Study of History and Type of Firewall

Shalini

Email id- shaliniruhil@gmail.com

Abstract

A firewall may block any harmful data from entering your network. Using a predetermined set of rules, firewalls prevent malicious traffic from entering a network. Users inside the network might be blocked from accessing specific resources by implementing these policies. The basic premise behind firewalls is that data travelling across networks from less secure locations should be verified and reviewed before being allowed access to more secure locations. In this way, access to a restricted area of a network can be denied to unwanted individuals, machines, and programmes. Without firewalls, hackers may easily get access to your network and use its computers and devices to launch attacks.

Key Words: Protecting, firewall, Internet, Security etc.

Introduction

A firewall is a security system that analyses incoming and outgoing network data and decides whether to allow or block it based on predefined rules. “Firewalls have been the first line of defence in protecting computer networks for almost twenty years. It is possible to use either a software-only firewall or a hardware-based firewall. As a defence against external hackers, firewalls block any potentially harmful network traffic. In order to protect internet-connected devices and networks from malware, firewalls are installed. Common types of firewalls used by corporations to protect their data and devices from outside dangers include packet filters, stateful inspection, and proxy server firewalls. We'll begin with a brief summary of each one.

History and Need for Firewall

Access Control Lists (ACLs) on routers were responsible for network security prior to the invention of Firewalls. Access control lists, or ACLs, are rules that specify whether a given IP address has permission to access a network.

However, ACLs have no way of knowing what kind of packet it is preventing. Additionally, ACL is insufficient to prevent malicious traffic from entering the network. This led to the development of the Firewall.

Organizational Internet access is now considered critical. However, there are advantages to having Internet connection, since it allows for communication between the company's internal network and the rest of the world. Danger will be posed to the company as a result of this. We require a Firewall to prevent intruders from accessing the internal network.

Generation of Firewall

Firewalls can be categorized based on its generation.

First Generation- Access to a network can be restricted using a packet-filtering firewall, which examines outgoing and incoming data packets and decides whether to let them through or block them based on the IP addresses of their senders and receivers as well as the protocols and ports they employ. It does protocol layer transport analysis (but mainly uses first 3 layers).

Every packet is handled separately by a packet firewall. They are unable to determine if a given packet belongs to an ongoing data stream. In accordance with their individual packet headers, only It can decide whether or not to accept the packets.

In order to determine whether or not to forward a packet, a firewall that employs packet filtering keeps a filtering table. Packets will be filtered based on the following criteria, taken from the filtering table provided:

- No data may enter from the 192.168.21.0 network.
- The TELNET server on the internal network (port 23) is not accessible from the outside.
- All traffic going for 192.168.21.3 from the outside is being denied.
- For the 192.168.21.0 network, you may access any standard service.

Second Generation- When compared to a packet filtering firewall, a stateful firewall's (one that employs Stateful Packet Inspection) ability to ascertain a packet's connection state gives it a significant performance advantage. Network connections, such as TCP streams, traversing it are monitored and their statuses recorded. The state table information would be used in conjunction with the established rules to make filtering decisions.

Third Generation- To analyse and filter packets at any OSI layer up to and including the application layer, an application layer firewall is required. It may filter out unwanted material and detect when particular programmes or protocols (like HTTP and FTP) are being exploited.

In other words, hosts operating proxy servers constitute Application layer firewalls. Each traffic must go via the proxy first, preventing direct communication between the two sides of the firewall. Depending on a set of regulations, it can either let traffic through or stop it..

Note: Application layer firewalls can also be used as Network Address Translator(NAT).

Next Generation Firewalls (NGFW) : As a result of the prevalence of threats like advanced malware and application-layer assaults in the current world, businesses are turning to Next Generation Firewalls. To counteract these new dangers, Next-Generation Firewalls (NGFWs) employ a wide range of features, including Deep Packet Inspection, Application Inspection, SSL/SSH inspection, and more.

Type of Firewall

On the basis of how they operate, the following are the most prevalent firewall types:

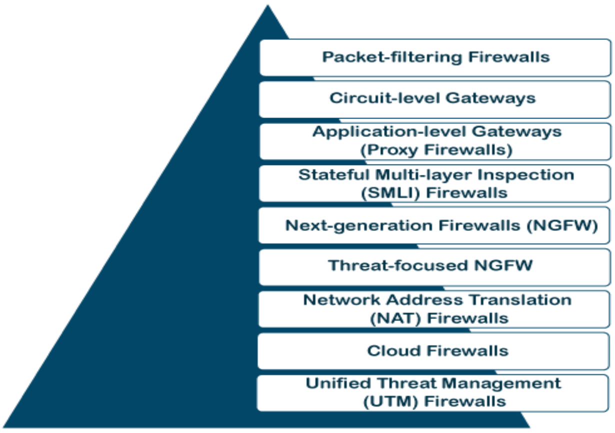
Packet-filtering Firewalls
Circuit-level Gateways
Application-level Gateways (Proxy Firewalls)
Stateful Multi-layer Inspection (SMLI) Firewalls
Next-generation Firewalls (NGFW)
Threat-focused NGFW
Network Address Translation (NAT) Firewalls
Cloud Firewalls
Unified Threat Management (UTM) Firewalls

Fig : Type of Firewall

As a common practise, firewalls are installed at the entrances of private networks to block access to those networks from the outside world. The primary function of a firewall is to prevent unauthorised users from accessing a private network. Three common types of firewalls protect a company's data and infrastructure. Here's a quick rundown of each one that we'll be providing.

