National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

A Survey on Software-Defined Networks (SDN) Firewall

Samreen Kour[1], Sudesh Kumar[2]

M. Tech, Dept. Of computer science, Shri Mata Vaishno Devi University, J&K, India[1]
Ph.D. scholar, Dept. Of computer science, Shri Mata Vaishno Devi University, J&K, India[2]

ABSTRACT

The exposure to Software-Defined Networking (SDN) paradigm is the only incentive for the concept of programmable networks that has presently retaken substantial momentum. For future Internet, SDN is one of the general rising solutions. SDN is defined by its two prominent characteristics, including the data plane and control plane decoupling and giving network application development programmability. The result of which, SDN is located to offer better performance, more proficient configuration, and higher flexibility to assist inventive network designs. Network security is the main challenge in SDN. This survey gives the overview of different SDN firewalls reflected in various research papers, and many techniques for improving SDN security through firewalls. In this survey, we analyze various research paper on network security through the firewall, deliberate their technologies, taken their comparisons and come out with best techniques presented.

Keywords: Open flow, Mininet, Network security, data plane, control plane, firewall, Software-Defined Networking.

I. INTRODUCTION

Nowadays networks are growing rapidly; various new devices are added to the network, makes it difficult to manage. Though out the network, it is quite difficult for an IT member to configure the access control lists. These complex networks make problematic situations for network administrators to bid the same set of access, routing, security, QoS and other policies to increasing computer users, which left the enterprise or businesses to a security violation, cost in-efficacy and time consuming and other negative out-turn.

SDN has been created and is being developed to overcome the vendor dependences for any modification in the devices and able to handle and manage the whole network easily. In this type of networking, the control plane and the data plane, both are separated in order to achieve programmability.

OpenFlow based firewall of current standard achieves programmability by separating the firewall hardware and control software so that the control software will not be constrained by the disadvantages of the hardware. Controller, the control plane takes all the routing decisions. This means decisions of SDN switches, the data plane depends on the control plane, hence in this way gives the programmability to the network.

A need for virtualization to carry out experiments because physical test beds are expensive and not always a researcher has an infrastructure to conduct research for study purposes of SDN. SDN has a virtualization technique namely Mininet which is specifically network emulation software. Mininet emulates the beginning of a genuine virtual network which runs real kernel, switch and application code with switches, hosts and an SDN controller using the limited resources on a single computer all using a single command. Mininet uses all the three components of SDN architecture, namely, the Controller (POX), the Controller Applications (Northbound API) and OpenFlow protocol (Southbound API). The architecture of SDN is shown in Fig. 1. Table 1 gives a comparison between conventional networking and Software-defined networks.

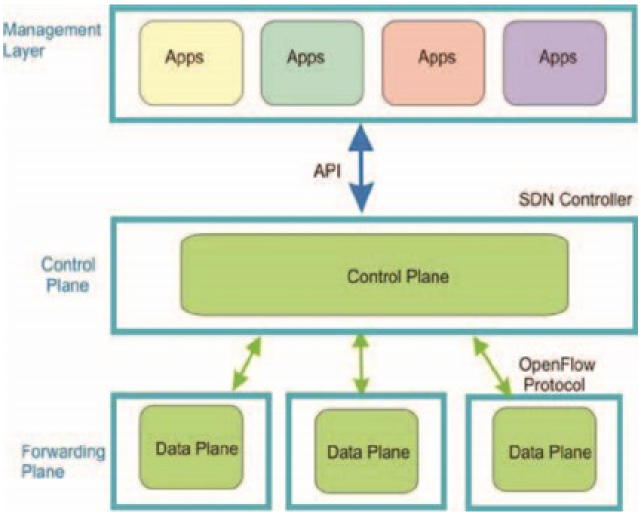

Figure 1. Software Defined Network Architecture

Table1: Comparison between Conventional networking and SDN

	Conventional	**SDN**
Features	For each problem needs a new protocol, complex network management	Decouples data and control plane and hence have programmability.
Configuration	Error-prone distributed control plane with manual configuration	Open software automated Configuration and logically centralized validation
Performance	Limited scalability and relatively inflexible and static configuration	Use of APIs for dynamic global control with cross-layer information
Innovation	For new innovations, Complex hardware implementation, long standardization process and limited testing environment	Ability to adapt to network changes, Easy software implementation for quick deployment, updating, and configuration across the network

