IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-8, Aug 2019 E-ISSN: 2347-2693

Effective Stateful Firewall in Software-Defined Networking

Aung Htein Maw

Dept. of Computer Systems and Technologies, University of Information Technology, Yangon, Myanmar

Corresponding Author:ahmaw.uit.edu.mm

DOI: https://doi.org/10.26438/ijcse/v7i8.269274 | Available online at: www.ijcseonline.org

Accepted: 12/Aug/2019, Published: 31/Aug/2019

***Abstract*—** A firewall is a critical security appliance for the mitigation of the security attacks not only in the traditional network, but also in software-defined networking (SDN). Previous firewall applications over SDN controller are implemented with one of two firewall concepts: centralized firewall and distributed firewall. Centralized firewall method incurs controller overhead problem as the controller acts as a centralized firewall which maintains firewall rules and filters out the traffic. Distributed firewall method comes out the complicated firewall configuration, additional cost in rules maintenance in each switch, and less sensitive to the topology. This system proposes a firewall rules installation based on topology-aware selectively distributed stateful firewall with source-based DoS attack defense mechanism. The purpose of this system is to overcome not only the performance issues but also security issues. This paper finally shows that the stateful firewall application can not only track the TCP flow, but also reduce latency plus table lookup time up to 16% in long-lived flow and 50% in short-lived flow. Moreover, according to the security perspective, the accuracy for the DOS detection and mitigation of stateful firewall application is 98.93 % of SYN flooding attack and 92.09% for UDP flooding attack.

Keywords*—Stateless Firewall, Stateful Firewall, SDN*

I. INTRODUCTION

Software Defined Networks (SDN) is a new network architecture that provides central control over the network. This control works as if it is an operating system that can send instructions and apply changes through its interface. This operating system is called the controller. Various types of application are implemented in the controller. As information security has become an ongoing concern in all areas of an information system [21], SDN also has various types of security applications.Among them, the common security application is a firewall for preventing the DoS attacks.

The SDN firewall can be divided into two types: stateless and stateful firewall. Although the stateful firewall is more secure than a stateless firewall, it has some challenges. They are the detection of the new connection, monitoring the state of connections in the network, minimizing monitoring overhead, and security. In the detection of new connection challenge, monitoring and catching a new connection appearance by all the network switches forward all network traffic to the controller could lead to controller overhead severely increasing in latency. The second challenge, monitoring state of connections in network, Connection tracking is important in removing the connection in connection list right after detecting connection termination. Hacker can try to retransmit the modified packets belonging to the terminated connection. For the third challenge of stateful firewall, minimizing monitoring overhead, Additional delay is causing because monitoring state of the connection involves packet extraction for state information. The controller has to reduce this delay to meet the demanding QoS. The final challenge is security. As SDN is a Centralized Control system, it is attracted to a DoS attack.

Denial of Service (DoS) is an attack which makes information or data unavailable to its intended hosts. The most basic attacking methods are Ping flood, UDP flood, and SYN flood Attack. In ping flood, the attacker sends large amounts of ping packets to the victim's computer in an attempt to overload it. In the UDP flood, the attacker sends large amounts of UDP packets to the victim's computer in an attempt to overload it. The SYN flood attack is a DOS attack that exploits the 3-way handshake mechanism to consume resources of a target server. The attack itself is very simple: the attacker sends repeatedly a large number of TCP SYN [5]. Depending on the location of implementation, defense mechanisms can be categorized as: source-based defense mechanism (i.e. the mechanisms are deployed near the sources of attack and focus on restricting the network customers from generating DDoS attack). Destination-based defense mechanism (i.e. the mechanisms are deployed near the victim), and network-based defense mechanism (i.e. the mechanisms are deployed inside networks and on the routers of the autonomous systems)[6].

According to the challenges of stateful firewall, this system is implemented to overcome the limitation of basic packet filtering, reduce firewall setup service, reduce controller processing, reduce communication overhead between the control plane and data plane, detect and mitigate DDoS attacks. Thus, this system proposes a firewall rules installation based on topology-aware selectively distributed stateful firewall with source-based DoS attacks defense mechanism. The purpose of this system is to overcome not only the performance issues but also security issues. This system will be evaluated by comparing the performance of stateless SDN firewall and testing by the penetration of a DoS attack.

