International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Detecting DOS Attacks in Software Defined Networking and Cloud Computing

Roniya Ssan Jacob[1], Dr. Kalimuthu .M[2]

[1]M.Tech. Scholar, Department of Comouter Science, Believers Church Caarmel Engineering College, Kerala, India
roniyajacob07[at]gmail.com

[2]Guide, Department of Comouter Science, Believers Church Caarmel Engineering College, Kerala, India

Abstract: ***Wireless networks are web that aren't attached by cables. The use of a cellular net enables enterprises to steer clear of the pricey strategy of introducing cables. The Software-Defined Networking (SDN) technology is combined with the traditional Cloud network to form Software Defined Clouds (SDC).SDC is steered to forge a good Cloud ecosystem by lengthening the virtualization perception to all resources. She centralized controller performs all control functions in a network, it requires strong security. Most important attacks in SDC is Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks. The DoS attacks can be overcome by adding distributed Firewall with Intrusion Prevention System (IPS). The proposed system is for two DoS attacks, ICMP and SYN flooding attacks. The conveyed Firewall with IPS security distinguishes and keeps the DoS assault viably.***

Keywords: SDN, OFP, DDoS, Firewall and IPS

1. Introduction

Cloud Computing and Software-Defined Networking (SDN) are modern trends in both academia and industry, because they support certain essential networking features for users. The main features supported by Cloud Networking are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. In both Cloud Networking and SDN, security issues have been considered as the main problem to find the solution. In SDN, the control plane is decoupled from the data plane and network devices are controlled by the centralized controller using the Open Flow Protocol (OFP). Hence, the SDN controller may get chance of various security attacks. Among various security threats to SDN, those threats at the data plane and the application plane shall be controllable by the network operator and the Application Service Providers (ASPs) using the techniques suggested by the various researchers or some experienced persons. However, special attention is required for the SDN control plane security attacks; especially the Denial of Service (DoS) attack [1, 2].The objective is to develop a recommendation model that considers different rule formation to detect dos attacks. To provide the central control for attack detection using SDN through cloud computing. SDN brings us a new chance to defeat DoS attacks in cloud computing environments. This approach is to increase the functionality and capacity of wireless networks using Software Defined Network (SDN) and cloud computing technologies. The files that send through this network has the capability to reduce the loss of data due to the increased security by detecting the intrusions.

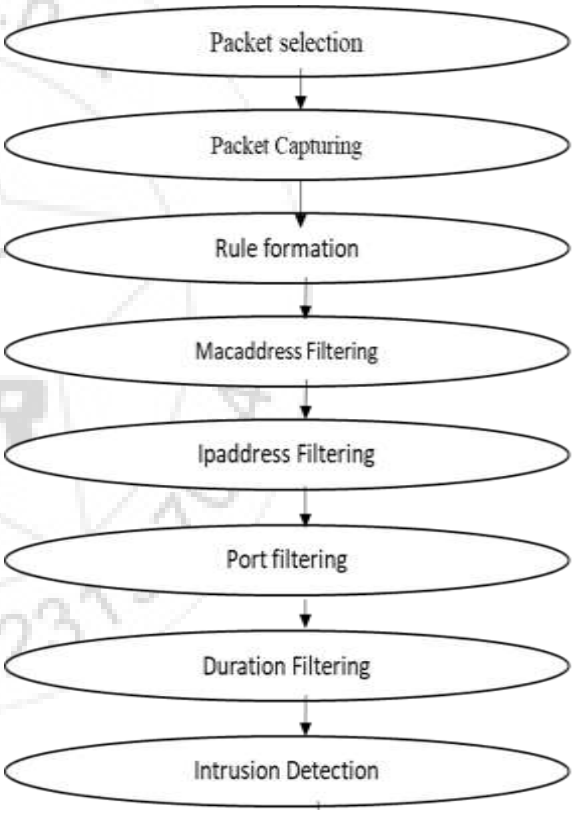

Figure 1: Flow chart showing the processes described in this paper.

To overcome the DoS attacks, this work introduced a distributed Firewall with Intrusion Prevention System (IPS) for SDC. From the simulation results and discussion, the distributed Firewall with IPS security detects and prevents the DoS attack effectively.

2. Module Description

(1)Packet Capturing-

Software-Defined Networking (SDN) technology is combined with the traditional Cloud network. Nowadays,

the increased use of network causes the increase of data. So that the user can upload the required packets that needs security.

Figure 2: Select Packet

(2) Rule Formation-

There are four rules for security purpose. They are applied to the packets that are already imported.

