IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 4.819

Volume 5, Issue 2, May 2021

Traditional Firewall vs Next Generation Firewall (NGF)

Manish Kumar Kumawat
M.Sc. Information Technology
Sir Sitaram and Lady Shantabai Patkar College of Arts and Science, Mumbai, India

Abstract: *A firewall is a piece of hardware or software that prevents unauthorized access to or from a computer device. It may be carried out using both facilities and scripting, or a combination of the two. Firewalls are often used to prevent unapproved (untrusted) Internet clients or traffic from accessing private Internet networks. This paper examines the Firewall architecture, traditional Firewall types its features, advantages, and limitations, and next generation firewall similarities and differences compared to the traditional firewall*

Keywords: Next generation firewall, traditional networks, Types of traditional firewall systems, Limitations, similarities and differences between two firewalls

I. Introduction

1.1 Firewall Architecture

A firewall is a hardware system that tracks outgoing and incoming network traffic and determines whether specific traffic should be allowed or blocked based on a collection of security rules. To deter attacks, firewalls carefully analyse incoming traffic using pre -defined rules and filter traffic from unsecured or suspicious sources. Firewalls protect traffic at a computer's ports, which are the points where data is shared with external computers. A firewall may be hardware, software, or a combination of the two.

II. Related Work

Dr. Ajit Singh and Madhu Pahal reviewed the various forms of firewalls in 2013. They've looked at network firewalls to assist businesses. Multiple networks that want to share information over the network, as well as the environment. A firewall protects internet traffic and is less restrictive to outbound and inbound content, as well as giving internal users the illusion of anonymous FTP and www access to the internet[1].

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd representatives presented research in 2016 on how to create a more secure network by integrating firewall capability and firewall technologies. The findings of the experiment prove that the suggested concept is capable of constructing a stable network. This study discussed how firewalls are used to shield infrastructure from outside intruders and how Virtual Private Networks (VPN) allow encrypted access to the corporate network over nonsecure publ ic networks [2].

Jayesh Surana, Kriti Singh, Neha Bairagi, Nivedita Mehto, Nupur Jaiswal present a review paper in which they give a review about what is the firewall and what are various advantages and disadvantages of using it and discuss some techniques.

III. Traditional Firewalls

A traditional firewall is a type of network security system that performs stateful inspection of network traffic as it enters or exits a network, based on state, port, and protocol. As a result, a traditional firewall primarily manages control flow. the traditional firewall also has a VPN(Virtual private network feature). It can only track traffic on layers 2 and 3.

3.1 Types of Traditional Firewalls

A. Packet Filters

Using predefined rules, packet filtering prevents a local network from unwanted intrusion. Knowledge is sent over a network in the form of packets, which travel in their own way through IP networks. This small packets are only

DOI: 10.48175/568

allowed to pass through a node if they match predefined filtering rules; otherwise, they are dropped. As a result, the network layer firewalls' filtering rules in a packet filtering firewall tend to be extremely effective in providing protection mechanisms.

A. Advantages

- Filtering headers is quick and easy.
- Cost-effective
- It does not use a lot of resources.

B. Limitations

- There is no user verification.
- They can be difficult to set up.
- They don't have a lot of logging options.

3.2 Application-Level Gateway

An application gateway, also known as an application level gateway (ALG), is a network security firewall proxy. It filters incoming node traffic according to such criteria, ensuring that only network application data is filtered. File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP), and BitTorrent are examples of network applications.

A. Advantages

- The secure network is totally hidden from the Internet.
- It has the same filtering capabilities as a packet filtering firewall.
- Application inspection firewalls are more capable of preventing attacks than stateful firewalls.

B. Limitations

- It has a slower response time
- Performance.
- Require modification of client.

IV. Circuit-Level Gateway

A circuit-level gateway is a firewall technique that secures UDP and TCP connections and operates between application layers including the session layer and (OSI) network models. Unlike application gateways, circuit-level gateways keep track of TCP data packets and session contentment in order to ensure that firewall rules and policies are followed. [3].

4.1 Advantages

- Filtering individual packets is overlooked.
- Circuit level gateways are comparatively inexpensive
- Implementation is easier.

4.2 Limitations

- Just accepts TCP connections.
- Individual packets are not filtered by circuit level gateways.

4.3 Disadvantages of Traditional Firewall

- It doesn't have an IDS(Intrusion Detection System).
- Cannot efficiently control internet traffic.
- It cannot protect against any attacks that bypass the firewall [3].
- A traditional firewall is unable to scan every packet that passes through them for virus contents.

Traditional Evolution to Next-Generation Firewall:

V. Next-Generation Firewall

A next-generation firewall (NGFW) is a hardware or software-based device security mechanism that can detect and counter sophisticated attacks by applying security measures at the application, port, and convention levels. [4].

A Next-Generation Firewall (NGFW) is a coordinated system stage that combines a traditional firewall with other system network device filtering functionalities, such as an application firewall that uses deep packet inspection (DPI) as part of line deep packet inspection (DPI), an intrusion prevention system (IPS), and/or other procedures, such as SSL and SSH interference, website filtering, and QoS/bandwidth management [4].

