International Journal of Pure and Applied Mathematics
Volume 119 No. 10 2018, 709-717
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

An Enhanced SDN Firewall for Unstructured Local Network

[1]C.R. Greeshma, [2]N.R. Keerthi and [3]Nima S Nair
[1]Dept of Computer Science & IT,
Amrita School of Arts & Sciences, Kochi,
Amrita Vishwa Vidyapeetham, India.
greeshmacr95@gmail.com
[2]Dept of Computer Science & IT,
Amrita School of Arts & Sciences, Kochi,
Amrita Vishwa Vidyapeetham, India.
keerthikrishna004@gmail.com
[3]Dept of Computer Science & IT,
Amrita School of Arts & Sciences, Kochi,
Amrita Vishwa Vidyapeetham, India.
nimasnair@gmail.com

Abstract

Software Defined Networking is a recent kind of stratified technology facilitate network management such as initialization, modification and manage the system behavior in a flexible way using open interfaces. Separate control plane from data plane by reducing the impact of failure and enhance resilience in resource management. SDN can manage the upsurge in security by providing tighter control on the network. The main purpose of the proposed system suggests an approach that integrates the address translation mechanism for LAN along with the SDN controller firewall and remaps the IP address into another by overcoming the end to end IP traceability, delay in communication and additionally maintains reinforcement by conveyance of packets. Efficient in reviewing the packets by adding policy rules in the firewall and reduce the internal traffic results in the displacement of packets in a secured and faster manner. Moreover, with the help of centralized controller facilitates the optimization and configuration of network by customizing the controller.

Key Words: Firewall, network address translation, SDN controller.

1. Introduction

SDN is the modernized networking technology which is used to manage convoluted networks and can programmatically construct, control, customize, initialize and administer the behaviour of network through open interfaces[1].An SDN established network design enables higher flexibility and vendor-neutral which benefits organizations, data center operators, end users etc. The notion of SDN was initially promoted by Nicira Networks. SDN is correlated with openflow protocol and has a diverse set of design specifications. The SDN rupture the data plane from the control plane. A Data plane (forwarding plane or user plane) manage the data transfer from and to with the clients, it decides the destination of the arriving packets to the router. A control plane is accustomed to route the packets, the control plane packets are originated or destined to the router and is liable for configuring the system, managing, updating and enhancing the routing table information. The data plane act like an abstraction of all hardware side in a network where control plane act as a brain controlling unit [2]. The router processes the packets in the control plane and lastly updates the routing table information. In SDN the controller is referred to as the brain of the network, handles the flow control and facilitate intelligent networking [3]. SDN help organizations in dealing with big data more efficiently by managing the throughput and connectivity, SDN moreover supports cloud based traffic by delivering resources dynamically on demand in organizations, Controller also helps to have a centralized view of the whole network. An SDN architecture is directly programmable by cause of, it can be decoupled from forwarding functions, as the administrators can dynamically accustom the network traffic outflow to accommodate changes as needed. Furthermore, it is said to be centrally managed as the controller maintain a global view of the network. It is programmatically configured and is based on vendor-neutral an open standard. [4].

NAT-Network Address Translation let on the devices like router which act as a mediator between a public and private network, it is a mechanism which is used to translate the private IP into public or vice versa. NAT was initially developed to defend the paucity of IP addresses. While the internet has grown larger in a short period of time, the current assessment shows that there exist about 100 million computers and 350 million users who heavily use internet, in such a case there is a need for billion and billions of IP addresses to connect a system with the internet. Consequently, in order to overcome this problem NAT was developed [5]. A NAT act as a single separate device between a local network and a public network (Internet) and can share a common IP addresses. While accessing a system from outside a network, the IP address of the internal network is translated to the computer's unique address from the router's address. The table contents can be viewed by the computers outside a network. All the systems in the LAN network has a private IP. Computers outside the network

can only view a single IP address while connecting to an internal network. A NAT also contribute security because the IP addresses in a local network is hidden from the external(public)network, this makes it more challenging for an attacker to commence an attack on an internal host. Nevertheless, the local networks are accessible to attack, to overcome this defect a NAT is connected with firewall. Firewall adds an additional security and can remove or block unwanted data, also prevents our host from illegal access connections[6].