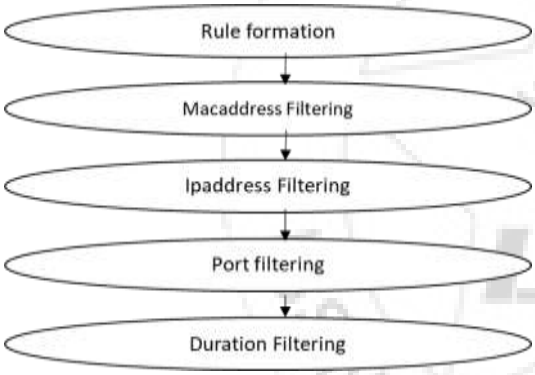

Figure 3: Rule Formation

In PC organizing, Media Access Control MAC Filtering (or EUI sifting, or layer 2 address separating) alludes to a security get to control strategy whereby the 48-bit deliver allotted to each system card is utilized to decide access to the system. Macintosh delivers are remarkably appointed to each card, so utilizing MAC separating on a system allows and denies organize access to particular gadgets using boycotts and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network [3].IP Filtering is a great way to limit access to your site for specific groups of IP addresses. PFilter (commonly referred to as ipf) is an open-source software package that provides firewall services and network address translation (NAT) for many Unix-like operating systems. The author and software maintainer is Darren Reed. IPFilter supports both IPv4 and IPv6 protocols, and is a stateful firewall [4].

(3)View Rules

This allows viewing different filtering rules that are applied to the packet already captured. A distributed Firewall with Intrusion Prevention System (IPS) for SDN helps to detect the DOS attack.

Figure 4: View Applied Rules on Packet

(4) Intrusion Detection

The distributed Firewall with IPS (Intrusion Prevention System) security detects and prevents the DoS attack effectively. The Firewall and IPS modules on SDN switches screen the activity at an edge level. The SDN switch that recognizes the irregularity will speak with the SDC controller. The SDN switch that recognizes the irregularity will speak with the SDC controller. The Firewall and IPS modules at the SDC controller examine the bundle encourage for potential noxious movement. The IPS at that point keeps the interruption by sending an alert, dropping bundles or resetting the associations or obstructing the movement from the culpable hub lastly logging the data. Further, the controller refreshes the Firewall govern in SDN changes to drop parcels from the hub.

3. Basic Concept

One of the fundamental security bolsters for a system is Firewall. When a Firewall is not properly configured or misconfigured in a network, that will mislead the users, where they are in the assumption that the network is protected by the Firewall [5].When a Firewall is not properly configured or misconfigured in a network, that will mislead the users, where they are in the assumption that the network is protected by the Firewall [2]. Suh, et al. [5] studied an IP based Firewall for the SDN controller. Similarly, a Layer 2 SDN Firewall for the POX controller was investigated in [5]. In one of the other studies, a framework for SDN security services is discussed that combines the centralized Firewall system and DDoS-attack mitigation system [6]. On the other hand, distributed Firewall implementation on SDN switches are found in [8-10]. In order to optimize the Firewall rules in the Access Control List (ACL), the authors in [7] proposed an Integer

Linear Programming (ILP) based solution for placing rules on SDN switches. In [8, 9], the specifications for defining the MAC filter rules on SDN switches are investigated using Big Switch Abstraction (BSA).

4. Optimization Techniques

The clients get associated with the Cloud through their Internet get to. The access organize is overseen by an ISP, likewise called as Network Service Provider (NSP). Practically speaking, the remote system hubs, for example, developed Node B (eNB), Gateway (GW) Serving GW (SGW) and Packet Data Network GW (PGW) oversaw by the NSP are associated with the SDN controller by means of the Southbound Interface, while the applications impart by means of the Northbound Interface. The SDN switches keep up the MAC stream table that contains Firewall rules for each stream, activity stream measurements, and time stamp. Firewall rules are utilized to take choice on approaching bundle; movement stream insights, e.g., parcels every second, is utilized to look at the conduct of a stream utilized by IPS module and the time stamp is utilized to keep the govern briefly to limit the memory utilization in SDN switches. A Firewall control in a MAC table is alive until the point that the time stamp period. At first, MAC stream tables in the SDN switches are void. Henceforth, the SDN switches send the principal parcel to the SDN controller by means of the Southbound Interface. The Firewall modules at the controller have the entire ACL, which is arranged by the Cloud head. On the off chance that any Firewall lead in the ACL is coordinated with the goal MAC address, the SDC controller imparts to the SDN switch.

For instance, a host sends an ARP ask for to the Data Center; the Data Center at that point reacts with a Data Center MAC address. Presently, the interloper parodies the message and sends another ARP reaction to the host with the gatecrasher MAC address rather than the Data Center MAC address. The gatecrasher would now be able to capture all the host movement before sending it on to the Data Center. In this manner, ARP examination guarantees that the interloper can't send an ARP reaction with their MAC address. After the ARP assessment, parcel is investigated for interruption recognition by the IPS module in the SDC controller.

The IPS module at the SDN switch screens the measure of control messages. Likewise, the bundle stream rate for each stream is observed to confirm the ICMP flooding assault on parcel check. On the off chance that there is any anomalous conduct in that rush hour gridlock, the IPS module at the SDN switch advances a few bundles from the stream to the controller to dissect further for Intrusion Detection.

