AFRICAN JOURNAL OF SCIENCE, TECHNOLOGY AND SOCIAL SCIENCES

Journal website: https://journals.must.ac.ke

A Publication of Meru University of Science and Technology

Dynamic deep stateful firewall packet analysis model

Eunice Kailanya,*[1] Mary Malowe Mwadulo,[1] Amos Omamo[1]

[1]*School of Computing and Informatics. Meru University of Science and Technology.*

ARTICLE INFO

KEY WORDS

Firewalls

Stateful firewall packet analysis

Network Models

Network security

ABSTRACT

The Covid 19 pandemic has brought forth a myriad of challenges. Consequently networks are widely used and more network threats are evolving. There is therefore need to improve network tools in order to control threats. Stateful firewall is a network tool that build up packet filters by keeping record of packet passing through the network in a state table, so that when a new packet arrives, the stateful firewall filtering mechanism first checks to determine whether the information is similar to the one in state table, in order to allow or blocked a packet. Although several stateful firewall models have been developed to filter network packets, there is no model that is able to filter the entire parts of a network packet which include the header, trailer and payloads. In the stateful firewall models developed, mixed research methodology have been used. The models are developed in python programming language; an experimental research design is used, string matching and pattern matching algorithms are used in developing the models.

* Corresponding author: Eunice Kailanya. Email: ekailanya@must.ac.ke

https://doi.org/10.58506/ajstss.v1i2.20

AFRICAN JOURNAL OF SCIENCE, TECHNOLOGY AND SOCIAL SCIENCES ISSN :2958-0560

Introduction

It is important to understand the meaning of network, in general terms, network is a group of computers that are connected either using wired or wireless technology to allow sharing of resources, such as files, printers, or sharing of services (Bistouni & Jahanshahi, 2020). Securing networks has become a critical need in all the organizations as network threats are increasing day by day in terms of scale and sophistication, making networks insecure and unreliable. This is compounded by the ever-changing world of technology that leads to more interconnectedness among devices. Therefore, there is a need to improve the mechanisms used to detect network threat and improve network security (Siswanto et al., 2019). A firewall is a network security software that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules (Teng et al., 2022). In addition, a stateful firewall is a kind of firewall that keeps tracks and monitors the state of active network connection while analyzing incoming traffic and looking for potential traffic (Lei et al., 2021). For easy analysis of data transferred from the sender to the receiver over the network, data is divided into smaller small unit known packet, wherby,a packed has thee parts namely; the header, payloads and trailer (Aryeh et al., 2020). Through the use of packet sniffing method data packets can be filtered from hypertext transfer protocol application, because the user activity is more dominant in finding and downloading sites on the internet (Siswanto et al., 2019). Stateful firewall model address the issue of analyzing a packet through the use of Methods such as attack graphs, Bayesian networks, and Markov models, and continuous models, such as time series and grey models (Chadza et al., 2020). Consequently, open packet analyzer software known as "Wireshark" is used as a method of analyzing packet and it plays an important role to keep the network secure and fully operational (Kim et al., 2020) and (Ijariit Journal, n.d. 2017). In addition, an open source intrusion detection system known as "SNORT" can take all live packets from internet and captured the live packets with predefined rules (Irjet Journal, n.d.). Further, stateful firewall services are deployed as virtualized network function in the software defined networks to offer security and boost network scalability (Jamil & Kim, 2021). In addition, stateful firewall prototype is created based on programmable data plane, the method is able to extract, analyze and record the connection state information of data packets in the data plane by designing a finite state machine and a state table (Iru, n.d. 2020). stateful firewall model tool is developed that can check a wide variety of policies and verify if they are correctly implemented to enforce packet filtering (Yuan et al., 2020). also a customized symbolic model checking algorithm is developed to filter incoming and outgoing packets. Stateful firewall system model that can be embedded in network gateway and used to stream application layer in IP/TCP model is developed, the system model analyzes the packet using part of header field and part of application layer data (payload) of a packet (Tseng et al., 2017). A reference model based on packet filtering stateful firewall technology is developed, whereby all components are governed by centralized security policy and they can be deployed in a distributed fashion to achieve scaling (Thant et al., 2016).

