IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Comparative analysis of Firewall Techniques and it's performances

Dr. Nirmala S Gupta
Professor, Dept of CSE
Sri Venkateshwara College of Engineering. Bengaluru, India

Mr Abhishek V M
Student, Dept of CSE
Sri Venkateshwara College of Engineering. Bengaluru, India

Mr Abhi Puttaswamy M P
Student, Dept of CSE
Sri Venkateshwara College of Engineering. Bengaluru, India

Mr Eragam Kamal
Student, Dept of CSE
Sri Venkateshwara College of Engineering. Bengaluru, India

Mr Dhanunjaiah R
Student, Dept of CSE
Sri Venkateshwara College of Engineering. Bengaluru, India

Dr.Ambika B J,
Assistant Professor Senior Scale,
Department of CSE,
Manipal Institute of Technology Bengaluru,Manipal Academy of Higher Education,Karnataka, India.

ABSTRACT:
This paper explores the firewall security and performance relationship for different firewall systems. The firewall is a important component of the network for safe communication. A firewall acts as a barrier that provides security by controlling security threats. Through a thorough investigation of different firewall technologies, this research aims to recognize the strengths and weaknesses of each firewall system, determining the algorithm and method of network security. This paper is a structural study of research papers which have been carried out on the different Firewall technologies. This research paper focuses on comparative analysis of different methodologies used, accuracy in packet filtration, and the comprehensive evaluation of the performance of various firewall systems.

KEY WORDS: Firewall security, Packet filter firewalls, Kernel-based firewalls, Pre-filtering ACL, Cloud-based firewalls, Two-stage algorithm, Redial algorithm, Virtual Machine.

1.INTRODUCTION:

Firewalls are networking models that prevent unwanted access and protect critical assets from malignant traffic. Firewall is a system—either hardware or software, or a combination of both—that enforces security rules and regulations by allowing or blocking network transmissions and data packets to enforce control between two networks/packets to protect the inside network from outside network. A firewall could also be a program that might be running on a secured host computer. Firewalls are meant to enforce different security technology regulations on network of an organization. The firewall is an important component of the network for secure communication. There are several types of firewalls, such as software firewalls, hardware firewalls, physical firewalls, virtual appliance firewalls, kernel-integrated firewalls, distributed firewalls, network firewalls, and host-based firewalls which can secure data connections. A physical firewall is composed of physical components such as a motherboard, CPU, memory, and network interface cards [2]. The virtual firewalls are constructed entirely of software. The

physical firewall is unable to track the activities of a virtual machine when it connects to other virtual machines (VMs) running on different hypervisors (software used to run multiple VMs) over the same IP network. Since the physical firewall only supports IP-based policies, it won't recognize a virtual machine's new IP address [2]. It is possible for a distributed firewall to track the traffic that flows through virtual machines on the same virtual switch, and among virtual machines running on different hypervisors and the internet. Network firewalls are those that help to provide security between networks and run on network hardware. Firewalls that are host-based are designed to filter traffic coming to the hosts or end devices. The Distributed Firewalls are a software applications installed on individual hosts. It safeguards enterprise network servers as well as end-user machines by preventing unauthorised intrusion. Hardware firewalls provide protection to a local network and are usually part of a TCP/IP router. The software firewalls are the computers with firewall software that offers protection from intruders and may also provide internet connectivity between private LAN and public network/ internet. The research surveys the influence of firewall complexity on security rules, acknowledging that the complexity increases , so does the resulting rule list and latency. This results in a closer examination of the application programming interface (API), which serves as the gateway to accessing data from virtual platforms, influencing the optimization process on firewalls. This research aims to contribute valuable insights into the arena of firewall performance, by evaluating their role in security technology regulations within networks, we seek to identify the performance of different firewall techniques that have advanced over the past few years.

2. LITERATURE SURVEY:

Automated Firewall Configuration in Virtual Networks [1] - Daniele Bringhent, Guido Marchetto, Riccardo Sisto, Fulvio Valenza, and Jakiliddin Yusupov [1]. The research paper presents a novel, fully automated methodology for the optimal allocation and configuration of packet filter firewall in a Network Function Virtualization environment. The method, pointed at dropping human errors and resource consumption, is planned to be extended to other Network Security Functions and integrated into mitigation mechanisms for automatic response to cyber-attacks.

A virtual data center comparison of different firewalls' performance [2]- Hanane Aznaoui, Canan Batur sahin [2]. The research paper investigates the efficacy of various firewalls in a virtualized data center, emphasizing the dynamic rule-updating capability of kernel-based firewalls that ensures uninterrupted security settings across hypervisors. The methodology involves monitoring and filtering traffic at the kernel level in different scenarios.