SDN control plane is the central point of attack that's why various outlines were introduced for securing the control plane. The main points of attacks are at control layer, data plane layer, SDN layer. Admittance to the central servers by an unauthorized person that control software can perhaps control the full network and destruct it seriously.

The incoming and outgoing data packets that flow through a system is strained by the Firewalls. It uses set of instructions to filter network traffic that moves to or from over the network. These instruction sets are responsible for whether to permit or block the data traffic. The instructions of a firewall can appraise one or more features of the packets such as the destination or source port, protocol type, and destination or source host address.

The paper follows the following pattern: In section1: introduction, followed by section2, a survey of techniques (literature review), section3: analysis and section4: conclusion.

II. LITERATURE REVIEW

A. Firewall PK: Security tool for centralized Access Control List Management

In the following research, the author discussed an application firewall PK. For gathering different network security, also provided with an interface. It offers decision making of performance and security. Compound test cases were considered, indicating the weakness and strength of CISCO. This application allows the network control routers and monitoring and was built on real-time-scenario. In addition, a threat flag is activated which offers accurate and faster shield against security threats. Decision making and manual configuration of the router is restricted. CISCO one PK offers the functionality of many devices in a single application. For blocking attacks on the network, the firewall was developed. Only confirmed applications are allowed by the network controller.

B. FLOWGUARD: Building Robust Firewalls for Software-Defined Networks [2]

To assist not only exact discovery but also the actual determination of firewall policy destructions in dynamic SDN networks, a comprehensive framework, FLOWGUARD. To sense firewall policy desecrations when network states are restructured, it investigates network flow path places. In addition, with the help of numerous innovative resolution plans designed for various network update conditions it manages automatic and actual-time destruction resolutions. Enactment involves three components: violation resolution, violation detection, and flow tracking.

C. Mining a high level access control policy in a network with multiple firewalls [3]

This research paper proposed virtual firewalls configuration implementation through policy mining technique. The firewalls are separated and the arrangement is done using NET-RBAC. According to the requirement, the firewall policies can be changed that are defined at one place. The planned algorithm can be incorporated into broad-spectrum.

D. Building Firewall over the Software-Defined Network Controller [4]

This paper includes using OpenFlow making an SDN based firewall with a well-defined user interface. The reason behind the firewall is that each and every packet headers are investigated contrary to the firewall rule from higher to lower priority, and once matching fields are found in the rule executes stated action. Packets that do not match are dropped. Through a text-based graphical interface fitting firewall rules are conceivable. In the Internet world, an SDN firewall with a straightforward UI that incorporates priority switching can bring another trend of innovation.

E. Towards a Reliable SDN Firewall [5]

The major challenge is in developing an SDN firewall. Set-fields are modernized dynamically in Open-Flow network states. The rules in firewall overlap each other, simple flow policy violation isn't effective in the firewall. SDN firewall needs to investigate the ingress switch flow, damage, path of the destination and source.

F. Behavioural Security Threat Detection Strategies for Data Center Switches and Routers [6]

This paper includes problems in data center due to DDOS (distributed denial of service). For security threat finding and modification, the firewall is used. Packet header recognizes the flows. Minimum bandwidth threshold and observation interval, these two factors should be programmable in routers /switches to manage traffic individualities. Numerous DDOS attacks are labeled. The attacks are from various source and IP addresses. To advance security threat at different layers positioned on a virtual routing several test simulation and procedures are used. The communication between SDN and end-user rises the well-regulated network elements allowing smart decision making.

