A Comparative Study of Traditional Network Firewalls & SDN Firewalls

Gunjan Katwal
Department of Computer Science,
Himachal Pradesh University, Shimla, H.P., India

Manu Sood
Department of Computer Science,
Himachal Pradesh University, Shimla, H.P., India

Abstract- SDN (Software Defined Networking) is the network architecture that has gained attention of researchers inrecent past. Traditional networks were very complex and difficult to ma nage. SDN changed this by providing a standard interface (OpenFlow) between the control plane and the data plane. Its implementation is fully dependent on software so that we can handle and control the behavior of all the networking devices through programmatic control. This programmatic control provides variousways to findout the failures in the networking devices. So effectively SDN emerges as a networking architecture that has the ability to solve all the problems those were found in traditional architecture. Today SDN has become an important part of networking, so it is important to understand its behavior. It also provide security in the network. The security in SDN is provided by employing firewalls in the network. In this paper the authors discussed about the comparison between the traditional network firewalls and software defined networking firewalls.

Keywords-Firewalls, OpenFlow,SDN, Traditional network

I. INTRODUCTION

Software Defined Networking is a latest approach in the field of networking where there is acentralized software at the control plane which monitors and controls all the data flow and communication taking place in the data plane. SDN have a separate control plane and a data plane. SDN basically limits the effort to manually route the traffic and allot the router for the transferring of the data [1]. The routers in SDN are automatically allotted wherever they are needed for the traffic flow. This makes the SDN easy to use and a less time consuming approach of networking as there isa defined software in the control plane which defines the entire flow of the data. It was discovered basically to overcome the limitations of the current networking type.

In SDN architecture i.e. the three tier architecture, the control plane and the data plane are separated, network functionality and state are logically centralized, and there is the abstraction of network infrastructure from the applications [14].
The corefunction of the network is to transfer information from one point to another. The data travels and goes across multiple nodes in the network, and the efficient and effective data transfer is supported by the control provided by the network applications[11].
SDN has moved out as a means to improve programmability within the network to support the dynamic nature of future network functions and requirements[2].

1.1 Traditional Networks Vs SDN

In traditional networks there is a distributed control plane whereas in SDN there is a centralized control plane which manages the data flow. The foremost difference between the two is the flow of packets in the network [16]. SDN is more flexible than the traditional network as its ease of making changes to the software present in the control plane

and the change is appeared on the entire networking system wherever it is required. But in traditional networks we have to manually change each of the routers and have to configure the switches accordingly.

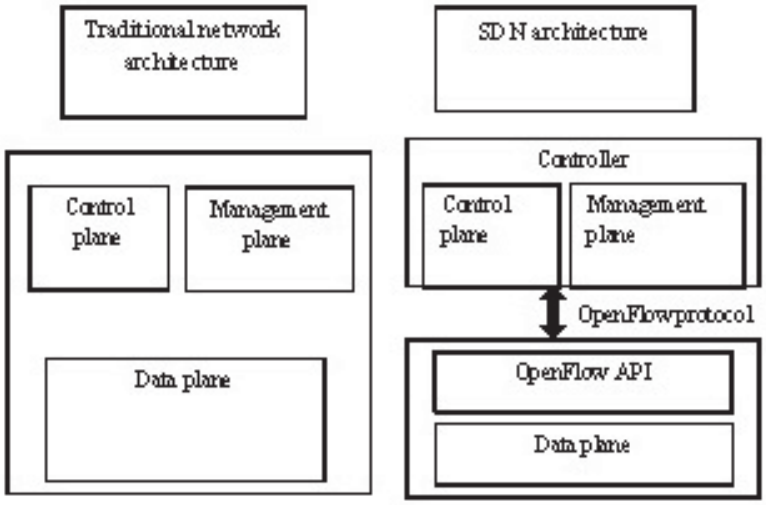

Figure1. Traditional Networks Vs SDN

The most important need for software defined networking (SDN) is to overcome the requirement of large datacenters this is due to the server virtualization provided by the SDN [3].
Some of the trends that drive the need for software defined networking are:
Changing traffic patterns: During the past years the network traffic patterns keeps on changing continuously. In theclient-server architecture, most of thedata transfer and sharing of resources takes place between one client and one server at a time, whereas in new applications there is a large access to different databases and servers that creates a rush in the network and hampers the speed of network, therefore requires more bandwidth.
The "consumerization of IT": Now a days, most of the people are using smart phones, tablets, notebooks, etc. to access the internet. IT world is under great pressure to accommodate these increasing mobile devices in aappropriate manner and also protects the user's personal as well as the corporate data from the theft or fraud [9].

