ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/374849694

SDN Integration with Firewalls and Enhancing Security Monitoring on Firewalls

Article *in* INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT · October 2023

DOI: 10.55041/IJSREM26202

CITATIONS
0

READS
176

2 authors, including:

Rohini S. Hallikar
Rashtreeya Vidyalaya College of Engineering
33 PUBLICATIONS **23** CITATIONS

SEE PROFILE

All content following this page was uploaded by Rohini S. Hallikar on 27 October 2023.

The user has requested enhancement of the downloaded file.

SDN Integration with Firewalls and Enhancing Security Monitoring on Firewalls

Aman Sablok
Dept. of Electronics and Communication.
RV College of Engineering
Bengaluru, India
amansablok.ec19@rvce.edu.in

Rohini S. Hallikar
Dept. of Electronics and Communication
RV College of Engineering
Bengaluru, India
rohinish@rvce.edu.in

Abstract—— **Software-defined Networking (SDN) has revolutionized the way networks are managed and operated by decoupling the control plane from the data plane. This separation allows for centralized control and programmability, offering greater flexibility, scalability, and agility in network management.Firewalls, renowned for their robust security features, play a critical role in protecting network traffic. Integrating SDN principles and technologies with Firewalls presents an opportunity to enhance their management, scalability, and orchestration capabilities. This paper explores the integration of SDN with Firewalls, focusing on leveraging SDN controllers and software defined networking architectures to augment the underlying BSD-based operating system. By integrating SDN controllers, organizations can centrally manage firewall policies, dynamically enforce security rules, and gain real-time visibility into network traffic. Furthermore, SDN enables efficient scalability of Firewalls by dynamically allocating resources and load balancing traffic. This paper also explores methods to enhance security monitoring and analytics on Firewalls. It focuses on leveraging advanced techniques, technologies, and integration approaches to optimize security monitoring and strengthen the firewall's ability to detect and respond to security threats. Security monitoring and analytics are crucial components of modern network infrastructure to detect and mitigate potential threats. Firewalls, known for their robust security features, serve as critical gateways for network traffic. Enhancing security monitoring and analytics capabilities on Firewalls can significantly improve threat detection, incident response, and overall network security posture.**

Index Terms—Firewalls , Software Defined Networking(SDN) , Enhancing

I. Introduction

Software-Defined Networking (SDN) is a network architecture that separates the control plane from the data plane, providing a centralized and programmable approach to network management. In traditional networks, network devices such as switches and routers handle both control and data forwarding functions. However, in an SDN environment, the control plane is decoupled and moved to a centralized controller, while the data plane remains in the network devices.

SDN introduces a logical abstraction layer called the "controller" that manages and controls the network. The controller communicates with the network devices through an open and standardized protocol, such as OpenFlow, to configure and manage their behavior. This centralization of control allows for dynamic and flexible network management, as administrators can program network behavior and policies from a single point of control.

Some key characteristics and benefits of SDN include:

- Programmability: SDN enables the network to be programmatically controlled through open APIs, allowing for automation, customization, and innovation in network management.
- Centralized Management: With SDN, network management tasks can be centralized, simplifying configuration, monitoring, and troubleshooting across the entire network infrastructure.
- Scalability and Flexibility: SDN provides scalability and flexibility by abstracting network services from the underlying hardware, enabling efficient resource allocation and dynamic adaptation to changing network requirements.
- Service Orchestration: SDN facilitates the orchestration of network services by integrating with cloud computing platforms and virtualization technologies, enabling the deployment and management of complex network architectures.
- Network Virtualization: SDN enables the creation of virtual network overlays, allowing multiple logical networks to coexist on the same physical infrastructure, providing isolation, security, and efficient resource utilization.
- Enhanced Security: SDN can enhance network security by enabling granular control over traffic flows, implementing security policies, and facilitating threat detection and response through centralized monitoring and analytics.

SDN has gained significant attention and adoption in various domains, including data centers, wide-area networks (WANs), campus networks, and service provider networks. It offers a more flexible, efficient, and agile approach to network management, addressing the limitations of traditional network architectures.

