Source-Based Defense Mechanism in SDN with Support Vectore Macine (SVM)

Dikyaran Yosuah A. M Bulo[1], Ida Wahida[2], Ridha Muldina Negara[3]

[1,2,3]Telkom University, Bandung
elpadango@student.telkomuniversity.ac.id[1], **wahida@telkomuniversity.ac.id[2]**,
ridhanegara@telkomuniversity.ac.id[3]

Abstract
DDoS (Distributed Denial of Service) is one of the cyber-attacks that make the network service unavailable. SDN (Software Defined Network) has tools to defeat the DDoS, because SDN has good features in defeating DDoS such as logically centralized controller, separation control plan, and programmability network. This journal purposed SVM (Support Vector Machine) that combined with Ryu controller that can predict the incoming packet based on the learned traffic, whether it is a normal packet or DDoS packet, and blocking the packet if the packet indicating the DDoS traffic. The result of the simulation was that SVM can mitigate the DDoS attack even with the biggest attack sequence.

***Index Terms*: Software-Defined Network (SDN), Source-Based Defense Mechanism, Distributed Denial of Service (DDoS), Support Vector Machine (SVM)**

1. INTRODUCTION

SDN is network management technology in which enables centralized network monitoring and centralization of security and policy control to improve performance and monitoring network [1]. Even though the SDN can improve the performance of the network, there are still security threads in SDN network one of them is DDoS, DDoS is a well-known cyber-attack that make the network source or network server unavailable by disrupting the services by sending a large amount of data or pinging the server with several hosts simultaneously.

Confidentiality, Integrity, and Availability (CIA) is a security requirement in which the model guides policy in network security [2]. Confidentiality is mean that the privacy of our data must be secured from people that threaten our data security. Integrity is mean that data that we save cannot be changed or modified by an unauthorized person. Availability is mean that service that cloud computing over should be available and can be accessed anytime and anywhere. Availability is crucial among the triad pilar of security since the core functionof the network is to provide on-demand service of different levels. DDoS (Distributed Denial of Service) and DoS (Denial of Service) flooding attacks are a threat for the Availability because DDoS can make the server and network resource unavailable to its intended users.

SDN has the features in Defeating the DDoS attacks [1] such as Separation of the control plan from the data plane, by separating the data plane from the data plane it enables establish easily, large scale attack and defense, logically centralized controller, this feature helps to build the consistent security policy, There are several ways to overcome the DdoS in SDN, the most effective and efficient way to overcome the DDoS attack however is to preventing the DDoS flood attacks the server (source) of the network. Source-based defense mechanism means to prevent the DDoS attack attacking the server and filtering the IP address of the network from anomaly traffic.

SVM (Support Vector Machine) on the other hand, can classify and can predict the incoming data based on the learned data. This thesis offers SVM that combined with the RYU controller and can be used to prevent the DDoS attack from attacking the server of the network by analyzing the incoming traffic and classifying the traffic to determine whether it was normal traffic or DDoS traffic based on the learned traffic data, and the RYU controller blocking the port of the attackers based on data from SVM.

2. SOFTWARE DEFINED NETWORKING

SDN is network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring. The architect of SDN SDN consist of three layers, which are:

