International Journal of Research in Advent Technology, Special Issue, Convergence 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Firewall Network Security

[1]Mr. Muqueet ur Rehman,[2]Prof. S. M. Dandage, [3]Dr. P. M. Jawandhiya
PLITMS, Buldana Maharashtra, India.
mrrehman750@gmail.com,dandage.sachin@gmail.com

Abstract- In today's modern world of computing, the Internet has become one of the basics of our lives. The Internet is now known for its availability of the information to the common user along with easy access. By connecting a private network to the Internet can expose confidential data to the malicious attack from anywhere in the world. Hackers or intruders could make access to your private information or your system. Users must be aware of these dangers, their implications and how to protect their data and their critical systems. One of the protection mechanisms underneath serious thought is that the firewall. A Firewall is a network security system that has some predetermined security rules to monitors and controls incoming and outgoing network traffic. A firewall typically puts a barrier between a trusted internal network and another outside network, such as the Internet, that is considered not to be trusted. Firewalls are broadly classified as a network firewall and host-based firewall. Network firewalls filter traffic between multiple networks they are either software running on general purpose hardware or hardware-based firewall appliances. The Host-based firewall serves a layer of software on one host that controls network traffic in and out of that single machine.
Index Terms- Firewall, Network Security, Network traffic, Hackers, Internet, Network.

1. INTRODUCTION

As in today's modern world of the internet, everything is going online for making the availability of the information and their access easier to the user. No doubt the internet has tremendous advantages that have made a great impact on everyone lives but security is also a main concern today. To provide a security, concept of Firewall came to use in 1980s.

The word firewall itself indicates the wall which protects from fire. It primarily permits keeping resources confidential and minimizes security risks.

The firewall can be a Hardware-based firewall and software-based firewall.

- Hardware-based firewall: These are mainly found in broadband routers that are to be considered as an important part of the network setup. Hardware Firewall has a capacity to protect every machine on a local network.
- Software-based firewall: These are the firewall that is installed in an individual user's system, software firewall allows users to customize some control on its functionality and features. It is a good choice for a single user to acquire protection from outside unauthorized access to his personal system. It is also named as Antivirus.

2. LITERATURE REVIEW

"A History & Survey of Network Firewalls" written By KENNETH INGHAM and STEPHANIE FORREST. They made a survey on the network firewalls where they reported the following important aspects of the firewall it's functioning and its different type along with its advantages and disadvantages. Forthe purposes of this paper, they define a firewall as a machine meeting the following criteria:

• The firewall act as a boundary between the two networks.

• All traffic between the two networks should pass through the firewall.

• The firewall mechanism allows some traffic to pass while blocking other traffic. The rules describing what traffic is allowed to enforce the firewall's policy. [1]

3. EVOLUTION OF FIREWALL

- First generation Firewalls: First-generation firewalls simply permit/deny engines for layer three traffic working much like a purposed access control list appliance. Originally, first-generation firewalls were primarily used as header-based packet filters, capable of an understanding source and destination information up to OSI layer four (ports). However, they could not perform any "intelligent" operations on the traffic other than "allow or deny it from this predefined source IP address to this predefined destination IP address on these predefined TCP and UDP ports".
- Second generation Firewalls: Second-generation firewalls were able to keep track of active network sessions, putting their functionality effectively at layer four. These were referred to as stateful firewalls or, less commonly, circuit gateways. When an IP address (for example, a desktop computer) connected to another IP address (say, a web server) on a specific TCP or UDP port, the firewall would enter these identifying characteristics into a table in its memory. This allowed the firewall to keep track of network sessions, which could give it the capability to block man-in-the-middle (MITM) attacks from other IP addresses.
- Third generation Firewalls: The third generation of firewalls ventured into the application layer i.e layers seven. These "application firewalls" were able to decode data inside network traffic streams for certain well-defined, preconfigured applications such as HTTP (the language of the web, DNS (the protocol for IP address lookups, and older, person-to-computer protocols such as FTP. Generally, they were unable to decrypt traffic, so they were unable

to check protocols like HTTPS and SSH. They were designed with the World Wide Web in mind, which made them well suited to detecting and blocking web site attacks that were generating a great deal of concern at the time, like cross-site scripting and SQL injection.