As SDN continues to evolve, research and development efforts focus on areas such as network programmability, security, performance optimization, and integration with emerging technologies like Internet of Things (IoT) and 5G networks. The widespread adoption of SDN promises to transform network infrastructure, enabling organizations to meet the growing demands of modern applications and services in a more efficient and scalable manner.

The integration of Software-Defined Networking (SDN) principles with Firewalls brings enhanced management, scalability, and orchestration capabilities to network security. By combining SDN and Firewalls, organizations can benefit from centralized control, programmability, and dynamic security policy enforcement. Here are some key aspects of SDN integration with Firewalls:

- Centralized Policy Management: SDN controllers can provide a centralized interface to manage firewall policies across multiple devices. Administrators can define security rules, access control policies, and threat prevention settings from a single point of control, simplifying policy management and ensuring consistency.
- Dynamic Policy Enforcement: SDN integration allows for dynamic security policy enforcement based on realtime network conditions and events. SDN controllers can communicate with Firewalls to dynamically update firewall rules, adjust access privileges, or redirect traffic based on network demands or security events, providing more agility and responsiveness.
- Enhanced Visibility and Monitoring: SDN integration enables comprehensive visibility into network traffic and security events. By leveraging SDN controllers, administrators can collect and analyze network telemetry data from Firewalls, gaining insights into traffic patterns, detecting anomalies, and improving security incident detection and response capabilities.
- Scalability and Load Balancing: SDN provides scalability and load balancing capabilities to Firewalls. By intelligently distributing network traffic across multiple devices, SDN controllers ensure efficient utilization of firewall resources, optimize performance, and improve network availability.
- Automation and Orchestration: SDN integration with Firewalls enables automation and orchestration of security policies and configurations. Administrators can use SDN controllers to automate repetitive tasks, streamline policy deployment, and integrate security functions with broader network orchestration frameworks, such as OpenStack or Kubernetes.
- Threat Intelligence Integration: SDN integration allows for the integration of external threat intelligence feeds with Firewalls. By leveraging threat intelligence sources, SDN controllers can update firewall rules and policies in real-time to block known malicious entities or patterns, enhancing the overall security posture of the network.
- Policy-driven Network Segmentation: SDN integration with Firewalls facilitates policy-driven network segmentation. Administrators can define and enforce security policies based on logical groupings, such as user roles, applications, or compliance requirements. This approach provides granular control over network access and enhances security isolation.

The integration of SDN with Firewalls provides a powerful combination of network control and security enforcement. It enables centralized policy management, dynamic enforcement, enhanced visibility, scalability, and automation, strengthening network security while offering flexibility and agility in managing firewall policies. Organizations can leverage SDN integration to achieve a more efficient and effective security infrastructure that adapts to evolving threats and network requirements.

Firewalls are a series of high-performance security devices developed by Juniper Networks. They are designed to provide robust network protection, threat prevention, and secure connectivity for various network environments. Here are some key features and capabilities of Firewalls:

- Unified Threat Management (UTM): Firewalls offer a comprehensive set of security features, including firewalling, intrusion prevention system (IPS), antivirus, antispam, web filtering, and application visibility and control. This integrated approach simplifies security management and reduces the need for multiple standalone security appliances.
- Advanced Threat Prevention: Firewalls incorporate advanced threat prevention mechanisms such as IPS, antimalware, and file-based malware analysis. These features help detect and block known and unknown threats, including zero-day exploits, to protect the network from malicious activities.
- VPN and Secure Connectivity: Firewalls support Virtual Private Network (VPN) technologies, enabling secure remote access for users and secure site-to-site connectivity between branch offices or partner networks. They provide industry-standard encryption and authentication protocols to ensure secure data transmission.
- Application-Aware Security: Firewalls can identify and control applications running on the network, allowing administrators to enforce granular policies based on application usage. This helps optimize network performance, prioritize critical applications, and block unauthorized or risky applications.
- Intrusion Detection and Prevention: Firewalls include an intrusion detection and prevention system (IDPS) that monitors network traffic for suspicious activity and alerts or blocks potential threats. This helps safeguard against network-based attacks and vulnerabilities.
- Network Segmentation and Micro-Segmentation: Firewalls support network segmentation by creating virtual routing instances and security zones. This allows

administrators to logically separate different parts of the network, restrict traffic flow, and apply specific security policies to each segment. Micro-segmentation provides an additional layer of security by isolating individual workloads or applications.

