International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-167 PAGE NO: 1018-1023
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

A SURVEY ON AUTHENTICATION AND HIGH PERFORMANCE OF NETWORK SECURITY USING NEXT GENERATION FIREWALL SYSTEM

S.Poornimavathi,
M.phil Scholar, Department of Computer Science,
Sri Vasavi College [SFW], Bharathiar University, Erode-638 316, India.
E-mail id: poornimavathi1994@gmail.com, Ph: 9500711222

ABSTRACT- Network security is a broad area of research. This paper will concentrate on a recent development in network security, which is next-generation firewall (**NGFW**) at the system perimeter. The paper will express how this moderately new type of firewall technology can be used in intrusion detection, analysis and response. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. This paper will benefit the security area by sharing useful knowledge and techniques related to Next Generation Firewalls. It will also help people to choose better firewall solutions for their enterprise.

Keywords: Firewall, network security, intrusion detection, DDoS attack, authentication, data integrity.

1. INTRODUCTION

Network systems and internet are so important in today's business. There also invite accidental or malicious attack on company's important data which can costs losses in terms of working hours, customers trust and actual revenue. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network Security helps to protects from a variety of threats and also need multiple layers of security. In this paper, implement the high performance network security by using next-generation firewall system. Firewalls achieve analyses of the traffic itself at least to the extent that they scrutinize the headers on data packets or envelopes adjacent data payloads or content.

1.1 OBJECTIVE

Firewalls make compulsory ingress policy rules to protect malicious and attack data from incoming the domain they protect. To achieve ingress policy enforcement, firewalls frequently implement some limited egress policy rules, to check requests from being sent by an entity in the protected domain to a suspicious, anomalous, or known-malicious thing in the unfrosted domain. Firewall policy rules may rely exclusively on an access control list that indicates which entities in an unfrosted domain should be allowed to transmit traffic through the firewall to an entity in the trusted domain.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-167 PAGE NO: 1018-1023
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

1.2 MOTIVATION

Security is a very complex topic as everyone has a different aspect of the risk involved in their enterprise. The master key to build a secure network is to find out the key aspects of the firewall predicts whether the traffic satisfies various criteria by which it is deemed admissible into or releasable from the trusted domain.

1.3 SCOPE

The scope of the system is very vast as it can be implemented in any organization where security is a major concern. A firewall that performs deep packet inspection is one that can parse and investigate traffic encoded the network protocol layers. A deep packet inspection firewall must have enough information of application level traffic or the criteria for inadmissible traffic. Depending on which type of policy is enforced the firewall will admit or block the suitable traffic. To implement an efficient protection system, we must influence the network topology and use distributed traffic monitoring and detection. The Internet Service Provider (ISP) network domains cover the edge networks where the protected systems are physically connected.

2. RELATED WORK

A firewall is a device that serves as a fence between networks providing access control, traffic filtering, and other security features. Firewalls are commonly deployed between trusted and untrusted networks, for example between the Internet and an organization's trusted private network. Firewalls can also be used internally to segment an organization's network infrastructure, for deploying a firewall between the corporate financial information and the rest of the company network. In firewall, making most favorable use of any security technology, process, or knowledge is sensibly a step in the right direction. The first generation of firewalls was referred to as packet filters. These devices functioned by inspecting packets to see if the packet coordinate the packet filter's set of rules. Packet filters acted on each individual packet did not pay any consideration to whether or not a packet was part of an active stream or flow of traffic. Today generally firewalls are based on stateful inspection. A firewall policy may include anomalies, where a packet may counterpart with two or more different filtering rules.

However, limitations in dealing out power of current generation firewalls prevents deep packet inspection from being useful to more than a small minority of the packets traversing the device.