Working of NAT

To deceive the insufficiency of IP addresses a provisional solution was developed known as NAT. A NAT controller is a single device such as router, to act as a mediator between a local network and internet. In a typical organization, network devices are connected to the router and the router then connected to the internet. While registering with ISP, receive an IP address which is available throughout the internet and is authorized to the router which is used. Router consist of a public IP address, were anyone on the internet can deliver packets, and the devices in the network consist of a private IP address that is enabled to those by the local router, which is not usable from the internet. When we try to access a web page using the computer, initially the sender creates data packets and sent to the router. Then build an entry in the translation table with senders IP and port number of the received packet, afterward converts the private source IP in to a public IP. Eventually, the packet is transmitted to the destination. At destination, process the request and sent back the reply packets to the sender through the router. The router receives the processed packets, and examines the matching public IP and port number in the translation table. The router rewrites the receivers IP with the local IP address and sent packet back to the starting host(sender) .

2. Background Study

In an unstructured network, the large LAN infrastructure using traditional firewall systems process different requests at a time, which requires high processing speed, updating table entries, storage space for retaining data. Therefore, use separate devices for security and NAT conversion which is expensive and difficult to maintain.

Working of Firewall in a Traditional LAN

Placing a Firewall Inside Network

Defining complex rules in the firewall is difficult to check and easily vulnerable to spoofing. Firewall will discard the packet if it is from an untrusted source within a LAN network. In reverse, when a packet from outside WAN-firewall can process the packet only after the NAT conversion.

Figure 1: Firewall Inside Network

Placing Firewall Outside Network

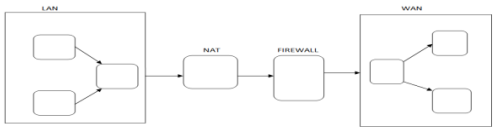

Figure 2: Firewall Outside a Network

When a packet arrives from an untrusted source or from an intruder can penetrate into the system, the packet is forwarded to the firewall only after the NAT conversion; before discarding the packet, it process the packet and update the tables.

Placing Firewall Inside and Outside Network

This will be one of the secure mode but have to place different firewall for security purpose. The cost of maintaining will be higher and consume much time by controller, whenever a packet is received from inside a network, first the firewall check for a match and only afterwards the packet is forwarded to NAT. Likewise whenever a packet reaches from an external network, the NAT performs the conversion only after filtering the packets through firewalls. Only the filtered packets are processed. Hence the time consumed for NAT conversion will be less and reduce the storage area.

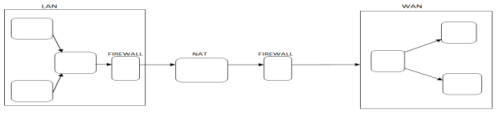

Figure 3: Firewall Inside and Outside a Network

3. Related Works

Taluja researches about Address translation mechanism and Filtering rules. NAT assigns public IP address to computers with in a private network hence limit the usage of address in local network for security purposes. Packet Filtering process will analyze and control the packets based on source and destination. Conversely this paper not focus much on firewall capacity but discuss short on few firewall techniques[7].

Bhanot research mainly focus on firewall rules- based on that packets will be passed on comparing it with the ip address. The firewall either drop, forward or send message to source on rule matching. Based on this paper decisions could not be taken by inspecting the packet content[8].

The early works of Sharma, Bhisham, and Karan Bajaj gives an excellent review on the pros and cons of firewall capacity, mainly focus on one packet firewall technique. And there is no technique to analyze which packet passing through

the firewall[9].

