A Survey of SDN-based Firewalls: Integration, Performance and Security Enhancements

Abu Sayed
Department of Computer Science and Engineering
Independent University, Bangladesh
Dhaka, Bangladesh
2030155@iub.edu.bd

Tauhidul Islam
Department of Computer Science and Engineering
Independent University, Bangladesh
Dhaka, Bangladesh
2030441@iub.edu.bd

***Abstract*—Software-Defined Networking (SDN) has revolutionized network architecture by decoupling the control plane from the data plane, enabling more flexible and dynamic network management. This paper analyzes the latest developments in SDN-based firewalls, emphasizing the improvements in integration, performance, and security. We describe approaches for implementing and assessing SDN firewalls and examine their key characteristics, advantages, and difficulties. Our analysis emphasizes how SDN may improve network security by integrating threat intelligence, centralized policy management, dynamic policy enforcement, and increased visibility.**

***Index Terms*—Firewall, Software-Defined Networking (SDN), Cybersecurity, Integration, Network Visibility, Machine Learning, Network Traffic Analysis**

I. Introduction

Modern networks are becoming more dynamic and complex, which calls for increasingly advanced security measures. Even though they are necessary, traditional firewalls frequently cannot keep up with the changing threat landscape and the demand for scalable administration. Software-Defined Networking (SDN) provides a possible solution , which offers a programmable network architecture that improves security policy implementation and maintenance.

Conventional firewalls have fixed characteristics that might be challenging to maintain and adjust because they are hardware-based. As networks grow and evolve, these firewalls face several challenges. Traditional firewalls struggle to expand as additional devices are added and network traffic rises, which leads to scalability concerns. It is difficult to adapt its static architecture to dynamic threats and changing network conditions. Managing firewall rules across many devices in large networks can be difficult and prone to error, which could lead to security vulnerabilities. Furthermore, the little information that traditional firewalls offer about user behavior and network traffic makes it more challenging to recognize and respond to sophisticated threats.

SDN-based firewalls use SDN's centralized control and flexibility to improve security monitoring, policy enforcement, and threat minimization. One of the main benefits is centralized control, which allows uniform policy enforcement across the network. SDN improves defense against attacks by enabling the dynamic and adaptive updating of firewall rules in real time in response to network conditions. By dividing the control plane from the data plane, it improves the ability to track and analyze data flows and provides increased visibility and analytics. Because SDN is more programmable, management is made easier by lowering the likelihood of configuration errors and strengthening security protocols. Furthermore, SDN permits seamless firewall capabilities scalability and flexibility without necessitating significant infrastructure changes.

Since its creation, SDN technology has advanced significantly in response to the need for network infrastructures that are more programmable and flexible. The goal of early SDN designs was to improve network administration and flexibility by dividing the control and data planes. SDN may now be used more widely thanks to the creation of the OpenFlow protocol, which standardized communication between the control and data planes. Industry-specific solutions were accessible as SDN advanced, giving carrier and business networks solid foundations. Advanced security capabilities like intrusion detection and prevention, firewall functionality, and automated threat response are all included in modern SDN solutions.

SDN-based firewalls are essential for modern networks for a number of reasons. The increasing complexity and emphasis of cyber attacks demands security measures that are dynamic and adaptive, something that traditional firewalls are unable to offer. Scalable, flexible security solutions that function in virtual environments are becoming more and more necessary as cloud computing and network virtualization gain traction. The growth of IoT devices increases the attack surface, necessitating strong security measures that can handle a variety of heavy traffic loads. Organizations must comply with strict regulations, which frequently call for sophisticated security systems and ongoing monitoring.

SDN-based firewalls, which offer improved flexibility, scalability, and efficacy in thwarting contemporary cyberthreats, constitute a major breakthrough in network security. The current state of SDN-based firewalls, including their integration, performance, and security developments, is covered in this paper's implementation and evaluation survey. We think that this survey will offer a comprehensive grasp of how SDN might change network security protocols.

II. Literature Review

According to recent studies, Software Defined Networking (SDN) is essential to the revolution of network security since it offers customized firewall solutions that are suited to a wide range of organizational requirements. Research highlights SDN's capacity to apply customized filtering algorithms and dynamically divide networks, solving the shortcomings of traditional firewalls, especially in healthcare contexts [1]. Comparative analyses have explored the performance implications of SDN-based firewalls on UDP traffic, and the results have shown trade-offs in packet delivery ratios and scalability issues [2]. When compared to traditional firewall techniques, the use of distributed firewalls in LAN environments has shown to be an effective means of intercepting threats from the inside as well as the outside, all while having minor effects on network throughput [3].

Research has focused on improving security settings through layer-based packet filtering combat flooding attacks, demonstrating SDN's flexibility and effectiveness in reducing network security risks [4]. In order to handle complexity and potential conflicts, formal verification frameworks that make use of TLA+ have been proposed to guarantee consistent enforcement of firewall rules across dynamic SDN topologies [5]. Through the use of the POX controller, implementation studies have demonstrated the usefulness of SDN-based firewalls in real-world scenarios and provided insights into their administration, integration, and performance advantages over conventional techniques [6].

