SDN based Intrusion Detection System for OpenStack Cloud

Sooraj V H, Prabhakar Krishnan

Abstract**: *By virtue of a large amount of virtual storage, cloud computing model provides Internet services at scale. The main advantage of cloud computing is that for memory intensive applications and services, the user does not have to buy or setup heavy and expensive computing infrastructure. OpenStack is an open source implementation of cloud platform. It is considered as one of the most researched and popular platforms to deploy both public and private clouds. Software Defined Networking is the paradigm shift that allows programming and central control of the network using software applications. This paper presents a novel approach to integrate the SDN technology and OpenStack platform, to address various problems in the network security and orchestration. We aim to improve the efficiency of the legacy Network Intrusion Detection Systems(NIDS) by taking advantage of the advanced programmable features of SDN. The intrusion information collected by the NIDS is forwarded to the control plane, and the controller decides the security policy based on threat analytics. This policy will then be forwarded to the corresponding switch to help it filter out the malicious traffic. The controller includes an SDN firewall using machine learning that can detect the malicious data packets and learn new patterns for detecting unknown future attacks in the network. This paper also demonstrates the efficiency of the proposed system in attack identification and mitigation case studies under network flooding and DDoS attacks on cloud. Through experimental analysis, we have also demonstrated that the proposed solution is improved in terms of sustaining throughput, latency and detection accuracy when compared to traditional IDS solutions.***

Index Terms**:*SDN, DDoS, IDS, IPS, Cloud, network security, OpenStack, OpenDaylight, Machine learning, firewall***

I. INTRODUCTION

Currently, core networking architecture is facing disruptive developments, due to emergence of paradigms such as “Software Defined Networking (SDN)” for control, “Network-Function Virtualization (NFV)” for services and so on. Service providers are transforming their business using NFV based services and SDN enabled networks. SDN architecture offers an easy programmable model, global view and control for modern networks, which demand for fast response to security incidents and dynamically enforce counter-measures to intrusions and cyber-attacks. The SDN provides interface to monitor or program with software applications, intelligently and centrally[1]. Regardless of the specific links between a server and devices, the central controller sends commands through a control-protocol OpenFlow[2] to switches to enforce policies and execute services on-demand. In network activities, SDN will allow multi-tasking. That needs less hardware and the costly network middleboxes, appliances that would be used in the traditional style are not needed. Cloud computing is rapidly growing to offer Internet services through various models. Cloud computing paradigm offers primarily the following features - First, it is a large-scale shared environment consisting of IT infrastructure with several physical and virtual machines. Second, cloud computing environment setup is quite complex. We should consider a diverse set of physical/virtual devices in a heterogenous multi-access network, with distinct configurations, to service a big number of varied cloud consumers/tenants. Thirdly, Conventional defense solutions rely on physical network path and security perimeter, which need predefined provisioning and planning. But the virtualized technologies not only bring in elasticity/flexible design but also capabilities to dynamically scale out to meet the run time demands of today’s applications. OpenStack technology has gained excellent popularity among leadership platforms for cloud computing. However, in large networks, there will be network congestion problem due to the static and serial network mode of connections of the systems. In the legacy cloud datacenters, networking policies and operations are executed by switches and routers that has mixed dataplane/control processing algorithms, to determine the routing paths. SDN is an emerging networking paradigm that offers dynamic reconfigurations and efficient traffic engineering through a programmable interface. It centralizes the network operational strategy and separates the packet “forwarding (Data Plane)” from the “routing (Control plane)” with a control channel OpenFlow [2] protocol. The network operations and behavior can be centrally controlled and programmable through applications using a rich set of Northbound protocol and APIs. Programmability, flexible reconfigurations, dynamic policy enforcement are the major features of SDN enabled network architectures. Network Function Virtualization(NFV) is another enabling technology in which dataplane network functions like firewall, load balancers, IDS, and routers are migrated from specialized hardware devices to VMs as software. Thus, we can decrease networking cost and use them completely as virtual machines. The *Service Function Chaining* (SFC) /Virtualized Network Function (VNF) is the latest operational strategy for Cloud services vendors to meet the complex QoS requirements and “service list or chain”. The whole

Revised Manuscript Received on July 06, 2019.