Traffic and Overhead Analysis of Applied Pre-filtering ACL Firewall on HPC Service Network [3] -Jae-Kook Lee, Taeyoung Hong, and Guohua Li [3]. The research paper presents a methodology that applies a pre-filtering Access Control List (ACL) policy aims to decrease the proportion of discarded packets from 90% to under 50%, which in turn lessens the traffic burden and CPU usage of the firewall. The paper also outlines forthcoming strategies to implement a machine learning approach for smart firewall examination and automated security system.

An innovative two-stage algorithm to optimize Firewall rule ordering [4]- Antonio Coscia, Vincenzo Dentamaro, Stefano Galantucci, Antonio Maci, Giuseppe Pirlo [4]. The paper proposes a two-stage algorithm for optimizing firewall security rules to minimize packet classification latency. The first stage uses a Directed Acyclic Graph for constraint modeling and rule identification, while the second employs a Genetic Algorithm for complete solution finding.

Design and Implementation of Firewall Security Policies using Linux Iptables [5]- M. G. Mihalos, S. I. Nalmpantis and K. Ovaliadis [5]. The paper presents a case study on Linux Net filter and iptables firewall technology, evaluating its routing and security aspects through a multi-VM-layered rules simulation. It highlights iptables efficiency in monitoring traffic, identifying malicious attacks, and potential drawbacks in application-oriented policies.

A Formal Model and Technique to Redistribute the Packet Filtering Load in Multiple Firewall Networks [6] - Luca Durante, Lucia Seno and Adriano Valenzano [6]. The paper introduces a innovative technique for redistributing filtering rules among cascaded firewalls to reduce packet processing overhead, using the transformation algorithm called REDIAL. The approach, verified through simulation, offers real-time firewall configurations, compatibility with prevailing systems, can be combined with other optimization techniques.

Security Issues of Firewall - Aakanksha Chopra [7]. The research paper explores the vulnerabilities of computer networks to various attacks and the limitations of conventional firewalls. It introduces the

Design and Implementation of a Distributed Firewall Management System for Improved Security [8] - Andrei-Daniel Tudosi, Adrian Graur, Doru Gabriel Balan, Alin Dan Potorac [8]. The paper introduces a novel Bash script that automates firewall management. This script integrates optimization algorithms and machine learning performance optimization, and includes a logging system for monitoring changes. This method improves network security procedures, minimizes human errors, and supports regulatory adherence.

3.COMPARATIVE ANALYSIS OF METHODOLOGIES:

Paper	Methodology / Technique	Performance	Pros	Cons
Automated Firewall Configuration in Virtual Networks- Daniele [1] 2023, IEEE	Automated Methodology	The allocation scheme and configuration of packet filters in the logical topology of a virtual network is automated. This is accomplished by solving a specially formulated problem of partial weighted Maximum Satisfiability Modulo Theories (MaxSMT) with the help of an advanced solver.	Offers automation of firewall configuration, guarantees correctness of solutions, optimizes resource usage by minimizing the number of firewalls and rules needed, and outperforms existing solutions.	Its complexity, dependence on the solver's performance, limited scope to packet filters, potential operational complexities due to unsupported scripts, and time-consuming initial setup and configurations.
A virtual data centre comparison of different firewalls' performance - Hanane Aznaoui, Canan Batur sahin [2] 2023, Journal of Advancement in Computing (JAC)	Kernel-Level Firewall Installation and Management	The execution of a kernel-based, distributed firewall in a virtualized data center can dynamically update its rules to adapt to changes in virtual machine IPs or networks, ensuring continuous connectivity and enhanced security.	Kernel-based firewalls, which operate effectively under all conditions and dynamically update their rules to accommodate changes in VM	other categories such as physical, virtual appliance, and application firewalls rely on IP-based policies and require manual updates by network managers for policy alterations when a VM's IP or network changes to maintain connectivity.
Traffic and Overhead Analysis of Applied Pre-filtering ACL Firewall on HPC Service Network [3] 2021, journal of communications and networks [3]	Pre-filtering with Access Control List (ACL)	The application of a pre-filtering ACL rule in a High-Performance Computing (HPC) service network reduces the ratio of released packets from 90% to less than 50%, decreases the number of anomalous IPs from 600 to 50, and accurately reduce the CPU load by 21.5%, thereby significantly reducing firewall's traffic overhead[3]	1.Stateful inspection firewalls can block many types of denial-of-service attacks and IPS. 2.Application-level gateways can detect and block attacks not visible at the OSI model network	1.Stateful inspection firewalls and application-level gateways have high processing overhead. 2.Application-level gateways and next-generation firewalls are complex to configure and maintain.
An innovative two-stage algorithm to	Two-stage algorithm:	The proposed two-stage algorithm significantly improves firewall	two-stage algorithm that uses a Directed Acyclic	methodology might be complex to implement, could

