International Journal of Trend in Scientific Research and Development (IJTSRD)
UGC Approved International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 5

The Empirical Study of the Evolution of the Next Generation Firewalls

Manisha Patil
Department of Computer Science
MIT ACSC ,Alandi (D), Pune, India

Savita Mohurle
Department of Computer Science
MIT ACSC ,Alandi (D), Pune, India

ABSTRACT

Even after adoption of network security policies and practices, unauthorized intrusion occurs. It is an attack in which attacker gets access in to the system by means of different hacking and cracking techniques. Firewall is hardware-software based network security system that uses rules to control incoming and outgoing network packet. A *firewall* controls access to the resources of a *network* through a positive control model. There are various traditional firewalls like Packet Filters, Application-level Gateways and Circuit-level Gateways which has certain pros and cons. To overcome disadvantages of traditional firewall, next generation firewalls are introduced. This paper gives the empirical study of tradition firewalls, and its evolution to Next Generation firewall like NGFW, UTM, Threat focused, its features and advantages.

Keywords: *Firewall, UTM, NGFW, Packet filter, Application level gateway, Network Security, Circuit level gateway, Threat focused*

I. INTRODUCTION

A computer network consists of two or more computers that are connected to share resources such as printers, scanner, databases, files, application. The computers on a computer network may be connected through coaxial cables, twisted pair, fibre optics, satellites, or infrared light beams. When computer network connected to the internet, even a standalone desktop easily get targeted by malicious software & hackers. A firewall can offer the security that makes you less helpless and also guard your data from being hacked. A firewall is an obstacle or safeguard that is intended to guard your PC, tablet, or phone from the malware that exist on the Internet**.** A firewall must guarantee that only authorized user's access an operating system or a computer connected to a network, securing the private information and defending computer users from identity theft. In most cases, firewalls block unauthorized access that computer users are not aware of [6].Data is exchanged between your computer and servers and routers in network, and firewalls monitor this data (sent in packets) to check whether they're safe or not.

II. FIREWALL ARCHITECTURE

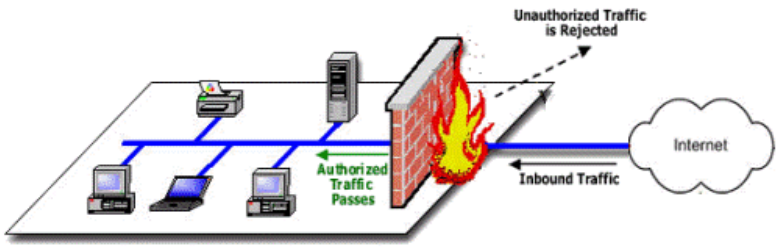

Fig 1: Architecture of Firewall

The fig.1.above shows firewall architecture. Firewall is an important component in computer network security architecture. A firewall is a software program or a hardware device that filters the information

(packets) coming through the Internet to your personal computer or a computer network. Firewalls may decide to allow or block network traffic between devices based on the rules that are pre-configured or set by the firewall administrator.

III. OBJECTIVE

The objective of the active research paper is to summarize evolution of traditional firewall, which concludes that traditional firewall has certain limitations. To overcome those limitations, the world's leading Information Technology Research and advisory company, Gartner Inc. define next-generation firewall. This paper discusses the features and advantages of the next-generation firewalls.

IV. RELATED WORK

In 2013 Dr. Ajit Singh and Madhu Pahal , reviews the different types of firewall. They have studied network firewall that helps the corporate environment as well as the other networks that want to exchange information over the network. A firewall protects the flow of traffic over internet and is less restrictive of outward and inward information and also provides internal user the illusion of anonymous FTP and www connectivity to internet [1]. In 2014, Deepika Sekhawat, Vaibha v Bhatnagarin their paper has reviewed the concept of firewall and explain the different type of firewall. They have explained three firewalls as an example to understand which firewall satisfies the factor they had proposed. It gives assistance for a Network Administrator for selecting a firewall [2].In 2015, Mohammad Imran, Dr.AbdulrahmanAlgamdi,Bilal Ahmad presents the paper which describes the importance of network security. They also explained different types of attack and why Firewall is used, and qualities of good firewall .They also described the working policies of firewall, explained different types of firewall like Packet filtering firewall, Stateful Firewall, Deep packet inspection firewall, Application-aware protocol, Application proxy firewall[4].In 2016 ,The members of Sri Lanka Institute of information technology Computing (Pvt) Ltd represents the research how to build a more protected network by combining both firewall capacity and firewall technologies. The experiment results show the proposed idea good enough to build a secured network. This research mentioned about how firewalls are used to protect resources from outside intruders and how Virtual Private Networks (VPN) enables to access the corporate network in a secure manner via non-secure public networks [3].

V. MATERIAL

A Firewall protects user computer/network from unauthorized Remote Access. It can Block Messages Linking to unwanted Content and monitors and controls the network traffic within network. According to the defined security policies, a firewall – hardware or software device allows multiple networks to communicate with one another. A firewall is used when there is a need for networks of varying levels of authorities to communicate with one another. Firewall software runs on a host, which is connected to both trusted and untrusted networks. The host operating system is responsible for performing routing functions, which many operating systems are capable of doing. The host operating system should be as secure as possible prior to installing the firewall software [1].Firewall provides the facility such as authentication, encryption, and content security.

A. Traditional Types of firewalls: Firewalls can be categorised into three types:

1. **Packet Filters:** A set of rules are applied based on matches of fields in the IP or TCP header to each incoming IP packet and then it is decided whether to forwards or discards it.

