A Brief Survey on Next Generation Firewall Systems over Traditional Firewall Systems

Saurav P.J

ABSTRACT

Introducing a next generation firewall security for all systems and devices. These Days, security is been a requirement and a need for all data's, information, details etc to be secured. Firewalls are also called as the great wall of networks, in which they protect heavy anonymous threats, bitcoins heist, packet filtering etc. Firewalls act as security gateways which examine the ingress and egress traffic between LAN and WAN networks. Where default, all firewalls filter and allow traffic to flow if it matches a precise rule exception, otherwise all traffic will be disavowed by an implicit deny-all rule that is the absolute and final rule of a firewall. Traditional network firewall cannot be used for latest iot devices and home security systems, to overcome the disadvantages of the traditional firewall, next generation firewalls are introduced. This paper gives the empirical study of tradition firewalls, and latest technology in Next Generation firewalls like (NGFW), UTM, which brings a new level of security among the unsecured world.

KEYWORDS: **Next generation firewall, traditional networks, IPS, IDS, UTM, special (NGFW) features, types of traditional firewall systems, limitations, similarities and differences between two firewalls, NGFW management and deployment.**

1.INTRODUCTION

A next generation firewall (NGFW) is, as Gartner says it, a "deep-packet inspection firewall that moves away from port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall". A next-generation firewall defines the latest evolution in firewalls that take traditional firewall objectives of packet filtering, network, port translations and stateful inspections adding additional filtering, that includes inspecting and prevention of network traffic. Execution of a firewall while executing these functions is important in determining which product should be selected by an organization.

When assessing firewall performance, there are several places that an organization will get the values. They could go to the product vendors and ask for the accomplishment of their products directly and they try to compare. One problem arises with this methodology: which are the values that the firewall might provide hypothetically not be an "apples-to-apples" comparison but an "apples-to-oranges" comparison. For example, products might report a value of number of packets through an interface. One product might count packets by sending packets with a low payload. Another product may count packets that are sent with a size of 64k payload.

Saurav P.J, B.E computer science engineering in "RAJALAKSHMI ENGINEERING COLLEGE". Thandalam, Chennai, Tamil Nadu, India. EMAIL: sauravpj@gmail.com.

The results for these two devices would be very different based on these testing methods. This makes comparisons of results almost impractical when getting values directly from the products.

Another way for an organization when attempting to compare firewall performance results, it can run the testing on their own. First, an organization must figure out how to configure a firewall. It would be incompetent to create the test cases, so therefore it would be best to go find the requirements for benchmarking a firewall.

As Stewart mentions: "Listing the types of firewalls is almost like listing the taxonomy of the animal kingdom in biology. The variations, models, and versions are numerous. In addition, opinions vary about what is and is not a firewall."

2.FIREWALL DIAGRAM

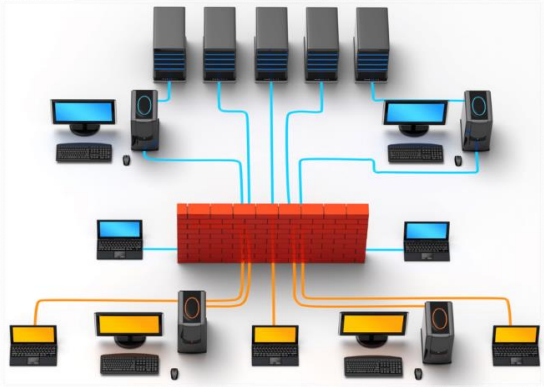

Figure-1 courtesy-google, general design of a basic firewall connection with network.

It is a simple firewall architecture that tells about various electronic devices which is been connected across the firewall device using internet as shown in the above figure.

A firewall is a software program or a hardware device that filters the information's (packets) coming via the Internet to your personal computer. Firewalls decide to allow or block network traffic between devices based on the rules that are pre-configured by the firewall administrator.

3.TRADITIONAL FIREWALLS

A traditional firewall is defined as a device that controls the flow of traffic allowed to enter or exit a point within the network. It can typically do, either using a "stateless" method or "stateful" method, depending on the type of protocol being used. Traditional firewalls can only track traffic on layers 2-4.