1.2 SDN Focuses on Some KeyFeatures

Separation or decoupling of the control plane and the data plane.A centralized controller and global view of the network Open interfaces between the devices in the control plane and those in the data plane.Programmability of the network by external applications.

1.3 Advantages of SDN

Global View: Global means open to all and available to all. SDN showers the global view of the network as it makes the network and services available to the users who wants to use it, at anytime and anywhere.
Flexible Traffic: SDN controller also allows other devices to get attached and configure with it which makes the SDN more flexible and agile.
Easily Programmable: In SDN, the control plane is easily programmable as per the need since it is separated from the data plane. Whenever we want to make changes, we can change thefunctionality of control plane by changing the logic programming in control plane, and hence the change will occur everywhere [15].

Platform for Innovation: As SDN is a latest networking approach, the separation ofdata plane and the control plane permits the chances forinnovation of new applications and services.

1.4 Controllers used for SDN

SDN separates the control plane of networking device like a switch or a router from its data plane, so as to makeit possible to control and manage the network from a centralized controller. The control plane [14]is also called the controller. This controller has a global view of the network and controls the flow through the network. As the controller is the intelligent agent, the switch only performs the actions requested by the controller. This makes the switches inexpensive and very simple. An SDN Controller [15] is called the "brain" of the network. It is the control point in the SDN network, passing information to the switches/routers below through the southbound APIs and the business logic above through the northbound APIs. An SDN controller platform specially contains a collection of modules which performs different networking tasks like gathering network statistics, making the list of all the devices within the network and the capabilities of each. OpenFlow and OVSDB are the two most popular protocols used by SDN Controllers to communicate with the switches or routers.

The section 1 includes the introduction of SDN, comparison between the traditional networks and SDN, need of SDN and the advantages of SDN. Thereafter, in section 2, SDN architecture is explained and each layer performs what function is justified. The third section includes some information about the firewalls and the types of firewalls. Section 4 will include the comparison betweenthe traditional network firewalls and the SDN firewalls. And the last section will include the conclusion of the entire paper and the future work to be done.

Table 1. Various SDN Controllers

Parameter	**POX**	**Ryu**	**Trema**	**Floodlight**	**Open Day Light**
Language Support	Python	Python	C, Ruby	Java	Java
Open flow Support	v1.0	v1.0, v2.0, v3.0	v1.0	v1.0	v1.0
Open Source	Yes	Yes	Yes	Yes	Yes
GUI	Yes	Yes	No	Web GUI	No
REST API	No	Yes	No	Yes	Yes
Platform Supported	Linux, Mac, Win	Linux	Linux	Linux	Linux, Mac, Win

II. SDN ARCHITECTURE

SDN architecture is having three layers, the lowest layer i.e. the Infrastructure Layer also called the Data Plane consists of the physical network devices which forwards the data and these forwarding devices also monitors the local information [12].

The one above layer is the Control Layer also called the Control Plane. It manages the data plane and defines network operation and also provides routes to the data. It consists of one or more softwares that communicates with the forwarding elements through the southbound interfaces. One of these southbound interfaces areOpenFlow [10][13] which basically separates the control plane and the data plane.

The Application layer consists of business or network applications which assist the control layer in network configuration. This layer also provides the features like manageability and provides security to the network [4].

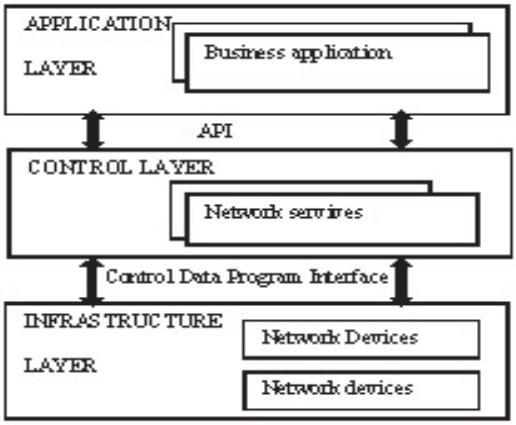

Figure 2.SDN Architecture

III. FIREWALLS

A firewall as the name implies acts as a security wall between the incoming data and the network system. It monitors and controls all the traffic that is going out from the network and that coming into the network [5].

Firewalls are generally configured to protect against unwanted and unauthorized user's access and their logins from the outside world. More sophisticated firewalls blocks the outside traffic to communicate with the insiders but allows the inside users to communicate freely with the outsiders [6].

