Introduction to Firewall Technology and Its Facilities with Respect to Modern Networking Vendor

Ibrahim Sayed
Department of Information Technology
S. S. & L. S. Patkar College of Arts & Science & V. P. Varde College of Commerce & Economics, Mumbai
ibrahisayed314@gmail.com

Abstract: *In this era of tremendous network growth, ots safety has gotten a lot of attention. In order to strengthen the computer network's security. One of the most effective technologies is the firewall. Its progress has also gained people's interest. This post will delve deeper into the topic of firewall technology and its providers also known as the vendors.*

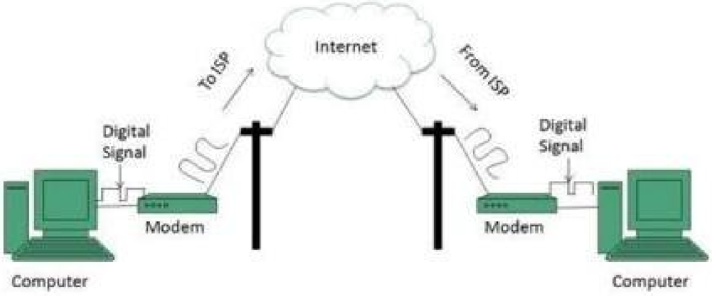
Keywords: Firewall technology

I. Introduction

In the world of computer network security, a firewall is a security protection mechanism. It connects the intranet to the extranet. The former is known to be a safe network. The latter is considered to be a less secure network. A firewall is made up of both software and hardware. The firewall is the sole way to communicate between the intranet and the extranet. The firewall is the most fundamental function for ensuring network data security. It has a strong protecting quality to it. At the same time, by obtaining security policy control (permission, rejection, monitoring), the information flow in and out of the network can be released and intercepted. The firewall is a tool for analysing data. Be able to decipher the information flow. You can also use a separator to filter the evaluated data flow. It also acts as a filter, limiting the flow of material that has been deemed hazardous. Allow secure information flow into the network by denying intranet access. Authorize the intranet's safe information flow. As a result, it can effectively safeguard network security. Ensure the intranet's security. Firewalls were once utilised as building dividers to keep fires from spreading. A protective wall is extended here to protect the internal network security. From a bodily standpoint. Each firewall can have a different physical implementation. However, it is typically a combination of hardware routers, hosts and software: A firewall is essentially a safeguard. Be utilised to safeguard network data, resources, and users' reputations.

1.1 Firewall Working Theory and Characteristics

A firewall's working concept. Fire walls follow predetermined configurations and rules. All data flows across the firewall should be monitored. Only authorised information is permitted. Also recorded are the relevant connection source, the server's communication display, and any attempted break-in. To make monitoring and tracking easier for administrators.

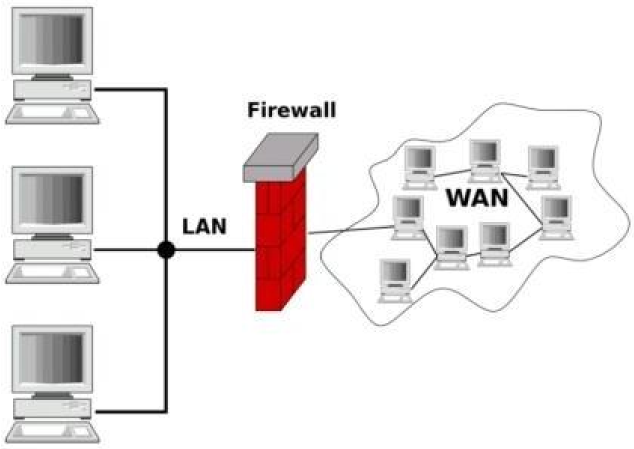


A firewall's properties. The following characteristics should be included in a good firewall: The first is that all information must pass through the firewall; the second is that it is only allowed to pass through the firewall if the security policy of the protected network allows it; the third is to record the information content and activities through the firewall; the fourth is to detect and alarm network attacks; and the fourth is that the firewall is immune to all types of attacks.

II. The Functionality of firewall

Technology for dynamic packet filtering. It also evolved into a technology for detecting states. Through a firewall, it is possible to intercept packets. Information about the Application Layer is extracted. To determine whether or not depending on the information's security, to refuse or allow. What is the goal of dynamic security?

It is possible to achieve network control. Information flows across firewalls can be dynamically managed. ports. Control services that are potentially dangerous. Insecure services can be efficiently controlled by firewalls. Establish a data policy. In advance, enter and exit the trust and distrust domains. You have the option to refuse risky services. external to the intranet It is also possible to define rule plans. When a startup and shutdown occur, automatically start and stop the programme. It is necessary to have a shutdown policy. It not only improves the intranet's security, but it also provides other benefits like flexibility. Security protection that is centralised. All of the software required to safeguard the intranet can be centralised using firewalls. All software updates and additions are included. As if it were a digital password. Authentication and passwords. Firewalls can be used to manage these security challenges from a central location. It has a high efficiency and is simple to use. Only by using the firewall as the focal point of the security strategy can centralised security protection be achieved. When compared to spreading security vulnerabilities across all hosts, this is a small price to pay. Firewall-based security management is more efficient and cost-effective. Strengthen the network system's access control. External network access services to the intranet can be set up using firewalls.