- Fourth generation Firewalls: The fourth generation firewall is today's current generation of firewalls which have the intelligence and capability to look inside packet payloads and understand how applications function. Fourth-generation firewalls can run application-layer gateways, which are specifically designed to understand how a particular application should function and how its traffic should be constructed and patterned. The most network appliances you will find today fall into the generally accepted fourth-generation firewall definition.

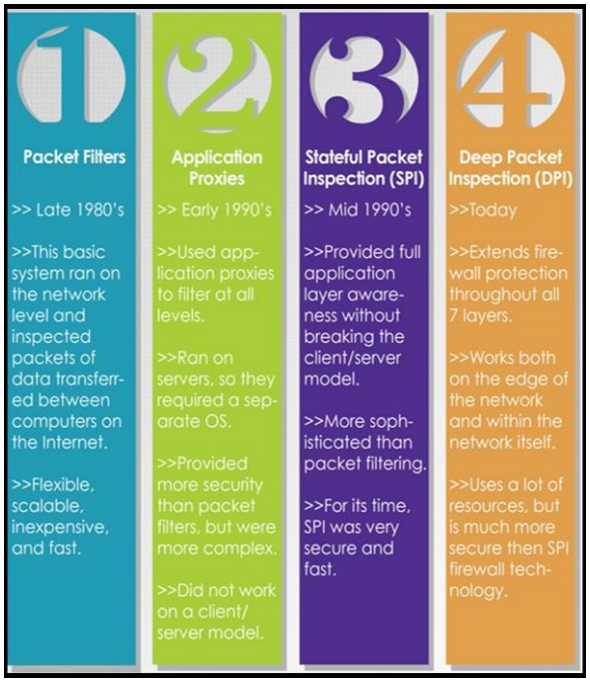

Figure 1: Firewall Generation

4. WORKING OF FIREWALL

There are two policies for the firewall to work

(1) Default- Deny Policy
(2) Default- Allow Policy

Default-Deny Policy: In Default–Deny policy the admin of the firewall creates a list of allowed network services and the rest of the network services are blocked.

Default – Allow Policy: In Default –Allow policy the administrator of firewall create a list of not allowed network services and rest of the network services are allowed.

A default-deny is the way to deal with firewall security is by a wide margin the more secure, however, because of the trouble in dealing with a system in that form, numerous systems rather utilize the default- permit approach. How about we expect for the minute that your firewall admin project uses a default- deny approach, and you just have certain admin empowered that you need individuals to have the capacity to use from the Internet. For instance, you have a web server that you need the overall population to have the capacity to get to. What happens next relies upon what sort of firewall security you have.

5. SOFTWARE FIREWALL

The software firewall is also known as a personal firewall. It is an application that mainly controls network traffic to and from a computer. Based on some security policy it allows permitting or denying communications. Typically, the software firewall act as an application layer firewall. The single computer scope of personal firewalls is useful to protect machines that are moved across different networks.

5.1. Features

Some common features are as follows:

- Block and alert the user about all unauthorized inbound or outbound connection attempts.
- Monitor applications that are interacting with incoming connections.
- Track recent incoming events, outgoing events, and intrusion events to monitor who has accessed or tried to access your computer.
- Allows the user to control which programs can and cannot access the local network or Internet and provide the user with information about an application that makes a connection attempt

5.2. Limitations

The Firewall protects internal network however, it does have some limitations.

- If the system is already compromised by malware or spyware these programs can also manipulate the firewall, because both are running on the same system. It may be possible to break rules or even completely shut down software firewalls in such a manner.
- A firewall can't notify if it has been configured incorrectly.
- The firewall may limit access from the Internet, but it may not protect the network from wireless and other access to the systems.
- The alerts generated can possibly make inactive users to alerts by warning the user of actions that may not be malicious.

Figure 2: Some Common available Software Firewalls.