- High Performance and Scalability: Firewalls are built to handle high network traffic volumes while maintaining low latency. They offer flexible scalability options, including chassis-based systems for large-scale deployments and virtualized instances for cloud environments.
- Centralized Management: Firewalls can be managed through Junos Space Security Director, which provides a centralized interface for configuration, monitoring, and reporting. This simplifies management tasks and allows for consistent security policy enforcement across multiple devices.

Overall, Firewalls deliver comprehensive network security with advanced threat prevention, secure connectivity, application-awareness, and scalability. They are suitable for a wide range of network environments, including small and medium-sized businesses, large enterprises, data centers, and service providers, where robust and reliable security is essential.

II. Literature Survey

[1] Computer security is a challenging issue. Networked computer security is even more challenging. When utilised appropriately, firewalls (barriers between two networks) can significantly improve computer security.The three primary classifications used by the writers for firewalls are packet filtering, circuit gateways, and application gateways. Usually, multiple of these are utilised simultaneously. Their discussion and examples concern UNIX systems and applications.

[2] This study synthesises current domestic and foreign firewall technology based on various firewalls' guiding principles, benefits, and drawbacks. It also analyses computer network security features and the major threat.In-depth analysis of the key factors is addressed through the synthesis and comparison of several methodologies.

[3] A network is protected from outside incursion by a firewall, which can be either software or hardware. It controls how much traffic can travel through a router that is connected to the network infrastructure. It is prohibiting unauthorised users from accessing the network from either inside the Local Area Network (LAN) or from outside via the Internet.

[4] This essay explores the inadequacies of firewall solutions in the present network environment and the state of network security as well as the advantages of using AI technology for threat detection. The paper then examines the benefits of AI firewalls and elaborates on their capabilities to develop learning models and realise autonomous evolution of threat detection capability.

[5] The purpose of this study is to evaluate the performance of a Next Generation Firewall that was installed to secure IoT in smart homes and corporate networks. The approach taken in this study is one of comparison, testing DDoS attacks, phishing, and SQL Injection on enterprise networks, smart home networks, and general networks.

[6] There are security hazards with every connection made between a local network and the WAN or Internet. The article's goal is to provide a quick overview of the fundamentals of protection, from definition to firewall implementation.

[7] An essential component of any security framework is the firewall. Most firewalls are made up of a lot of consecutive rules that are disorganised and difficult to understand. Misconfigurations are unfortunately very common and can have an impact on the firewall's dependability because network managers must manually configure a majority of the rules. Finding these anomalies is a difficult undertaking. In this research, we provide a simulation and verification model based on trees to determine whether a system's implemented firewall complies with the applicable firewall requirements.

[8] Modern network security is not complete without firewalls, which can identify and eliminate malicious packets before they may damage the network being secured. But because they have to filter a lot of packets rapidly, these firewalls can't always base their decisions on all of the packets' characteristics.

[9] Firewalls are crucial network components that offer immediate protection from network threats. Firewall rules are a requirement for this degree of defence. To control packet flows, traditional firewalls like Cisco ACL, IPTABLES, Check Point, and Juniper NetScreen use stated rules. The above rules could, however, result in rule conflicts that reduce the firewall's security or even cause it to run slowly.

[10] Security tools like firewalls are used to implement a company's security policy. Commercial firewalls, like those made by Juniper Networks and Cisco, are complicated and primarily intended for use by networking and security experts. They are not well suited for usage in academic settings. Commercial firewalls are also typically regarded as expensive hardware components.

[11] Firewall protection is only as effective as the policy that is set up to be followed. Real-world configuration data analysis reveals that corporate firewalls frequently enforce rule sets that go against accepted security standards. The foundation of business intranet security is a firewall. A systems administrator must set up and maintain a firewall once it has been purchased by a corporation in accordance with a security policy that suits the demands of the organisation.