The paper is organized as Section I introduced the software-defined network and how the firewalls are implemented. Section II provides the related works are presented. The architecture and the SDN firewall are described in SECTION III. SECTION IV discusses the experimental setup for the stateful firewall and the results are evaluated. SECTION V concludes the paper with the stateful firewall application can reduce latency plus table lookup time.

II. RELATED WORK

T. V. Tran et al.(Tran**,** Thuy Vinh, and Heejune Ahn. "*Flowtracker: A SDN Stateful Firewall Solution with Adaptive Connection Tracking and Minimized Controller Processing.*" *Software Networking (ICSN), 2016 International Conference on*. IEEE, **2016.**) proposed "FlowTracker: A SDN stateful firewall solution with adaptive connection tracking and minimized controller processing. The main contribution of this paper is reducing controller processing and communication overhead while maintaining accuracy and agility of stateful firewall by using topology learning- based for selective flow control installation approach. The limitation of this paper is that the authors used the overall whitelist and blacklist for trusted and untrusted MAC Addresses respectively. They did not use the exact predefined firewall rules (source IP, destination IP, source port, destination port, action) for filtering. They especially consider the performance and did not take into account security issues.

T. V. Tran et al(**Tran**, Thuy Vinh, and Heejune Ahn. "*A network topology-aware selectively distributed firewall control in SDN.*" *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*. IEEE, **2015.**) also proposed "A Network Topology-aware Selectively Distributed Firewall Control in SDN". The main contribution of this paper is to send only necessary firewall configuration rules considering the traffic flows and network topology. They reduced firewall setup time and shorten the firewall-violated traffic travel route. But, they implemented only stateless firewall application with MAC addresses.

J. G. V. Pena et al.(**Pena**, Justin Gregory V., and William Emmanuel Yu. "*Development of a distributed firewall using software defined networking technology*" *Information Science and Technology (ICIST), 2014 4th IEEE International Conference on*. IEEE, **2014.**) proposed "Development of a Distributed Firewall using Software Defined Network Technology". This paper is to develop a distributed flow-based firewall prototype by building around the features of OpenFlow (open SDN standard). The main contribution of this paper is: the rules are installed as flow the entries in the devices themselves instead of storing the rules set in the controller, any packets are not sent to the controller firewall inspection. The limitation of this paper is that the authors did not take into account the additional cost in switches due to maintaining entire firewall rule set in the flow table of each switch.

Andis Arins (Arins**,** Andis. "*Firewall as a service in SDN OpenFlow network*" Information, Electronic and Electrical Engineering (AIEEE) , 2015 IEEE 3rd Workshop on Advances in. IEEE, **2015.**) proposed "Firewall as a service in SDN OpenFlow network". This paper propose firewall as a service in ISP networks allowing end users to request and install match-action rules in ISP edges routers. The main contribution of this paper is proposing a state-of-the-art method for mitigating DDoS in SDN by providing remote API to discard DDoS. The limitation of this paper is that their firewall application is only considering for the DDoS mitigation on world wide scale. They did not consider the controller overhead issues.

III. ARCHITECTURE OF SDN FIREWALL

As this system is based on the SDN network, the overall architecture of this system is composed of three parts: controller, application, and forwarding network. The firewall is exiting on the application layer of this system. The firewall application is implemented with the combination of the two main methods: topology-aware selectively rule and source-based DoS attack defense method.

A. Topology Aware Selectively Rule installation with source-based DoS defense mechanism

This method installs the flow rule separately depending on the action of this rule. In general, flow rule has two types of actions: forwarded and dropping. The forwarding action can be forwarded to the controller or the destination host. To send packet successfully between a source host and destination host, two rules (from source to destination, and destination to source) are needed to install at the switches existing along the path. For dropping action, the firewall application installs the drop flow rule at the switch connected directly with the attacker host.

