ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SURVEY OF FIREWALLS IN SOFTWARE DEFINED NETWORKS

Tahira Mahboob*[1], Maria Shah[2] and Syeda Hadia Afzaal[3]
*[1]Department of Software Engineering, Fatima Jinnah Women University, Pakistan
[2,3]Department of Computer Science, Fatima Jinnah Women University, Pakistan

ABSTRACT

Network security refers to the actions deliberate to protect network. These activities protect the usability, reliability, integrity, and safety of the network and data. Software-defined networking authorizes network operators for more efficient and flexible to handle their networks accordingly. Software define networking simultaneously allowing the use of security and dependability techniques, such as access control or multi-path. Our research includes analyzing different research papers on network security and discuss their technologies, comparing them and taking out the best methods available. We hope that this research will prompt discussions in the SDN community and serve as a catalyzer to join efforts from the network security & dependability issues in the ultimate goal of building secure firewalls for software define networks.

Keywords: *DOS attacks, Intrusion Detection System, Firewall, Firewall policy Making, Open flow, Mininet, Network security, Software Define Networking, XML firewall, Unified threat Management(UTM).*

I. INTRODUCTION

Software-Defined Networking is an upcoming architecture that is active, convenient, low cost, and flexible, making it suitable for the high-bandwidth applications. This design od software define networking separate's the network control and forwarding functions resulting the network control to become directly programmable and making the infrastructure to be inattentive for applications and network services. The OpenFlow protocol is a prominent element for building Software define networking. It provides advantages such as directly programmable, Agile and Open standards-based and vendor-neutral.

With the advent of SDN schemes for securing the control plane traffic was introduced. Major threats for attacks are, attacks at controller layer, attacks at data plane layer, attacks at SDN layer, hardening an SDN system, securing the data plane layer, securing the controller layer. Software-defined networks have properties which prove to be easy opportunities for mischievous users and a source for attacks are for less secure network operators. The ability to control through software and the centralization of the network decisions in the controller provides space for attacks. Any unauthorized person with access to the central servers that control software can possibly control the entire network and damage it greatly.

Firewalls filter the inbound and outbound data traffic that flows through a system. A firewall use one or more sets of instructions to inspect network packets as they come in or go out of network .Depending on the instruction set allows the data traffic through or blocks it accordingly. The instructions of a firewall can evaluate one or more features of the packets such as the protocol type, source or destination host address, and source or destination port.

The paper follows the pattern of Introduction discussed in section 1, followed by survey of techniques in section 2 analysis in section 3 and conclusion in section 4.

II. LITERATURE REVIEW

2.1 An OpenFlow-based Prototype of SDN-Oriented Stateful Hardware Firewalls [1]

The hardware firewalls offer better protection
and performance than software firewalls. In the SDN-oriented hardware firewalls includes switches and controller software. The basic structure of a SDN-oriented stateful hardware firewall includes an OpenFlow enabled **"**dumb" switch and a firewall controller. The security rules are specified in the flow tables in both of the components. The firewall controller is in charge of making control decisions on unidentified traffic flows. The control decisions are specified as control rules in the flow tables. The "dumb" switch enforces the control decisions by regulating the traffic flows based on the control actions specified in its flow table.

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

FLOWGUARD, a comprehensive framework, to facilitate not only accurate detection but also effective resolution of firewall policy violations in dynamic OpenFlow-based networks. It checks network flow path spaces to detect firewall policy violations when network states are updated. In addition it conducts automatic and real-time violation resolutions with the help of several innovative resolution strategies designed for diverse network update situations. Implementation consists of three
components: flow tracking, violation detection and violation resolution.

2.3 Distributed firewall for p2p network in data center [3]

In this paper security of data center in cloud computing is very important. For network security firewall is important. Furthermore, XML firewall are used. Different types of distributed firewalls and their functionality according to performance, flexibility and implementation. Furthermore, DC-firewall main layers are executing, auditing and administrative. Two networks are used for network communication among virtual machines and management. Administrative Server is responsible for updation firewall rules, network status collection and higher management interface maintenance Distributed DC-Firewall communicates over private network. A “rabbit sdn” is developed for SDN platform. Firewall provides better communication and security.

