Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Adaptive Firewall Design for Household Networks

Reddyvari Venkateswara Reddy, Maddi Sandeep Manikanta,
Utkoor Prashanth, Chokkaraju Lalitesh Sai
Associate Professor, Department of CSE (Cyber Security),
CMR College of Engineering & Technology,
Hyderabad, India
B.Tech Students, Department of CSE (Cyber Security),
CMR College of Engineering & Technology,
Hyderabad, India

***Abstract*- Various cyber threats, especially SYN flooding attacks, that Distributed Denial of Service (DDoS) is a policy and implementation of an adaptive firewall. Such attacks are monitored, and their effect is mitigated in the SDN architecture. Thus, identifying any irregular patterns within the backlog queue can be used as a pointer for detecting SYN flood attacks, hence initiating corresponding defensive measures. Therefore, firewalls should mitigate against DDoS attacks by adjusting policies to adapt to changing threats on the network. In implementing an adaptive firewall, it is important to establish strong monitoring mechanisms and develop smart counteraction strategies to handle emergent risks. This approach ensures that the firewall functions effectively in maintaining maximum performance and availability for optimal network infrastructure security. To counteract sophisticated threats introduced by advanced hackers, organizations need to continuously refine policies through adaptation of this method to secure the backbone and reduce the potential vulnerability exposed through them.**

Keywords: **PfSense Firewall, Snort IDS, Ntopng Tool, Virtual Box, and Kali Linux.**

INTRODUCTION

In an ever-more interconnected world, the safety of home networks is essential. Cyber threats can be greatly enhanced with the rise of smart devices and the IoT (Internet of Things), which has broadened the attack surface [1]. Therefore, there cannot be a better time for a strong and adaptive firewall specifically designed for home networks [16]. The project "Adaptive Firewall Design for Household Networks" aims to solve this critical need by having an all-encompassing dynamic firewall infrastructure [20].

Often consisting of a wide range of gadgets, including computers, smartphones, smart TVs, and IoT devices, among others, home networks are prone to attacks such as malware infections, unauthorized access attempts, and data breaches. Indeed, traditional firewalls may provide some level of security, but they often lack the flexibility and sophistication to effectively counter contemporary cyber threats.

The main goal of the project is to develop robust network firewall solutions that will help secure household computer systems [20]. This involves adopting pfSense, which is an open-source firewall platform that is known for its stability and flexibility, to reach the intended goals. If pfSense is integrated with other tools like ntopng, Lightsquid, pfBlockerNG, and Snort [25].

Adaptability is one of the most important characteristics of a firewall proposal [8]. Dynamic environments are what home networks are known for, and as such, various devices always join and leave the network [11]. This means that the firewall should be capable of adjusting to these changes in real-time to enable an unbroken shield against any form of threat [12]. With dynamic rule sets and automated responses to threats, the firewall can adjust effectively against developing cyber risks without requiring perpetual human intervention [19].

Additionally, this project highlights preventative security measures like content filtering as well as intrusion detection systems [28]. By denying access to social media sites and other harmful sources of content, the firewall safeguards members within a household from exposure to inappropriate or malicious materials, especially those that children may accidentally open up [29]. Also, active monitoring of log files from firewalls coupled with patterns in network usage could lead to early detection of suspicious activities, thereby ensuring a timely response toward eliminating potential threats [22].

I. LITERATURE REVIEW

This research paper gives a bird's-eye view of network security by outlining both current issues and future trends. The latter looks at the technologies behind network security and solutions, giving practical clues on how to implement them in real-life situations. As of today, wireless network security is considered an integral part of the modern networking infrastructure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Northcutt, Novak, & winters (2001) addressed this issue with regard to network intrusion detection systems that provide the capacity for identifying and mitigating the effects of security threats. Nevertheless, Chen, Qian, & Mao (2013) take into account all perspective aspects of connectivity, from theoretical bases to real-life solutions [7].
Cheswick & Bellovin (1994) have based liberalism on firewall technology, covering ways to stop web space invasion. Linux-based designs used in the development as well as deployment of firewall systems are discussed by Wang and Wei (2007)[9]. Mirkovic et al. (2002) represent the essence of designing firewalls with due consideration to their reliability aspects. Finally, Fang et al [15]. (2009) introduce a design for packet-filtering firewalls built upon embedded systems that provides insights into resource-efficient solutions [24].