3.1 TYPES OF TRADITIONAL FIREWALLS

3.1.1 PACKET FILTERS

Packet filtering is a firewall technique that is used to control network access by supervising outgoing and incoming packets and allowing them to permit or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports. It is bounded by a set of rules.

3.1.2 APPLICATION-LEVEL GATEWAY

An application gateway or otherwise called as application level gateway (**ALG**) is a firewall proxy technique which offers network security. It filters incoming node traffic to certain specifications (conditions) which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and BitTorrent.

3.1.3 CIRCUIT-LEVEL GATEWAY

A circuit-level gateway is a firewall technique that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security and works between application layers such as the session layer and (OSI) network models. Unlike application gateways, circuit-level gateways monitor TCP data packets handshaking and session contentment of firewall rules and policies.

3.2 LIMITATIONS

- Firewall cannot scan every incoming packet for malicious contents. So, it cannot protect the internal network from virus threat. So Internal traffic cannot be handled effectively.
- It does not provide (IDS) Intrusion Detection System.
- It cannot protect against any attacks or threats that bypass the firewall.

These limitations should be undertaken seriously in the next generation firewall (NGFW) in which the security techniques will be advanced over traditional firewalls.

4. EVOLUTION OF NEXT GENERATION FIREWALL

Improved detection of encrypted applications and intrusion of prevention services. Modern threats like web-based malware attacks, targeted attacks, application-layer attacks, and more have a notable negative effect on the threat areas.

4.1 UNIFIED THREAT MANAGEMENT FIREWALL (UTM)

UTM is a firewall that focus on simplicity and ease of use. **UTM** devices have a limitation which will not be able to detect modern advance threats as they are unable to inspect deeply inside the packet and identify threats or malicious contents.

UTM firewalls bring advanced network security technologies to small and medium businesses and remote offices. Traditional firewalls can only **ACCEPT/BLOCK** traffic based on IP addresses and ports and offers little protection outside of that.

4.1.1 FEATURES OF UTM

Nearly all unified threat management application incorporates the same special features. Some of the applications may also include extra features in order to request to certain customers.

- Antivirus
- Antimalware
- Firewall
- Intrusion Prevention

- Virtual private networking (VPN)
- Web filtering

4.1.2 ADVANTAGES OF UTM

- Ease of use.
- Simple technique.
- No complexity.

4.1.3 ADDITIONAL KEY POINTS OF UTM

- UTM solutions recommend unique benefits to small and medium businesses that are looking to improve their security programs.
- they have certain capabilities of many specialized programs that are contained in a single appliance, UTMs decrease the complexity of a company's security system. Some UTM solutions provide additional benefits for companies that is in strictly regulated industries.
- Appliances that use identity-based security to report on user activity while enabling policy creation based on user identity meet the requirements of regulatory compliance such as HIPPA, CIPA, and GLBA.
- UTM solutions also help to protect networks against combined threats.

These threats consist of various types of malware and attacks that target separate parts of the network at once.

4.2 NEXT GENERATION FIREWALL(NGFW)

A next-generation firewall (NGFW) is an equipment or programming-based system security framework that can differentiate and square refined attacks by applying security approaches at the application level, and as well at the port and convention level.

A Next-Generation Firewall (NGFW) is a synchronised system stage that joins a conventional firewall with other system network gadget filtering functionalities, for example an application firewall exploiting as a fragment of line deep packet inspection (DPI), an INTRUSION DETECTION SYSTEM (IDS), Also (IPS) and/or various procedures, for example, website filtering, QoS/bandwidth management, antivirus inspection and outsider/third-party integration.

If we compare between traditional firewall and next generation firewall (NGFW) security-based systems, in which they have less similarities and more differences.

5. INTRUSION DETECTION SYSTEM and INTRUSION PREVENTION SYSTEM

5.1 IDS

Intrusion in lay terms which is unwanted or unauthorized interference and as it is unwanted or unauthorized, it is then normally with bad intentions. The intention of the intrusion is to gather information linked to the organization such as the structure of the internal networks or software systems like operating systems, tools/utilities, or software applications castoff by the organization and then pledge connections to the internal network and carry out attacks.