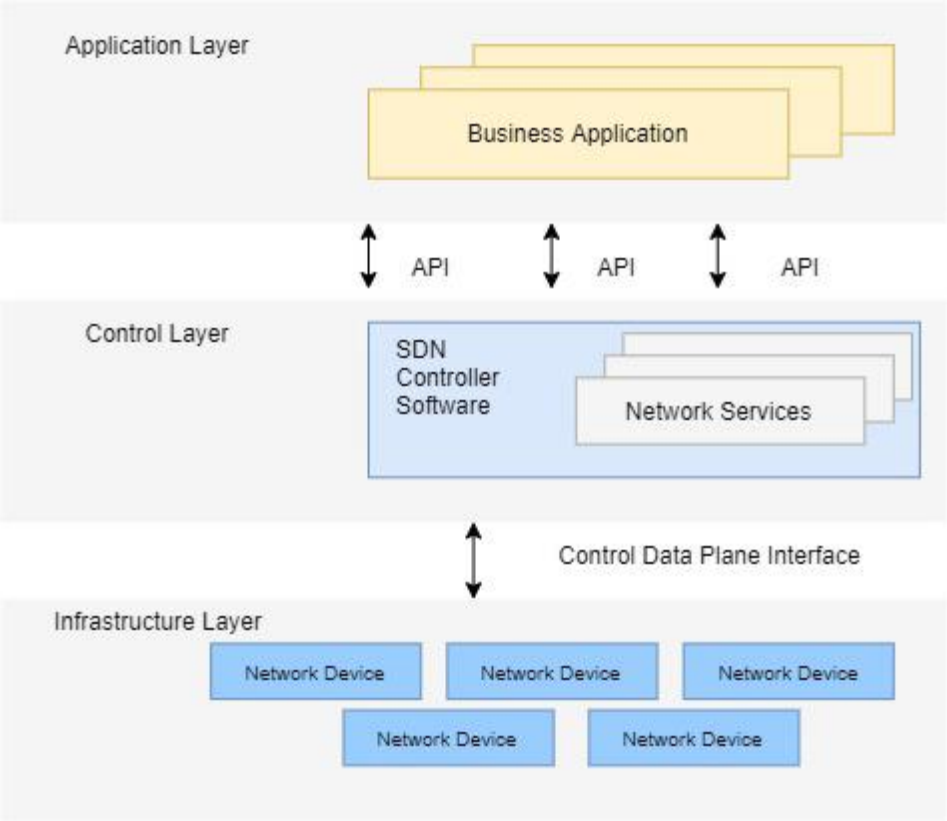

Fig. 1. SDN architecture.

- Application layer Application layer: It mainly consists of the end-user business application that consumes SDN communication and network service, example: Mininet hosts.
- Infrastructure layer Controller layer: Also known as the control plane, it consists of a set of software-based SDN controller providing a consolidated control functionality through open APIs to supervise the network forwarding behavior through an open interface, Controller layer also responsible for determining the policies and the flow of traffic throughout the network Control layer also supervised the network forwarding behavior through an open interface example: RYU, ODL, Floodlight, ONOS, etc.
- Control layer Infrastructure layer: Also known as the data plane it consists mainly of Forwarding Elements (Fes). layer that can control the SDN data path according to control layer instruction through Control-Data Plane Interface (CDPI) example: Switches and Router.