Research Methods

This article employs an exploratory research design on existing literature with a focus to generate a workable hypothesis to be tested in future empirical studies. The objective of the study is to explore and evaluate how stateful firewall models are developed, and analyze the functionality of existing stateful firewall models. In addition, the article identifies a gap whereby the filtering mechanism in stateful firewall models developed, filters information in header part of packet, header and trailer and in other models developed, the filtering mechanism filters the information in header and payloads parts of a packet, hence the existing stateful firewall models developed cannot analyze and filter the three parts of a packet, which includes the header, payloads and trailer to detect more threats in an entire packet. Moreover, the paper gives description on how the filtering mechanism can be improved through developing a dynamic deep stateful firewall packet analysis model to assure that all the three parts of a packets are analyzed and filtered to detect more network threat. The results of this article will be used in improving network security through developing firewall model that will ensure effectiveness in analyzing and filtering entire parts of a packet.

Discussion

Application area of stateful firewall

Stateful firewalls can be applied and used in different areas and sectors in networking; this includes and not limited to:

a) Specifying data plane devices

Data plane is the layer that transmit network traffic. Data plane is also referred to as, the forwarding plane, user plane, carrier plane or bearer plane. The main function of a data plane is to forward network traffic to its destination. A data plane can be thought as a 'worker' that sends data packets through routers but the routing decision is made by the control plane which can be compared with a 'manager' because it carries out the functions and processes that determine which path a packet is sent through. Stateful firewall determine how data plane devices such as routers, switches, filters network interface card and other devices process packets, also an open source, domain- specific known as Programming

protocol- independent packet processor (P4) can be used (Datta et al., 2019).

b) Extract, analyze and record connection state information of data packets

Stateful firewall capture packets at the network layer of the transmission control protocol/ internet protocol (TCP/IP), the captured packet is then analyzed. Analyzing a packet is the primary trace back technique in networking whereby details of all the data packets across a network are scrutinized. Therefore, stateful firewall build up packet filters by keeping record of packet passing through the network in a state table, so that when a new packet arrives at the firewall, the filtering mechanism first checks to determine whether the information is similar to the one in a state table, to either allow or block a packet. The state table maintained in stateful firewall stores session information such as source address, destination address, port number, connection status and protocol (Zouheir Trabelsi & Zeidan, 2019a).

c) Create and deploy new dynamic network services

Dynamic network services includes automatic reconfiguring of the network when a node is added or deleted, the capability of locating any user on the network and altering the network path due to congestion. The purpose of open network operating system (ONOS) is to meet the needs of operators wishing to build carrier-grade solution that leverage the economics of white box merchant silicon hardware while offering the flexibility to create and deploy new dynamic network services with simplified programmatic interfaces. A network access control list (ACL) which is made up of rules that can either allow access to a computer environment or deny is implemented to open network operating system (ONOS) in order to increase the level of security and performance (Oo & Maw, 2017). open network operating system (ONOS) support both configuration and real time control of the network, eliminating the need to run routing and switching control protocols inside the network fabric. By moving intelligence into the open network operating system cloud controller, innovation is enabled and end-users can easily create new network applications without the need to alter th

e data plane systems.

d) Detect unauthorized attempt

In a stateful firewall a connection begins with a three-way handshake, whereby three- way handshake involves both sides of the data transmission process synchronizing to initiate a connection, then acknowledge each other. In this process, each side transmits Information to the other side, and the firewall examine the process to see if there is anything missing or if something is not in the proper order. As the handshake occurs, a stateful firewall can examine the data being sent and use it to gather information regarding the source, destination, how the packets are sequenced, and the data within the packet itself. If an attempt of a packet whose information's is not similar to the information stored in a state table, the firewall can detect and block packet (Prabakaran et al., 2022).

e) Filters Internet Control Message Protocol (ICMP) error packets

an Internet Control Message Protocol (ICMP) error packet carries information about a connection. If information in an Internet Control Message Protocol error packet matches no connection, stateful firewall determines whether to discard the packet based on the current configuration.

Benefits of stateful firewall

Due to the ever-changing sophistication on network security, organizations feel overwhelmed in dealing with network protection mechanisms, therefore there is a need to take measures on physical and software preventative to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure through the use of a firewall.