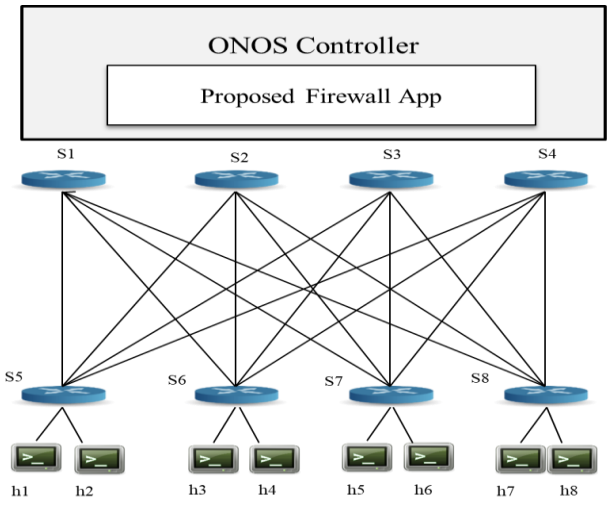


Figure 1. Overall architecture of SDN firewall

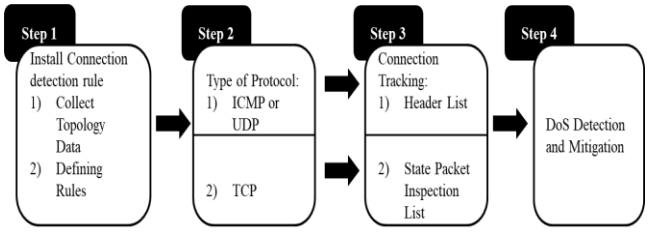


Figure 2. Flowchart of overall architecture

As shown in Figure 2, the workflow of this system can be divided into four steps:

Step 1: Install connection detection rule – It has two sub-steps: collect topology data and then define rules based on the collected data.

Step 2: Define the type of protocol - The connection tracking function is operated differently depending on the type of protocol.

Step 3: Connection Tracking – It has two separated list of information for different protocols. If the type of protocol for the incoming packet is ICMP or UDP, the system tracks the connection by using the header list. Otherwise, the state packet inspection list is used for the TCP packet.

Step 4: Dos Detection and Mitigation – This system detects the DoS attack by using a statistical analysis method (i.e. compare the number of incoming packets with the predefined threshold).

IV. EXPERIMENTAL SETUP AND EXPERIMENTS

This section is composed of two sub-sections: experimental testbed description, and the results of the experiment.

A. Experimental Testbed

We conduct our experiment on mininet emulator [16] with OpenFlow version 1.3[6] and ONOS [1] controller. Both of them are running on Dell Desktop PC with Intel(R) Core(TM) i7- 4790 CPU @ 3.60 GHz, 64 bits and 4 GB memory. The security level is proved on the leaf and spine network topology with eight switches and twelve hosts as shown in Figure 3.

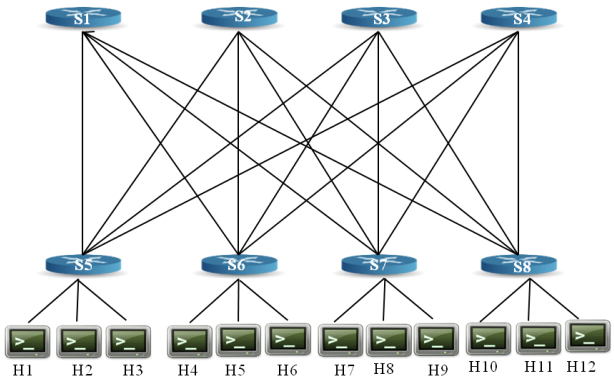


Figure 3. Leaf and Spine Topology

The performance is measured on the linear topology of an open virtual switch (OVS) with one host per switch. To compare the performance level, the stateless and stateful firewall application use the same linear topology

B. Experimental Results

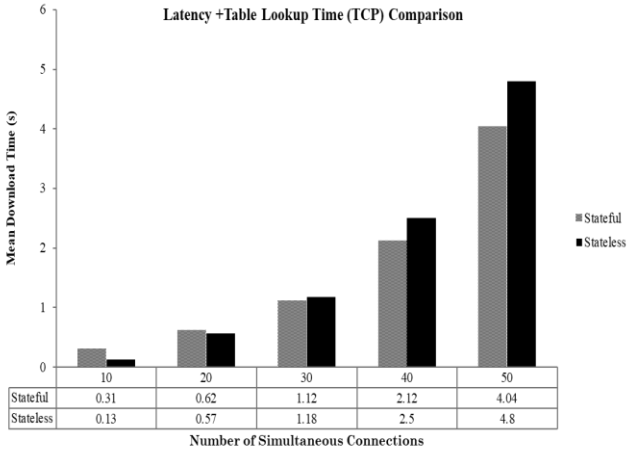
The results of the experiment are described with two sub-sections: the performance comparison of stateless and stateful firewall application, and the performance parameters of the security for the DoS detection and mitigation.