3. NETWORK TOPOLOGY

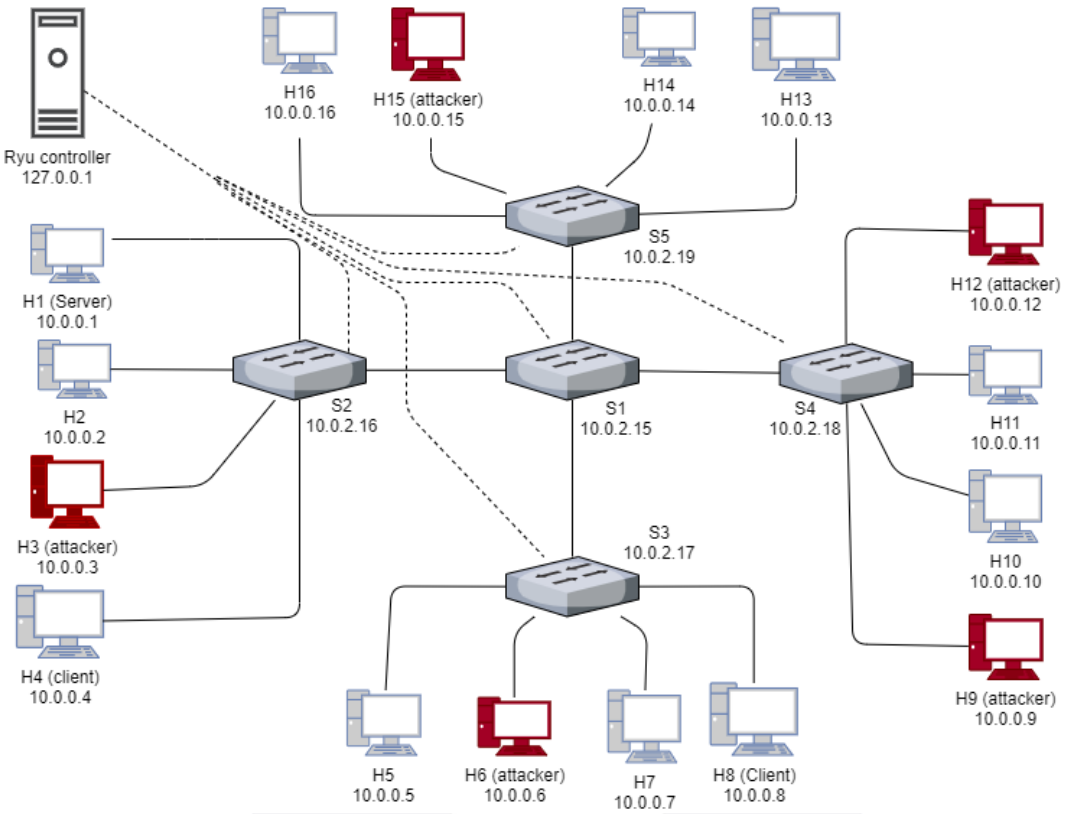

Fig. 2. Network Topology.

The topology of this simulation using the custom Mininet topology with Sflow-RT custom script with fanout 2 and depth 4 and topology tree which shows in Fig.2 shows. The topology
can be executed by using Linux command:

$ sudo mn –custom sflow-rt/extras/sflow.py –link tc,bw=10 –controller=remote,ip=127.0.0.1 –topo tree,depth=2,fanout=4

This simulation using tree topology with 5 switches and 16 hosts and the bandwidth of each host is 10 Mbps with IP 1.0.0.1 to 1.0.0.16 sequentially with controller's IP 127.0.0.1 and switch's IP 10.0.2.15. Host 1 acts as the server and host 8 acts as the client, while hosts 3, 6, and 9 will be the attacker and attacking the h1 simultaneously and continuously until the client finished sending the packet.

The packets that client send to the server is TCP packet with given bandwidth 10 Mbps and using iper3 as the packet generator.

4. SIMULATION SEQUENCE

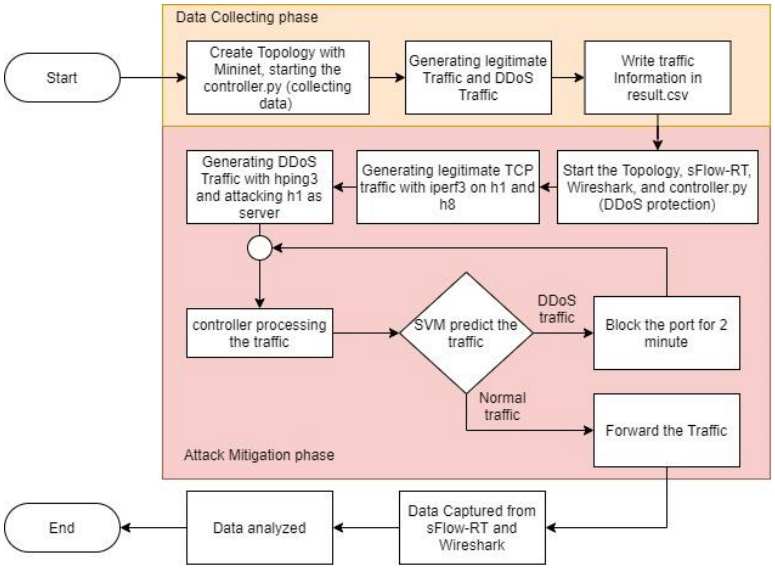

Fig. 3. Simulation Sequence.

Fig. 3 shows the simulation sequence of this journal. Thesimulation is started with SVM collecting the D DoS and normal traffic data for 5 minute and saved it in the result.csv. After that we start new topology but with SVM ready to mitigate the DDoS traffic. The normal traffic is generated using Iperf from server (h1) to client (h8) with h3, h6, h9, h12, and h15 as the attacker attacking the server (h1). SVM predicting the data traffic of the network, if the SVM prediction that the data traffic is DDoS the controller will block the port of the attacker for 2 minute and if the SVM predicting the data traffic is normal traffic then the packet will be forwarded to the client (h8). All the data is captured in sFlow-RT and Wireshark which later will be analyzed.