3.1 Types of Firewalls

A firewall can be software based or hardware based and is used to keep a network secure. It is a system designed to prevent unauthorized access to or from the network. Firewalls are mostlyused to prevent unauthorized Internet users from accessing private networks and private or confidential data by connecting to the Internet [7]. The main objective of firewall is to control theincoming and outgoing network traffic by analyzing the data packets and by determining whether it should be allowed through or not, based on a predefined set of rules. A firewall creates a bridge or security wall between an internal network that is assumed to be secure and trusted, and another network, such as the Internet, which is not assumed to be secure and trusted.

Personal firewalls are used to protect a single computer from unauthorized access. They can take the form of software or hardware.

Network firewalls protect the entire network from unauthorized access. They can be a hardware which is installed on the system or a software application or thecombination of both.
Software firewall applications are installed on top of the operating system and can be configured multiple purposes[17].
Packet Filtering Firewall monitors network traffic at the transport layer. It will look at each packet entering or going out of the network and accepts or rejects it based on the user defined rules. Packet filtering is extremely effective and transparent to users, but it is moredifficult to configure.

3.2 Network Layer Firewalls

Network layer firewalls usually build their decisions based on the source and destination addresses and also on the ports of different packets. A simple router is a typical network firewall as it only provides route to the packet without keeping in mind what the packet is going to do and from where it is coming.These firewalls are very fast and almost transparent to the users [6].

3.3 Application Layer Firewalls

Application layer firewalls acts as the hosts that run the proxy servers and does not allow the traffic to enter the network, and also perform logging checks and examine the traffic that is passing through them. Moreover they can be used as the network address translator, since the traffic goes in and out through an application which marks the origin of the connection from where it has been initiated [6].

IV. COMPARISON BETWEEN TRADITIONAL NETWORK FIREWALLS AND SDN FIREWALLS

Table 2. Comparison between Traditional Network Firewalls and SDN Firewalls

Parameters	**Traditional Network Firewall**	**SDN Firewall**
1. Stateful inspection	Track the state of traffic present on layers 2 to 4.	Track the state of layer 2 to 7.
2. Integrated IPS and IDS	The IPS or IDS deployment is done with the help of a separate appliance or an appliance that is logically separated with the single appliance.	Intrusion Detection System (IDS) and Intrusion Protection System (IPS) is fully integrated.
3. Identity Awareness	Not supported.	Keeps the track of the identity of local traffic device and user.

V. CONCLUSION AND FUTURE WORK

SDN provides us a new way to implement networking. This paper describes how SDN architecture is appropriateto meet the rapidly changing requirements of networking organizations and customers and the comparison between the traditional network firewalls and SDN firewalls. In traditional networks it was not possible to achieve scalability and flexibility. The centralized controller present in SDN architecture changed the functionality of hardware devices by changing the routing policy through programmatic control[15]. The comparison between the traditional and SDN firewalls depicts thst the SDN firewalls are more secure as compared to the traditional ones, they are more flexible. Further, the author will implement a firewall to provide security to the network and will define its functionality.

REFERENCES

[1] IEEE Communications Magazine July 2013Are We Ready for SDN? Implementation Challenges for Software-Defined Networksand-their-functions.html.
[2]http://warse.org/pdfs/2013/ijacst012102013.pdf.
[3] http://searchsdn.techtarget.com/answer/Why-do-I-needSDN-technology.
[4] Software-Defined Networking Using OpenFlow:Protocols, Applications and Architectural Design Choicesby Wolfgang Braun and Michael Menth.
[5]https://en.m.wikipedia.org/wiki/firewall_(Computing).
[6]http://searchnetworking.techtarget.com/tutorial/ Introduction- to-firewalls.
[7]http://sankar-information-security.blogspot.in/2012/09/types-of-firewalls-and-their-functions.html.
[8] http://www.tomsitpro.com/articles/next-generation-firewall-vendors.
[9] https://googleweblight.com/part-3-is-software-defined-networking-sdn-changing-everything.
[10]OFLOPS: An Open Framework for OpenFlowSwitch Evaluation by CharalamposRotsos,NadiSarrar, Steve Uhlig,Rob Sherwood,_, and Andrew W. Moore.
[11] Software-Defined Networking: A ComprehensiveSurvey Diego Kreutz, Member, IEEE, Fernando M. V. Ramos, Member,Paulo Verissimo, Fellow, IEEE,Christia,Esteve Rothenberg, Member, IEEE, SiamakAzodolmolky, Senior Member, IEEE,and Steve Uhlig, Member, IEEE.
[12]A Compass Through SDN Networks ThomasZinner1, Michael Jarschel, Tobias Hossfeld, Phuoc Tran-Gia1 and Wolfgang Kellerer.
[13] Software-Defined Networking: The New Normfor Networks ONF White Paper.
[14] Software-Defined Networking Using OpenFlow:Protocols, Applications and Architectural Design Choices by WolfgangBraun and Michael Menth.