Sooraj VH, Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering,Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India. Email: soorajvh@am.students.amrita.edu

Prabhakar Krishnan, Amrita Center for Cybersecurity Systems and Networks, Amrita School of Engineering,Amrita Vishwa Vidyapeetham, Amrita University, Amritapuri, India. Email: kprabhakar@am.amrita.edu.

virtualized network infrastructure is managed by an NFV-MANO (Management and Network Orchestration) system. Due to SDN’s global view, granular path management and programmable model, the next logical advancement is to position SDN control for the NFV infrastructure in Cloud datacenters. The recent SDNFV converged proposals approach to solve the bottlenecks in VNFs service-chaining by extending the SDN to deliver optimal services [3]. To address the problems in Cloud security, SDN enabled architecture can alleviate the security threats in the network side. SDN follows centralized decision-making on information traffic in networks[4]. In reaction to evolving network needs and network threats, policies can be enforced quickly. The latest SDN OpenFlow standards have brought advanced features to realize sophisticated protocol-header/state-machine level matching and execute custom function handlers for matching flows. In this paper, we are proposing a SDN-Cloud firewall system , with distributed monitoring in switches and security remediation in the controllers. Our early experiences with this proposed system, show that the processing costs is minimal and in acceptable overhead range, for implementing the cooperative safety scheme in SDN. In addition, this scheme protects the SDN architecture from controller overloading and undoubtedly defending down-stream services in the network. We introduced new mechanisms in our framework for detecting and preventing the malicious packets in the network. Our framework is used as a NIDS firewall and perimeter defence solution in the cloud environment against DDoS amplification, flooding and malicious attacks. This paper is organized as : Section I provides an introduction to cloud computing, Openstack and SDN, Section II provides the background of the enabling technologies in the OpenStack Cloud platform, overview of the SDN centric Cloud architecture and sets the context, Section III discusses the prior research work in the related area, Section IV presents our proposed solution and architecture, Section V describes the design and implementation, Section VI presents the evaluation and experience with an early prototype of the system and Section VII concludes the paper.

II. BACKGROUND AND MOTIVATION

In this section we provide the background of the enabling technologies in the OpenStack Cloud platform , overview of the SDN centric Cloud architecture, the advantages and sets the context for the proposed solution.

A. SDN based Cloud Computing

Cloud networks are highly exposed to large attack surface and delivering reliable services is the key metric in the service-level-agreements (SLA). In the rapidly changing security landscape, new attacks and targeted cyber-attack campaign are emerging every day. So, the detection schemes and remediation strategies need to be updated periodically in the IT networks, which leads to frequent churn of equipment (hardware/software/middleboxes) inventories and eventually integrating the new solutions is also a challenge. Thanks to virtualization technologies, launch of new solutions and updates to SDN/NFV based mechanisms are simple and cost effective as well.

1) Centralized cloud network delivery

SDN offers a centralized vision of the domain of the network, thus providing centralized management. SDN with the programmability and virtualized technologies not only bring in flexible design, predefined provisioning and planning, but also capabilities to dynamically scale out to meet the run time demands.

2) Holistic approach of enterprise management

SDN enables application provisioning and On-demand service in the cloud enterprise network, which have many applications in Cloud services. SDN allows experimenting on the virtualized network topologies and launching of new solutions, software updates to SDNFV based mechanisms are simple and cost effective as well.

3) Granular Security

Managing granular security and access control policies in modern virtualized datacenters is a daunting task. Due to some components residing in physical infrastructure, consistent application of firewall and security policy in the virtual networks is a difficult task. SDN provides simple and flexible, centralized application interface for managing the QoS policies, securing and threat control. As SDN is rapidly replacing traditional networks in data centers, it also opens up the attack surface for more cyber-attacks, the most critical vulnerability is the control plane saturation. So, by designing a reliable topology, the security granularity results will be better for SDN-enabled cloud networks.