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

The paper involves creating a firewall over the SDN controllers using OpenFlow with a well-designed
user interface. The logic of this firewall is that each packet headers are checked against the firewall rule from highest to lowest priority, and performs specified action once matching fields
are found in the rule. Any unmatched packets are dropped. Installing firewall rules are possible from an external entity through a text-based user interface. An OpenFlow-based firewall with a straightforward UI that integrates priority switching can bring another wave of innovation in the Internet world.

2.5 A Layer2 Firewall for Software Defined Network [5]

This paper introduces a layer2 fire-wall implementation using a tree topology with one controller, three switches, and four hosts. The implementation uses POX controller at control plane of the architecture. A Layer2 Firewall was constructed using Mininet, Oracle VirtualBox Xming X Server for Windows and PuTTY SSH client to establish remote connections to virtual hosts. The research focuses on layer2 firewall implementation by modifying code provided with POX controller and the results show extended functionality and better performance to control data traffic accordingly.

2.6 Behavioral Security Threat Detection Strategies for Data Center Switches and Routers [6]

In this paper problem in data centers due to distributed denial of service. A firewall for security threat detection and mitigation. Techniques and implementation of security threat in DC EDGE switches/routers. Flows are identified by packet header. The two parameters i.e. observation interval and minimum bandwidth threshold should be programmable in switches/routers to handle traffic characteristics. Various DDOS attacks are described. The attacks are from multiple source and IP addresses. Various methods and test simulation are used to improve security threat at different layers deployed on a virtual routing. The interaction between SDN and end user increases the controllable network elements enabling smart decision making.

2.7 Development of a Distributed Firewall Using Software Defined Networking Technology [7]

The research is to explore security possibilities by
focusing on the development of a firewall prototype that maximizes the advantages of SDN. The features of OpenFlow, an open SDN standard, a distributed flowbased firewall prototype was developed and tested on a simulated network through Mininet. The development of the firewall prototype is created by the traditional packet filtering firewall in an OpenFlow environment wherein all packets would go through the controller before being dropped or passed to its destination host. For every device connected to the controller, the firewall prototype creates

a firewall object specifically linked to that device without affecting latency. The firewall also controls traffic by directly modifying the flow tables of devices providing more speed without affecting connectivity.

2.8 FirewallPK: Security tool for centralized Access Control List Management [8]

In this research firewallpk an application is discussed, providing an interface for collecting different network security. It provides enactment and security decision making. Multiple test cases were designed, demonstrating the strength and weakness of CISCO. An application based on real-time-scenario enables the network monitoring and control routers. In addition to, a threat flag is triggered which provides faster and accurate protection against security threats. Manual configuration and decision making for router is limited. CISCO onePK provides functionality of multiple devices in single application. firewall is developed for blocking network security attacks. The network controller should allow only verified applications.

2.9 Improving Network Security through SDN in cloud Scenario [9]

In this paper, network security remains a major challenge. It is necessary for network to defend the attacks. The system is distributed over several agents which is aware of administrative policy. Earlier approaches focused on using separate VLAN for blocking traffic. Internet users have not that much knowledge, when download many software which are not reliable. To overcome the limitation of cloud network security, access and security policies have to deploy. The three categories of data build is the base for creating policies. Forwarding decisions detect malicious traffic from the cloud environment, services provide detailed information. OPENSTACK provides computing capabilities for service provisioning, virtual switches for traffic forwarding implementations and monitoring and measurements capabilities to be aware of what happens in the evaluation environment

2.10 Towards a Reliable SDN Firewall [10]

Developing a SDN firewall is more challenging. In Open-Flow network states, set-fields are updated dynamically. In firewall simple flow policy violation isn’t effective, the rules in firewall overlap each other. SDN firewall needs to check for violation, ingress switch flow, track of the source and destination.