(1) Performance Comparison of Stateless and Stateful firewall: To get the performance effect of the two applications, latency result together with flow table lookup time is measured on the increasing number of simultaneous connection (10 to 50) by setting up the web servers depending on the number of TCP connection and one host accesses the servers at the same time. The web servers are created by using Simple HTTPServer in mininet hosts and parallel download HTTP requests are sent from the client host with a combination of xargs[17] and wget command. This command uses web server URL list while sending parallel downloading requests to web servers.

Figure 4 and Figure 5 show the latency results plus table lookup time for concurrent long-lived flows and short-lived flows. Stateless and Stateful used in these figures are referenced as stateful firewall application and reactive forwarding application respectively. As the number of simultaneous connection is increasing and flow table has to keep a large number of their flow rules without timeout value expire, the table lookup time for reactive forwarding application is longer than the stateful firewall application. The mean delay time by reactive forwarding application is more than stateful firewall application from 5% to 16% for long-lived flow as shown in Figure 4 and from 11% to 50% for short-lived flow as shown in Figure 5.

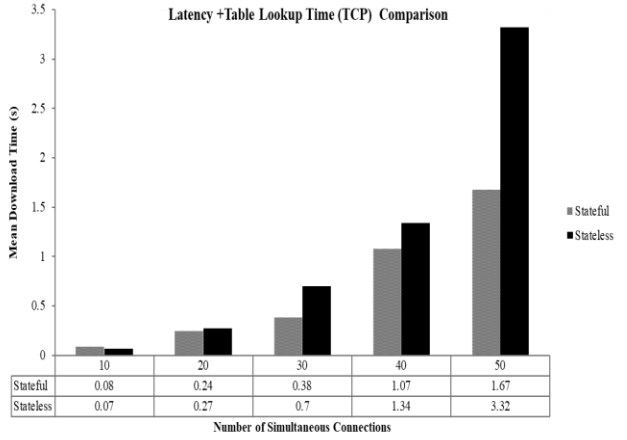
The maximum delay time by reactive forwarding application for long-lived flow and short-lived flow is 0.76s and 1.65s respectively. The time differences between the two applications in long-lived flow are less than the one in short-lived flow because flow rule removing in the short-lived flow is faster than long-lived flow as the downloading time for short-live flow is shorter than long-lived flow.

(2) Performance Parameters of security for DoS detection and Mitigation by stateful firewall: For measuring the performance parameters of security (i.e. Detection Rate (DR), False Negative Rate (FNR), False Positive Rate (FPR), and Accuracy (ACC)), we used the leaf and spine testbed as shown in Figure 5



	10	20	30	40	50
Stateful	0.31	0.62	1.12	2.12	4.04
Stateless	0.13	0.57	1.18	2.5	4.8

Figure 4. Short-lived flow time comparison result



	10	20	30	40	50
Stateful	0.08	0.24	0.38	1.07	1.67
Stateless	0.07	0.27	0.7	1.34	3.32

Figure 5. Long-lived flow time comparison result

Firstly, we construct the Web server at host h1 and DNS server at host h2 for testing the SYN flooding attack for TCP protocol and UDP flooding attack for UDP protocol respectively. We used h12 as the attacker host. We also used hping3 command [18] for launching attacks. As we used the statistical analysis method for differentiating normal and malicious traffic, we must define a threshold before doing the attack on the network. For finding the baseline of network traffic, we generate and monitor the Web traffic and DNS traffic using D-ITG tool [19] by accessing the servers from all clients concurrently for one minute. The baseline value is defined as how many number of the same packets continuously incomes to the network within one second. By taking the maximum value of each service from the monitoring result, we define the baseline for the service. After defining the baseline, we monitor and launch the attack on each server alternatively.