4) Cloud abstraction

SDN essentially creates network abstractions to allow increased flexibility and application-aware behaviors for various Cloud-IoT applications. While there are still open problems in the datacenters, the emerging paradigms such as SDN, NFV, SD-WAN, SD-Security, Software-Defined IoT and their rapid adoption in the enterprise data centers, opens up new opportunities to re-define the security and defense schemes. Applications and QoS implemented in SDN have advantages in managing a massive cloud network.

B. SDN-Centric Cloud Architecture

Fig.1 illustrates the reference architecture of common Cloud computing systems enabled by SDN. The cloud manager controls all cloud tenants and resources, the incoming provisioning requests. The cloud manager also conducts energy-efficient resource management and resource monitoring. The SDN controller interfaces with Cloud manager via northbound API, controls network-related functions. The SDN controller has the functions of network orchestration, policies, topology discovery, routing and network monitoring to be enabled through the SDN controller. The Cloud Manager provides computing resources (physical hosts) to run virtual machines , while the SDN controller manages network resources (switches) by installing flow-rules on switches through southbound OpenFlow protocol.

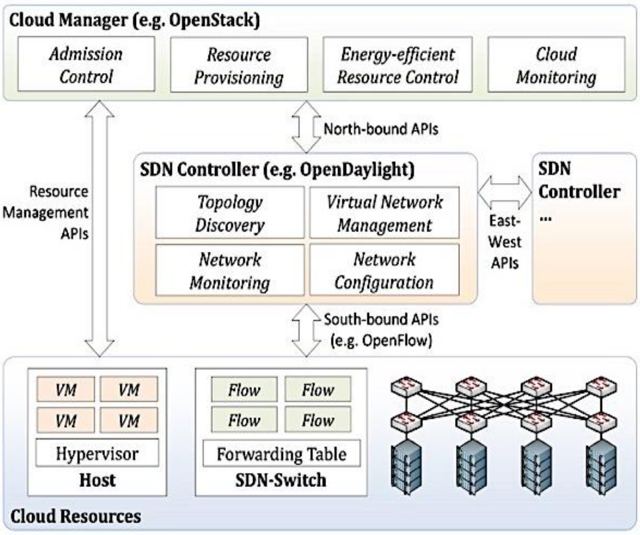

Fig 1.SDN centric Cloud Architecture [5]

C. SDN - OpenStack Communication

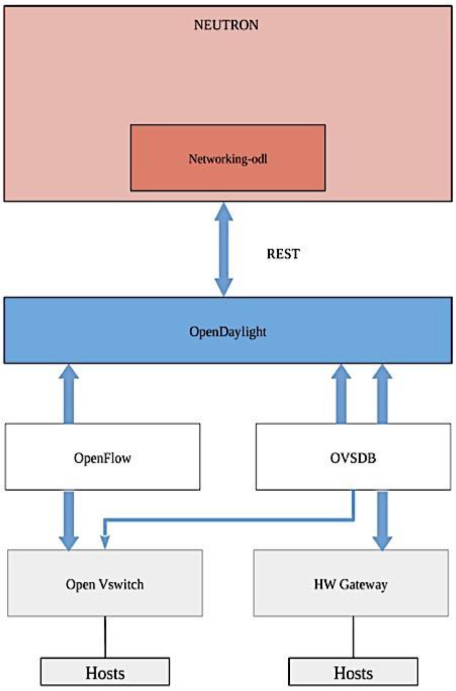

Fig 2.Architecture of OpenStack and SDN ODL

OpenStack architecture is extensible for integrating the SDN layers and to build a reliable and secure Cloud computing infrastructure (Fig.2). Neutron is the networking component of OpenStack architecture, that ensures that all virtual machines (VMs) have a proper network. Neutron module helps integrate SDN services with OpenStack. Networking-ODL is an OpenDaylight (ODL) plug-in for OpenStack and it is responsible for carrying OpenStack network packets to the ODL controller. The public REST APIs are used to communicate between OpenStack Cloud and OpenDaylight SDN. This model simplifies the network traffic orchestration, as OpenStack's native Neutron does not have L3 routing capability and leverages on Linux kernel bridge[6]. Therefore, OpenStack networking scheme is not scalable and secure to tackle the rapid growth of multi-access internet connections and cloud services. The controller for OpenDaylight utilizes *NetVirt*, that configures OpenvSwitch and offers the required networking environment. This involves networking Layer 2, IP routing, security groups and other network abstractions.

