help to protect networks and devices from unauthorized access and malicious activity. Some of the main functions of a firewall include:

1. Traffic filtering: Firewalls monitor incoming and outgoing network traffic and make decisions about whether or not to allow that traffic to pass through based on predefined security rules and policies. This helps to block unwanted traffic and allow only authorized traffic to pass through.
2. Access control: Firewalls can be used to control access to specific resources, such as websites or applications. This can help to prevent unauthorized access to sensitive information and resources.
3. Malware and virus protection: Firewalls can be configured to block traffic from known malicious sources, such as known malware or virus-infected hosts. This can help to protect networks and devices from malware and viruses.
4. Intrusion detection and prevention: Firewalls can be configured to detect and prevent intrusions by monitoring for and alerting on suspicious activity, such as failed login attempts or abnormal traffic patterns.
5. Logging and monitoring: Firewalls can be configured to generate logs of network activity, which can be used to detect and troubleshoot security incidents.

6. Network Address Translation (NAT): Firewalls can be used to hide internal IP addresses from the external network and translate internal IP addresses to a single public IP address.
7. VPN support: Some firewalls can support and terminate VPN connections, allowing remote users to connect to the internal network securely.

In summary, a firewall's main function is to monitor and control network traffic, ensuring that only authorized traffic is allowed to pass through, while blocking malicious or unwanted traffic, providing an additional layer of security to the network.