5. FLOWCHART OF THE CONTROLLER

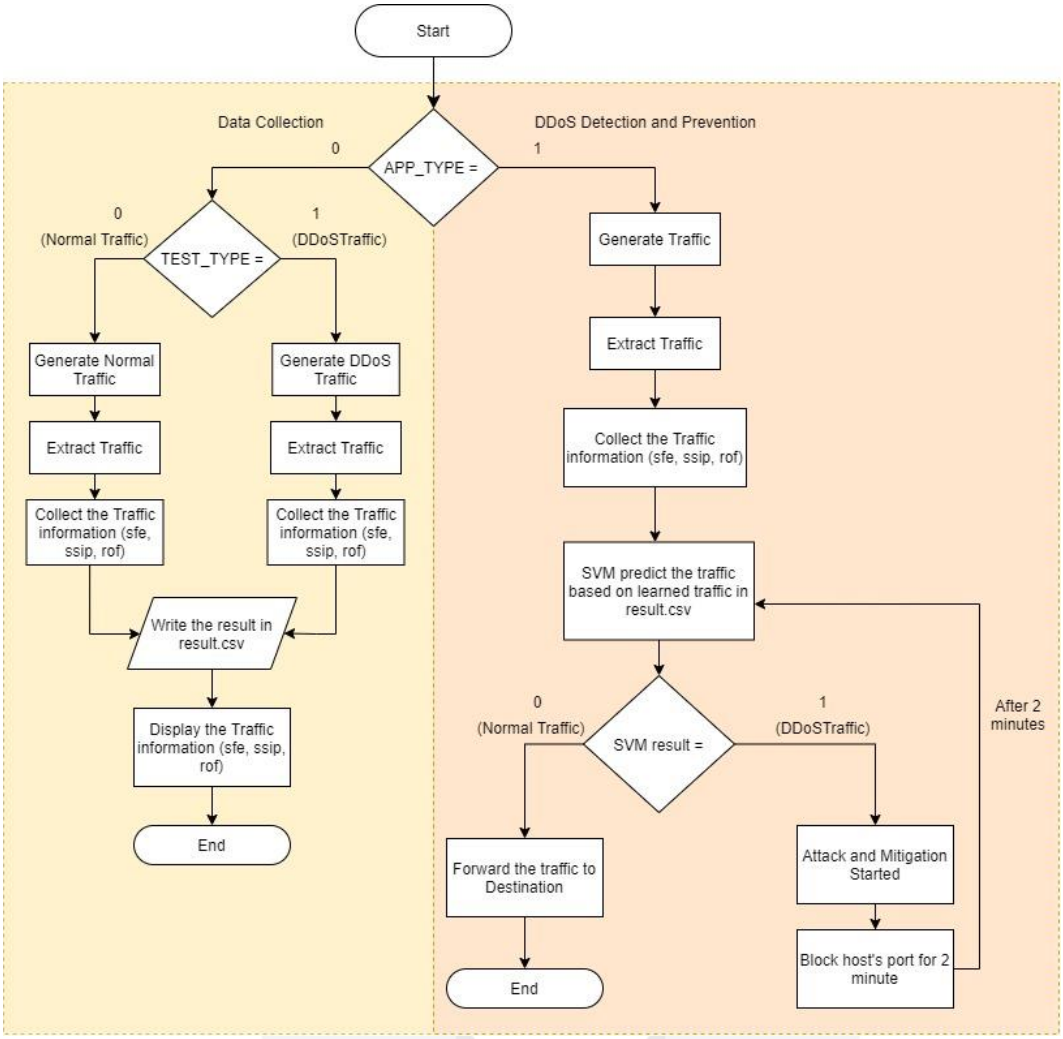

Fig. 4. Flowchart Controller.

The controller that used in this simulation is the RYU controller which has been modified so the controller can be work with SVM. The controller can be executed by Linux command:

$ ryu-manager controller.py

The controller is started with choosing the APP TYPE, 0 for data collection and 1 for DDoS Detection and Prevention.

For the APP TYPE = 0, the controller will be collecting the data from traffic that later will be generated. After choosing the APP TYPE, we choose the TEST TYPE 0 for normal traffic and 1 for DDoS traffic.

The next sequence is generating the normal and DdoS traffic, the normal traffic is generating by pinging from all host for 5 minutes, and for DDoS traffic is generated by using hping3 and sending various packets to h1 so the SVM has the data.