3. EXISTING METHODOLOGIES

Previously, implemented two fundamental choices either block the whole thing in the interest of network security, or enable everything in the importance of your business. These choices left little room for compromise.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-167 PAGE NO: 1018-1023
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

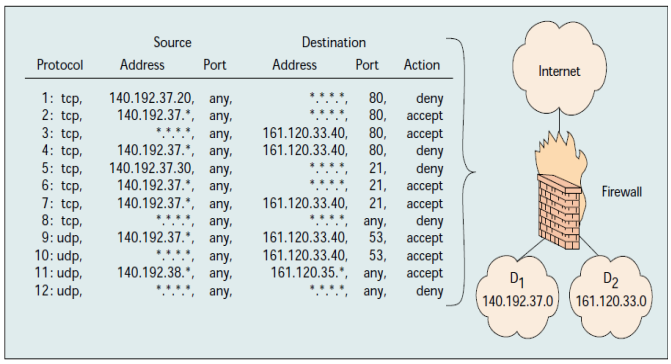

Fig 1: An example of Typical Firewall Filtering Policy

As shown in the figure, the firewall filtering policy is shown in which the action is taken on the packets at the source and destination level. Filtering is done by using the parameters such as protocol, IP address and port used for communication. A firewall security policy is a list of prearranged rules that define the events performed on network packets based on specific filtering conditions. A rule is composed of a set of filtering fields such as protocol type, source and destination IP addresses and ports, as well as an action field. The filtering fields of a rule characterize the possible values of the consequent fields in actual network traffic that matches this rule. Filtering actions are either to accept, which permits the packet into or from the secure network, or to deny, which causes the packet to be blocked. The packet is permitted or blocked by an explicit rule if the packet header information matches all the network fields of this rule. Modeling of firewall rule relations is important for analyzing the firewall policy and designing management techniques such as anomaly discovery and policy editing. To be able to build a useful model for filtering rules, we need to determine all the relations that may relate packet filters.

4. ENTERPRISE REQUIRMENTS

The network encompasses several external sites together with hospitals and clinics as well as various vendors and suppliers. They do not control those exterior sites, they must provide access to them and that the approach they have adopted is that they "do not trust anything outside of their campus" they found themselves in the condition where they had a security policy and no ability to enforce it as they could not be sure of what applications were being used. In general, they house their Web servers inside their Demilitarized Zone (DMZ) so they can control the applications that run on those servers. As a part of the connection if they were running programs such as Bit Torrent they were vulnerable to being charged with breaking copyright laws. In addition, if they were supporting recreational applications such as Internet Radio, they were wasting a lot of WAN (Wide Area Network) bandwidth. Traditional firewalls do not provide any application layer filtering so if you are attacked above Layer 3 you are compromising with your security. The IT organization had been looking at adding other security functionality such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). What enterprises wanted, is to avoid the complexity of having a large number of security appliances.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-167 PAGE NO: 1018-1023
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

5. PROPOSED METHODOLOGIES

Next Generation Firewall provides a way to securely enable the applications to users need by allowing access while preventing cyber security threats. NGFW is the core of the enterprise security platform, designed from the ground up to address the most complicated threats. The next-generation firewall inspects all traffic inclusive of applications, content, and threats and ties it to the user, in spite of location or device type. The application, content, and user the elements that run your business become essential components of your enterprise security policy. Policy based routing provides the independence to route packets based on the organization's needs, as an alternative of routing packets based exclusively on their target IP address and the local routing table. There are many reimbursement to policy based routing however this subsection addresses using policy-based routing to put into practice a transparent web proxy. The main advantage of this technique is leveraging a separate web security gateway appliance in a transparent manner; the policy based routing is configured to transmit HTTP, HTTPS and FTP traffic to the web security gateway, which listens for the traffic and acts as a transparent/implicit proxy. This would allow use of supplementary specialized network and security services not frequently present in NGFWs, such as web caching and HTTPS traffic inspection.