An Intrusion Detection System (IDS) is a software/hardware combination that detects the intrusions into a system or network. IDS set off a firewall by providing a comprehensive inspection of both the packet's header and its contents thus safeguarding against attacks, which are otherwise identified by a firewall.

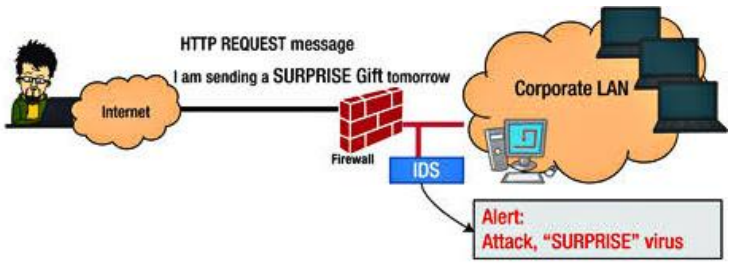

Figure-2 courtesy-google, example for IDS and its importance.

5.2 IPS

It works in the same zone of the network as a firewall system, among the outside world and the internal network. IPS is very much aggressive which rejects network traffic created on a security profile if that same packet characterizes a known security threat. An **Intrusion Prevention System** (IPS) is a network security/threat prevention technology that analyses network traffic flows to detect and prevent vulnerability abuses. These Vulnerability abuses normally come in the form of malicious inputs to a target application or service that attackers use to take over the control and interfere machine or an application.

the Intrusion Detection System (IDS) acts as a predecessor —which is a passive system that scans traffic and reports back on threats—the IPS is positioned in order that it is in the direct communication path between source and destination, actively examining and taking automated actions on all traffic flows that enter the network.

5.2.1 IPS FUNCTIONS

- Sending an alarm to the administrator.
- Dropping the anonymous packets.
- traffic is been blocked that comes from the source address.

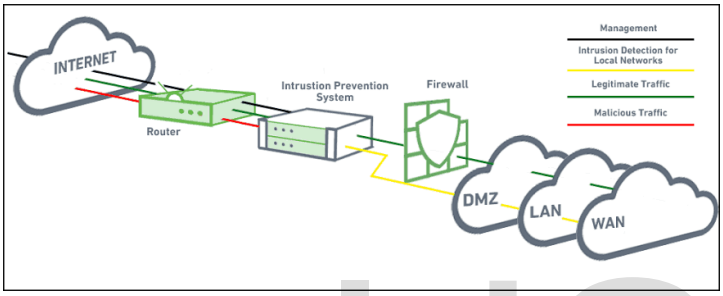

Figure-3 courtesy-google, example for IPS and its importance.

6. NGFW FEATURES

- Application Recognition.
- Stateful Inspection.
- Integrated Intrusion Protection System (IPS).
- Bridged and Routed Approaches.
- Utilization of external intelligence sources.

Threat detection system is well advanced for more security purposes. This firewall has more capabilities for threats being analysed. Some features are visibility driven; threat focused etc.

6.1 NGFW NETWORK VISIBILITY

- Threat activity across users, hosts, networks, and devices.
- The visibility of Where and when a threat originated, where else it has been across your extended network, and what it's doing now.
- **Active applications** and **websites**.
- Communications between virtual machines, file transfers, etc.

6.2 NGFW FLEXIBLE MANAGEMENT AND DEPLOYMENT OPTIONS

- Management for every **use case** - choose from an on-box manager or centralized management across all appliances.
- Deploy **on-premises** or in the **cloud** via a virtual firewall.
- Customize with features that meet your needs – simply turn on subscriptions to get advanced capabilities.
- Choose from a wide range of throughput speeds.

6.3 ADVANTAGES OF NGFW

- It packs traditional firewall functionality with intrusion prevention, antivirus and protocol filtering.
- It scans content to avoid data leakage and stop threats with detailed, real-time traffic inspection.
- Immediately respond to attacks.
- Improved detect evasive or suspicious activity.
- Reduce complexity.

7. SIMILARITIES AND DIFFERENCES BETWEEN THESE TWO FIREWALL SYSTEMS

7.1 SIMILARITIES

- Static packet filtering that forms packets at the interface to a system network.
- Stateful inspection or dynamic packet filtering, which checks each association on each interface of a firewall for the authenticity.
- Network address translation for the re-mapping of the IP addresses contained into packet headers.
- 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.