To measure the performance parameters of security for SYN flooding attack, we monitor the network for three minutes by using a packet capturing tool, tcpdump [20]. During the monitoring time, we launch the attack for one minute.

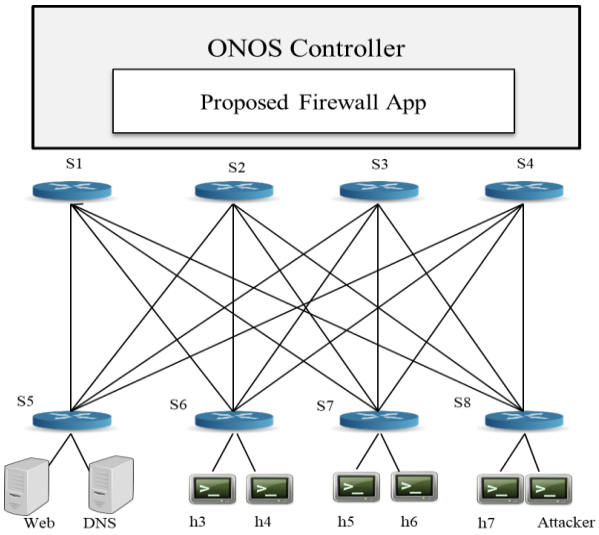


Figure 6. Leaf and Spine Topology for DoS Detection and mitigation

Similarly, we measure the security performance parameters for UDP flooding attack as the SYN flooding attack.
DR measures the percentage of correctly identified attacks over all the actual attacks and is computed using (1).

$$DR(\%) = \frac{TP}{TP + FN} * 100 \qquad (1)$$

FAR measures the percentage of legitimate traffic incorrectly identified as attack over the entire legitimate traffic and is computed using (2).

$$FAR(\%) = \frac{FP}{FP + TN} * 100 \qquad (2)$$

FNR measures the percentage of attack incorrectly identified as legitimate over the entire attack traffic and is computed using (3).

$$FNR(\%) = \frac{FN}{FN + TP} * 100 \quad (3)$$

ACC measures the percentage of true detection over the entire traffic trace and is computed using (4).

$$ACC(\%) = \frac{TP + TN}{TP + TN + FP + FN} * 100 \quad (4)$$

By using the above equations, the final results of the two attacks are listed in Table 1. By reviewing the performance parameters of the two servers, this system could detect and mitigate the SYN flooding attack more than the UDP flooding attack. The reason is that the incoming packet rate of UDP traffic itself is high that becomes delay to be able to differentiate the normal and malicious packets.

TABLE I . Performance parameters for DoS Detection and Mitigation

Service	Performance Parameters			
	DR(%)	FAR(%)	FNR(%)	ACC(%)
Web	98.03	0.13	1.9	98.93
DNS	86.80	0.78	13.19	92.09

V. CONCLUSION

Stateless firewall has limitation in keeping track of the connections state. Thus, attacker might bypass the firewall by claiming to be part of an existing TCP connection. Centralized SDN firewall makes more controller workload as the network is larger and firewall policy is more complex. Likewise, Distributed SDN firewall causes additional maintaining cost for rules and matching time for packets on each switch. Therefore, this research implement distributed SDN stateful firewall by using the topology aware selectively flow rule method based on the predefined exact firewall policy. Moreover, DoS detection and mitigation is composed together with the firewall in order to be higher security.

The statefull firewall application is able to reduce latency plus table lookup time up to 16% in long-lived flow and 50% in short-lived flow. As the security point of view, it produces the accuracy for the DoS detection and mitigation is 98.93% and 92.09 % for SYN flooding attack and UDP flooding attack respectively. Since the wireless network security is advancing consistently [22], we will implement the stateful firewall for the software-defined wireless network.

REFERENCES

[1] Tran, Thuy Vinh, and Heejune Ahn. "*Flowtracker: A SDN Stateful Firewall Solution with Adaptive Connection Tracking and Minimized Controller Processing.*" *Software Networking (ICSN), 2016 International Conference on*. IEEE, **2016**.

[2] Tran, Thuy Vinh, and Heejune Ahn. "*A network topology-aware selectively distributed firewall control in SDN*." *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*. IEEE, **2015**.

