SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ECT301 – COMMUNICATION NETWORK

III B.E. ECE / V SEMESTER

UNIT 4 –NETWORK & DATA SECURITY

TOPIC – FIREWALL

INVENTION

- The first firewall proposal, or packet filter, came in 1989 by Jeff Mogul of Digital Equipment Corp. (DEC), marking, therefore, the first generation.

FIREWALL

- A firewall in a communication network is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

- Its primary purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet.

TYPES OF FIREWALL NETWORK

1) **Packet Filtering Firewalls**
2) **Stateful Inspection Firewalls**
3) **Proxy Firewalls**
4) **Next-Generation Firewalls (NGFW)**

➢Firewalls play a critical role in securing networks by preventing unauthorized access, protecting against cyberattacks, and enforcing security policies. They are a fundamental component of a layered security approach in modern communication networks.

TYPES OF FIREWALL NETWORK

1) **Packet Filtering Firewalls:** These examine packets of data and decide whether to allow or block them based on predefined rules, such as source and destination IP addresses, port numbers, and protocols.

2) Stateful Inspection Firewalls: These keep track of the state of active connections and make decisions based on the context of the traffic. They are more sophisticated than packet filtering firewalls because they understand the state of the connection.

TYPES OF FIREWALL NETWORK

3) Proxy Firewalls: These act as intermediaries between clients and servers, forwarding requests on behalf of the clients. They can hide the internal network structure and provide an additional layer of security by filtering and inspecting traffic at the application layer.

4) Next-Generation Firewalls (NGFW): These integrate additional features beyond traditional firewalls, such as intrusion prevention systems (IPS), deep packet inspection, and application-layer filtering. NGFWs provide more advanced threat detection and prevention capabilities.

ADVANTAGE & DIS ADVANTAGE

ADVANTAGES:

Access Control: Firewalls provide a barrier between internal and external networks, allowing organizations to control and restrict access to sensitive information and resources.

Network Security: Firewalls help prevent unauthorized access to a network and protect against various cyber threats, including malware, viruses, and unauthorized access attempts.

ADVANTAGE & DIS ADVANTAGE

DISADVANTAGES:

False Positives/Negatives: Firewalls may generate false positives, blocking legitimate traffic, or false negatives, allowing malicious traffic to pass through. Fine-tuning firewall rules is essential to minimize these issues.

Complexity: Configuring and managing firewalls can be complex, especially for larger networks. Misconfigurations can lead to security vulnerabilities or disruptions in network services.

FIREWALL & ANTIVIRUS

BASIS FOR COMPARISON	FIREWALL	ANTIVIRUS
Implemented in	Both hardware and software	Software only
Operations performed	Monitoring and Filtering (Specifically IP filtering)	Scanning of infected files and software.
Deals with	External threats	Internal as well as external threats.
Inspection of attack is based on	Incoming packets	Malicious software residing on a computer
Counter attacks	IP spoofing and routing attacks	No counter attacks are possible once a malware has removed

WHAT HAPPENS IF WE DON'T USE FIREWALL?

➢If you don't use a firewall or if your firewall is improperly configured, your computer or network may be more vulnerable to a variety of security threats.

1. **Unauthorized Access**
2. **Malware Infections**
3. **Denial of Service (DoS) Attacks**
4. **Network Vulnerabilities**
5. **Data Exfiltration**
6. **Lack of Logging and Monitoring**
7. **Compromised Privacy**
8. **Increased Risk of Phishing and Social Engineering Attacks**


Thank
you!