© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 09 | October – December 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Firewalls and its types: A review

Pooja Bansal

Email id poojasinghal273@gmail.com

Abstract

Protecting our sensitive data from undesired and unauthorised sources is a major concern nowadays. There are a variety of methods and gadgets that may give varying degrees of security and aid in the protection of our personal information. A 'firewall,' for example, keeps our computers and data safe and secure by preventing illegal access. firewalls as well as other related subjects in this post, such as why we need firewalls, their roles, their limits, how they operate, and so on.

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

Introduction

"Incoming and outgoing traffic is monitored by a firewall, which chooses whether to allow or prohibit it based on a set of security criteria. For more than two decades, firewalls have been the principal line of security for computer networks. A software-only firewall or a hardware-based firewall may be employed. Firewalls filter out unwanted or damaging network traffic as a safeguard against outside hackers. Firewalls safeguard computers and networks linked to the internet against malicious software. Three of the most prevalent kinds of firewalls used by businesses to secure their data and devices from outside threats include packet filters, stateful inspection, and proxy server firewalls. We'll start by giving you a short rundown of each of them.

Type of Firewall

Firewalls are often used in private networks to prevent other parties from accessing the network. Firewalls' principal role is to protect an organization's computer network against unwanted incoming or outgoing access. The data and equipment of a firm are secured by the three most popular types of firewalls. We'll give you a brief overview of each one.

1. Packet Filters

To control network access, the Packet Filter Firewall analyses outgoing and incoming packets. To assess whether or not to accept or reject a packet, it examines its IP address, packet type, port number, and other pre-established criteria. Packet filtering may assist small networks, but it may be challenging to set up larger networks. It's vital to understand that these kinds of firewalls can't protect you from all types of attacks. They

can't handle attacks that take advantage of application layer weaknesses or spoofing. The simplest basic firewalls monitor packets for security breaches and block traffic if a security rule is not met. This firewall analyses the specifics of each data packet that enters from the network router, including surface-level data, destination and source IP addresses, port numbers, and protocol headers.

2. **Stateful Inspection**

SPI (dynamic packet filtering), often known as SPI, is a sophisticated firewall architecture that analyses traffic streams from beginning to end. By assessing packet headers and examining packet states, these firewalls can prohibit unauthorised traffic from accessing the network. These firewalls operate at the network layer of the OSI model, making them more secure than typical packet filtering firewalls.

3. **Proxy Server Firewalls**

Proxy server firewalls, also known as application level gateways, excel at securing network resources effectively by filtering communications at the application layer. Proxy firewalls mask your IP address while restricting the sorts of traffic you may transmit and receive. They do a comprehensive security analysis of the protocols they support, taking the protocol in issue into consideration. Proxy servers improve network performance and deliver the best Internet experience possible..

4. **Application Gateways**

That also refers to application-level gateways or proxy firewalls implemented at the application layer. Rather of connecting directly to your network, the connection is formed via the proxy firewall. The proxy firewall receives a request from the external client. The proxy firewall transmits the request to one of the internal devices or servers after validating that it is genuine. Internal devices may request access to a website, and the proxy device will forward it while hiding its own and its network's identity.

5. **Circuit Level Gateways**

Circuit-level gateways, which operate at the session layer, verify and monitor TCP connections. Similar to packet filtering firewalls, they execute a single check and use little resources. As a result, they function at a higher OSI (Open Systems Interconnection) model (OSI). They are in charge of assessing the safety of a connection. Circuit-level gateways hide internal users' IP addresses and identities from the outside world by establishing a virtual connection on their behalf.

6. **NAT firewalls**

In order to safeguard private networks from outside incursions, public addresses may be issued to groups of devices. NAT obfuscates individual IP addresses. When an IP address is looked up on a network, attackers are unable to access particular data. Both NAT and proxy firewalls act as gateways between groups of devices and the outside world, enabling them to interact safely..

7. **Web application firewalls**

Online application firewalls (WAF) filter, monitor, and block data packets as they pass via websites and web applications. WAFs are often placed in front of one or more web pages or apps. WAFs may be implemented via server plugins, cloud services, or network appliances.

8. **NGFW firewalls**

Online application firewalls (WAF) filter, monitor, and block data packets as they pass via websites and web applications. One or more WAFs that reside on the network, host, or in the cloud may protect one or more websites or apps. WAFs may run on a server, in the cloud, or over a network.

Benefits of Next-Generation Firewalls

- **Intrusion Prevention Systems**

Intrusion Prevention Systems monitor network traffic for harmful activity. It is an inline security component that keeps network speed high.

- **Deep Packet Inspection**

Deep Packet Inspection examines a packet's content and source. It may also reroute internet services or IP addresses. DPI may also help ISPs avoid IoT device exploitation in DDOS attacks by rejecting malicious requests from devices.

- **Global Threat Intelligence**

Global Threat Intelligence protects enterprises and people against known and developing cyber threats, regardless of source. It also reduces attack likelihood by providing immediate, predictive, and reputation-based threat information.

- **Application Control**

Security and privacy are guaranteed for data utilised by and exchanged between apps. It prevents unauthorised apps from operating in a manner that compromises data. Controls for input and forensics are included.

The Power-Packed Benefits of Cloud-based Firewalls

- **Easy Deployment and Scalability**

Using software-defined cloud-based firewalls is simple. They can be set up in a fraction of the time it takes conventional firewalls and cause minimum business impact. So they're easy to maintain and enhance. Unlike physical barriers, they can be scaled to infinity. The FWaaS maintains parity as bandwidth increases. Businesses may operate without concern about traffic volume.

- **Automatic Updates**

Speed is crucial for increased security. The top FWaaS provide automated, real-time upgrades to combat new threats.

- **Availability**

The availability of FWaaS is unmatched by on-premises firewalls. Redundancy (power, HVAC, network, etc.) is included into FWaaS as well as support services, automated backup plans, and incident failover. So cloud solutions are more dependable.

- **Identity and Access Management**

Cloud firewalls may filter traffic from the internet, tenants, virtual data centres, virtual networks, etc. In addition, the top ones can identify between bot and human traffic. They handle access policies and connections. They interface with access control providers to offer fine-grained filtering.

- **Migration Security**

FWaaS blocks out harmful requests from the web, virtual data centres, and tenants. They strengthen security between cloud and physical data centres. So they help enterprises move to cloud infrastructure.

- **Performance Management**

Cloud-based firewalls come with tools for controlling performance, use, visibility, configuration, logging, and other aspects. Most include a complete dashboard that may be operated remotely..

Conclusion

A firewall is a network security device that monitors and filters incoming and outgoing network traffic in accordance with a company's security policies. A firewall is the barrier that divides a private internal network from the public Internet at its most basic level. A firewall's principal objective is to let non-destructive traffic in while keeping bad traffic out. A firewall is a kind of network security hardware or software that monitors and filters inbound and outbound network traffic based on a set of security rules. It acts as a barrier

between private networks inside an organisation and public networks (such as the public Internet). To protect the computer from viruses and attacks, a firewall's main objective is to enable non-threatening communication while restricting hazardous or undesired data transfer". A firewall is a cybersecurity solution that filters network traffic and helps users avoid hazardous malware from getting Internet access on compromised workstations..

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).