7.2 DIFFERENCES

- Non-disruptive, in-line, bump-in-the-wire (BITW) arrangement, in which a secrecy firewall lives inside the subnet so that it can filter traffic channel activity between hosts.

- Integrated signature-based intrusion prevention system (IPS), which indicates different kinds of attacks to filter and gives a brief report.

- Ability to integrate information from outside the firewall, including index-based arrangements, white records, and boycotts.

- Recognizable proof of applications using predefined application signatures, payload examination, and header inspection. Network security strategies are implemented at application level since the security segments are turned down into territory of abuse by malicious contents.

- Next generation firewall systems have extensive control and visibility of applications that it can identify using analysis and signature matching.

- They can use white lists, or a signature based IPS to distinguish between safe applications and unwanted stuffs, which are then detected using SSL decryption.

These are some similarities and differences between next generation firewall (NGFW) and traditional firewall systems.

8. CONCLUSION

This paper gives a brief study on next generation firewall systems over traditional firewall systems. Internal structures and systems are been explained clearly. Advantages and other special features like similarities and differences between these two firewalls have also been pointed out unambiguously. Deep Packet Inspection be the integration of Intrusion Detection (IDS) and Intrusion Prevention (IPS) can nowhere reach the old capabilities of traditional firewall technology. It is the best network security systems that can be used to block and quarantine attacks/threats according to the security policies. Going forward will there be successive progress in network technology and advancement which in turn will have the capabilities to detect and block advanced threats and attacks.

9. REFERENCES

1. 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.
2. Manoj R Chakravarthy / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3), 2016, 1212-1215, ISSN:0975-9646.
3. https://www.researchgate.net/publication/271893800_Next-generation_firewalls_Security_with_performance.
4. Manisha Patil | Savita Mohurle "**The Empirical Study of the Evolution of the Next Generation Firewalls**" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-1 | Issue-5, August 2017, pp.193-196, url:https://www.ijtsrd.com/papers/ijtsrd2259.pdf.
5. https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more.DIGITAL GUARDIAN leads a new edition 2017 by Gartner magic quadrant report by CHRIS BROOK.
6. https://gtb.net/why-gtb/blog/when-traditional-firewall-doesn%E2%80%99t-go-far-enough.GTG GOBAL TELECOM October 2, 2017 By Joel Njoroge.
7. https://www.techopedia.com/ Techopedia™ is a. It was started by the father-and-son team of Dale and Cory Janssen. **Dale Janssen - Co-founder Janalta Interactive Inc.**
8. https://www.gajshield.com/index.php/nextgenerationfirewall Mr. SONIT JAIN who is the CEO of GAJSHIELD in2002, GajShield is striving to deliver robust and best in class security mechanisms.
9. https://searchsecurity.techtarget.com/ RENOWNED CONSULTANTS including JOHNA TILL JOHNSON, CEO and founder of Nemertes Research, Nick Lewis, CISSP, Michael Cobb, CISSP-ISSAP.
10. https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_11 Intrusion Detection and Prevention Systems **Authors**: UMESH HODEGHATTA RAO and UMESHA NAYAK **Open Access**: Chapter **First Online:** 01 September 2014.
11. Imperial journal of interdisciplinary research (IJIR) VOL-2, ISSUE-5,2016, Next-Generation Firewalls, ISSN :2454-1362.
12. https://www.varonis.com/blog/ids-vs-ips/Yaki Faitelson and Ohad Korkus - founded Varonis in 2005. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips.

13. https://www.cisco.com/c/en/us/products/security/firewalls/. **Cisco Systems, Inc.** is an American multinational technology conglomerate. Cisco Systems was founded in December 1984 by Leonard Bosack and Sandy Lerner, two Stanford University computer scientists.
14. https://www.cisco.com/c/dam/en/us/products/collateral/security/next-gen-firewall.pdf.
15. https://digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls. **Digital Guardian** is an American data loss prevention software company. The company was founded in 2003 under the name Verdasys.