II. OBJECTIVE

The objective of the project is to strengthen our cyber security through the installation of resilient network-level firewall solutions. This project will establish a comprehensive as well as proactive defense against unauthorized access, cyber threats, and possible security breaches within their network infrastructure [5]. Implementation of this project will involve the use of advanced hardware and software-based firewalls that are capable of monitoring, analyzing, and controlling both incoming and outgoing traffic on the network. As such, we shall be much more secure as a network while protecting critical assets and confidential data from ever-increasing sophisticated cyber threats [2]. In addition to this, it should be noted that the project goals for firewall implementation are in line with best practices in the industry as well as compliance standards so that we can meet or exceed regulatory requirements [9]. Among others, these would include configuring firewall rules, intrusion prevention systems (IPSs), and virtual private networks (VPNs) for a layered defense approach. Furthermore, this initiative is also about how the company's incident response capability can be elevated by integrating firewalls with monitoring and alerting systems [10].

III. SYSTEM REQUIREMENTS

To guarantee that the operating system, virtualization software, and network management tools can operate at the same time, a relatively large RAM of 16GB and above is required in the hardware. For effective storage of the operating system, virtual machines, and network monitoring data, it's highly recommended to have at least one 50GB solid-state drive (SSD).
Performing tasks related to virtualization and network monitoring efficiently will call for a fast processor, such as an Intel Core i5 or higher. Software Requirements:

1. Operating System (OS): Linux distributions: Several Linux distributions exist that can be used as host operating systems for both virtualization software and network monitoring tools.

2. PfSense: In this installation, PfSense acts as an OS designed specifically for firewall and router functions aimed at securing a home or enterprise network.

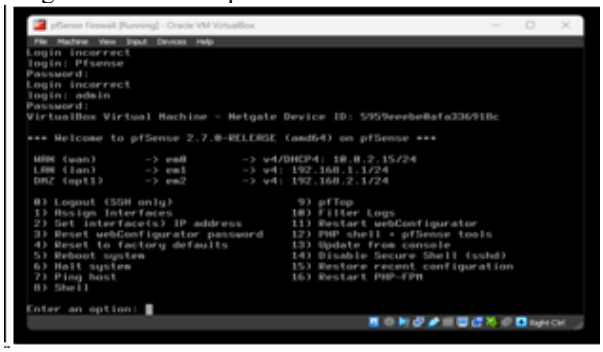

Fig-1: PfSense Firewall

Virtualization Software:
Virtual Box: Virtual Box is a famous open-source virtualization platform where users run several guest-operating systems simultaneously on one host machine. It can deploy VMs meant for testing networks or experimenting with them.

Fig-2: Virtual Box

Fig-3: Ntopng Monitoring Tool

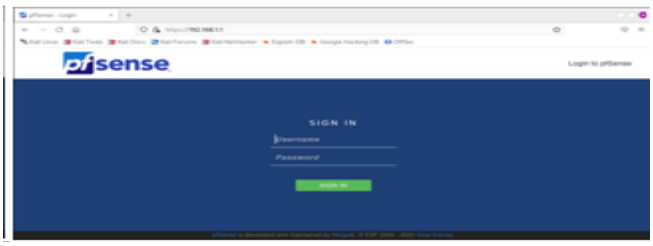

Fig-4: PfSense Website

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

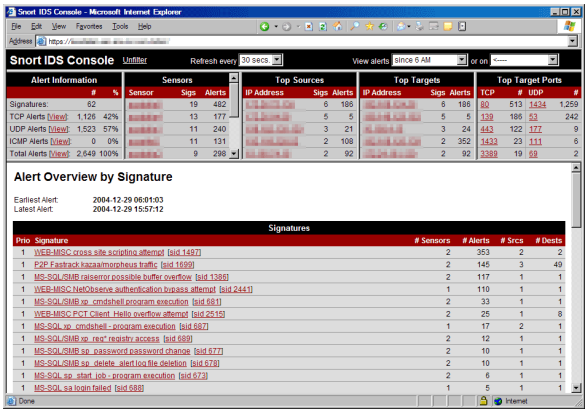

Fig-5: Snort IDS

IV. PROBLEM DEFINITION

The current network infrastructure lacks a strong and tailored software firewall solution to meet the organization's security needs effectively. Without a robust firewall system, the network becomes susceptible to unauthorized access, malicious activities, and potential threats, risking the confidentiality, integrity, and availability of critical data and services.

V. EXISTING SOLUTIONS

1. Cisco ASA: Adaptive security appliance ASA is a product with strong security and it scales well. It has advanced malware protection, an IPS, site-to-site VPN, and application visibility and control that are very robust. In the light of this therefore, Cisco ASA not only caters for small businesses but also large organizations hence becoming a universal solution to network security issues in any organization that needs reliable network security.

