LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 28A

THE ROLE OF FIREWALL IN CYBERSECURITY

**TASK 28A:**

* Provide a detailed explanation of what a firewall is in the context of network security and elaborate on the various types of firewalls along with their operational mechanisms

[](https://www.kaspersky.com/resource-center/definitions/firewall)

A firewall is a network security device that monitors and controls traffic to and from a network based on predetermined security rules.

With many organizations using private networks to send sensitive documents and information, there is an increased need to provide adequate security to protect those data. Usually, firewalls are positioned at the front line of a network and configured so that any data entering or exiting the web has to go through it. If done correctly, the authorized users of the network can access every resource offered by the network while simultaneously keeping out unauthorized users, hackers, malicious programs, and viruses that try to invade the network. They are essential for networks prone to attack, such as wireless networks.

**Key Functions of Firewalls:**

1. Traffic Filtering: Firewalls screen data packets (pieces of data) in the network's flow-in and flow-out directions, allowing or blocking them according to certain rules.

2. Access Control: They decide which applications, services, and devices can access the network, thus protecting sensitive resources.

3. Threat Detection: Some can detect and prevent other types of [threats](https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks), such as viruses, malware, or suspicious behavior.

**Types of Firewalls**

1: **Packet Filtering**: are small chunks of data within public traffic like the internet. Packet filtering firewalls with established security settings screen each packet for signs of predetermined red flags. If even a tiny part of the packet is suspicious, then the packet is blocked right away.

2: **Proxy Service**: acts as an intermediary between two endpoint systems. Information about all public sources is stored in a requesting system. Incoming traffic meets the firewall and is sent to the requesting system for verification, after which the firewall can either block or allow the traffic based on the result from the requesting system.

3: **Stateful Inspection**: is the most sophisticated and modern form of firewall. A vast trustworthy database holds all the significant attributes, such as each connection’s IP address and ports. During each session, the firewall compares all incoming traffic against the information in the database. If the comparison is favorable, the traffic is let through, but if it isn’t, it is automatically denied. This firewall is better because it is less memory-intensive and more efficient.

4: **Circuit Level Firewalls**: protect a network by providing session-level control over network traffic. Although its operation method is similar to packet filtering, it generally works at a much higher level. They often act as relays between incoming packets and the host server and are often combined with other firewall types, such as proxy servers.

5: **Next-Generation Firewalls (NGFW):** are highly sophisticated firewalls designed to address advanced security threats at the application level. This type of firewall uses intelligent, context-aware security features that can better filter malicious software. In addition, NGFW has extra layers of protection not commonly found in other types of traditional firewalls.

Network Layer Vs. Application Layer Inspection

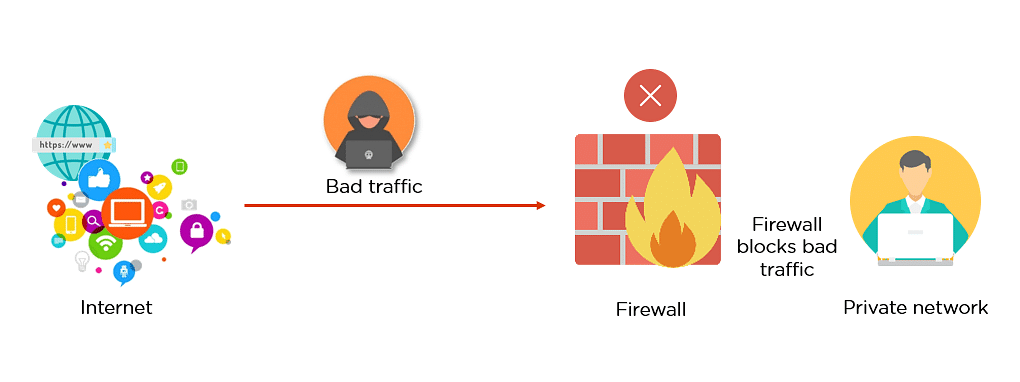
Network Layer Inspection: Network Layer Inspection works at the third layer of the OSI model. Its prime focus is basic packet filtering, where filtering takes place based on IP addresses and protocols such as [TCP](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model), UDP, and port numbers.

It checks the source and destination addresses of the data packets and allows or blocks the transmission accordingly. This inspection type is fast and efficient but does not delve into the inside of the data contents.

Application Layer Inspection: On the other hand, Application Layer Inspection works at Layer 7 of the OSI model. It goes deeper, inspecting the actual content of the data being transmitted, such as the HTTP request, email, or file transfer.

Because this kind of inspection can comprehend specific application protocols and behaviors, this type of protection will find more sophisticated threats like malware, SQL injections, or cross-site scripting.

Data is often lost or held hostage when malware, viruses, or hackers access the network or an individual system. Firewalls make this extremely difficult by blocking access to private networks using susceptible filters.



**Functions of Firewall:**

* The most crucial role of a firewall is to create a border between an external network and a guarded network. The firewall inspects all the packets entering and leaving the guarded network. Once the inspection has been done, a firewall can differentiate between benign and malicious packets with the help of a set of pre-configured rules.
* The firewall enforces such packets, whether in a rule set or without rules, to ensure that they do not enter the protected network.
* The source, destination, and content information is provided in packet form. Each may differ at each level of the network, and with it differs the set of rules. Firewalls read the packets and then reform the rules to instruct the protocol where to send them.

Firewalls are essential to network security as they shield your network from malicious software and viruses that seek to steal or destroy data. There are different firewalls, but they can be either software-based or hardware-based (like routers).