III. RELATED WORK

In this section, we will present an overview of various approaches identified in our literature survey for integrating SDN into OpenStack cloud platform. In [7] Huang et al. implemented IPS in the control plane but restricted to the POX controller. The authors of [8] combine IDS with virtual switches, but there was no presentation of the evaluations and result discussions about fine-grained latency and forwarding delay. In [9] the authors introduced a Cloud based Intrusion prevention systems with SDN. They used flow-table "*match-action/send_to_controller*" features in the recent version of OpenFlow specification. S. Shin and G. Gu introduced a new framework in [10] called "CloudWatcher", using a policy script - the network packets are diverted automatically to be scanned by external threat analytics systems. In [11] OlenaTkachova et al. analyzed the integration of SDN solution with OpenStack, and OpenDaylight controller, which has higher reliability than Floodlight and RYU SDN controllers. The author of [12] described advances in the use of the SDN dataplane firewall for OpenStack and compared the performance with traditional Linux IPS iptables. In [13] Qiao Yan and F. Richard Yu have conducted a comprehensive study of DDoS mitigation with SDN capabilities and also discussed some crucial SDN control channel limitations and vulnerabilities. In [15] authors demonstrated a SDN based firewall for a Cloud network. The threat detection and security policies are implemented in software running on the control plane and the administrator is provided an API to enforce the data security policy of the firewall. Nevertheless, they present only a general design without evaluation results and result analysis. The authors [16] proposed a MAC/IP filters-based IDS solution but has limitation with filtering malicious payload complex traffic. The authors of [17] implemented SDN based defense solution, using artificial intelligence to protect the network from malicious packet flow by analyzing the payloads in the packet.

IV. PROPOSED SOLUTION

SDN integrated OpenStack Cloud (Fig 3) comprises threat monitoring mechanisms at the dataplane switches and mitigation mechanisms on the controller.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

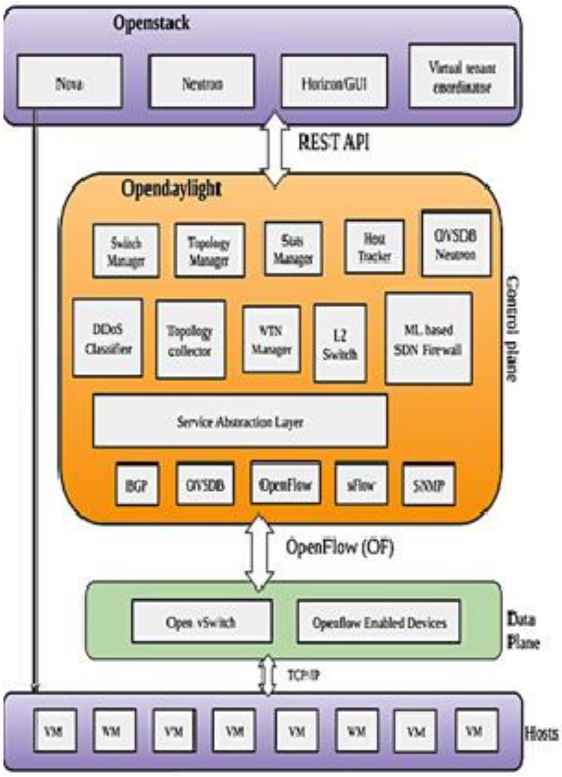

Fig 3.SDN Integrated Cloud Management Framework

An overview of the main components of our framework are presented below.

