**firewall control incoming and outgoing traffic on network predetermined security rules**

**INTRODUCTION:-**

**A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules**. Either hardware, software, or a combination of both, the firewall establishes a barrier between a trusted internal network and untrusted external networks such as the Internet.

A firewall is a security device that monitors network traffic. It protects the internal network by filtering incoming and outgoing traffic based on **a set of established rules**. Setting up a firewall is the simplest way of adding a security layer between a system and malicious attacks.

**Technical related;**

A firewall is placed on the hardware or software level of a system to secure it from malicious traffic. Depending on the setup, it can protect a single machine or a whole network of computers. The device inspects incoming and outgoing traffic according to predefined rules.

Communicating over the Internet is conducted by requesting and transmitting data from a sender to a receiver. Since data cannot be sent as a whole, it is broken up into manageable**data packets** that make up the initially transmitted entity. The role of a firewall is to examine data packets traveling to and from the host.

What does a firewall inspect? Each data packet consists of a **header** (control information) and **payload** (the actual data). The header provides information about the sender and the receiver. Before the packet can enter the internal network through the defined port, it must pass through the firewall. This transfer depends on the information it carries and how it corresponds to the predefined rules.

**Pros;-**

* Monitors Network Traffic. All of the benefits of firewall security start with the ability to monitor network traffic. ...
* Stops Virus Attacks. Nothing can shut your digital operations down faster and harder than a virus attack. ...
* Prevents Hacking. ...
* Stops Spyware. ...
* Promotes Privacy.

**Cons;-**

* Cost. Firewalls does have an investment depending on the types of it. ...
* User Restriction. It is no doubt that firewalls prevent unauthorized access to your system from the network. ...
* Performance. ...
* Malware Attacks. ...
* Complex Operations.

**Applications;-**

A firewall **blocks undesired traffic**. Firewalls work on the filtering rules set up by the administrator of the network. Rules, also known as access control list, can be based on parameters ranging form IP addresses to domain names, protocols, programs, or ports.

A firewall is **a piece of software that filters incoming and outgoing network traffic and stops messages that violate the rules that define allowable traffic**. It is typically placed between the Internet and an internal network. Its primary job is to eliminate as much undesirable network traffic as possible.

**Features;-**

* Unified Security Management. Organizations must cope with rapidly increasing network security complexity
* Threat Prevention
* Application and Identity-Based Inspection
* Hybrid Cloud Support \* scalable performance
* 