6. BACKGROUND TRAFFIC

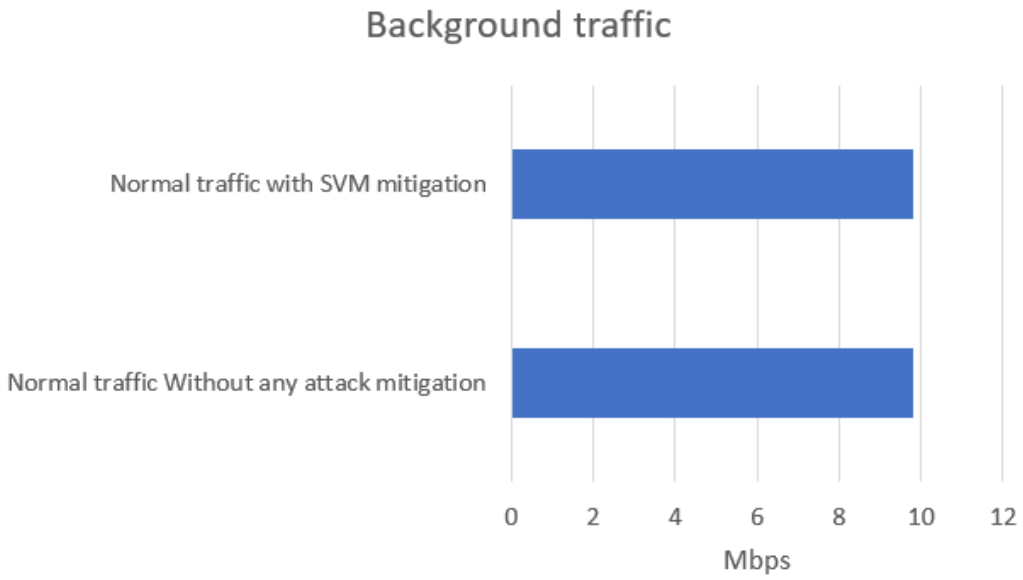

Fig. 5. Throughput of Background Traffic

Background traffic is generated traffic data without any DDoS attack. In this simulation there are two types of background traffic, first is normal traffic with SVM mitigation it means that iperf only sends the TCP traffic from h1 to h8 with SVM mitigation. The second is normal traffic without any attack mitigation it means that iperf sends TCP traffic from h1 to h8 without any attack mitigation. Fig. 5 shows that the throughput of both background data is the same which is 9.8 Mbps it means that the SVM does not interfere with the data traffic.