1. *Control Plane*

This section contains the modified OpenDaylight SDN controller with new mechanisms for monitoring and security. We used secure inband messaging for attack categorization and to generate relevant defense *match-action* flow-rules in switches using libraries for defense action.

2. *Cloud layer*

In this layer, we implement OpenStack, with associated plug-ins and expansions in networking subsystem. Users will communicate with services using the REST API, and the Nova layer will take responsibility for managing the VMs.

3. *Data plane*

This plane consists of OpenvSwitch, OpenFlow enabled switches, hybrid gateways, and core switches. The switches are managed by OpenDaylight controller and communicate with OF protocol. The corresponding attacked switch will send an in-band notification to the gateway switch or controller to request if any anomaly is identified. A light-weight IDS is also embedded with the OpenFlow switches. The network flows will be continuously monitored, if any anomalous flow detected, that flow is flagged and sent to the SDN firewall in controller, using in-band message to receive further mitigation flow-rule match-action like diversion or drop or filter. An SDN firewall with Analytics engine using fine-grained machine learning based attack-classification, is included with the controller which is capable of identifying malicious traffic flows in the network. The advanced systems analyze the payload of a packet to distinguish malicious flow. The incoming packet of that malicious flow will be intercepted by the OF pipeline flow-table match-action rules on the switches. The monitoring service using MD-SAL(Model-Driven Service Abstraction Layer), which is accountable for receiving the payload straight from the software vSwitch.

V. DESIGN AND IMPLEMENTATION

The OpenDaylight controller supports OpenFlow protocol and other open SDN standards and specifications. The north-bound interface offers a wealthy number of APIs. The main purpose of REST APIs is to integrate with cloud system such as OpenStack. The SAL(Service Abstraction Layer) is the most important architectural layer, because its main function is to map a variety of networking technologies from a diverse set of hardware suppliers to a common abstract data model. In the integrated architecture, the neutron plugin ML2 (Modular Layer 2) interacts with the OVSDB (Open vSwitch Database Management Protocol) Neutron implementation of ODL (OpenDaylight), which in turn forwards commands to OVS stack/OVSDB through OpenFlow protocol. The plugin performs all networking operations such as creation, updating, and removing of the virtual networks, as well as providing interconnection between VMs, Cloud Controller and also to external network. Each plugin has a compute node agent module and connects to node’s virtual switch(OVS vSwitch). The workflow in Neutron is i) the Neutron server receives a request for operation through the API ii) An entry added to the database through the neutron server and invokes the appropriate plugin by calling REST API iii) Once this request has been received, the plugin will call the southbound protocols to make the required connections to the network components. The new SDN mechanisms, plugins, interface modules are designed for optimizing and securing the OpenStack networking operations. A tenant requests OpenStack for resources in the typical cloud computing workflow and then the Nova components provision computing resources for the new instances. A virtual network is scheduled by the SDN OpenDaylight (ODL) controller through a RESTful call. The ODL will call OpenFlow and OVSDB to setup virtual network and deliver the Flow rules to OpenFlow switches. Virtual network configuration and topologies are stored by the topology manager. We integrate SDN and OpenStack with a package that contains anti-DDoS functions. The vSwitch will monitor the whole network and detects attacks. Then perform mitigating network function to limit threats in the data plane and regularly communicate statistics to the SDN controller (ODL) via the Neutron plugins.