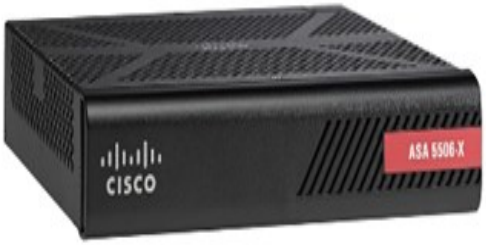

Fig-6: Cisco ASA

2. Juniper SRX: Juniper SRX (Services Gateway) is a powerful security service meant for different sizes of networks such as; unified threat management (UTM), IPS, application visibility, web filtering identity based firewalling SSL VPN connectivity etc., which address broader aspects of Security services. Thus it addresses the requirements of data centers, service providers and enterprises by giving them scalable options so as to ensure secure.

Fig-7: Juniper SRX

3. Palo Alto Networks Firewall: Palo Alto Networks Firewall is known for its next-generation firewall functionality as well as advanced threat prevention capabilities. It applies application-based policies, URL filtering, intrusion prevention systems (IPS) and SSL decryption among others which fortify the defenses of an organization against cyber attacks. Advanced Threat Protection being a high priority and need for granular control over application traffic means that this Firewall can be effectively employed by such companies.

Fig-8: Palo Alto Network Firewall

VI. WORK FLOW

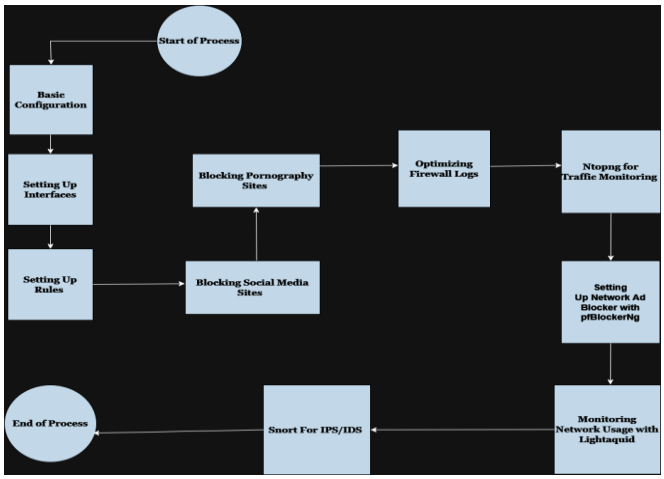

Fig-9: Work Flow

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

1. Basic Setup: It might include the basic infrastructure of the network, such as IP addresses and subnet masks.
2. Interface setting Up: At this stage, you can set up firewalls, determine which networks are trusted and untrusted, and also control or enable specific ports.
3. Block Pornography Sites: This implies configuring the network to limit access to obscene websites.
4. Block Social Media Sites: Like preventing pornographic sites from being accessed through a network, this process is intended for configuring the network so that it won't allow any access to social media platforms' sites.
5. Rules setting Up: These probably refer to certain basic rules for managing traffic on a network, such as enabling or denying traffic from some IP addresses and ports.
6. Monitoring Traffic with Ntopng Optimization: It must be configured correctly in order to capture different types of data about traffic within a given network as well as analyze it.
7. Configuring Network Ad Blocker with pfBlockerNG: This should be configured using an open-source DNS-based ad blocker, thereby stopping ads alongside other malicious content.
8. Snort for IPS/IDS: There are countless other things regarding Snort, which is just an open-source intrusion detection system (IDS) whose configuration is required to track down all sorts of threats within a specific network.

VII. ARCHITECTURE

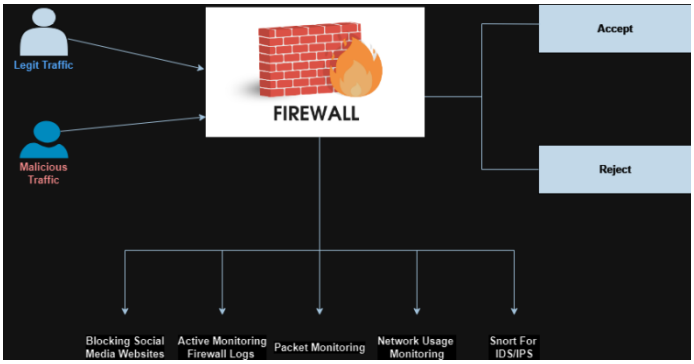

Fig-10: Architecture

1. The real deal Traffic: This is the traffic that goes across the firewall and finally reaches its destination on some network.
2. Dissdyke Data: It represents inbound data that may be harmful or untrustworthy, thus being blocked by the firewall to prevent security breaches.
3. Firewall: It is placed as a demarcation between a trusted internal network and an untrusted external network like the Internet, where packets coming through are evaluated against established security rules to allow them in or deny them access.