7. DDOS TRAFFIC

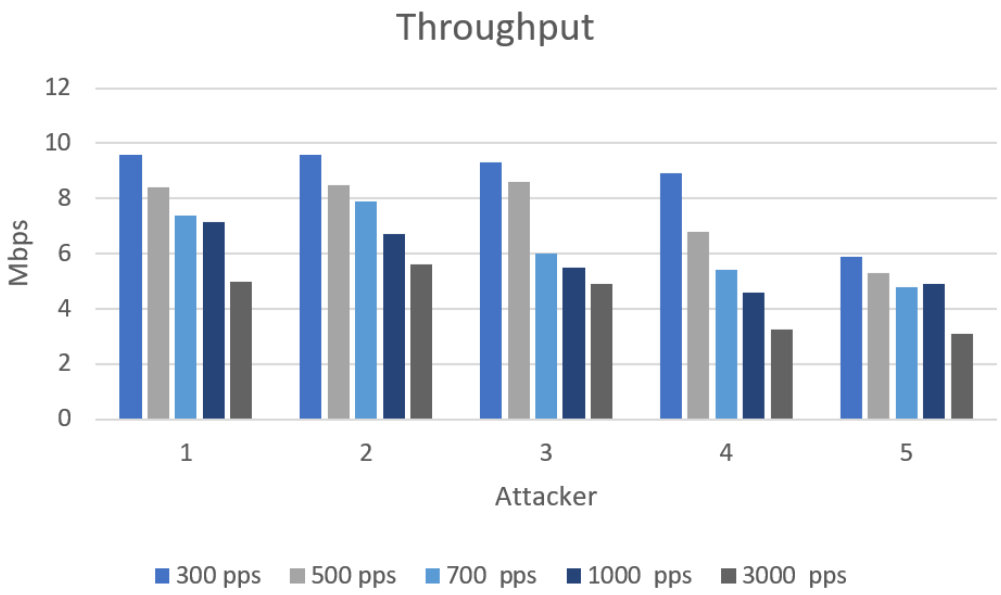

Fig. 6. DDoS Throughput Without Attack Mitigation

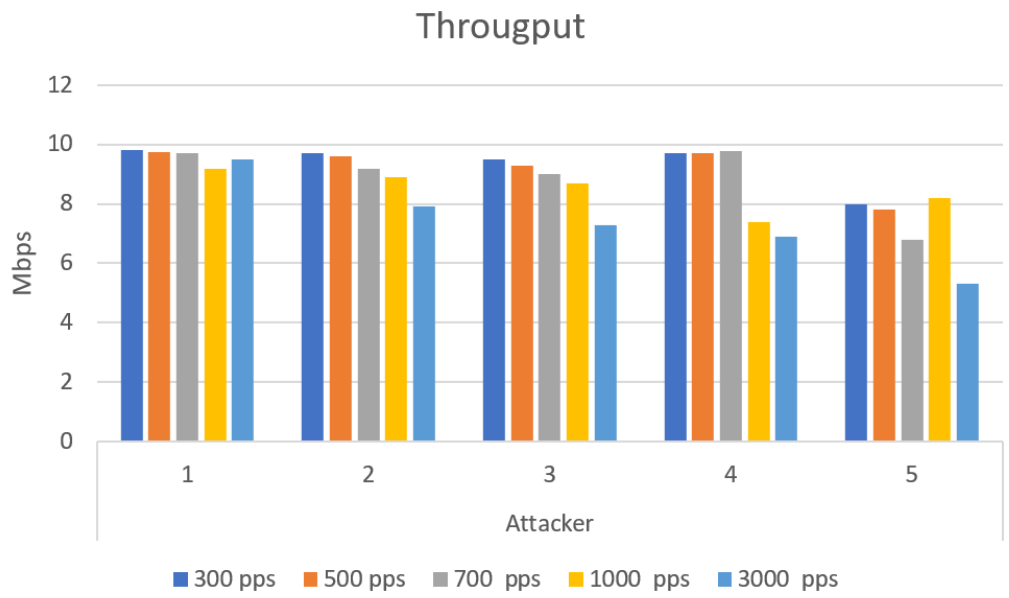

Fig. 7. Throughput of DDoS Attack with SVM mitigation

In this chapter we analyze, the effect of DDoS on the server, with SVM mitigation and without any mitigation. The DdoS attack scenario is attacking the server (h1) with 1, 2, 3, 4, and 5 attacker hosts with 300 PPS, 500 PPS, 700 PPS, 1000PPS, and 3000 PPS. The attack started after 10 seconds of data being generated.

1) Throughput of DDoS attack without SVM mitigation: In Fig.6 the 1 attacker with 300 PPS slightly impacting the throughput server with average throughput 9 Mbps and themost effective DDoS attack is DDoS with 4 attackers with 3000 PPS that make the throughput of the server become 3.25 Mbps and 5 attackers with 3000 PPS that make the throughputof the server become 3.1 Mbps.

2) Throughput of DDoS attack without SVM mitigation: Fig. 7. shows the throughput of SVM mitigation is better than throughput SVM without any mitigation it indicates that the SVM successfully mitigated the DDoS traffic even the biggest attack damage SVM mitigation can still mitigated.

8. CONCLUSION

The author proposed a source-based defense mechanism using SVM that combined with RYU controller to overcome the DDoS attack with random IP. By comparing the result of the simulation SVM combined with RYU mitigation successfully mitigate the DDoS attack.

Reference

[1] Yan, Qiao, F. Richard Yu, Qingxiang Gong, and Jianqiang Li., “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges.” IEEE Communications Surveys & Tutorials., vol. 18, no. 1, pp. 602-622. OCT, 2016.

[2] S. Qadir and Quadri, ”Information Availability: An Insight into the MostImportant Attribute of Information Security,”Journal of Information Security,vol. 07, no. 03, 2016.)

[3] J. Li, H. Jiang, W. Jiang, J. Wu and W. Du, ”SDN-based Stateful Firewall for Cloud,” 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 2020, pp. 157-161, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00037.

[4] K. Park and H. Lee, “On the effectiveness of route-based packet filtering for distributed DoS attack preventi
Commun. Rev, vol. 31, no. 4, pp. 15–26, Aug. 2001.

[5] K. Argyraki and D. R. Cheriton, “Scalable network-layer defense against internet bandwidth-flooding attacks,” IEEE/ACM Trans. Netw., vol. 17, no. 4, pp. 1284–1297, Apr. 2009.