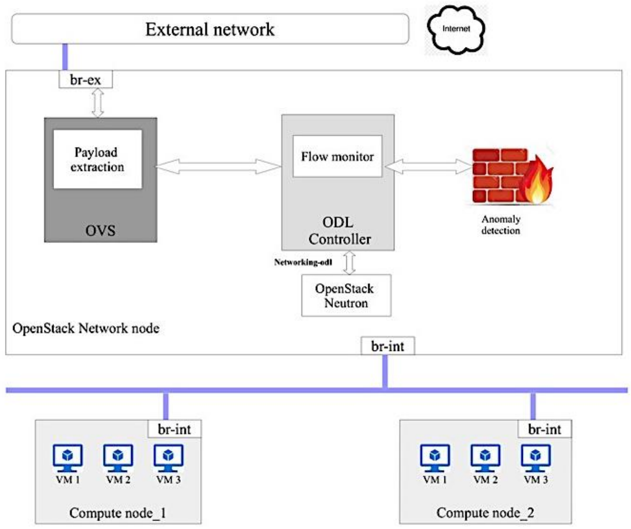

Fig 4.SDN based Cloud Firewall Scheme

We implement an SDN firewall that uses machine learning to detect malicious traffic flow in the network. Fig 4 illustrates our advanced SDN Firewall controller integrated into the OpenStack cloud platform, for monitoring and defending against network attacks. Different compute nodes in the organization intranet will interact with *br-int* using VXLAN which is a LAN tunnel technology, However, the network node connects to the Internet by using *br-ex*. The metadata and payload in the received packets are extracted by the OpenvSwitch. The flow monitor will track each network flow and SDN-based firewall, using advanced anomaly detection and ML systems, predicts whether the packet obtained is malicious or benign and enforce the appropriate actions in the network. The packets with the same 5-tuple on both directions are classified as the same flow if both happen within this ‘flow-duration’. In SDN, the OpenFlow based switches maintain flow-tables, use a standard ‘flow table architecture’ and other legacy network(non-SDN) the devices use one or more of protocols such as “SNMP, NetFlow, IPFIX and sFlow”. The OvS SDN stack (both Controller and switches) support these legacy protocols as well. After we have gathered flow-level information, we can extract several features from these flows to study the behaviors that occur in the network. The flow anomaly detection algorithms can analyze, categorize the flows from all the SDN (switches and controllers) and non-SDN components in the global network.

Through ML static or dynamic models, the normal flows or malicious or suspicious flows are detected. This ML system also reads from various key indicators and patterns of known attacks. It can then classify the flows as benign/suspicious. These signatures are stored in a high-speed datastore, typically in-memory database and indexed with various criteria such as “severity of attacks, whitelist (allow) and blacklist (block)”. This signature database is periodically updated and in-sync with security community-maintained threats databases. To evaluate the detection accuracy, we implemented a standard Bloom-filter based anomaly detection mechanism in the SDN Firewall. We measured the false positive rate of the detection mechanism. By varying bloom filter size and hash functions, we observed the false-positives under DoS attack. The results show that the SDN based firewall security system has acceptable and practical detection accuracy.

VI. Evaluation and Analysis

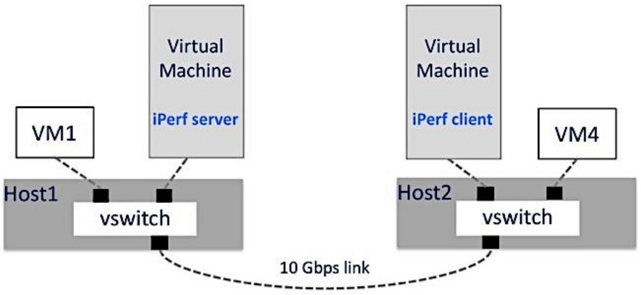

Fig 5.Testbed Network Topology

Fig 5. depicts the testbed network topology we have set up for evaluating our solution.If we use SDN, which has several advantages over the traditional network, the Cloud network can be made even more reliable for service delivery. The current trend shows the majority network traffic in datacenters is TCP and 65% of DDoS attacks are “TCP-SYN/RST flooding, DNS and NTP amplification” attack. So, we used TCP traffic for analysis. While the legitimate traffic is flowing in the network between end-points, we generate a heavy hitting background attack traffic from various traffic-generators, all the machines connected to multiple switches in the network, through the same SDN/Fog Gateway controller. The hping3 tool (TCP-New Flow test) is used to launch TCP SYN Flooding attack to target host. This method involves saturating the link and legitimate traffic are not serviced in time. The significant improvement is that with SDN defence, the defence rules can be deployed in constant time at multiple points in the network.