6. HARDWARE FIREWALL

6.1. Packet Filtering Firewall

Network layer firewalls, also called packet filters, operate at a low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall admin may define the rules, or default rules may apply. The term "packet filter" originated from the context of BSD operating systems. Filtering decisions are based on:

(1) The IP address of the incoming data.
(2) IP Destination Address.
(3) TCP or UDP source port and destination port.
(4) ICMP message type.
(5) Connection initialization datagram using TCP ACK bit.

6.1.1. Types of Packet Filtering

The packet filtering generally falls into two sub-categories:

(1) Stateful packet filtering.
(2) Stateless packet filtering.

The data travels through the internet in the packet form. Each packet contains a header that provides information about the packet, its source, and destination, etc. The packet filtering firewalls check these packets to allow or deny them. In this case, the firewall may or may not remember the information.

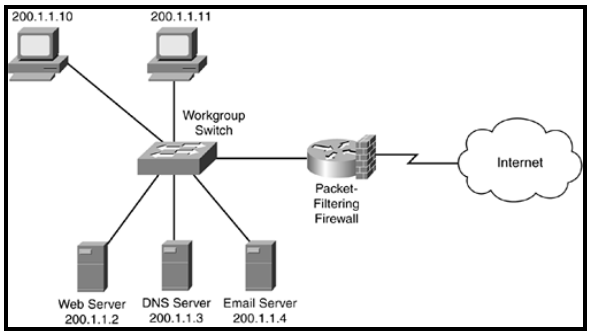

Figure 3: Packet Filtering Firewalls.

6.2. Application Level Gateway

Application-layer firewalls work on the application level TCP/IP stack and take away all packets traveling to or from an application. On checking all the packets for improper content, firewalls can restrict or prevent the spread of networked computer worms and Trojans. The more is the inspection criteria the more is the latency to the forwarding of packets to their destination. Application firewalls function by determining whether to accept any given connection to the process. It work like a packet filter but application filters follow filtering rules on a per-process basis instead of filtering connections on a per-port basis. Because of per-process rule sets limitations, application firewalls are beginning to be overthrown by a new generation of application firewalls that depend on mandatory access control (MAC), also referred as sandboxing, to protect vulnerable services.

6.2.1. Advantages of Application Level Gateway

Application Gateway Firewall has many advantages over packet-filtering and stateful firewalls, including the following:

- They only authenticate individuals, not devices.
- Hackers have a harsh time with spoofing and implementing DoS attacks.
- They can monitor and filter application data.
- They can provide detailed logging.

6.2.2. Limitations of Application Level Gateway

Even with its advantages, Application Gateway Firewalls has the following limitations:

- They process packets in the software.
- They support a small number of applications.
- They sometime require special client software.
- The main limitation of AGFs is that they are many processes intensive. They require much CPU cycles and memory to process every packet, which sometimes creates throughput problems. Additionally, detailed logging can create disk space problems.

6.3. Circuit Level Gateway

Circuit-level gateways mainly work on the session layer of the OSI model between the application and the transport layer of the TCP/IP stack. They monitor TCP handshaking between packets determining whether a requested session is accepted. Information passed to a remote computer through a circuit-level gateway to have originated from the gateway. It represents the technology of next to the first generation.

Firewall technology tracks TCP handshaking among packets to confirm a session is genuine. Firewall traffic is based on particular session rules and may be controlled to acknowledged computers only.

Circuit-level firewalls cover up the network itself from the external, which is helpful for interdicting access to impostors. But circuit-level firewalls do not clean entity packets. This is beneficial for hiding information about protected networks. Circuit-level gateways are inexpensive and have the advantage of hiding

information about the private network that they protect. On the other hand, they are unable to filter individual packets.

6.3.1. Advantages of Circuit Level Gateway

Circuit Level Gateway has the following advantages:

- Higher security than packet filters.
- Only need to analyze a few allowable applications.
- Easy to log and examine all incoming traffic.