2.11 Improving cloud network security using the Tree-Rule firewall [11]

In this research a new model for firewall applicable in many scenarios and offers benefits. Limitation of listed-Rule firewall are discussed and new firewall is proposed. Security problem arise in large enterprises. Decision making needs a policy creation. System assessment is slow vulnerability is increasing. Different threats are detected from the live detection system. Simulation were stored in distributed rather then centralized. Furthermore, a scoring policy for traffic is set. SDN policies are made for simple configure forwarding devices, an additional component is required for policy creation and management. The new network security provides more reliable and faster reaction time. Forwarding decisions can mitigate malicious traffic from and to the cloud environment

2.12 Mining a high level access control policy in a network with multiple firewalls [12]

In this research paper implementation of virtual firewalls configuration through policy mining technique is proposed. The firewalls are divided the configuration is done using NET-RBAC. THE POLICIES are defined at one place and it can be changed according to requirement. The proposed algorithm can be unified to general.

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

In this paper merits and demerits of SDN are discussed. SDN separates control plane from data. SDN provides new security mechanism and threats. SDN provides network security functions by design but problem arises in SDN information security due to centralized control plane. The key security aspects are confidentiality, authenticity, integrity, availability and consistency. New changes are taking place in SDN but it is not implemented largely. Network operators detect and mitigate network attacks. Network threat defense mechanisms are cryptography, firewalls, network based intrusion detection Systems (NIDS), and a unified threat management (UTM). SDN cannot provide cryptographic measures to counter network-based sniffing or spoofing attacks. SDN is improving on its security threats.

2.14 Virtual Firewall Performance as a Waypoint on Software Defined Overlay Network [14]

This paper proposes a virtual firewall implemented over SDN and forwarding graph. Experiments and performance on industrial deployment of virtual firewall are discussed. A single virtual firewall can handle the workload by providing high latency and high availability. Virtual firewall can give more protection to the near server rather than small practical firewall placed further from server. The merits of virtual firewall includes, power, space, faster configuration, faster implementation and replacement of practical firewall. The demerit of virtual firewall is cost operation, complexity of defining rules and their closeness to the server for protection.

III. ANALYSIS

J.Collings and J. Liu [1] in their paper "An Open Flowbased Prototype of SDN Oriented Stateful Hardware Firewalls" discusses the technique in which Enabling"dumb"switch and a firewall controller is used . This provides simple network security level with low cost. It provides reliability but no extensibility.

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

X. Jiat and J. Wang [3] in their paper "Distributed Firewall for P2P Network in Data Center" uses Rabbic SD N Platform technique in which network security level is complex and cost is high .It do not provide extensibility and reliability.

M. Park, B. Lee, S. Yang [4] in their paper "Building Firewall overthe Software Defined Network Controller" discusses Tree topology with POX written in Python which provides security with low cost . It is an Open Flow-based firewall with a user interfase that includes priority switching can bring wave of technology over the Internet.

T. Javid,T. Riaz and A.Rasheed [5] in their paper "A Layer2 Firewall for Software Defined Network" uses Mininet Virtual network creation with tree topology which provides network security with low cost . The technique provides extended functionality and better performance to control data traffic more efficiently.

R.Krishnan, R.Krishnan and D.Mcdysan [6] describes "Behavioral Security Threat Detection Strategies for Data Center Switches and Routers" using Layer 2-4 Behavioral security threat detection method provides complex security level. This techniques bring in additional flow awareness in the system to enable smarter decision making in data flow throughout the network.

J. Pena and W.Yu [7] describes "Development of a Distributed Firewall Using Software Defined Networking Technology" detailing reliability and Confidentiality. The technique provides more speed without affecting connectivity.
R. Trandafir, M. Carabas, R.Rughinis and N. Tapus [8] in their paper " FirewallPK: Security tool for Centralized Access Control List Management"describes Cisco One Platform Kit framework which provides complex security level. They discusses enactment and security decision making.

S.Seeber , G.Rodose [9] describes "Improving Network Security Through SDN in Cloud Scenarios" using Policy making, IDS monitoring and security regulation with complex security level and low cost .It do not provide flexibility but completes all the parameters required .
H. Hu ,W. Han ,G. Ahn ,and Z.Zha [10] discusses "Towards a Reliable SDN Firewall" using Policy techniques .providing simple security level with low cost. . SDN firewall needs to check for violation, entrance switch flow, track of the source and destination addresses.

Z.HE,TH.CHOMSIRI, P.NANDA,Z.TAN [11] in their paper "Improving cloud network security using the Tree-Rule firewall" using technique A hierarchal tree set fire wall algorithm: NF_IP_FORWARD providing simple security with low high cost . It does not provide flexibility, but do not provide reliability.