G. An OpenFlow-based Prototype of SDN-Oriented Stateful Hardware Firewalls [7]

The software firewalls offer inferior safety and enactment than hardware firewall. In SDN-oriented hardware, firewalls comprise controller and switches software. An OpenFlow enabled firewall controller and a “dumb” switch are used in the elementary configuration of an SDN-oriented stateful hardware firewall. In the flow tables of both the components, security rules are specified. The control judgments are made by firewall controller on mysterious traffic flows. In the flow tables, stated control decisions are basically controlled rules. The control rules stated in the flow table are imposed by the "dumb" switches by regulating the traffic flows rely on the control actions.

H. **Virtual Firewall Performance as a Way point on Software Defined Overlay Network** [8]

This paper suggests a virtual firewall applied over forwarding grid and SDN. Also discusses try-outs and enactment on the industrial deployment of the virtual firewall. By providing high latency and high availability, a single virtual firewall can handle the workload. A virtual firewall can provide more safety to the near server rather than small practical firewall located further from the server. The advantages of virtual firewall consist of space, replacement of practical firewall, power, faster implementation, and faster configuration and the various demerit of the virtual firewall are the complexity of defining rules, cost operation, and their nearness to the server for protection.

I. **Improving Network Security through SDN in cloud Scenario** [9]

Network security remains the main challenge in this paper. It is essential for the network to block the attacks. Over numerous agents which are conscious of administrative policy, the system is spread. For blocking traffic earlier tactics concentrated on using distinct VLAN. While downloading different software, internet users do not have much awareness which one is reliable and which is not. Access and security policies have to install to overcome the limitation of cloud network security. The base for creating policies is building the three categories of data. From the cloud environment, forwarding decisions sense malicious traffic, detailed information is provided by services. Virtual switches offer measurements and monitoring capabilities to be alert about what happens in the assessment environment, computing capabilities for traffic forwarding implementations, and OpenStack for service provisioning.

J. **A Layer2 Firewall for Software-Defined Network** [10]

This paper involves a firewall application for layer2 using three switches, four hosts, and one controller, all together make a tree topology. The application uses control plane as POX controller. PuTTY SSH client, Mininet, and Oracle Virtual Box Xming X Server for Windows, these all are used for building a Layer2 Firewall. PuTTY SSH client is basically used for launching remote connections to virtual hosts. This implementation emphases on layer2 firewall application by adjusting code offered by POX controller and the results show better performance and comprehensive functionality to control data traffic consequently.

K. **Improving cloud network security using the Tree-Rule firewall** [11]

This research discusses a new firewall application model in different cases and provides benefits. In this paper, new firewall is proposed after discussing the disadvantages of listed-Rule firewall. In large enterprises, security issues arise and also decision making wants a policy formation. System evaluation is slow, weaknesses increasing. From the live detection system, different threats are noticed. The simulation was stored in distributed not in centralized and also for traffic scoring policy is set. An additional module is necessary for policy creation and management because SDN rules are prepared for simple configure forwarding devices. The new network security offers faster reaction time and more reliability. Malicious traffic from and to the cloud environment can be alleviate by forwarding decisions.

L. **Distributed Firewall for P2P Network in Data Center** [12]

The important point in this paper is a data center security in cloud computing. Firewall is important for network security. In addition, XML firewall is used. According to performance, flexibility, and implementation, various types of distributed firewalls and their functionality are used. Moreover, DC-firewall major layers are auditing, executing, and executive. For network interaction among virtual management and machines, two networks are used. Higher management interface maintenance, updating firewall rules, and network status collection, these all are the responsibilities of administrative Server. For SDN platform, a "rabbit Sdn" is developed. In this implementation, the firewall offers well security and communication.