Stateful firewall is most commonly used firewall in enterprises today, they build up packet filters by keeping record of packet passing through the network in a state table, so that when a new packet arrives at the firewall, the filtering mechanism first checks to determine whether the information is similar to the one in the state table, and if not, the packet is blocked. The reason why stateful firewall is commonly used is that, it is efficient and cost-effective hence it is generally suitable to enforce network security. Stateful firewall have many benefits that promote cybersecurity in industries and institutions.

a) High scalability

it is easy to create network node for all network request, integrate the same network node between new flows and examine between new-on demand network nodes as well as existing ones in stateful firewall (Moradi et al., 2021). In stateful firewall, It is easy to detect if a packet is part of an existing connection or if it is trying to establish a new connection. Stateful firewalls are more sophisticated than packet filters because they can keep track of the state of connections. and can make decisions based on that state.

b) Awareness of state of a connection

Stateful firewalls typically build a state table and use this table to allow only returning traffic from connections currently listed in the state table. After a connection is removed from the state table, no traffic from the external device of this connection is permitted. Therefore, these types of connections are more difficult to spoof. For example, with hypertext transfer protocol, connections are very short lived, so if a hacker noticed the connection being torn down and tied to sneak in

some data by spoofing the transmission control protocol port numbers and internet protocol addresses, the data would be stopped because the connection entry already would have been removed (Han et al., 2016).

c) Do not require opening of large port numbers

Another benefit of stateful firewall is that they do not require one to open a large range of port numbers to allow returning traffic back into the network. The state table is used to determine whether this is returning traffic; otherwise, the filtering table is used to filter the trafficThis way, the firewall only needs to open up ports for outgoing traffic when there's no established connection. between the two hosts.tha advantage of stateful firewall over stateless firewall is that stateful firewall can remember connections because it has to determine whether any of the packets are part of an existing connection through comparing the new information with the existing information stored in a state table, while a stateless firewall only needs to open up a port, on which it is listening. Stateless firewall does not remember connections and it cannot tell whether the packet is part of an established connection, or not so it needs to continuously open and close ports for incoming and outgoing traffic depending on whether there is an existing connection or not (Nife & Kotulski, 2020) .

d) Prevent more kinds of denial of service attack

A denial of service occurs when a legitmemate users are unable to access information systems, devices, or other network resources due to the actions of malicious threat actors.stateful firewall can prevent spoofing by checking if the incoming traffic has a source address consistent with the original addresses and this is done by comparing information of the new packet with information in a state table,The state table is a list of the information about the connection that is being established to determine if an incoming packet is allowed or denied and what type of response should be sent to the sender.Stateful firewall also has a routing table which gives the states of each connection, that is whether the connection is active or not. The routing table ensures the best performance for stateful firewall. In addation stateful firewall has a rule table which defines how packets from a given connection should be filtered based on its state in the first layer whaich is a state table (Zouheir Trabelsi & Zeidan, 2019b).

e) Reduces memory space consumption

Stateful firewall reduces memory space consumtion by keeping all connection related information in one session entry. And this results to additional processing time particularly for session timeout attribute processing. Stateful firewall also, do not need many ports open for properfor proper communication, it offer extensive logging capabilities and robust attack prevention.They are able to keep track of the state of a packet as it traverses an internetwork. This is done by assigning a connection to a specific session and storing information about that session in the memory (Z. Trabelsi & Zeidan, 2018).

f) Improve Network security

in a stateful firewall a check point is integrated into networking stack of the operating system kennel, the check point monitors all traffic entering and leaving the system to ensure that no packet is processed by any of the higher protocol stack layers until the firewall first verifies that the packet complies with the network security access control policy.by tracking both state and context information, stateful firewall provides a great degree of security than earlier approaches to firewall protection. The stateful firewall inspects incoming traffic at multiple layers in the network stack, whil providing more granular control over how traffic is filtered. Network security is improved. A stateful firewall checks the current state of an ongoing connection and decides whether or not to allow the data transfer based on that information. The firewall can also maintain a log of connections, which can be used for future reference. Stateful firewalls are more effective than stateless firewalls because they can detect and block attacks, such as those involving spoofing, which do not use an ongoing connection to penetrate the system (Iru, n.d.).