Diagrammatical dissection:

1. Accept: Allows normal intra-network flows
2. Reject: Blocks malicious network traffic from entering
3. Blocking social media websites and pornographic sites: The reasons for this have primarily been directed towards disallowing such sites so that they do not offer any dangerous content.
4. Active monitoring and continuous scanning for suspicious activities.
5. Packet Monitoring/IIP Checking individual data packages for misbehavior, malware content, etc.
6. Network Usage Monitoring: Checks total levels of network traffic to identify potential failures.
7. Snort for IDS/IPS refers to using Snort, which is an open-source intrusion detection and prevention system that can check network traffic for signs of security attacks and even block them.

VIII. CONCLUSION

In conclusion, our project is introducing a high-level network software firewall that has been designed with only a few rules. This solution has complete logging capability, packet filtering, and content control, and it can integrate the Intrusion Detection and Prevention System (IDS/IPS) as well as deep packet inspection for strong protection against possible threats. Acting as an alert watchdog, the firewall will supervise the network traffic, thereby ensuring the safe operation of the internet.

IX. RESULTS

Fig-11: PfSense Login

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

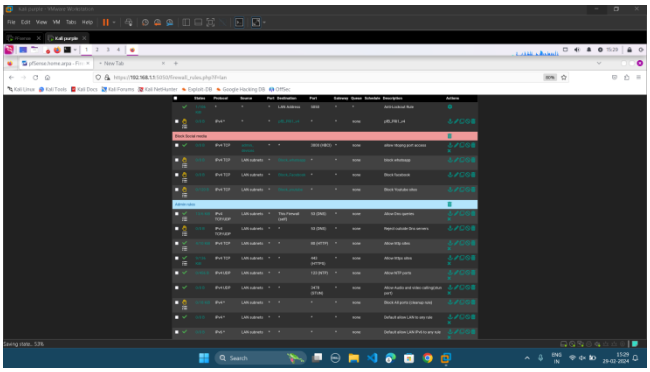

Fig-12: Setup Rules

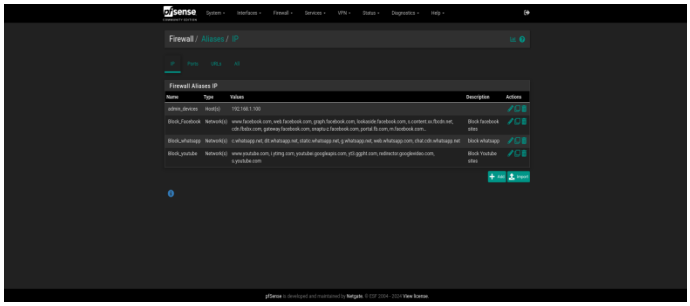

Fig-13: Aliases for Social Media Websites

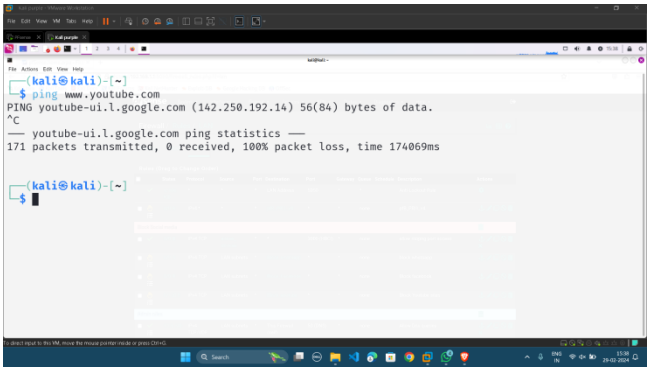

Fig-14: Blocking YouTube Website

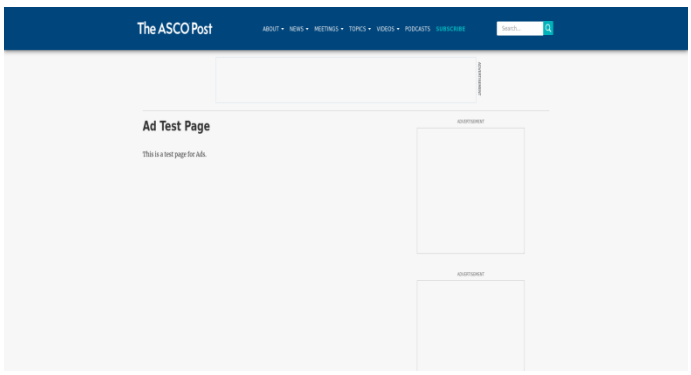

Fig-15: Blocking Ads in Websites

X. REFERENCES

[1] Douligeris, C., & Mitrokotsa, A. (2004). Network Security: Current Status and Future Directions. Wiley.