[12] The drawback of the Internet's rising popularity is that security threats are getting worse. The computer security community has created firewalls, technologies that assist shield users' systems from damage when they connect to the Internet and other networks outside of their control, with initial backing

from the US government. Numerous business firewall products are selling well on the global market.

[13] In order to divide and isolate the components of an industrial control network, the IEC 62443 security standards establish the ideas of zones, conduits, and security levels. Network segmentation logically divides the control network into several communication zones in order to prevent unwanted traffic from moving across zones with varying levels of trust.

[14] Due to the massive amounts of data generated every day in the information age, we have now reached the era of big data. People use computer networks frequently in their daily lives. Networks and information systems are crucial foundational components in the development of social infrastructure and economic development. A hostile attack that disrupts a network attack will result in more serious security incidents, protecting the national economy and the public interest.

III. Scope

This paper gives a brief about the integration of the Software Defined Networking with the Series firewalls. Network security is improved by the application of Software-Defined Networking (SDN) concepts and Firewalls, which enable greater control, scalability, and orchestration capabilities. Organisations can gain centralised control, programmability, and dynamic security policy enforcement by combining SDN and Firewalls. This paper also highlights the addition of certain commands onto an Device that include the enhancing of the security and stability of the series firewalls. The commands are added using a certain algorithm which makes the device function accordingly and enhanes the stability and security of the device. Enhancing the security of devices is crucial to protect network infrastructure from evolving threats. By implementing the security measures, organizations can enhance the security of devices and mitigate potential risks, ensuring the integrity and confidentiality of network traffic and protecting against unauthorized access or malicious activities. Some measures include Strong Authentication, Secure Management Interfaces, Firewall Rule Optimization, Threat Intelligence Integration and some others. This defines the scope of the paper. [15]

IV. Design Methodology

The design methodology for the integration of SDN with series firewalls include :

Recognise the network requirements, such as security guidelines, traffic patterns, scalability requirements, and performance requirements. Find out the precise aims and objectives for integrating SDN with Firewalls. Specify the use cases where SDN integration with Firewalls will be beneficial. For instance, dynamic policy enforcement, centralised policy management, or improved security analytics. Sort the use cases in order of importance and viability. Choose an SDN controller by comparing them all and selecting the one that best suits your organization's needs. Firewall compatibility, support for open standards like OpenFlow, scalability, and vendor reputation are a few things to take into account. Select the integration strategy depending on the capabilities of the Firewall and the SDN controller you have chosen. Use of APIs, network protocols, or particular integration modules offered by the manufacturer are available options. Assure that the Firewalls and the SDN controller are compatible and cooperative. Create data models and abstractions to represent the configuration and policies of the Firewall in the SDN controller. As a result, the controller can efficiently comprehend and handle Firewall settings. If necessary, think about utilising current industry standards or creating unique models. Create channels of communication between the Firewalls and the SDN controller. Configuring interfaces, protocols, and authentication systems may be necessary for this. To safeguard the integration, create suitable access controls and ensure secure communication. Create the logic necessary for managing security policies for Firewalls in the SDN controller. As part of this, firewall rules, access control policies, threat prevention settings, and any necessary dynamic policy adjustments based on network conditions or events must all be established and enforced. To improve threat detection and response, integrate security analytics tools with the SDN controller. This could entail using machine learning algorithms, integrating with external threat intelligence feeds, or gathering and analysing network telemetry data. After that test and validate the SDN interaction with Firewalls thoroughly. To make sure that the functionality, performance, and compatibility are all correct, test various use cases, policy setups, and security scenarios. Address any problems or restrictions found. [16]

Implement the SDN integration in a controlled environment and evaluate its efficiency. Keep an eye on how the integration affects network activity, security incidents, and general network performance. Continually assess the integration and make adjustments in light of operational feedback. Describe the operational methods, configuration information, and integration architecture in writing. Network administrators and security staff should receive thorough training on administering and troubleshooting the SDN integration with Firewalls. SDN integration with Firewalls is a process that is always being improved. Keep up with the most recent vendor updates, SDN and security technologies, and business best practises. Evaluate the integration's performance on a regular basis and make adjustments to meet changing network requirements and security concerns. By following this methodology SDN integration with series firewlls can be attained.