M. Blessing or Curse? Revisiting Security Aspects of Software-Defined Networking [13]

The following paper, the author discusses disadvantages and advantages of SDN. As SDN separates both data and the control plane, it offers new security threats and mechanism. SDN offers network security utilities by design but due to centralized control plane difficulty arises in SDN information security. The key security features are authenticity, confidentiality, integrity, consistency, and availability. In SDN, various new changes are taking place but it is not applied fundamentally. Network operators notice and alleviate network attacks. Unified threat management (UTM), Cryptography, network-based intrusion detection Systems (NIDS), and firewalls, these are the Network threat defence mechanisms. To counter network-based spoofing or sniffing attacks, SDN cannot provide cryptographic actions. SDN is refining on its security dangers.

N. Development of a Distributed Firewall Using Software Defined Networking Technology [14]

This research is to discover security prospects by concentrating on the growth of a firewall model that exploits the benefits of SDN. The topographies of OpenFlow, an open SDN standard, a distributed flow-based firewall model was established and tested on Mininet, a simulated network. In an OpenFlow environment, the advance of the firewall model is formed by the traditional packet filtering firewall in which all packets would go through the controller before being fell or delivered to its destination host. The firewall model creates a firewall object explicitly linked to that device without disturbing latency for each and every device connected to the controller. By modifying the flow tables of devices directly, provides more speed without affecting connectivity, in this way traffic is controlled by the firewall.

III. ANALYSIS

R. Trandafir, M. Carabas, R. Rughinis and N. Tapus [1] in their paper "Firewall PK: Security tool for Centralized Access Control List Management" talk over Cisco One Platform Kit framework which offers complex network security level. They discussed security decision making and the performance.

H. Hu, W. Han, G. Ahn, and Z.Zhao [2] in their paper "FLOWGUARD: Building Robust Firewalls for Software Defined Networks" talk over the technique in which with low-cost Flow tracking, violation resolution and violation detection is accomplished and offers security. It provides no extensibility but flexibility, and reliability.

L. Sche hlmann, S. Abt, H. Baier [3] in their paper "Mining a high-level access control policy in a network with multiple firewalls" talk over unified hierarchy, Policy mining, and unified merger technique in which network security is complex with a high cost.

M. Park, B. Lee, S. Yang [4] in their paper "Building Firewall over the Software Defined Network Controller" talk over Tree topology with POX which offers low-cost security. It is an OpenFlow based firewall with a user interface that contains priority switching can bring the trend of technology over the Internet.

H. Hu, W. Han, G. Ahn, and Z. Zha [5] discusses in their paper "Towards a Reliable SDN Firewall" talk over Policy techniques in which network security level is simple and the cost is low. SDN firewall needs to check for entrance switch flow, violation, the track of the destination and source addresses.

R. Krishnan and D. Mcdysan [6] in their paper "Behavioural Security Threat Detection Strategies for Data Center Switches and Routers" talk over Layer 2-4 Behavioural security threat detection technique offers complex network security level. This method carries additional flow alertness in the system to permit smarter decision making in data flow all the way through the network.

J. Collings and J. Liu [7] in their paper "An OpenFlow based Prototype of SDN Oriented Stateful Hardware Firewalls" talk over the system in which "dumb" switch and a firewall controller are used. This offers simple network security with low cost. It provides no extensibility but reliability.

C. Decusatis P. Mueller, [8] in their paper "Virtual Firewall Performance as a Waypoint on a Software Defined Overlay Network" talk over virtual firewall executed on VMware with increased performance and in low cost.

S. Seeber, G. Rodose [9] in their paper "Improving Network Security through SDN in Cloud Scenarios" talk over IDS monitoring, Policy making and security regulation in which network security level is complex with low cost. It concludes all the parameters required but does not provide flexibility.

T. Javid, T. Riaz and A. Rasheed [10] in their paper "A Layer2 Firewall for Software Defined Network" talk over tree topology using Mininet Virtual network creation, which offers low-cost network security. The technique provides better enactment and comprehensive functionality to control data traffic more efficiently.

Z. HE, TH. CHOMSIRI, P. NANDA, Z. TAN [11] in their paper "Improving cloud network security using the Tree Rule firewall" talk over hierarchal tree set firewall algorithm: NF_IP_FORWARD in which network security is simple with a high cost. It does not provide flexibility as well as reliability.