[3] Pena, Justin Gregory V., and William Emmanuel Yu. "*Development of a distributed firewall using software defined networking technology*" *Information Science and Technology (ICIST), 2014 4th IEEE International Conference on*. IEEE, **2014**.

[4] Arins, Andis. "*Firewall as a service in SDN OpenFlow network*" Information, Electronic and Electrical Engineering (AIEEE) , 2015 IEEE 3rd Workshop on Advances in. IEEE, **2015**.

[5] Rao, S., and S. Rao. "*Denial of service attacks and mitigation techniques: Real time implementation with detailed analysis*" *This paper is from the SANS Institute Reading Room site* (**2011**).

[6] Rajkumar, M. Nene. "*A Survey on Latest DoS Attacks: Classification and Defense Mechanisms*" *IJIRCCE* 1.8 (**2013**).

[7] Ivan Pepelnjak, "What can openflow tables do?", https://www.youtube.com/watch?v=7R91K0d2r2E.

[8] "*Attack Detection and Defense Mechanisms*" Juniper Networks, Inc.1194 North Mathilda Avenue Sunnyvale, California 94089 USA 408-7 45-2000 www.juniper.net, **2016**.

[9] Morzhov, Sergey, Igor Alekseev, and Mikhail Nikitinskiy. "*Firewall application for Floodlight SDN controller*" Control and Communications (SIBCON), 2016 International Siberian Conference on. IEEE, **2016**.

[10] Pena, Justin Gregory V., and William Emmanuel Yu. "*Development of a distributed firewall using software defined networking technology*" Information Science and Technology (ICIST), 2014 4th IEEE International Conference on. IEEE, **2014**.

[11] Suh, Michelle, et al. "*Building firewall over the software-defined network controller*" Advanced Communication Technology (ICACT), 2014 16th International Conference on. IEEE, **2014**.

[12] Trabelsi, Zouheir. "*Teaching stateless and stateful firewall packet filtering: A hands-on approach*" 16th Colloquium for Information Systems Security Education. **2012**.

[13] Dillon, C., and Michael Berkelaar. "*OpenFlow (D) DoS Mitigation*". Technical report (February 2014), http://www. delaat. net/rp/2013-2014/p42/report. pdf, **2014**.

[14] Low, Christopher. "*Icmp attacks illustrated*" SANS Institute URL: http://rr. sans. org/threats/ICMP attacks. php (12/11/2001) (**2001**).

[15] Shieha, Alaauddin. "*Application Layer Firewall Using OpenFlow"* **(2014).**

[16] Mininet Network Emulator, http://mininet.org.

[17] Xargs command, Internet:http://man7.org/linux/man-pages/man1 /xargs.1.html.

[18] Hping3 Security Tool[online]. Available from: https://www.hping. org/hping3.html.

[19] D-ITG, Distributed Internet Traffic Generator, http://www.grid.unina.it/software/ITG/.

[20] Tcpdump[online].Availablefrom: https://www.tcpdump.org/manpages/tcpdump.1.html.

[21] Y. Perwej, "The Hadoop Security in Big Data: A Technological Viewpoint and Analysis", International Journal of Scientific Research in Computer Science and Engineering, Vol.**7**, Issue.**3**, pp.**1-14**, June **2019**.

[22] G. Abare, "A Proposed Model for Enhanced Security against Key Reinstallation Attack on Wireless Networks", International Journal of Scientific Research in Network Security and Communication, Volume-**7**, Issue-**3**, ISSN: 2321-3256, Jun **2019**.

Authors Profile

Aung Htein Maw received the Master of Information Science (M.I.Sc.) degree from University of Computer Studies, Yangon (UCSY), in 2001, the master degree in Engineering Physics (Electronics) from Yangon Technological University (YTU), Myanmar, in 2002, and the Ph.D degree in Information Technology from UCSY, in 2009. He is one of the professor of Faculty of Computer Systems and Technologies, University of Information Technology. His research interests include Data Science and Advanced Network Systems. He has published technical papers in these areas, in the conference proceedings and jounals like IEEE and ACM Computing Survey. He has been cooperated at Research Collaborator in AssiaConnect Project and Subject Matter Expert in Asean Cyber University (ACU) project.