Secondly monitoring network security is essential for spotting and preventing any threats to network infrastructure. The aim of this abstract is improving security monitoring for Series Firewalls, which are frequently used as important security components in a variety of network scenarios. The goal is to increase security monitoring for Firewalls' detection and response capacities as well as its overall effectiveness. This study investigates several approaches and methods to improve security monitoring for Firewalls. The study starts off by defining particular security monitoring goals, like spotting

network intrusions, spotting malicious activity, and making sure security policies are being followed. Appropriate monitoring needs are defined by an awareness of the network architecture and any security issues.

Here in this paper we face a memory leak problem which means that there in no extra space in the memory and the memory block are not being freed. A software fault known as a memory leak happens when a programme neglects to release memory that has been allocated after it has served its purpose. As a result, memory that the programme can no longer access or use continues to be allocated, gradually building up unreleased memory over time. This may result in a steady rise in the program's memory consumption, which could eventually harm its performance and even result in crashes.

When dynamically allocated memory, such as that created by the operations malloc() or new(), is not correctly deallocated using the related deallocation functions, such as free() or delete(), memory leaks commonly result. Below is an example :

```
void MLE ()
{
      int n*=new int[10];

      //no statements to free memory;
      //Memory Leak;

}
```

Fig. 1. Memory leak

An array of integers is dynamically allocated in the previous Fig. 1 using new, but memory is never released using delete. Because the memory is still allocated even though it is no longer required, this causes a memory leak. A memory leak can have a number of negetive impacts such as the increased memory usage, performance degradation and unpredictible behaviour. On facing such errors we need to follow the basic steps like firstly we need to create our work space , enter the code , rectify it , build it and flash it onto a device to verify and validate the results.

```
#include <stdlib.h>

void vulnerable_function()
{
    char* buffer = malloc(100);

    // ...

    free(buffer);

    // ...

    free(buffer); // Double free vulnerability
}

int main()
{
    vulnerable_function();

    return 0;
}
```

Fig. 2. vulnarability function

The above figure shows the vulnaraebility function by the void vulnarable function which is being called in the main function.

V. RESULTS

A more secure firewall system can result in a number of advantages that strengthen and stabilise the network infrastructure. Among the outcomes of successfully strengthening firewall security are the following:

- Improved Network Protection: Firewalls can better detect and stop harmful activity by adding improvements including regular updates, intrusion detection and prevention systems, and strict access limits. As a result, there is improved defence against potential data breaches, network incursions, and unauthorised access attempts.
- Reduced Attack Surface: Improving firewall security entails analysing and enhancing firewall policies, getting rid of pointless rules, and making sure that the setup is correct. By closing off possible exploitation points, these activities reduce the attack surface. Critical assets are protected from unauthorised access by a firewall that is properly configured.
- Timely Vulnerability Mitigation: Frequent software patches and updates guarantee that firewalls have the most recent security patches, bug fixes, and performance enhancements. Organisations can actively reduce risks and the chance of successful attacks targeting firewall gaps by quickly fixing known vulnerabilities.
- Improved Visibility and Logging: Setting up firewall logging and monitoring features improves the ability to see network traffic, potential security incidents, and shady activity. This enables earlier security incident identification, quicker incident response, and more fruitful forensic investigation. Comprehensive logs are also useful for regulatory obligations and compliance checks.