6.3.1. Limitations of Circuit Level Gateway

- Additional overhead for processing on each connection Circuit-level Gateway
- Stand-alone system.
- The Specialized function performed by an Application-level Gateway
- Sets up two TCP connections
- The gateway relays TCP segments from one connection to another without testing the contents

6.4. Proxy Filter

Proxy server: Checks all the messages that are entering and leaving the network. The proxy server hides the true network addresses. A proxy server acts as an agent for requests from clients for getting resources from other servers. A client connects to the proxy server to request the services such as a file, connection, web page, or other resources, available from a different server. The proxy server examines the request according to its filtering rules.

Proxy server: Checks all the messages that are entering and leaving the network. The proxy server hides the true network addresses. A proxy server acts as an agent for requests from clients for getting resources from other servers. A client connects to the proxy server to request the services such as a file, connection, web page, or other resources, available from a different server. The proxy server examines the request according to its filtering rules. If filter validates the request then proxy provides resources by making the connection with relevant server and request service for the client. A proxy server optionally alters the client 's request or the server's response, and sometimes it may serve the request without requesting the specified server. In this case, it 'caches' responses from the remote server, and returns frequent requests for the same content directly.

7. ADVANTAGES OF FIREWALL

Following are the firewall strengths when designing network security:

- Firewalls are excellent at enforcing security policies. They should be configured to restrict communications to what management has determined and agreed with the business to be acceptable.
- Firewalls are used to restrict access to specific services.
- Firewalls can alert specific people of specified events.
- Information hiding, in which a firewall can ``hide" names of internal systems or electronic mail addresses, thereby revealing less information to outside hosts.
- Centralized and simplified network services management, in which services such as FTP, electronic mail, gopher, and other similar services are located on the firewall system rather to being maintained on many systems.

8. LIMITATIONS OF FIREWALL

Following are the firewall weaknesses when designing network security:

- Firewalls are only effective for the predefined rule they are configured to enforce. A remaining permissive rule set will diminish the effectiveness of the firewall.
- Firewalls are unable stop social engineering attacks or an authorized user intentionally using their access for malicious purposes.
- Firewalls cannot enforce security policies that are absent or not defined.
- If the traffic does not pass through firewall cannot stop attacks.
- The most obvious being that certain types of network access may be hampered or even blocked for some hosts, including telnet, FTP, X Windows, NFS, NIS, etc. However, these disadvantages are different from firewalls; network access could be restricted at the host level as well, depending on a site's security policy.

9. FUTURE SCOPE OF FIREWALL

The firewalls can be deployed not only software but also hardware, from a system admin's point of view they have to be able to perform real-time network traffic inspections without affecting throughput.

A large set of rules that filters data packets impacts network performance and causes bottlenecks. The future firewall needs to be distinguishable between legitimate and illegitimate traffic automatically to identify and plug never-before-seen threats on the fly.

Anti-malware scanning capabilities are not beyond the firewall capabilities, but the current network performance impact needs to be addressed. Multipurpose firewalls that are capable of performing more than Intrusion detection will begin to integrate other threat-prevention technologies. Based on the current adaptability of high-speed Internet, one thing is certain: Whether it is hardware or software, firewalls need to be able to filter traffic throughput of at least 10 GB per second in upcoming years. Firewalls will continue to evolve, and it is clear that their strength of capabilities and functionalities will expand as well.

REFERENCES

[1] KENNETH INGHAM (Kenneth Ingham Consulting) STEPHANIE FORREST (University of New Mexico) The University of New Mexico Computer Science Department Technical Report 2002-37. Report name "A History and Survey of Network Firewalls".

[2] Mark Rhodes-Ousley "The Complete Reference INFORMATION SECURITY" 2nd Edition, part no: - 3-15/343.
[3] Kurose & Ross "Computer Networking A top-down Approach" 6th Edition Part no: - 8-9/731.
[4] Imran, Mohammad, Abdulrahman Algamdi, and Bilal Ahmad. "Role of Firewall Technology In Network Security". International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Issue 12 December 2015.
[5] S.C. Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N. Liyanage, A.A.T.K.K. Amarasinghe, D. Dhammearatchi. "High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies". International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016504ISSN 2250-3153 www.ijsrp.org.