Issues and challenges of stateful firewall packet analysis

Notwithstanding stateful firewall great potential benefits, organizations must overcome numerous issues and challenges that are inhibiting stateful firewall to offer effective network security. To get grounded in and eventually master stateful firewall and enjoy the full potential, it is important to overcome key challages to ensure effectiveness of stateful firewall in order to improve network security.the challages incudes;

a) Difficult in creating strong network segment

network segmentation is a key strategy for establishing defense-in-depth against attackers. The key benefits of using strong network segmentation are as follows: it can slow down attackers, improve overall data security, make implementating a policy of least privilege (POLP) easier and reduce the damage caused by a breach. Configuring firewall deployments to create strong network segmentation is a crucial strategy for enterprises because of these benefits. The longer it takes attackers to break out from one system to another. The more time your cybersecurity experts have to identify and contain the breach. It also means reducing the total amount of data and assets that attackers can access at once, limiting damage (Toluwanise, 2021).

b) Lack of standards

When Managing program updates many stateful firewall solutions are software- based and will, thus need periodic updates to their software to close potential vul-

nerabilities and to update their definitions of hostile traffic. Keeping a firewall up to date is one of the most basic firewall management procedures that enterprises need to engage in, but such software updates are still easily missed when overworked. Using a managed stateful firewall service can help to ensure that these critical updates are carried out immediately, which minimizes risk.

c) Performace issues

Stateful firewall often perform at slower rate than the link capacity of their network interfaces. This causes a problem when a host with a network interface that is faster than the firewall internal processor attempt to send data through the firewall (TCP burst typically occur at or near maximam data rate of the sending host's interface). Since the firewall must buffer the traffic-bursts send to it by the data transfer host until it can process all the packets in the bursts, input buffer size is critical.uufortunately stateful firewall have small input buffers since they are typicallydesigned to scale to large number of low speed flows.rather than a few high- speed data flows.if stateful firewall input buffers are too small to hold the bursts from the data transfer host, packet loss will results- offen causing severe performance problems (Tran & Ahn, 2017).

d) Proper authentication mechanism

The basic stateful firewall is designed to protect a network from attacks. It is usually used to prevent unauthorized access to the network. A stateful firewall is a type of firewall that provides protection for network connections and tracks the state of each connection. Stateful firewalls are typically implemented on networks that have sensitive data and require high security, such as military networks or banks. The main goal of a stateful firewall is to control the flow of traffic on the network, but it also offers additional security features such as user authentication. However, while stateful firewalls offer strong protection against outside threats, they have weak user authentication because they rely on an external user database to authenticate information (Saxena et al., 2022).

e) Application Layer Attack prevention issues

Stateful firewalls are not designed to protect against application layer attacks. They are designed to protect against network layer attacks such as spoofing, denial of service and other similar types of network-based exploits. Application layer attacks, on the other hand, are those that exploit vulnerabilities in the application itself. For example, a SQL injection attack exploits a vulnerability in an application's code that is used to execute SQL queries and commands against a database server (Chowdhary et al., 2018).

f) Lack of Effectiveness with User Datagram Protocol (UDP)- or Internet Control Message Protocol (ICMP)-based traffic

Stateful firewalls are not as effective with User Datagram Protocol- or Internet Control Message Protocol-based traffic because they cannot track the state of the session. Stateful firewalls are often used to filter out unwanted traffic that is not necessary for the network. They do this by tracking the state of a session, which is a series of packets between two hosts that have been identified as belonging to a single communication. This process is called "stateful inspection" (Monir & Akhter, 2019).

g) Management issues when blocking hostile traffic without impacting legitimate request

While stateful firewalls need to block potential hostile traffic, they also need to avoid impeding legitimate traffic requests. Otherwise, the network users experience will suffer- creating inconveniencies and reduce productivity.

h) Log information issues

Stateful firewall is a network security system that monitors and controls the incoming and outgoing traffic based on the state of the connection. The logs are used for monitoring, troubleshooting and auditing purposes.Stateful firewall does not have any log information because it only logs information about packets that are successfully matched with a rule.