Traditional firewall functions such as packet filtering, network address translation (NAT), URL blocking, and virtual private networks are combined in NGFW (VPNs). It also complies with the Quality of Service features (QoS). Intrusion protection, SSL and SSH inspection, deep -packet inspection, reputation-based malware identification, and device recognition are among the features. NGFWs scan packet payloads and match signatures for malicious behaviors like exploitable attacks and malware. It aims to add more OSI model layers to the system.

5.1 Features

- Stateful Inspection
- User Control(Identity Awareness)
- URL filtering
- Application control
- Intrusion Detection/Prevention System (IDS/IPS)

5.2 Advantages

- Single Console Access: we can access the firewall from the single console.
- Multi-Layered Protection: next-generation firewall inspect the traffic from layer 2 to layer 7.
- Optimal Use of Network Speed: Regardless of the number of computers or authentication protocols, the next-generation firewall still achieves its maximum throughput.
- It cuts down on the number of security appliances that are required.

VI. Evolution Of Next-Generation Firewalls

6.1 Unified Threat Management Firewall (UTM)

The only firewall that includes user identities in firewall rule matching requirements is the UTM firewall, which allows businesses to customise policies and classify users directly by username rather than IP address. It's a strong hardware firewall that offers stateful and deep packet inspection to protect businesses from IP spoofing, access control, user authentication, and network and application-level security.

Small and medium enterprises, as well as remote and branch offices, will benefit from UTM firewalls, which carry sophisticated network security capabilities to them. Traditional firewalls can only restrict or allow traffic based on IP addresses and ports, and they have no security beyond that. In today's Internet, where many applications send and receive traffic over ports that are normally enabled by traditional firewalls, this strategy is rapidly becoming obsolete.

6.2 Features of UMTS

- Single hardware platform.

DOI: 10.48175/568

- 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

6.3 Advantages of UTM

- Cost-effectiveness
- Flexibility and Adaptability
- Centralized Management
- Cost-effectiveness
- Ease of development

VII. Similarities And Difference

Traditional Firewall and. Next Generation Firewall (NGF):

7.1 Similarities

Clearly and broadly useful of both traditional firewalls and the NGFWs is the almost same – both firewall intension is to secure an association's system and the information resources of associations system. As far as the product parts bundled by the two, traditional firewalls and the NGFWs both incorporate some same variety of the accompanying Static packet sifting that squares packets at the interface to a system network, in light of conventions, ports, or at addresses [4].

- Both Traditional Firewall and. Next-Generation Firewall has a network- and port address translation (NAT) feature.
- Virtual private network (VPN) supports the security features of a private network over the segment of an association which directs the web or the other open network [5].
- Stateful inspection, also known as dynamic packet filtering, verifies the validity of each association on each firewall interface.

7.2 Differences

Traditional Firewall	Next Generation Firewall (NGF)
Traditional Firewall is old security system.	Next Generation Firewall (NGF) is new security system.
Traditional firewalls only cover from layer 2 to Layer 4.	Next-Generation Firewall only covers from layer 2 to Layer 7.
It does not have a full set of security capabilities.	It supports a number of defence technologies.
It does not support Application-level awareness.	It supports Application-level awareness.
It supports only Partial Application Visibility and Application Control.	It supports Detailed Application Visibility and Application Control.
It does not support IPS (Intrusion Prevention System).	It supports IPS (Intrusion Prevention System).
It has lower Throughput and performance compare to Next-Generation Firewall.	It has higher Throughput and performance compare to Traditional Firewall.

DOI: 10.48175/568

VIII. Conclusion

This paper examines the Firewall architecture, traditional Firewall types its features, advantages, and limitations, and next-generation firewall similarities and differences compared to the traditional firewall. The firewall of the future. After a brief review, we have come to the conclusion that the next-generation firewall combines traditional firewall functionality with its own. It is a hardware -software network defense solution that detects and blocks advanced threats by applying security policies and lowering the overall cost of ownership.

References

[1]. Dr.Ajit singh, Madhu Pahal, Neeraj Goyat , A Review Paper On Firewall, "International Journal For Research In Applied Science And Engineering Technology" ,Vol. 1 Issue II,.

[2]. 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

[3]. Saurav P.J, A Brief Survey on Next Generation Firewall Systems over Traditional Firewall Systems, International Journal of Scientific & Engineering Research Volume 11, Issue 1, January-2020 795.

[4]. Manoj R Chakravarthi, Next Generation Firewall- A Review, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016.

[5]. Manisha Patil, Savita Mohurle, the Empirical Study of the Evolution of the Next Generation Firewalls, Volume - 1

[6]. Jayesh Surana, Kriti Singh, Neha Bairagi, Nivedita Mehto, Nupur Jaiswal, Survey on Next Generation Firewall, Volume 5, Issue 2.

[7]. Imperial journal of interdisciplinary research (IJIR) VOL -2, ISSUE-5,2016, Next-Generation Firewalls, ISSN :2454-1362

[8]. 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.

DOI: 10.48175/568