optimize Firewall rule ordering - Antonio Coscia, Vincenzo Dentamaro, Stefano Galantucci, Antonio Maci, Giuseppe Pirlo [4] 2023, Elsevier	topological sorting algorithm, Genetic Algorithm	performance by minimizing packet classification latency through optimal reordering firewall security rules.	Graph and a Genetic Algorithm for efficient firewall rule optimization, with dynamic system performance adjustments, offering significant improvements in network communication speed and security.	introduce stochastic bias, may have limitations due to dependency constraints, lacks a detailed comparative analysis with other methods, and its effectiveness in real-world scenarios might vary.
Design and Implementation of Firewall Security Policies using Linux Iptables - M. G. Mihalos, S. I. Nalmpantis and K. Ovaliadis [5] 2019, journal of Engineering Science and Technology Review[5]	Iptables as an implementation mechanism	To optimize iptables performance, prioritize rule ordering, use jumps, summarize addresses, optimize large rulesets, and consider splitting rules based on the IP address distribution.	Iptables, an open-source and robust firewall technology, excels in traffic monitoring, malicious attack detection, and managing complex tasks like load balancing and traffic flow prioritization, although it has some limitations in handling application-specific policies.	The performance of a firewall can decrease when handling a high volume of traffic
A Formal Model and Technique to Redistribute the Packet Filtering Load in Multiple Firewall Networks - [6] 2021, IEEE	Transformation algorithm called REDIAL	REDIAL is a technique that optimizes firewall security by reallocating filtering rules among cascaded firewalls, thereby reducing packet processing load, enhancing real-time configuration capabilities, and maintaining compatibility with existing systems, all of which have been validated through simulation.	increases packet processing rate by redistributing the packet filtering load among multiple firewalls, adapting to traffic changes while preserving network security.	its specificity to certain network configurations, lack of real-world implementation guidance and dependence on specific traffic conditions.
Security Issues of Firewall - Aakanksha Choprab[7] 2016, International Journal of P2P	Encryption algorithm: AES-256 (Advanced Encryption Standard), RSA-4096	Host-resident security solution that offers enhanced network protection by filtering traffic, enforcing centralized policy control, and eliminating single point failures in perimeter firewalls.	Firewalls offer enhanced security and centralized protection, maintenance complexity	Packet filtering firewalls lack advanced rule-based models, circuit level gateways fail to filter individual packets, and application level gateways.

4.RESULTS COMPARATIVE ANALYSIS:

Automated Firewall Configuration in Virtual Networks:

The presented methodology computes the optimal allocation of packet filter firewalls in a fully automatic way. The proposed approach uses both traditional and virtual network with service graph allocation and configuration which optimizes number of firewall and of rules, has scalability 100FW-90S [1].

A Virtual Data Center Comparison of Different Firewalls' Performance:

A kernel-based, distributed firewall is the best way to protect against viruses [2]. Virtual machine IP addresses and networks can vary, and the kernel-based firewall can dynamically update its rules to keep pace with such changes [2].

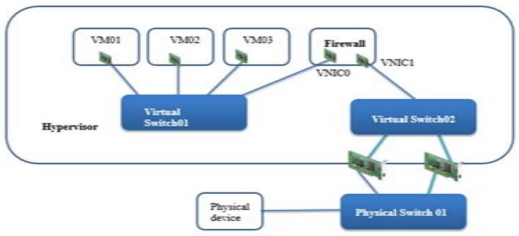

Fig 1. Firewall virtual appliance

Traffic and overhead analysis of applied pre-filtering ACL firewall on HPC service network:

To reduce the overhead of the firewall, they added and applied method-based ACL policy in front of the firewall that allows access only to the infrastructure nodes in a service. The results show that the ratio of the dropped packets is reduced from 90% to less than 50% [3].

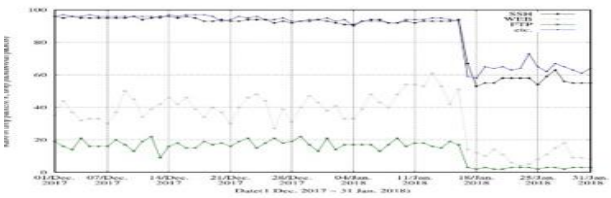

Fig 2. Ratio of the dropped packets for all services with pre-filtering ACL [3].