Stateful firewall systems with flow-based scheduling, which show enhanced scalability and decreased network overhead through distributed controller configurations, are examples of advances in SDN security [9]. SDN's potential for adaptive security measures is further highlighted by the promising prediction and mitigation of attacks demonstrated by the integration of machine learning with stateful firewalls [10]. The integration of SDN principles has enhanced the optimization of threat detection and incident response with classical firewalls, resulting in improved administration, scalability, and security monitoring capabilities [11].

Studies have indicated that SDN control planes can efficiently lower the amount of network traffic and resource usage while permitting the safe gathering and enhancement of firewall rules, thus enhancing the security and efficiency of network operations [12]. SDN-based Layer II firewalls have the potential to enhance network security and dependability by optimizing network performance and successfully mitigating Denial of Service (DoS) attacks [13]. Moreover, software-defined networking (SDN)-based web application firewalls have proven successful in preventing online attacks such as SQL injection. This is accomplished by efficiently identifying and reducing hazards through the use of programmable and centralized control [14].

All of these research point to the revolutionary potential of SDN in network security via adaptive firewall solutions. They highlight how SDN may enhance network performance, manage increasing cybersecurity concerns in a variety of contexts and applications, and enhance security management [15, 16]. Future paths in research are poised to substantially improve SDN-based firewall solutions, ensuring robust network security in ever-more complex digital landscapes. These include creating formal verification techniques, integrating with cutting-edge technology like artificial intelligence, and looking into ways to improve scalability.

III. Methodology

A. System Architecture

The SDN-based firewall system is structured into three primary layers: the Infrastructure Layer, the Control Plane, and the Application Layer.

- Infrastructure Layer: This layer includes sender/receiver hosts and Open vSwitches (OVS). It collects network statuses such as traffic statistics, network topology, and usage, which are sent to the control plane for processing.
- Control Plane: The control plane acts as an intermediary between the application layer and the infrastructure layer, processing instructions from the application layer. The Ryu SDN controller was selected for its research-friendly environment and extensive use in academic settings.
- Application Layer: This layer hosts the firewall application, which uses the control plane's data to enforce security policies and manage network traffic. The application implements multi-stage filtering techniques to control packet flow based on header entities and detect flooding attacks.

B. Flow Table and Controller Interaction

Communication between the infrastructure and control layers is facilitated using the OpenFlow protocol. The developed firewall application filters packets based on their headers and monitors traffic patterns to identify potential threats.

C. Flow Control Algorithm

The flow control algorithm designed to detect and respond to flooding attacks operates in four stages:

- Flow Addition: Adding flows to the flow table based on packet header information.
- Packet Filtering: Filtering packets based on size using queues.
- Packet Counting: Counting packets per second and applying controller-defined rules.
- Action Against Violations: Enforcing actions against packets exceeding defined limits.

Bandwidth (Mbits/sec)	Packet Loss (With Firewall)	Jitter (With Firewall)	Packet Loss (Without Firewall)	Jitter (Without Firewall)
1.25	0.22%	0.017	0.11%	0.008
1.25	0.11%	0.014	0%	0.017
1.25	0.22%	0.018	0.22%	0.011
1.25	0.34%	0.008	0.34%	0.11
1.25	0.12%	0.007	0.11%	0.008
5.03	0.52%	0.02	0.07%	0.014
5.02	0.42%	0.008	0.02%	0.01
5.03	0.52%	0.021	0%	0.011
5.03	0.49%	0.017	0.14%	0.018
5.02	0.41%	0.021	0.02%	0.017
10.1	0.95%	0.033	0%	0.007
10.2	1.50%	0.021	0.11%	0.019
10.1	1.40%	0.024	0.02%	0.016
10.1	0.50%	0.041	0.11%	0.018
10.1	1.50%	0.022	0.12%	0.009

TABLE I
CONSOLIDATED UDP TRAFFIC DATA

D. Experimental Setup

- Environment Setup: VirtualBox was used to create a virtual network environment running Mininet, an SDN network emulator. The Mininet emulation included network topologies with OpenFlow-enabled switches managed by the Ryu controller. Remote access and command execution were facilitated using MobaXterm, and network performance was measured using IPerf.
- Topology and Tools: Mininet topologies were created with and without firewalls between private and public zones. Firewalls were implemented as OpenFlow v1.0 L2 learning switches extended with stateful access control rules. The firewall, written in Python, controlled TCP, UDP, and ICMP traffic.
- Evaluation Metrics: Firewall performance was evaluated using metrics such as UDP disordered packets and jitter, which measures packet inter-arrival time. A comparative analysis assessed network performance with and without the firewall. [2][8][11][15]