Solutions and mitigation factors

a) Implementation of Arbor Edge Defense (AED)

Implementation of Arbor Edge Defense (AED) is an inline security appliance deployed at the network perimeter. Arbor Edge Defense can eliminate the dedicated denial of service threat and the danger to stateful devices all while assisting organization in continued efforts to maintain availability to business- critical applications and services. dedicated denial of service attacks are obviously increasing in frequency and complexity when measured by the amount and variety of vector involved in each attack. And now the more employees are working from home even after pandemic, attackers are taking advantage of increased threat surface provided by virtual private network (VPN) devices and firewalls. Arbor Edge Defense (AED) is designed to sit on the edge of the network between the internet and network's stateful devices and protect them from the attackers designed to take them down.

b) Need for deep-packet inspection

Accurate network traffic identification is an important basis for network traffic monitoring and data analysis is the key to improve the quality of user services, therefore network traffic identification method that uses deep packet inspection technology to identify most traffic is

needed in order to reduce the workload that needs to be identified. Deep packet inspection also helps in classifying, identifying and differentiating the application of network traffic, the traffic of different applications can be subdivided to provide users with personalized network services and improve the network quality and user satisfaction (Hhs et al., 2019).

c) Automate the process of firewall updating

With improvements in technology, many processes have become faster and easier. It may not always be possible for firewall administrators to constantly check for updates and perform software updates regularly. This leaves the network at risk of security breaches. To avoid any lapse in updating stateful firewall, one can automate the process instead.an automated system can be scheduled to check for available updates and implement the updates when they find one. This reduces the need for human intervention and keeps the firewall secure and robust at all time (Togay et al., 2022).

d) Need for Better Logs Management

Log information management is a key component to maintaining network security. The stateful firewall configuration requires the ability to log all traffic that crosses it. This includes data such as source and destination Internet Protocol addresses, protocol, session duration and application usage. The logs are used for monitoring, troubleshooting and auditing purposes. They are also essential for forensic investigations in case of a security breach. Logs provide the Stateful firewall with visibility into the network traffic that passes through it. This allows administrators to identify potential threats that might be targeting their networks and take corrective action before they become an issue.

e) Resolving stateful firewall program updates

The first step in managing stateful firewall program updates is understanding how it work. The second step is understanding what the changes to the system will be and how it can affect the network. The third step is deciding when to update the stateful firewall program and what kind of update should be. If an organization has a lot of traffic, there may not be enough time for testing new updates before deployment so an incremental update should be considered (Dixit et al., 2018).

f) Developing proper authentication Mechanism

stateful firewall are different from packet filtering firewalls because they keep track of connections and allow or deny packets based on their understanding of the current state. The need for proper authentication mechanism in Stateful firewalls is to ensure that only authorized traffic is allowed to pass through the firewall. This also prevents unauthorized users from accessing sensitive data and systems. In the enterprise world, firewalls are often used to protect the system against unauthorized access. This is done by controlling the traffic that can enter or exit from a specific point of access. One way to do this is by using stateful firewalls. Stateful firewalls are able to maintain an active record of all the connections that have been made on an interface and can also identify packets for which it is not yet known whether they are part of a connection or not. They have some limitations, though. The first one is that they require authentication. Without authentication, stateful firewalls cannot differentiate between legitimate and illegitimate packets being sent in and out of the protected network (Saxena et al., 2022).

g) Conducting regular firewall security audit

Security audits are necessary to ensure that the firewall rules comply with the organizational, as well as external security regulations that apply to the network. Unauthorized firewall configuration changes that are a policy violation can cause non-compliance. It is important for network administrators to carry out regular security audits to non-authorized changes have taken place. security audits are most essential when there is stateful firewall migration activity or when there are bulk configuration changes made on stateful firewall.

h) Improve process request based on access control

Access control is one of the fundamental in stateful firewall controls, to ensure network security and data integaty.In a stateful firewall, the packets are analyzed and filtered based on the type of connection or protocol they belong to. The firewall looks at the header information in the packet, such as its destination Internet Protocol address, port number, protocol type, and then decides whether or not it should be allowed through. If it should be allowed through, then it will allow all packets associated with that connection to pass through until the session terminates. Stateful firewall is a form of packet filtering that monitors a session's progress for the purposes of maintaining state about the session. Stateful firewalls are typically used to control access to an internal network or resources on the Internet. As such, stateful firewalls maintain information about each connection they process and then act accordingly based on these rules (Z. Trabelsi & Zeidan, 2018).