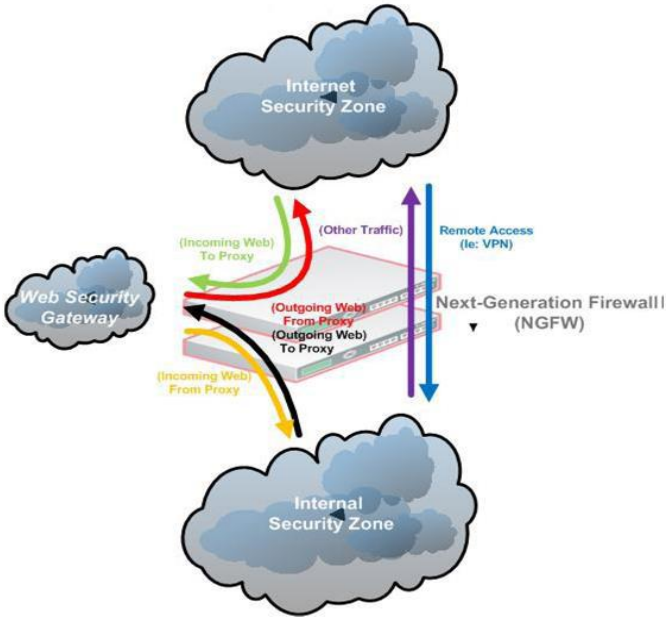

Fig 2: Policy Based Routing on Next Generation Firewall

In particular, firewalls are typically placed at a point where site accessed in Wide Area Network (WAN). This is the logical place for a policy and security control point for the WAN. It is understandable that IT organizations have deployed work-around to attempt to make up for the limitations of traditional firewalls. This approach has serious limitations including the fact that the firewall helpers often do not see all of the traffic and the deployment of multiple security appliances significantly drives up the operational costs and complexity. In order for the firewall to avoid these limitations and reestablish itself as the logical policy and security control point for the Wide Area Network, need is a Next Generation Firewall.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-167 PAGE NO: 1018-1023
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

The following features represent a sample of security services offered by Next Generation Firewall:

• **Application Identification:** The firewall must be able use deep packet inspection to look beyond the IP header 5- tuple into the payload of the packet to find application identifiers. A library of application signatures developed that includes identifiers for all commonly used initiative applications, recreational applications, and Internet applications. The library needs to be easily extensible to include signatures of new applications and custom applications.

• **Prolonged Stateful Inspection:** Application sessions can be tracked beyond the point where dynamic ports are selected, the firewall will have the ability to support the detection of application-level anomalies that signify intrusions or policy violations.

• **SSL Decryption/Re-encryption:** The firewall will need the ability to decrypt SSL-encrypted payloads to look for application identifiers. When this inspection is performed and policies applied, allowed traffic would be re-encrypted before being progressed towards its destination. Secure Socket Layer (SSL) proxy functionality, together with application identification, will remove the port 443 blind spot.

• **Control:** Traditional firewalls works on a simple deny or allow model. In which, everyone can access an application that is deemed to be good. Nobody can access an application that is deemed to be bad. This model had supplementary validity at a time when applications were monolithic in design and earlier the Internet made a wide variety of applications available.

• **SSL Proxy:** Manage encoded threats by selectively terminating SSL connections, decrypting, analyzing traffic, and re-establishing encrypted connections transparently.

• **Data Leakage Prevention (DLP):** Control flow of intellectual property, credit card numbers and other sensitive information.

• **Network Access Control (NAC):** Integrate with Network Access Control (NAC) solutions in provisioning appropriate network access.

6. CONCLUSION

This paper has concentrated on exploring and explaining the counter measures which are used to improve the security of networked computers. The basic concept of a network and the need for an effective security policy was introduced. The correct implementation, deployment and configuration of all of these systems form some of the most effective measures that are available in the battle for the defense of computer systems. The most robust NGFWs enable administrators to control and administer both business and non-business associated applications to enable network and user efficiency, and they can scan files of unlimited size across any port and without security or performance degradation. The number of

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 3, 2017 ISSN: 2348-6600
Reference ID: IJCS-167 PAGE NO: 1018-1023
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

immediate files or network streams does not limit high-end NGFWs, so infected files do not have an opportunity to slip through undetected when the firewall is under heavy load. In addition, NGFWs can apply all security and application control technologies to SSL encrypted traffic, ensuring that this does not become a new malware vector into the network.

7. FUTURE WORK

In future this system can be extended by using large data sample set and by incorporating as many major attacks possible also more accurate threshold value can be found which can help to making the firewall system more precise in network security.

8. REFERENCES

[1] Alex X. Liu Eric Torng Chad R. Meiners, Department of Computer Science and Engineering Michigan State University East Lansing, U.S.A 978-1-4244-2026-1/08 2008 IEEE

[2] LI Xingyu, JIANG Tingting, Heilongjiang University,China Heilongjiang Polytechnic, China IEEE Workshop on Electronics, Computer and Applications 2014

[3] Ehab S. Al-Shaer and Hazem H. Hamed, DePaul University e-Transactions on Network and Service Management, Second Quarter 2004

[4] Mr.Vikrant G. Madankar, Prof. Ranjit R. Keole, Implementation Of High Performance Network Security Using Next Generation Firewall System, IJJEAT, ISSN: 2321-8134, April-2015.