4. Problem Statement

Usually LAN mapping is done by a router beside NAT enabled. Router maintains and updates the routing table and connect large number of networks. Conversely, can update bandwidth but with the higher degree of filtering increases latency. Consequently, if large quantity of data to filter the router function may get slower, difficult to maintain and with the flaws in security easily prone to attacks. In order to provide security need to incorporate firewall device in the network additional to the router.

5. Proposed Design

To make the IP addressing effective incorporate firewall and address translation in controller, so that no need to install separate NAT boxes and firewall in the router. Alternatively each device have to individually forward packet to the succeeding system which is centrally maintained by the controller. SDN uses layered technology provides flexibility in configuration and resource management.

The forward plane (switch) which is accountable for forwarding the packet and the control plane (controller) is capable of creating policy and implementation. According to the rules, packet examination and decision will take place in the controller and automatically refurbish the table entries. When a packet is transmitted from one network to another if it arrives at the switch forwarded to the controller compare the destination IP address with flow table entries, if matching address found-packet will be forwarded for NAT conversion else it dropped[10]. Moreover, controller work centrally, easy to define and customize rules. Ordinarily, NAT service is inactive, based on requirement add or remove rules. When a NAT rule is removed the related sessions associated with it will be detached. The benefits of using firewall in SDN are, the internal traffic cannot be seen and filtered in the traditional firewall. The SDN based firewall can act as both policy checker and packet filter.

6. Implementation

Whenever a packet is needed to be sent from one network to another, and if a packet reaches the switch, it forwards the packet to the controller. The firewall and NAT will be placed inside the controller, were the packet will be checked first by the firewall and if it matches with the rules specified, eventually forwards the packet to NAT and corresponding packet private IP address is transmuted to public IP address, send to the destination port. Similarly in reverse, the packet coming into the controller is analyzed initially with the firewall and if equitable with the rules, corresponding NAT conversion will be done. Finally the packet onward to the requested host[11].

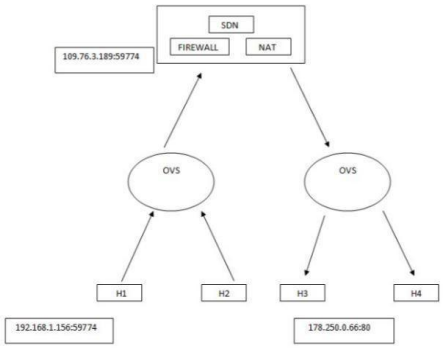

Figure 4: Packet Flow in SDN based Network

Table 1: Route Table

INSIDE LOCAL	INSIDE GLOBAL	OUTSIDE LOCAL	OUTSIDE GLOBAL
192.168.1.156 :59774	178.250.0.66 :80	178.250.0.66 :80	109.76.3.189 :59774

H1=System inside a network

H2=System inside a network

H3=System outside a network

H4=System outside a network

OVS=Open vSwitch

We have simulated NAT and firewall in the controller using mininet by configuring 4 hosts, 2 switches and a controller. The scripted modules for NAT, firewall and table lookup is in python.