2. **Application-level Gateways:** It is also called a Proxy Server that acts as a relay of application level traffic. Using application user contact gateways, the request is granted only for authentic users .The application gateway is service specific such as FTP, TELNET, SMTP or HTTP.

3. **Circuit-level Gateways:** Circuit-level gateway can be a standalone or a specialized system. The gateway sets up two TCP connections, since it does not allow end-to-end TCP connections. Once the TCP connections are established, the gateway relays TCP segments from one connection to the other without examining the contents. The security function determines which connections will be allowed and which are to be disallowed.

Even though firewall provides security to the users, all the above types of Firewall in section A have certain limitations as mention below:

- Firewall cannot scan every incoming packet for virus contents. So, it cannot protect the internal network from virus threat.
- It does not provide Intrusion Detection System (IDS).
- Cannot handle internet traffic effectively.
- It cannot protect against any attacks that bypass the firewall.
- It does not protect against the internal threats from traitors.
- Firewalls can't protect against tunnelling over most application protocols.

According to the world's leading Information Technology Research And Advisory Company, Gartner, Inc.'s definition, a next-generation firewall must include:

- Standard firewall capabilities like state full inspection.
- Integrated intrusion prevention.
- Application awareness and control to see and block risky apps.
- Upgrade paths to include future information feeds.
- Techniques to address evolving security threats.[7]

B. Traditional Evolution to Next-Generation firewall.

1. Unified threat management (UTM) firewall.

UTM firewall is only the firewall that inserts user identity in firewall rule matching criteria, allowing enterprises to configure policies and identify users directly by the username rather than through IP addresses. It is a powerful hardware firewall that provides stateful and deep packet inspection thereby protecting enterprises from IP spoofing attacks, access control, user authentication, network and application-level protection. This paper will explore the development of UTM working criteria, functions and prove how it is better in comparison with the ordinary firewall and VPN [5].UTM firewalls bring advanced network security technologies to small and medium businesses and remote/branch offices. Traditional firewalls can only block/accept traffic based on IP addresses and ports and offer little protection outside of that. This approach is quickly becoming obsolete in today's Internet where many applications send/receive traffic over ports that are typically allowed by traditional firewalls.

Features of UMTS:

- Single hardware platform.
- Unified management interface.
- One vendor contract / contact.
- Reduced data centre footprint.
- Power consumption reduction.
- Minimized point of failure/latency.
- Simplified network security architecture.
- Blended threat protection.

Advantages of UTM:

- Reduced complexity
- Ease of development
- Integration
- Easy trouble shooting

2. Next-generation firewall (NGFW)

NGFW combines the features of traditional firewalls such as packet filtering, network address translation (NAT), URL blocking and virtual private networks (VPNs). It also follows the functionality of Quality of Service (QoS).Features include intrusion prevention, SSL and SSH inspection, deep-packet inspection and reputation-based malware detection as well as application awareness. NGFWs use a more thorough inspection style, checking packet payloads and matching signatures for harmful activities such as exploitable attacks and malware. Its goal is to include more OSI model layers.

Features:

- Application Awareness.
- Stateful Inspection.
- Integrated Intrusion Protection System (IPS).
- Identity Awareness (User and Group Control).

- Bridged and Routed Modes.
- Ability to utilize external intelligence sources.

Advantages:

- It bundles traditional firewall functionality with intrusion prevention, antivirus and protocol filtering.
- Capable to monitored and updated from a single console.
- It scan content to prevent data leakage and stop threats with detailed, real-time traffic inspection
- It reduces the number of security appliances needed.

3. Threat-focused NGFW

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

Features:

- Visibility-Driven.
- Threat-Focused.
- Platform-Based.

Advantages:

- Know which assets are most at risk.
- Quickly react to attacks.
- Better detect evasive or suspicious activity.
- Greatly decrease the time from detection to cleanup.
- Ease administration and reduce complexity.

VI. CONCLUSION

This paper gives the brief study of the next generation firewall over traditional firewall. The next generation firewall. After brief study we come to the conclusion that the next generation firewall combines features of traditional firewall and has its own features too. It is hardware-software based network security system to detect and block sophisticated attacks by enforcing security policies with simplified management and lowers the total cost of use.

REFERENCES

1) Dr.Ajitsingh, MadhuPahal, NeerajGoyat , "A Review Paper On Firewall", International Journal For Research In Applied Science And Engineering Technology ,Vol. 1 Issue II, September 2013, ISSN: 2321-9653.

2) Deepika Sekhawat and Vaibhav Bhatnagar, Factors for Selecting Firewall with Comparative Study, International Journal of Advance Research InComputer Science and Management Studies , Volume 2, pg 58-61,ISSN: 232 7782, 2014, , Issue 11,

3) 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, pg. 504-508,April 2016, ISSN 2250-3153

4) Mohammad Imran, Dr.Abdulrahman A.Algamdi, Bilal Ahmad, "Role of firewall Technology in Network Security", International Journal of Innovations & Advancement in Computer Science, Volume 4, Issue 12, December 2015. ISSN 2347 – 8616

5) VinitAgham, "Unified Threat Management ", International Research Journal of Engineering and Technology, Volume: 03, Issue: 04 , Apr-2016, Page 32 -35, E-ISSN: 2395 -0056

6) ThaierHayajneh, Bassam J. Mohd ,AwniItradat, and Ahmad Nahar Quttoum ,"Performance and Information Security Evaluation with Firewalls", International Journal of Security and Its Applications Vol.7, No.6 (2013), pp.355-372.

7) www.gartner.com

8) www.nptel.ac.in.