Category	Details
Virtual Environment	VirtualBox
SDN Emulator	Mininet
SDN Controller	POX Controller
Network Tools	MobaXterm, IPerf
Firewall Implementation	OpenFlow v1.0 L2 learning switches with stateful access control, Python
Evaluation Metrics	UDP Disordered Packets, Jitter
Topology	Mininet topologies with/without firewalls
Security Policy Management	Implemented in POX controller
Performance Monitoring	Network performance comparison
Additional Considerations	Memory leak problem

TABLE II
DETAILS OF THE EXPERIMENTAL SETUP

Algorithm	Average Prediction Accuracy (%)
Bayesian Network	92.87
Native–Bayes	87.81
C4.5	84.92
Decision Tree	83.18

TABLE III
PREDICTION ACCURACY OF DIFFERENT ALGORITHMS

E. Additional Implementation on POX Controller

- Layer-Specific Firewall Rules:
  - Layer 2 (MAC Address): Controlled traffic based on MAC addresses.
  - Layer 3 (IP Address): Controlled traffic based on IP addresses.
  - Layer 4 (Port Numbers): Controlled traffic based on port numbers.
- Protocol-Specific Rules: Specific scenarios were demonstrated where TCP and UDP traffic on different ports were either allowed or blocked based on the implemented firewall rules.
- Performance Monitoring: The impact of firewall rules on network performance was monitored, focusing on metrics such as packet loss, latency, and throughput. Results were visualized using network topology diagrams and controller output screenshots, providing a clear understanding of the firewall's effectiveness.

REFERENCES

[1] G. Rezaei and M. R. Hashemi, ”An SDN-based firewall for networks with varying security requirements,” in *2021 26th International Computer Conference, Computer Society of Iran (CSICC)*, March 2021, pp. 1-7.

[2] M. F. Monir and S. Akhter, ”Comparative analysis of UDP traffic with and without SDN-based firewall,” in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, January 2019, pp. 85-90.

[3] C. Wang, ”Construction and Deployment of a Distributed Firewall-based Computer Security Defense Network,” *Int. J. Netw. Secur.*, vol. 25, pp. 89-94, 2023.

[4] R. Iqbal, R. Hussain, S. Arif, N. M. Ansari, and T. A. Shaikh, ”Data Analysis of Network Parameters for Secure Implementations of SDN-Based Firewall,” *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 77, no. 2, pp. 1575-1598, 2023.

[5] Y. M. Kim and M. Kang, ”Formal verification of SDN-based firewalls by using TLA+,” *IEEE Access*, vol. 8, pp. 52100-52112, 2020.

[6] S. Deshmukh, A. Gawde, and N. Nagori, ”Implementing Software Defined Networking (Sdn) Based Firewall Using Pox Controller,” *International Journal of Innovations in Engineering Research and Technology*, vol. 8, no. 09, pp. 168-174.

[7] T. Kapus, ”Improved Formal Verification of SDN-Based Firewalls by Using TLA+,” *IEEE Access*, 2023.

[8] Y. Gautam, K. Sato, and B. P. Gautam, ”Layer Based Firewall Application for Detection and Mitigation of Flooding Attack on SDN Network,” PhD dissertation, Muroran Institute of Technology, 2022.

[9] B. P. Kavin, S. R. Srividhya, and W. C. Lai, ”Performance evaluation of stateful firewall-enabled SDN with flow-based scheduling for distributed controllers,” *Electronics*, vol. 11, no. 19, pp. 3000, 2022.

[10] S. Prabakaran, R. Ramar, I. Hussain, B. P. Kavin, S. S. Alshamrani, A. S. AlGhamdi, and A. Alshehri, ”Predicting attack pattern via machine learning by exploiting stateful firewall as virtual network function in an SDN network,” *Sensors*, vol. 22, no. 3, pp. 709, 2022.

[11] A. Sablok and R. S. Hallikar, ”SDN Integration with Firewalls and Enhancing Security Monitoring on Firewalls,” *IEEE Access*.

[12] S. Kim, S. Yoon, J. Narantuya, and H. Lim, ”Secure collecting, optimizing, and deploying of firewall rules in software-defined networks,” *IEEE Access*, vol. 8, pp. 15166-15177, 2020.

[13] A. Mahmud, K. I. Musa, and U. M. Joda, ”Software defined network approach for layer II based distributed firewall,” *Int. J. Intellectual Discourse*, vol. 4, no. 3, pp. 202-217, 2021.

[14] F. M. Alotaibi and V. G. Vassilakis, ”Toward an SDN-Based web application firewall: Defending against SQL injection attacks,” *Future Internet*, vol. 15, no. 5, pp. 170, 2023.

[15] R. Iqbal, ”Towards secure implementations of SDN based firewall,” *Journal of Independent Studies and Research Computing*, vol. 20, no. 2, 2022.

[16] F. N. Nife and Z. Kotulski, ”Application-aware firewall mechanism for software defined networks,” *J. Network and Systems Management*, vol. 28, no. 3, pp. 605-626, 2020.