An innovative two-stage algorithm to optimize Firewall rule ordering: This paper proposed an innovative two-stage algorithm aimed at minimizing packet classification latency by optimally reordering FW security rules [4]. The proposed first stage algorithm encodes the precedence relationships between the rules using a directed-acyclic graph (DAG) [4].

Design and Implementation of Firewall Security Policies using Linux Iptables:

Linux and iptables have excellent performance of routing traffic throughout the virtual network, iptables has been configured to define if the traffic is legitimate to flow around the routing source and destinations [5].It drastically represented all malicious attacks simulation that was performed at the RouterFW [5].

A formal model and technique to redistribute the packet filtering load in multiple firewall networks: The process of packet filtering by a firewall involves identifying a rule that aligns with each incoming packet and subsequently executing the relevant action on that packet. Firewall rules are checked sequentially and, as soon as a match is found for the incoming packet, the corresponding action is executed reducing packet processing overhead during overload conditions, such as traffic peaks or DoS attacks [6].

Security issues of firewall:

A Distributed Firewall serves as a tool to enforce a security policy across a network domain, utilizing a specific policy language. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate [7].

Design and Implementation of a Distributed Firewall Management System for Improved Security:

By automating distributed firewall management, our solution brings increased efficiency and effectiveness to network security operations [8].

CONCLUSION:

Based on comprehensive review of eight research papers on firewall security published from 2016 to 2023, the most effective firewall and firewall technique identified is the optimal allocation scheme and configuration of packet filtering firewalls in virtual networks. This method is distinguished by its all-encompassing capabilities, including network distribution and setup, enhancement, and the ability to scale effectively. While all eight papers contributed significantly to these findings, the specific papers that hoisted out were those focused on optimal allocation scheme and configuration of packet filtering firewalls in virtual networks. In the future, the focus is to work on proposed methodology to further optimize performance of the firewall.

REFERENCES:

[1] Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F., & Yusupov, J. (2022). Automated firewall configuration in virtual networks. *IEEE Transactions on Dependable and Secure Computing*, *20*(2), 1559-1576.

[2] Aznaoui, H., & Şahin, C. B. (2023). A Virtual Data Center Comparison Of Different Firewalls' Performance. *Journal of Advancement in Computing*, *1*(1), 1-8.

[3] Lee, J. K., Hong, T., & Li, G. (2021). Traffic and overhead analysis of applied pre-filtering ACL firewall on HPC service network. *Journal of Communications and Networks*, *23*(3), 192-200.

[4] Coscia, A., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G. (2023). An innovative two-stage algorithm to optimize Firewall rule ordering. *Computers & Security*, *134*, 103423.

[5] Mihalos, M. G., Nalmpantis, S. I., & Ovaliadis, K. (2019). Design and Implementation of Firewall Security Policies using Linux Iptables. *Journal of Engineering Science & Technology Review*, *12*(1).

[6] Durante, L., Seno, L., & Valenzano, A. (2021). A formal model and technique to redistribute the packet filtering load in multiple firewall networks. *IEEE Transactions on Information Forensics and Security*, *16*, 2637-2651.

[7] Chopra, A. (2016). Security issues of firewall. *Int. J. P2P Netw. Trends Technol*, *22*(1), 4-9.

[8] Tudosi, A. D., Graur, A., Balan, D. G., & Potorac, A. D. (2023, September). Design and Implementation of a Distributed Firewall Management System for Improved Security. In *2023 22nd RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). IEEE.

[9] Lavanya N L, Nirmala S Guptha , "Detection and Mitigation of Vampire Attacks in Wireless AD-HOC Sensor Networks", AEIJST, Vol 2, Issue 4, April 2014,2348- 6732

[10] Vikas A V , Nirmala S Guptha , "Secure of Data on stored Cloud from Decentralized Access Control with Anonymous Authentication" , (AJETI), 2018, 200-204, ISSN:2347-7385

[11] Nirmala S Guptha, Kiran Kumari Patil "Detection of Macro and Micro Nodule Using Region **International Journal of Intelligent Engineering & Systems",** INASS Journal, Vol.11, No.2 2018,

[12] Nirmala S Guptha, Kiran Kumari Patil "Earth Movers Distance Based CBIR Using Adaptive Regularized Kernel Fuzzy C-Means Method Of Liver Cirrhosis Histopathological Segmentation", **International Journal of Signal and Imaging Systems Engineering, Inderscience Publishers**, Vol.10, Nos.1/2 2017, (IJSISE; e-ISSN: 1748-0701, p-ISSN: 1748-0698), pp39-46.