- Strengthened Access Control: Reducing the danger of unauthorised access requires the use of robust authentication techniques like multifactor authentication (MFA) and the stringent enforcement of access control regulations for firewall management. Improved access controls increase network security by preventing hostile actors from compromising firewall configurations or obtaining administrator rights.
- Security Standard Compliance: Firewall improvements frequently follow security best practises and standards. Organisations can demonstrate compliance with industry rules like the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) by following these recommendations. Customer trust is fostered and data protection is improved by compliance with such standards.
- Enhanced Resilience: Organisations can spot potential vulnerabilities and incorrect firewall configurations through routine security assessments, penetration testing, and debugging operations. By increasing the firewall infrastructure's resilience, this lowers the possibility of service interruptions and guarantees the ongoing availability of network resources.
- Proactive Security Posture : Taking a proactive stance in terms of security is encouraged by the process of improving firewall security. It emphasises constant examination of new threats, continuous monitoring, and the development of a security-conscious culture inside an organisation. These actions assist organisations in keeping up with changing security challenges and adjusting their defensive tactics as necessary.

Overall, by enhancing firewall security, organizations can expect a more robust and reliable network infrastructure, improved protection against threats, and enhanced resilience against potential security incidents. These results contribute to safeguarding sensitive data, maintaining business continuity, and minimizing the impact of cyber attacks

```
void MLE()
{
      int* n=new int[10];

      //.....We need to deallocate the memory

      delete[] n; //This is the proper deallocation.
}
```

Fig. 3. Deallocating the memory normally

The above figure shows the deallocation of the memory using the normal ways or the delete function that simply deallocates the memory

```
void MLE()
{
      std::unique_ptr[]>n(new int[10]);

      // Deallocate the memory

} // Here memory is automatically deallocated when numbers goes out of scope.
```

Fig. 4. Deallocating the memory using unique pointers

The above function shows the deallocation of the memory using smart pointers (e.g., std::shared ptr, std::unique ptr) to automatically manage memory deallocation. This eliminates the need for explicit deallocation and ensures proper cleanup even in the presence of exceptions or early returns.

VI. Conclusion

In conclusion, the integration of Software-Defined Networking (SDN) with firewalls offers several benefits and opportunities for enhancing network security and management. By combining the centralized control and programmability of SDN with the advanced security features of firewalls, organizations can achieve more efficient, flexible, and scalable network security solutions.

- Centralized Policy Management: SDN enables centralized policy management, allowing administrators to define and enforce security policies consistently across the network. By integrating firewalls into the SDN controller's management plane, security policies can be dynamically provisioned and updated based on network conditions, user requirements, or security events. This simplifies policy management, reduces configuration overhead, and ensures consistent enforcement across the network.
- Dynamic Traffic Steering: SDN provides granular control over network traffic flows, allowing intelligent traffic steering based on security policies. By integrating firewalls with the SDN controller's data plane, network traffic can be dynamically redirected to appropriate firewall instances for inspection and enforcement. This enables the efficient use of firewall resources, load balancing, and scalability to handle varying traffic patterns and security demands.
- Enhanced Visibility and Analytics: SDN integration with firewalls offers improved visibility into network traffic, security events, and threats. The centralized SDN controller can collect and analyze traffic data from various network devices, including firewalls, enabling real-time monitoring, anomaly detection, and security analytics. This holistic view of network traffic and security events facilitates proactive threat mitigation and better-informed decision-making.
- Rapid Security Incident Response: SDN's programmability and integration with firewalls enable faster and more effective security incident response. Security policies can be dynamically adjusted to isolate compromised devices, reroute traffic, or apply additional

security measures. With SDN's automation capabilities, security incident response workflows can be streamlined, allowing organizations to respond promptly to security events and minimize potential damage.

- Scalability and Agility: SDN's architecture offers scalability and agility benefits when integrated with firewalls. With centralized management and control, administrators can easily scale security policies and firewall instances to accommodate network growth and changing security requirements. SDN's programmability allows for quick policy updates and adaptability to new security threats or compliance regulations.

The integration of SDN with firewalls brings numerous advantages, including centralized policy management, dynamic traffic steering, enhanced visibility, rapid incident response, scalability, simplified network segmentation, and interoperability. By leveraging the strengths of SDN and firewalls, organizations can achieve improved network security, operational efficiency, and adaptability to evolving threats and network requirements.

Enhancing the security of firewalls is crucial for safeguarding network infrastructure and protecting sensitive data. Enhancing the security of firewalls is a multi-faceted endeavor that involves implementing robust access controls, regular updates, monitoring, incident response, and ongoing security assessments. By taking a comprehensive and proactive approach to firewall security, organizations can significantly improve their defense against threats, reduce vulnerabilities, and protect critical assets and data from unauthorized access or compromise.