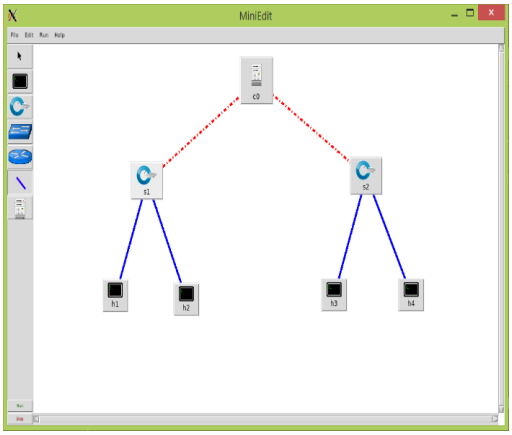

Figure 5: Incorporating Firewall and Nat in SDN

pseudo code

1. A packet pass from one network to another (H1->H3)
2. The packet forwarded to the controller by switch without inspecting contents(OVS->Controller)
3. Firewall check for IP address matchings, if a match is found, forwarded to NAT else packet dropped.
4. NAT convert the private address of the packet to public address(source address as controller address) and forwarded to the destination address H3.(Controller ->H3)
5. When packet re-enter into the network from outside(destination address as controller address)(H3->Controller).
6. Again firewall inspects the incoming packet, if IP address is matched, forwarded to NAT else packet dropped.
7. NAT convert the public address of the packet to private address(source address as controller address) and forwards the packet to destination address of H1.

While using this packet filtering techniques unauthorized packets will be dropped from authorized packets. NAT allocate public IP to private network and prevent hackers from accessing data using unauthorized IP address.

Incorporating Firewall and NAT in SDN Controller overcome the drawbacks of traditional firewall. No need to place different devices for inspecting packets coming in and out of the network hence reduce the time for unwanted conversions. As the controller is centrally defined, it is easy to maintain.

7. Conclusion

Firewall is a technique that authorizes network access and protect from unreliable accesses. NAT prevents the usage of exceeding IP address of an organization. The proposed research paper is efficient in reviewing the packet by discarding the intruders. The packets are processed by NAT, when it is forwarded by the firewall, after the rule matching moreover able to avoid unnecessary conversions and preceding table updations. Thus packets will be transferred in a secured and faster manner.

8. Future Works

The proposed research discusses about combining distinct firewall technologies like packet filtering firewalls and NAT in controller. With the developmental progress in the technology different application services are used but cause problems in FTP, SNMP, SIP when NAT interferes with IP header files. Therefore, application is needed to be rewritten to work properly. Our future works focus on the development of a system which can accommodate these services with the combination of NAT and firewall.

References

[1] Caraguay A.L.V., Lopez L.I.B., Villalba L.J.G., Evolution and challenges of software defined networking, IEEE SDN for Future Networks and Services (2013), 1-7.

[2] Pallavi N., Anisha A.S., Leena V., Detection of Incongruent Firewall Rules and Flow Rules in SDN, Advances in Intelligent Systems and Computing 517 (2017).

[3] Farhady H., Lee H., Nakao, A., Software-defined networking: A survey, Computer Networks 81 (2015), 79-95.

[4] Anan M., Al-Fuqaha A., Nasser N., Mu T.Y., Bustam H., Empowering networking research and experimentation through Software-Defined Networking, Journal of Network and Computer Applications 70 (2016), 140-155.

[5] Chen W.E., Chen B.E., An effective NAT traversal mechanism for SIP/IMS services in SDN-enabled all-IP mobile networks, Wireless Personal Communications 84(3) (2015), 2171-2185.

[6] Yoon C., Park T., Lee S., Kang H., Shin S., Zhang Z., Enabling security functions with SDN: A feasibility study, Computer Networks 85 (2015), 19-35.

[7] Taluja S., Verma P.K., Dua R.L., Network Security Using IP firewalls, International Journal of Advanced Research in Computer Science and Software Engineering 2(8) (2012), 348-354.

[8] Bhanot A., Leenajain, Implementing Network Security Policies: Packet Filtering Mechanism, International Journal of Emerging Trends and Technology in computer Science 2(3) (2013).

[9] Sharma, Bhisham, Karan Bajaj, Packet Filtering Using IP Tables In Linux, IJCSI International Journal of Computer Science Issues 8(4) (2011).

[10] Tran T.V., Ahn H., Challenges of and solution to the control load of stateful firewall in software defined networks, Computer Standards & Interfaces 54 (2017), 293-304.

[11] Tharaka S.C., Silva R.L.C., Sharmila S., Silva S.U.I., Liyanage K.L.D.N., Amarasinghe A.A.T.K.K., Dhammearatchi D., High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies, International Journal of Scientific and Research Publications 6(4) (2016).