[2] Chen, T., & Abu-Amara, H. (2007). Network Security Technologies and Solutions. Cisco Press.

[3] Harkins, D., & Carrel, D. (2007). Wireless Network Security: A Beginner's Guide. McGraw-Hill Education.

[4] Northcutt, S., Novak, J. I., & Winters, S. (2002). Network Intrusion Detection: An Analyst's Handbook. New Riders.

[5] Chen, Y., Qian, H., & Mao, Z. M. (2018). Network Security, Springer.

[6] Ferguson, P., Peralta, R., & Ross, G. (2007). Network Security Essentials: Applications and Standards. Pearson.

[7] Cheswick, William R., and Steven M. Bellovin. "Firewalls and internet security: repelling the wily hacker." Addison-Wesley Professional, 2003.

[8] Wang, Weijun, and Lei Wei. "Design and Implementation of Firewall Systems Based on Linux." 2010 International Conference on E-Product, E-Service, and E-Entertainment (ICEEE), pp. 1-4. IEEE, 2010.

[9] Mirkovic, Jelena, Sven Dietrich, and David Dittrich. "Internet firewall design: An introduction." International Conference on Dependable Systems and Networks, 2002, Proceedings., pp. 253-262. IEEE, 2002.

[10] Fang, Qing, Weirong Jiang, and Shufeng Ren. "A design of packet filtering firewall based on embedded systems." 2008 International Symposium on Computer Science and Computational Technology, vol. 3, pp. 425–428, IEEE, 2008.

[11] Carrara, Giuliano, Roberto Giorgetti, and Romano Fantacci. "Enhancing the security of packet filtering firewalls." In Proceedings of the 20th IEEE International Conference on Advanced Information Networking and Applications, pp. 1061–1066, IEEE, 2006.

[12] Li, Ming, et al. "Improving the performance of packet filtering firewalls through machine learning techniques." IEEE Transactions on Network and Service Management 15.4 (2018): 1633–1646.

[13] Wang, Wei, et al. "An adaptive approach to packet filtering firewall configuration using genetic algorithms." Journal of Network and Computer Applications 35.2 (2012): 573-582.

[14] Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks. Pearson Education.

[15] Stallings, W. (2013). Network security essentials: applications and standards. Pearson.

[16] Zou, D., Zhu, J., & Chen, H. H. (2009). Intrusion Detection Systems and Cybercrime.

[17] Xie, Y., Yu, X., & Tyan, H. (2014). Intrusion Detection Systems and Cyber Security: First International Conference, IDSCS 2009, Beijing, China, December 10-11, 2009.

[18] Zhang, Z., Zhu, J., & Chen, H. H. (2008). Special Issue: Intrusion Detection Systems and Cyber Security.

[19] Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K., & Kar, S. (2014). Network anomaly detection: A machine learning perspective. CRC Press.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

[20] Choo, R., & Dionysiou, I. (2012). Intrusion Detection Systems.

[21] Roesch, M. (1999). Snort: Lightweight intrusion detection for networks.

[22] Bace, R., & Mell, P. (2001). NIST Special Publication on Intrusion Detection Systems.

[23] Rash, M., Misra, I., & Nayak, N. (2018). An Introduction to Intrusion Detection Systems.

[24] Kumar, N. N., & Kaur, P. (2013). A Comprehensive Review on Intrusion Detection System.

[25] Wu, M., & Robertazzi, T. G. (2004). A survey of intrusion detection systems in wireless sensor networks.

[26] Abomhara, M., & Koien, G. M. (2015). The Impact of Network Intrusion Detection Systems on Performance.

[27] Grégio, A. R., Silva, E. C., Silva, R. M., & Nakamura, L. H. (2012). A review of intrusion detection systems in wireless sensor networks.

[28] Sung, T. K., Mukkamala, S., & Abraham, A. (2003). Intrusion Detection Systems.

[29] Alazab, M., Hobbs, M., & Abawajy, J. (2012). Intrusion Detection Systems: A Survey and Taxonomy.