Interruption recognition is likewise alludes to discovery of noxious movement in PC systems. Large portions of the Intrusion Detection Systems (IDS) accessible today are signature-based. IDS works as an infection scanner, via looking for a known character or mark for every particular interruption occasion. Consequently, signature based IDS is just on a par with the degree of the refreshed mark database. Since SDN switches have the memory restriction, signature based IDS usefulness is kept at the SDC controller.

Naive-Bayes-Classifier algorithm

Naive Bayes is a simple technique for constructing classifiers: models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite set. It is not a single algorithm for training such classifiers, but a family of algorithms based on a common principle: all naive Bayes classifiers assume that the value of a particular feature is independent of the value of any other feature, given the class variable [10]. For example, a fruit may be considered to be an apple if it is red, round, and about 10 cm in diameter. A naive Bayes classifier considers each of these features to contribute independently to the probability that this fruit is an apple, regardless of any possible correlations between the color, roundness, and diameter features [10].

5. Results and Discussion

Figure 5 demonstrates the aftereffect of parcel send through proposed framework. Programming Defined Networking (SDN) innovation is joined with the conventional Cloud organize. These days, the expanded utilization of system causes the expansion of information. So the client can transfer the required parcels that necessities security. There are four standards for security reason. They are connected to the bundle that are as of now foreign made. This permits to see diverse sifting decides that are connected to the parcel as of now caught. A disseminated Firewall with Intrusion Prevention System (IPS) for SDN recognizes the DOS assault. The disseminated Firewall with IPS (Intrusion Prevention System) security identifies and keeps the DoS assault successfully.

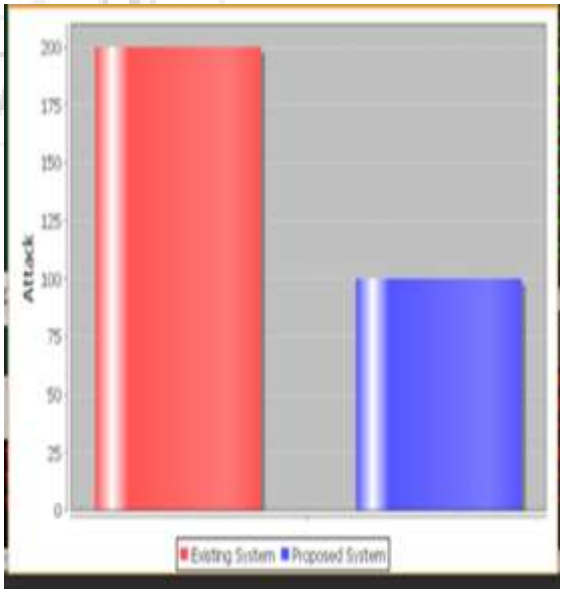

Figure 5: Attack Detection

6. Conclusion and Future Scope

In this work, the system design of SDN and SDC was exhibited and different security dangers that exist in SDN layers were depicted. From the writing study, DoS assaults are more intricate than different assaults. For location and counteractive action of DoS assaults, the appropriated Firewall is joined with IPS security. The Firewall and IPS security modules in SDN switches perform Firewall activity from the impermanent run and confirm the atypical parcels in the information plane. The conveyed Firewall with IPS could distinguish and keep the DoS assault successfully by utilizing distinctive principles. One without bounds extension is should be added more assault location principles to accomplish great outcomes quick.

Reference

[1] S Scott-Hayward, S Natarajan and S Sezer, (2016) "A Survey of Security in Software Defined Networks", IEEE Comm. Surveys and Tutorials, pp. 623-654.
[2] I Ahmad, S Namal, M Ylianttila and A Gurtov, (2016) "Security in Software Defined Networks: A Survey", IEEE Comm. Surveys and Tutorials, pp. 2317-2346.
[3] A Wool, "A Quantitative Study of Firewall Configuration Errors", IEEE Computer, Vol. 37: Iss. 6, 2004, p.p 62-67.
[4] https://en.wikipedia.org/wiki/MAC_filtering
[5] https://en.wikipedia.org/wiki/IPFilter
[6] J Jeong, J Seo, G Cho, and J Park, "A Framework for Security Services Based on Software-Defined Networking" Proc. of Int'l Conference on Advanced Information Networking and Applications, 2015, p.p 150-153.
[7] S Zhang, F Ivancic, C Lumezanu and Y Yuan, "An Adaptable Rule Placement for Software-Defined Networks", Proc. of Int'l Conf on Dependable Systems and Net, 2014, pp. 88-99.
[8] J Gregory V. Pena and W Emmanuel Yu, "Development of Distributed Firewall Using Software Defined Networking Technology", Proc. of Int'l Conf on Information science and Technology, pp. 449 – 452, 2014.
[9] P Rengaraju, Senthilkumar S and C-H Lung, "Investigation of Security and QoS on SDN Firewall Using MAC Filtering", Proc. of 6th IEEE Int'l Conference on Computer Communication and Informatics, 2017.
[10] https://en.wikipedia.org/wiki/Naive_Bayes_classifier