L.Sche hlmann ,S.Abt, H. Baier. [12] in their paper "Mining a high level access control policy in a network with multiple firewalls" describes Policy mining, unified hierarchy, unified merger technique providing complex network security mechanism with high cost .

S.Hachan, N. Boulahi, F.Cuppens, [13] in their paper "Blessing or Curse? Revisiting Security Aspects of Software-Defined Networking" describes SDN evaluation, SDN security benefits and threats which do not provide flexibility besides other parameters described.
C. Decusatis P. Mueller, 2014 [14] in their paper "Virtual Firewall Performance as a Waypoint on a Software Defined Overlay Network" describes virtual firewall implemented on vmware increase performance and in low cost.

Table1 defines the parameters discussed in the surveyed papers relating to SDN in wireless and mobile networks.

Table2 Analyze parameters referring to experiments, tests and algorithms performed in research paper.

Table3 demonstrates parameters of surveyed papers. Yes: author has discussed certain parameter No: author has not discussed certain parameter in the research paper.

IV. CONCLUSION

SDN security is the main challenge. This research paper uses a survey of different SDN firewalls discussed in various research papers. Different techniques for improving SDN security through firewalls. The survey shows multiple firewalls implementation in different scenarios, implementation's cost. The survey shows which firewall improves more security in SDN. The main techniques discussed are as Flow tracking, violation detection and violation resolution, Tree topology with POX written in Python, Policy mining, unified hierarchy, unified merger. These techniques provides better security in low cost. For future work, our recommendation is multiple techniques for SDN firewalls.

REFERENCES

1. J.Collings and J. Liu, "An Open Flowbased Prototype of SDN Oriented Stateful Hardware Firewalls", 2014.
2. H. Hu ,W. Han ,G. Ahn ,and Z.Zhao,"FLOWGUARD:Building Robust Firewalls for Software-Defined Networks",2014.
3. X. Jiat and J. Wang "Distributed Firewall for P2P Network in Data Center",2013
4. M. Park, B. Lee, S. Yang "Building Firewall over the Software Defined Network Controller",2013.
5. T. Javid,T. Riaz and A.Rasheed "A Layer2 Firewall for Software Defined Network",2014.
6. R.Krishnan, R.Krishnan and D.Mcdysan "Behavioral Security Threat Detection Strategies for Data Center Switches and Routers",2013
7. J. Pena and W.Yu "Development of a Distributed Firewall Using Software Defined Networking Technology",2013.
8. R. Trandafir, M. Carabas, R.Rughinis and N. Tapus " FirewallPK: Security tool for Centralized Access Control List Management,2014
9. S.Seeber , G.Rodose "Improving Network Security Through SDN in Cloud Scenarios",2010
10. H. Hu ,W. Han ,G. Ahn ,and Z.Zha "Towards a Reliable SDN Firewall",2013.
11. Z.HE,TH.CHOMSIRI, P.NANDA,Z.TAN "Improving cloud network security using the Tree-Rule firewall",2014
12. L.Sche hlmann ,S.Abt, H. Baier "Mining a high level access control policy in a network with multiple firewalls",2014.
13. S.Hachan, N. Boulahi, F.Cuppens, "Blessing or Curse? Revisiting Security Aspects of Software-Defined Networking", 2013
14. C. Decusatis P. Mueller,"Virtual Firewall Performance as a Waypoint on a Software Defined Overlay Network",

Parameters	Definition
Security	The policies adopted by a network administrator to prevent an unauthorized access into the network.
Performance	It refers to measures of service quality provided.
Efficiency	Measure of how efficient a network can protect against malicious attacks.
Flexibility	Ability of system to adapt to changes and improve along with changing techniques.
Confidentiality	Set of rules that limits network access on certain types of information
Extensibility	A systemic measure of the ability to extend a network system.
Reliability	Network consistently to perform according to its specification required.

Table1. Selected Parameters in the surveyed papers relating to SDN in wireless/mobile networks.

