Introduction to Firewall in Computer Network

A Firewall manages the secure in-flow and out-flow of data in a device. It monitors the network traffic and acts as a barrier between the trusted and untrusted network.

The concept of Firewall is important for people interested in understanding the network security aspect of a computer device and also for those looking forward to strengthening their Computer Awareness.

This is even an important topic from the perspective of competitive exams which comprise Computer Knowledge as a compulsory subject. Candidates will find all the necessary information well-explained here, along with well-explained notes.

Basics of What is a Firewall

What is a Firewall?
A Firewall is a security system to protect an internal network from unauthorized servers and networks based on predefined rules. It acts as a barrier and only allows the secured network to send or receive data.

How does a Firewall work?
A Firewall analyses the network traffic and filters it so that the unsecured and suspicious networks cannot attack the system. The point where information is exchanged with an external network is called a port.

How is Firewall different from an Antivirus?
A firewall is a security network designed to protect computer systems and networks from malicious attacks. Whereas, Antivirus is is a software utility program designed to protect a system from internal attacks from viruses. Get a tabulated and detailed comparison between the two at the Difference Between Firewall and Antivirus page.

With regard to a Firewall, another term which is frequently being used is a Computer Network. To get a detailed explanation and understanding of networking, candidates can visit the linked article.

Related Links	
Storage Devices	Input and Output Devices
Important Computer-related Terms	Computer Abbreviations
Computer Shortcut Keys	High-Level Computer Languages

History and Development of Firewall

Discussed below is a brief account of the evolution and development of Firewall and why it had become an important part of network security.

The term ‘Firewall’ actually meant a wall which intended to confine a fire within a line of adjacent buildings. It was only in the late 1980s when this was acknowledged as a computer terminology.

It was during this time that the Internet has started to emerge as a new tool for global use. Thus, having a means which could secure the transmission and flow of data was required by many.

Until the Firewall was introduced, routers performed the same function as it restricted the number of people who could use a particular network.

For more information regarding the Fundamentals of Computer, visit the linked article.

Computer Related Difference Between Articles	
Difference Between Virus and Malware	Difference Between TCP/IP and OSI Model
Difference Between RAM and ROM	Difference Between Virus and Worm
Difference Between IPV4 and IPV 6	Difference Between WWW and Internet

Types of Firewall

There are various types of Firewalls. Described below are each of them in detail for a better and simplistic understanding:

1. Packet Filtering Firewall

- One of the oldest types of Firewall
- This type of Firewall creates a checkpoint at the traffic router. Only the secure and verified IP address or networks are allowed for the further flow of data
- The data packets are not verified, i.e. the information or data is not opened at the Firewall stage
- They are easy to use and do not overload the device and do not affect its processing or functioning speed

2. Application Level Gateway Firewall

- It is also known as Proxy Firewall
- When the user connects with the destination server, it forms a connection with the application gateway

- The proxy then connects with the destination server and takes up the decision of forwarding the data packets
- It is a bit more secure in comparison to Packet Filtering Firewall
- Strong Memory and processors are required for using this Firewall

3. Circuit Level Gateway Firewall

- This works as the Sessions layer of the OSI Model
- Using this, two Transmission Control Protocol (TCP) connections can be set up together
- It can easily let the flow of data packets continue without consuming major computer resources
- These Firewalls are not much efficient as they do not check the data packets and incase a data packet comprises malware, it will allow it to pass if the TCP connections are successfully done

4. Stateful Inspection Firewall

- It is a combination of data packet inspection and TCP connection. Until both the fields are verified, the information cannot be approved
- They are less straining for the computer resources
- However, they are a bit slow in comparison to other Firewalls

5. Next-Generation Firewall

- The recently launched Firewall systems are known as the Next-Gen Firewalls
- Under this, the data packets are also thoroughly checked before being passed on to the destination address
- These are still on the platform of improving and evolving and intend to use modern technology for automatic detection of errors and network safety

6. Software Firewall

- Any firewall which is installed in a local device or a cloud server is called a Software Firewall
- They can be the most beneficial in terms of restricting the number of networks being connected to a single device and control the in-flow and out-flow of data packets
- Software Firewall also time-consuming

7. Hardware Firewall

- They are also known as Physical-appliance based firewalls
- It ensures that the malicious data is stopped before it reaches the endpoint of the network at risk

Other Related Links	
Web Browsers	Internet
Types of Computer	Difference Between MS Excel and MS Word
MS Excel	MS PowerPoint

Functions of a Firewall

Following are the function of a Firewall. Candidates can refer to these to apprehend the basic functions of a Firewall:

- Any data which enters or exits a computer network has to pass through the Firewall
- All the valuable information stays intact if the data packets are securely passed through the Firewall
- Every time a data packets passed through a Firewall, it records it which allows the user to record the network activity
- No data can be modified as it is held securely within the data packets

Precisely, a Firewall ensures that all the data is secure and any malicious data trying to enter the internal network is not allowed to pass through.

Candidates looking for study material or tips to prepare, can visit the Preparation Strategy for Competitive Exams page and get the list of major exams along with a structured study plan.

For any further information or exam updates, notes, etc., candidates can turn to BYJU'S for assistance.