REFERENCES

[1] S. Bellovin and W. Cheswick, "Network firewalls," IEEE Communications Magzine, vol. 32, no. 9, pp:50-57, 1994, DOI: 10.1109/35.312843

[2] Xin Yue, Wei Chen and Yantao Wang, "The research of firewall technology in computer network security," 2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA), Wuhan, 2009, pp. 421-424, doi: 10.1109 /PACIIA. 2009.5406566

[3] Firkhan Ali Bin Hamid Ali, "A study of technology in firewall system," 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA), Langkawi, Malaysia, 2011, pp. 232-236, doi: 10.1109 /ISBEIA. 2011.6088813.

[4] S. -d. Krit and E. Haimoud, "Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically," 2017 International Conference on Engineering MIS (ICEMIS), Monastir, Tunisia, 2017, pp. 1-7, doi: 10.1109 /ICEMIS. 2017.8273003.

[5] Z. Wang, "Research on Feature and Architecture Design of AI Firewall," 2021 5th Annual International Conference on Data Science and Business Analytics (ICDSBA), Changsha, China, 2021, pp. 75-78, doi: 10.1109 /ICDSBA 53075.2021.00024.

[6] B. Soewito and C. E. Andhika, "Next Generation Firewall for Improving Security in Company and IoT Network," 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia, 2019, pp. 205-209, doi: 10.1109 /ISITIA. 2019.8937145.

[7] W. Weber, "Firewall basics," 4th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services. TELSIKS'99 (Cat. No.99EX365), Nis, Yugoslavia, 1999, pp. 300-305 vol.1, doi: 10.1109 /TELSKS. 1999.804748.

[8] R. Barakat, F. Catal, N. Tcholtchev, Y. Rebahi and I. Schieferdecker, "Industrial Grade Methodology for Firewall Simulation and Requirements Verification," NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2020, pp. 1-7, doi: 10.1109/NOMS47738.2020.9110345.

[9] Villanustre, Flavio Wald, Randall Koshgoftaar, Taghi Zuech, Richard Robinson, Jarvis Muharemagic, Edin. (2014). Using feature selection and classification to build effective and efficient firewalls. 10.1109/IRI.2014.7051979.

[10] T. Chomsiri, X. He, P. Nanda and Z. Tan, "An Improvement of TreeRule Firewall for a Large Network: Supporting Large Rule Size and Low Delay," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 2016, pp. 178-184, doi: 10.1109 /TrustCom. 2016.0061.

[11] Z. Trabelsi and V. Molvizadah, "Edu-firewall device: An advanced firewall hardware device for information security education," 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 2016, pp. 278-279, doi: 10.1109 /CCNC. 2016.7444779.

[12] A. Wool, "A quantitative study of firewall configuration errors," in Computer, vol. 37, no. 6, pp. 62-67, June 2004, doi: 10.1109 /MC. 2004.2.

[13] J. P. Anderson, S. Brand, L. Gong and T. Haigh, "Firewalls: an expert roundtable," in IEEE Software, vol. 14, no. 5, pp. 60-66, Sept.-Oct. 1997, doi: 10.1109/52.605932.

[14] D. Zvabva, P. Zavarsky, S. Butakov and J. Luswata, "Evaluation of Industrial Firewall Performance Issues in Automation and Control Networks," 2018 29th Biennial Symposium on Communications (BSC), Toronto, ON, Canada, 2018, pp. 1-5, doi: 10.1109/BSC.2018.8494696

[15] A. Banerjee, S. P. Maity, R. K. Das, "On throughput maximization in cooperative cognitive radio networks with eavesdropping," IEEE Communications Letters, vol. 23, no. 1, pp. 120-123, January 2019.

[16] A. Banerjee, S. P. Maity, "On residual energy maximization in cognitive relay networks with eavesdropping," IEEE Systems Journal, vol. 13, no. 4, pp. 3836-3846, December 2019.

View publication stats