X. Jiat and J. Wang [12] in their paper "Distributed Firewall for P2P Network in Data Center" talk over Rabbit SDN Platform technique with complex network security level and high cost. It does not offer reliability and extensibility.

S. Hachan, N. Boulahi, F. Cuppens, [13] in their paper "Blessing or Curse? Revisiting Security Aspects of Software Defined Networking" talk over SDN security benefits, SDN evaluation, and threats. It describes other parameter but does not provide flexibility.

J. Pena and W. Yu [14] in their paper "Development of a Distributed Firewall Using Software Defined Networking Technology" specifying reliability and Confidentiality. The method offers more speed without disturbing connectivity.

IV. CONCLUSION

SDN is going to be the future of networking as it becomes a very proficient technology. By programming the control plane, including the centralized control which helps in handling the whole network. In this why SDN offers flexibility to the network. It becomes more valuable in case of controlling, synchronization, providing scalability and management of data in large data centers. Also, the Virtualization and Abstraction of resources helps in hiding complexity and securing the network. In short, we can say that future is SDN. In SDN, the important places where we need to pay attention are, security of Control plane since whole control of SDN is centralized in control plane, need to prevent from several attacks, the Security of southbound interface needs special care as control transfers through this interface and also due to SDN openness, system allows to write control programs so it is crucial to design some protocols or use existing protocols proficiently that will check the perfection of programming logic before implementation of SDN. So, in SDN there are still different fields where we need to pay attention. Network security is the main challenge in SDN. This survey paper gives the overview of different SDN firewalls deliberated in various research papers, and many techniques for improving SDN security through firewalls. The survey shows numerous firewalls implementation in different scenarios and cost of implementation. The main methods discussed are violation resolution, Flow tracking, and violation detection, unified merger, Tree topology with POX, unified hierarchy, and Policy mining. At low cost, these methods offer better security. Finding new and improving existing techniques for SDN-based firewalls is another area of research.

V. REFERENCES

[1] R. Trandafir, M. Carabas, R. Rughinis and N. Tapus "Firewall PK: Security tool for Centralized Access Control List Management", 2014.

[2] H. Hu, W. Han, G. Ahn, and Z. Zhao, "FLOWGUARD: Building Robust Firewalls for Software-Defined Networks", 2016.

[3] L. Sche hlmann, S. Abt, H. Baier "Mining a high-level access control policy in a network with multiple firewalls", 2016.

[4] M. Park, B. Lee, S. Yang "Building Firewall over the Software Defined Network Controller", 2016.

[5] H. Hu, W. Han, G. Ahn, and Z. Zha "Towards a Reliable SDN Firewall", 2013.

[6] R. Krishnan, R. Krishnan and D. Mcdysan "Behavioural Security Threat Detection Strategies for Data Center Switches and Routers", 2013.

[7] J. Collings and J. Liu, "An OpenFlow based Prototype of SDN Oriented Stateful Hardware Firewalls", 2014.

[8] C. Decusatis, P. Mueller, "Virtual Firewall Performance as a Waypoint on a Software Defined Overlay Network", 2015.

[9] S. Seeber, G. Rodose "Improving Network Security Through SDN in Cloud Scenarios", 2010.

[10] T. Javid, T. Riaz and A. Rasheed "A Layer2 Firewall for Software Defined Network", 2014.

[11] Z. HE, TH. CHOMSIRI, P. NANDA, Z. TAN "Improving cloud network security using the Tree-Rule firewall", 2015.

[12] X. Jiat and J. Wang "Distributed Firewall for P2P Network in DataCenter", 2013.

[13] S. Hachan, N. Boulahi, F. Cuppens, "Blessing or Curse? Revisiting Security Aspects of Software-Defined Networking", 2014.

[14] J. Pena and W. Yu "Development of a Distributed Firewall Using Software Defined Networking Technology", 2013.