III. Hardware Firewall Vs Software Firewall

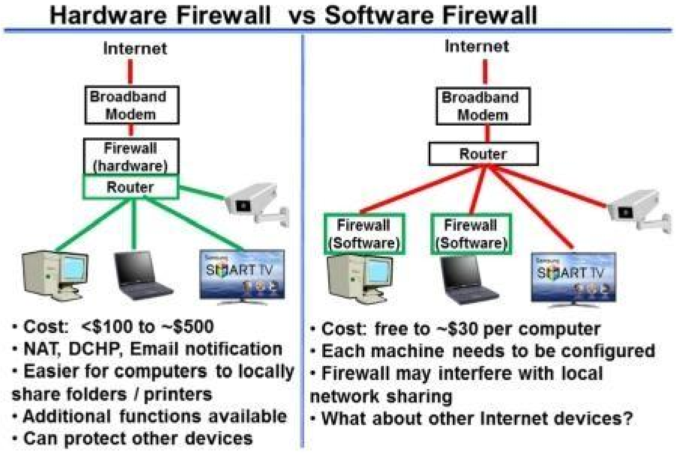
- **Software Firewall:** A software firewall is a form of computer software that is installed on a computer or server. Its main goal, depending on the software firewall you choose, is to protect your computer/server from outside efforts to control or acquire access. Any suspicious outgoing requests can also be checked using a software firewall.
- **Hardware Firewall:** A hardware firewall is a physical piece of equipment that is designed to conduct firewall functions. A hardware firewall can be a computer or a piece of specialised equipment that acts as a firewall. The router that sits between the PC and the internet gateway has a hardware firewall built in.

3.1 Firewall Vendors

Businesses today want high-availability, secure, efficient, and safe Internet connectivity. With Firewall Firm's Protection solutions, you'll get a comprehensive firewall and security service that's designed to thoroughly secure your business's network and systems, allowing you to use the Internet without fear – and best of all, we'll manage the entire solution for you. While continuously evolving to accommodate your changing business demands, your Firewall Firm Protection solution will enable "good" traffic to pass through your network while keeping "bad" traffic out. All of this is included in Protection services:

DOI: 10.48175/568

- **Web Content Filtering** – limit access to specific websites for enhanced employee productivity and protection against inappropriate content
- **Hardware & Software** – upgrades are provided, as well as real-time updates to your security, spyware, and virus content to keep new threats at bay. Protect yourself totally from online threats with Total Security.
- **Simplified administration** - receive reports on your network's availability, blocked threats, backup, Internet usage, and policy modifications.


Hardware Firewall vs Software Firewall
Internet
Broadband Modem
Firewall (hardware)
Router
SMART TV
• Cost: <$100 to ~$500
• NAT, DCHP, Email notification
• Easier for computers to locally share folders / printers
• Additional functions available
• Can protect other devices
Internet
Broadband Modem
Router
Firewall (Software)
Firewall (Software)
SMART TV
• Cost: free to ~$30 per computer
• Each machine needs to be configured
• Firewall may interfere with local network sharing
• What about other Internet devices?

Implementing a complete security solution for your organisation is no longer a choice in today's society. That's why the specialists at Firewall Firm have devised a security approach to ensure that everything you've worked for is fully protected. Even when we're not physically present, Security Monitoring solutions allow Firewall Firm to keep a constant, proactive eye on your network. You gain the peace of mind to focus on what really matters - your business – when you know your network, systems, and data are secure.

- Among the services we provide for security monitoring are:
- Keep an eye on the health of your systems. 24x7x365
- Monitoring of performance. Thresholds are set up to detect low disc space, high CPU utilisation, and other performance-related situations.
- Application monitoring is used to discover potential problems with the application. even if the server is operational

Full hardware and software inventories are part of asset management.

- Updates to the desktop operating system and antivirus software are available.
- Reports detailing uptime, security patching, and performance at the end of each month

3.2 Popular Fire Wall Vendors in India

Company that manufactures firewalls in India

The first thing that comes to mind for any enterprise or small medium business when it comes to network administration and security is a solid and secure firewall.

Embedded firewalls are programmes with relatively restricted capabilities that run on a low-power CPU machine. Software firewall appliances: a system that can run on standalone hardware or as a virtual appliance in a virtualized environment.

Firewall hardware appliances: A hardware firewall is designed to be installed as a network device, with adequate network ports and CPU to handle a variety of tasks. From securing a small network to securing a large network, we've got you covered.