i) Establishing secure data connection through three-way-handshake

The three-way handshake is a key part of the TCP/IP protocol. It is the process between two hosts to establish a connection. The three-way handshake begins with an initial connection request from one host to another. This is followed by a request from the second host to confirm that it has received the first message and finally there is an acknowledgement sent back by the first host to confirm that it has received and accepted the second message. Therefore it is vital to establish secure data connection through three-way-handshake becouse three-way-handshake ensures that both sides knows that they are ready to transfer data and it also allows both sides to

agree on the initial sequence nimbers, which are sent and acknowledged.

Conclusions

Securing networks has become a critical need in all the organizations as network threats are increasing day by day in terms of scale and sophistication, making networks insecure and unreliable. This is compounded by the ever-changing world of technology that leads to more interconnectedness among devices. Despite the fact, that stateful firewall is capable of keeping tracks of connection in a state table for easy comparison of current state of information from past ones, to make decision whether to allow or block a packet, the filtering mechanism in stateful firewall does not analyze the entire parts of a packet, therefore the following two hypotheses are derived: the development of dynamic deep stateful firewall packet analysis model that will analyze entire parts of a packet which includes the header, payloads and trailer. dynamic deep stateful firewall packet analysis model will also detect more network threats and perform the following activities; locate, recognize, categorize or block packets having hidden data and specific codes that are not located, recognized, categorized or blocked hence improving effectiveness of stateful firewall.

References

Aryeh, F. L., Alese, B. K., & Olasehinde, O. (2020). Graphical analysis of captured network packets for detection of suspicious network nodes. *8686 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*. https://doi.org/10.1109/CyberSA49311.2020.9139672

Chadza, T., Kyriakopoulos, K. G., & Lambotharan, S. (2020). *Analysis of Hidden Markov Model Learning Algorithms for the Detection and Prediction of Multi-Stage Network Attacks*.

Chowdhary, A., Huang, D., Alshamrani, A., Sabur, A., Kang, M., Kim, A., & Velazquez, A. (2018). *SDFW: SDN-based Stateful Distributed Firewall*. http://arxiv.org/abs/1811.00634

Datta, R., Choi, S., Chowdhary, A., & Park, Y. (2019). P4Guard: Designing P4 Based Firewall. *Proceedings - IEEE Military Communications Conference MILCOM*, *2019-Octob*(October), 64–69. https://doi.org/10.1109/MILCOM.2018.8599726

Dixit, V. H., Kyung, S., Zhao, Z., Doupé, A., Shoshitaishvili, Y., & Ahn, G. J. (2018). Challenges and preparedness of SDN-based firewalls. *SDN-NFVSec 2018 - Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, Co-Located with CODASPY 2018*, *2018-Janua*, 33–38. https://doi.org/10.1145/3180465.3180468

Han, W., Hu, H., Zhao, Z., Doupé, A., Ahn, G. J., Wang, K. C., & Deng, J. (2016). State-Aware network access management for software-defined networks. *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT*, *06-08-June*(November 645[1]), 1–11. https://doi.org/10.1145/2914642.2914643

Hhs, H. D. Q. G., Dqj, R., Lx, R. Q. J., Frp, T. T., Dqg, T., Vdwlvidfwlrq, X., Dffruglqj, F., Wkh, W. R., Ri, W. S. H. V, & Dssolfdwlrqv, Q. (2019). *1Hvhdu6k Rq 7Hwzrun 7Udiilf , Ghqwlilfdwlrq Edvhg Rq*. *Itnec*, 1887–1891.

Iru, E. L. (n.d.). *6'1 Edvhg 6Wdwhixo)Luhzdoo Iru &Orxg*. 6–10.