1. **Packet Filters**

The Packet Filter Firewall examines incoming and outgoing data packets to determine who may and cannot access the network. It checks the packet's IP address, packet type, port number, and other parameters to determine whether or not to accept it. While packet filtering may help with smaller networks, it may be difficult to implement in larger ones. It's crucial to remember that firewalls of this sort can't fend against every possible threat. Specifically, they are helpless against spoofing and vulnerabilities at the application layer. The most fundamental firewalls inspect incoming packets for security flaws and shut off the connection if a rule is broken. This firewall examines the surface-level data, IP addresses, ports, and protocol headers of each incoming data packet from the network router.

2. Stateful Inspection

SPI, or dynamic packet filtering, is a type of advanced firewall design that performs end-to-end analysis of data streams. These firewalls are able to prevent unwelcome traffic from entering the network by analysing packet headers and packet states. This type of firewall provides more security than traditional packet filtering firewalls since it operates at the network layer of the OSI model.

3. Proxy Server Firewalls

By filtering traffic at the application layer, proxy server firewalls (also called application level gateways) are highly successful at keeping networks safe. Your IP address is hidden behind a proxy firewall, which also limits the types of traffic you may send and receive. They perform in-depth security checks on the protocols they back, factoring on the specific protocol at hand. A high-quality Internet experience is provided by proxy servers, which also boost network efficiency.

4. Application Gateways

Also included in this category are application-layer mechanisms like proxy firewalls and gateways. The proxy firewall is used to establish a connection instead of directly accessing your network. The remote client makes a request to the proxy firewall. After determining that the request is legitimate, the proxy firewall forwards it to one of the internal devices or servers. The proxy device will send the request from an internal device to the requested website while concealing the identity of both the proxy device and the network it is part of.

5. Circuit Level Gateways

In order to ensure that all data is transmitted securely, TCP connections are verified and monitored by circuit-level gateways, which operate at the session layer. They do a single check and consume few resources, much as packet filtering firewalls. This allows them to operate on a more advanced level of the OSI (Open Systems Interconnection) paradigm (OSI). They're the ones that have to figure out how secure a link is. By creating a virtual connection in place of the user, a circuit-level gateway protects the anonymity and IP address of the internal user from the outside world.

6. NAT firewalls

Public addresses can be assigned to collections of devices for the purpose of protecting private networks against intrusion. In order to hide private IP addresses, NAT is used. IP address lookups on a network prevent access to sensitive information by malicious users. The network address translation (NAT) firewall and the proxy firewall both play the role of a gateway between a network of devices and the outside world.

7. Web application firewalls

Websites and web applications are subject to filtering, monitoring, and blocking by online application firewalls (WAF). WAFs are typically set up in front of many websites or applications. Network appliances, cloud services, and server plugins can all be used to deploy WAFs.

8. NGFW firewalls

Websites and web applications are subject to filtering, monitoring, and blocking by online application firewalls (WAF). Some websites and apps may be protected by many WAFs, which might operate locally, on a remote server, or in the cloud." Depending on the configuration, WAFs can operate locally, in the cloud, or via the network.

Conclusion

A firewall is a piece of network security hardware that keeps tabs on all data travelling in and out of an organization's network and filters it based on predetermined rules. Simply said, a firewall is the wall that separates an intranet from the wider Internet. The primary function of a firewall is to restrict malicious traffic while let non-destructive traffic through. Firewalls are a type of network security hardware or software that monitor and filter incoming and outgoing network traffic according to a predetermined set of security rules. It separates the internal networks of a company from the outside Internet (such as the public Internet). The primary function of a firewall is to prevent harmful or unwanted data from leaving the system while still allowing non-threatening communication. A firewall is a form of network security software that blocks harmful programmes from accessing the Internet from compromised computers.

References

1. Wojciech Konikiewicz & Marcin Markowski (2017), Analysis of Performance and Efficiency of Hardware and Software Firewalls, Vol. 9, No. 1, pp. 49
2. Richa Sharma & Chandresh Parekh (2017), A Study and Its Classification, Volume 8, No. 4, May – June 2017
3. Xin Yue, Wei Chen, Yantao Wang (2009). The research of firewall technology in computer network security. DOI:10.1109/PACIIA.2009.5406566
4. Miss. Shwetambari G. Pundkar & Prof. Dr. G. R. Bamnote (2014), Analysis of firewall technology in computer network technology in computer network security,
   Vol.3 Issue.4, April- 2014, pg. 841-846
5. Steven Thomason (2012), Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices, Volume 12 Issue 13 Version 1.0 Year 2012
6. RahatAfreen, S.C. Mehrotra, (2011). A Review on Elliptic Curve Cryptography for Embedded Systems. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011, Pp 84-103.
7. Srivaths Ravi, AnandRaghunathan, Paul Kocher, Sunil Hattangady, (2004). Security in embedded systems: Design challenges. ACM Transactions on Embedded Computing SystemsVolume 3Issue 3August 2004 pp 461–491https://doi.org/10.1145/1015047.1015049.
8. Junfeng Fan; LejlaBatina; Ingrid Verbauwhede (2009). Light-weight implementation options for curve-based cryptography: HECC is also ready for RFID. 2009 International Conference for Internet Technology and Secured Transactions, (ICITST).