S#	Author	Security	Performance	Efficiency	Flexibility	Confidentiality	Extensibility	Reliability
1.	J. Collings and J. Liu 2014	Yes	Yes	No	No	No	No	Yes
2.	H. Hu ,W. Han,G.Ahn,and Z.Zhao,2013	Yes	Yes	Yes	Yes	No	No	Yes
3.	X. Jiat and J.Wang,2010	Yes	Yes	No	No	Yes	No	No
4.	M. Park, B. Lee, S.Yang 2014	Yes	Yes	Yes	Yes	No	Yes	Yes
5.	T. Javid, T. Riaz and A.Rasheed,2014	Yes	Yes	Yes	Yes	No	Yes	No
6.	R. Krishnan, R. Krishnan and D.cdysan,2014	No	No	No	No	Yes	No	Yes
7.	J. Pena and W. Yu, 2014	Yes	Yes	Yes	Yes	No	Yes	Yes
8.	R. Trandafir, M.Carabas, R.Rughinis and N. Tapus,2014	Yes	Yes	No	No	No	No	Yes
9.	S.Seeber, G.Rodosek,2014	Yes	Yes	Yes	No	Yes	Yes	Yes
10	H. Hu , W. Han , G. Ahn , and Z. Zhao,2013	Yes	Yes	Yes	No	No	No	Yes
11	Z.HE,TH.CHOMSIRI,P.NANDA,Z.TAN, 2014	Yes	Yes	No	No	No	Yes	Yes
12	L.Schehlmann, S.Abt, H.Baier.	No	Yes	Yes	Yes	Yes	No	No
13	S. Hachan, N.Boulahi,F.Cuppens, 2014	Yes	Yes	Yes	No	Yes	Yes	Yes
14	C. Decusatis, P. Mueller, 2014	Yes	Yes	Yes	No	No	Yes	Yes

Table-2 Analysis of Parameters

Table-3 Technical Analysis of Research Papers

S#	Paper Name	Technique	Security level	Cost	Test cases use different input
1	**An OpenFlow-based Prototype of SDN-Oriented Stateful Hardware Firewalls**	Enabling "dumb" switch and a firewall controller.	Simple	Low	GENI test bed, scaling latency
2	**FLOWGUARD: Building Robust Firewalls for Software-Defined Networks**	Flow racking,violation detection and violation resolution technique	Simple	Low	Flowguard on floodlight, flow tracking, violation and detection
3	**Distributed Firewall for P2P Network in Data Center**	Rabbit SDN Platform technique	Complex	High	Delay for transmission, standard is 1
4	**Building Firewall over the Software-Defined Network Controller**	Tree topology with POX written in Python	Simple	Low	SDN firewall.SDN , functionality,SDN attributes
5	**A Layer2 Firewall for Software Defined Network**	Mininet virtual network creation with tree topology	Simple	Low	Wireshark ARP rules for three switches were added
6	**Behavioral Security Threat Detection Strategies for Data Center Switches and Routers**	Layer 2-4 behavioral security threat detection technique	Complex	Low	Virtual switch, 8gbps affic,500mbps traffic on single server
7	**Development of a Distributed Firewall Using Software Defined Networking Technology**	OpenFlow Single Switch Topology for networks	Complex	ND	Functionality test, connectivity
8	**FirewallPK: Security tool for centralized Access Control List Management**	Cisco One Platform Kit framework	Complex	ND	Connection of CISCO with API, onePK API
9	**Improving Network Security Through SDN in Cloud Scenarios**	Policy making, IDS monitoring and security regulation	Complex	High	ND
10	**Towards a Reliable SDN Firewall**	Policy flow violation, Flowguard, enables SDN security	Simple	Low	ND
11	**Improving cloud network security using the Tree-Rule firewall**	A hierarchal tree set firewall algorithm:N F_IP_FORWARD	Simple	High	In LAN, In cloud environment, In EXSI, In Hyper-V
12	**Mining a high level access control policy in a network with multiple firewalls**	Policy mining, unified hierarchy, unified merger	Complex	High	ND
13	**Blessing or Curse? Revisiting Security Aspects of Software-Defined Networking**	SDN evaluation, SDN security benefits and threats	ND	ND	ND

14	**Virtual Firewall Performance as a Waypoint on a Software Defined Overlay Network**	Virtualized firewall, VMware in LINUX	Comple x	High	Firewall with imix,ipv4,firewall with UDP