A. Fortinet

FORTINET

B. Cisco

C. Palo Alto Networks

D. Check Point Software Technologies

E. Juniper Networks

F. Sophos

G. ForcePoint

H. Barracuda

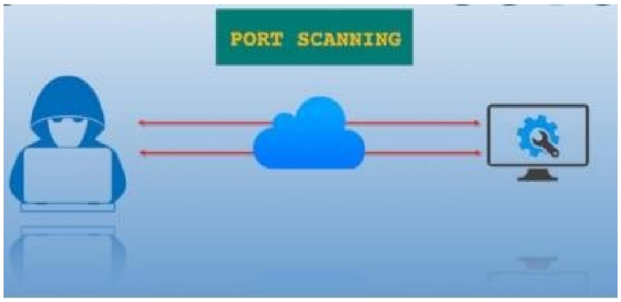
I. Sonic Wall

SONICWALL™

IV. Where is Firewall Mostly Used?

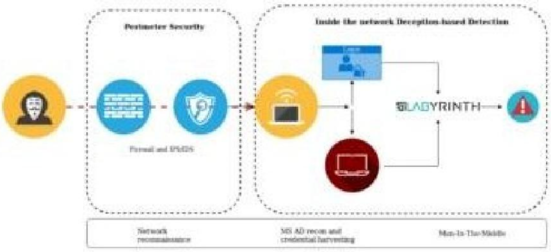
4.1 Scan Attacks

Scanners are applications that automatically find security flaws on a remote or local host . Hackers can use scanners to discover the distribution of various TCP ports on remote servers without leaving a trace, as well as collect a wealth of useful information about the target host such as whether to log in anonymously, whether there is a writable FTP directory, whether TELNET services are available, and so on.



4.2 Deception Attack

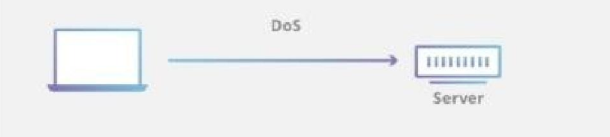
IP deception, DNS deception, and WEB deception are the three types of deception attacks. The following mostly explains the IP deception attack's principle and process. IP spoofing is a sophisticated attack technique for TCP/IP networks. First, the target host is chosen; second, the trust mode is discovered, and finally, the target host's trusted host is discovered. The trusted host is disabled during IP deception. When the connection is established, a system backdoor is installed to allow unauthorised access.



4.3 Denial-of-service Attack

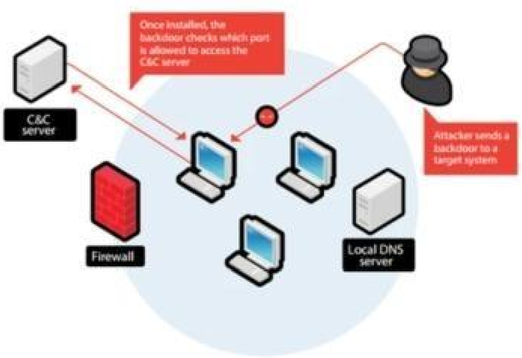
Denial-of-service attacks come in a variety of forms. Their core premise is to exploit flaws in the Windows operating system or the TCP/IP protocol to transmit a huge number of specified packets to the target host, rendering it unable to offer normal services.

The server must wait at this point and does not end the connection until. Because of the attacker's persistent delivery of such packets, the server eventually refused to offer services due to overload.



4.4 Back-Door

Because programmers apply modular programming techniques in the construction of some sophisticated functions of the software. Generally, after the programme is completed, each module's back door should be removed. However, for various reasons, back doors are occasionally not deleted, and some persons with nefarious intents utilise rigorous search methods to locate and use these back doors, then enter the system and conduct an assault.


Once installed, the backdoor checks which port is allowed to access the C&C server
C&C server
Attacker sends a backdoor to a target system
Firewall
Local DNS server

V. Conclusion

To summarise, the above research will contribute to a better understanding of computer network firewall technology. As Networking Aspirants, we must always conduct practical research and effectively summarise more scientific firewall technology in order to maintain a high degree of computer network security. I'm hoping that by combining the above explanation, I'll be able to provide a useful reference for relevant technical experts.

References

[1]. Computer Network Security Research [J] Based on Firewall Technology Tang Xiao bin. 2018(07): 38 in Digital World.

[2]. Liu Fa sheng, Gu Kui ye. China Electronic Testing, 2016(22): 63-64, Analysis of Computer Network Security Governance and Firewall Technology [J].

[3]. Wang Qiangqiang is number three. [J] of China Digital World, 2019(08): 244. Analysis on Application of Firewall-based Technology in Computer Security Construction.

[4]. This is a road race. SME Management and Technology (Mid-Year Journal), 2020 (08): 39-40. Countermeasure Research on Strengthening Computer Network Security Management in the Context of E- Commerce, SME Management and Technology (Mid-Year Journal), 2020 (08): 39-40.

[5]. Peng Zhen yu yu yu yu yu yu yu Cyber security technology and application, 2020 (08): 3-4, is based on research into computer network security and preventive countermeasures.

[6]. Computer Network Security and Firewall Technology Analysis by Zhang Rui [J] Computer Knowledge and Technology, 2012(24): 5787-5788.

DOI: 10.48175/568