Lei, S., Xia, C., Li, Z., Li, X., & Wang, T. (2021). HNN: A Novel Model to Study the Intrusion Detection Based on Multi-Feature Correlation and Temporal-Spatial Analysis. *IEEE Transactions on Network Science and Engineering*, *8*(4), 3257–3274. https://doi.org/10.1109/TNSE.2021.3109644

Monir, M. F., & Akhter, S. (2019). Comparative analysis of UDP traffic with and without SDN-based firewall. *7st International Conference on Robotics, Electrical and Signal Processing Techniques, ICREST 2019*, 85–90. https://doi.org/10.1109/ICREST.2019.8644395

Moradi, N., Shameli-Sendi, A., & Khajouei, A. (2021). A Scalable Stateful Approach for Virtual Security Functions Orchestration. *IEEE Transactions on Parallel and Distributed Systems*, *32*(6), 1383–1394. https://doi.org/10.1109/TPDS.2021.3049804

Nife, F. N., & Kotulski, Z. (2020). Application-Aware Firewall Mechanism for Software Defined Networks. *Journal of Network and Systems Management*, *28*(3), 605–626. https://doi.org/10.1007/s10922-020-09518-z

Oo, N. H., & Maw, A. H. (2017). *Stateful Firewall Application on Software Defined Networking*. 38–44.

Prabakaran, S., Ramar, R., Hussain, I., Kavin, B. P., Alshamrani, S. S., Alghamdi, A. S., & Alshehri, A. (2022). *Predicting Attack Pattern via Machine Learning by Exploiting Stateful Firewall as Virtual Network Function in an SDN Network*.

Saxena, A., Muttreja, R., Upadhyay, S., Kumar, K. S., & U, V. (2022). *P4Filter: A two level defensive mechanism against attacks in SDN using P4*. https://arxiv.org/abs/2205.12816v2

Siswanto, A., Syukur, A., Kadir, E. A., & Suratin. (2019). Network traffic monitoring and analysis using packet sniffer. *Proceedings - 2019 International Conference on Advanced Communication Technologies and Networking, CommNet 2019*, 24–27. https://doi.org/10.1109/COMMNET.2019.8742369

Teng, L., Hung, C., & Wen, C. H. (2022). *P0SF : A High-Performance Stateful Firewall on Commodity P4-Programmable Switch*. *c*, 1–5.

Thant, M., Thu, K. M., Ye, K. Z., & Sin, S. T. T. (2016). Development of firewall optimization model using by packet filter. *Proceedings - 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation, UKSim 2016*, 273–278. https://doi.org/10.1109/UKSim.2016.45

Togay, C., Kasif, A., Catal, C., & Tekinerdogan, B. (2022). A

Firewall Policy Anomaly Detection Framework for Reliable Network Security. *IEEE Transactions on Reliability*, *71*(1), 339–347. https://doi.org/10.1109/TR.2021.3089511

Toluwanise, O. (2021). *BY*.

Trabelsi, Z., & Zeidan, S. (2018). Enhanced session table architecture for stateful firewalls. *IEEE International Conference on Communications*, *2018-May*. https://doi.org/10.1109/ICC.2018.8422079

Trabelsi, Zouheir, & Zeidan, S. (2019a). *Resilence of Network Stateful Firewalls against Emerging DoS Attacks : A Case Study of the BlackNurse Attack*.

Trabelsi, Zouheir, & Zeidan, S. (2019b). Resilence of network stateful firewalls against emerging DoS attacks: A case study of the blacknurse attack. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, *2019-Novem*. https://doi.org/10.1109/AICCSA47632.2019.9035323

Tran, T. V., & Ahn, H. (2017). Challenges of and solution to the control load of stateful firewall in software defined networks. *Computer Standards and Interfaces*, *54*, 293–304. https://doi.org/10.1016/j.csi.2017.01.012

Tseng, K. K., Lo, J., Liu, Y., Chang, S. H., Merabti, M., Ng, F. C. K., & Wu, C. H. (2017). A feasibility study of stateful automaton packet inspection for streaming application detection systems. *Enterprise Information Systems*, *11*(9), 1317–1336. https://doi.org/10.1080/17517575.2016.1234070

Yuan, Y., Moon, S. J., Uppal, S., Jia, L., & Sekar, V. (2020). NetSMC: A custom symbolic model checker for stateful network verification. *Proceedings of the 73th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2020*, 181–200.