A. IPS and IDS Performance

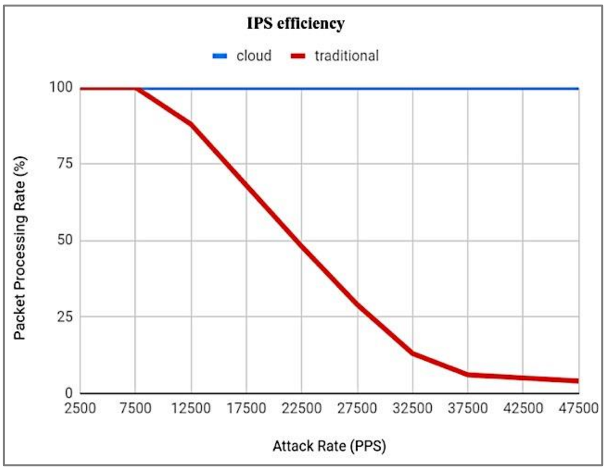

Fig 6.IPS Efficiency

Intrusion Prevention System: we measured the “total-packets processed/sec” with increasing attack intensities. The outcome demonstrates that traditional IPS drops packets and as the speed rises from 12 K pps to 0 at 37 K pps, efficiency reduces. Under the same attack, our framework’s IPS supports normal packet processing. (Fig.6)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

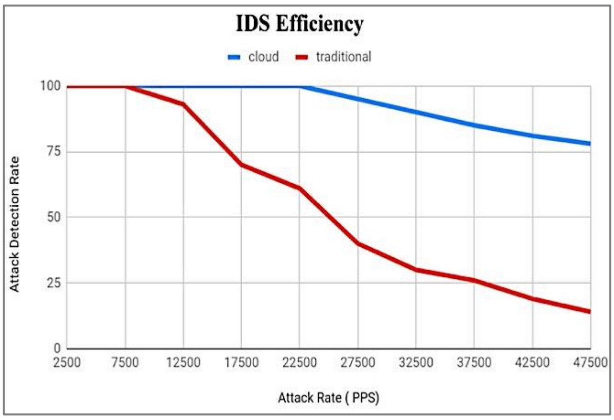

Fig 7.IDS Efficiency

Intrusion Detection System Efficiency: From this chart we can see that legacy IDS performance decreases with increasing attacks intensities. At the same time SDN based IDS in our framework withstands large attacks. (Fig 7)

B. Scalability and Attack Response

On large scale, we simulated a series of attacks, which involved more than 10000 rules/filters, to blacklist/drop those packets from a list of IPs, sent to switch after every attack. Our experiments show that the traditional firewall takes longer time to add new rules and at about 8,000 drop-rules on the classic-IDS firewall simply becomes a bottleneck in the network. But with our SDN-based Firewall, the controller could rapidly add defense action rules on the switches, as high as 200,000 drop-rules at a time and there was no limit to saturate the SDN based IDS firewall.

C. Throughput, Latency, CPU Utilization

When the OpenStack cloud network in under DDoS attack from attacker hosts, we measure the throughput, latency for the benign traffic between two normal hosts. It is measured by running the *iPerf* test without firewall and with SDN-Firewall, between two applications, topology as illustrated in the Fig.5. In the test without SDN firewall, the entire network became unresponsive, higher latencies and throughput crashed to zero and the normal applications terminated. But with our SDN firewall enabled, the OpenStack sustained the performance of the normal hosts, even under high attack rates. For NFV workloads, with can get 20~50% higher throughput than under various packet size and number of concurrent flows. For Enterprise workload, our saves around 50% CPU cycles and get 10~20% higher throughput.

D. Attack Detection

To measure how fast our system detects the attack in the mixed network traffic, we setup a regular legitimate traffic passing through the switch. After some delay, we start the attack traffic from a custom-attacker machine. The DoS Flooding traffic is detected and dropped at the switch.

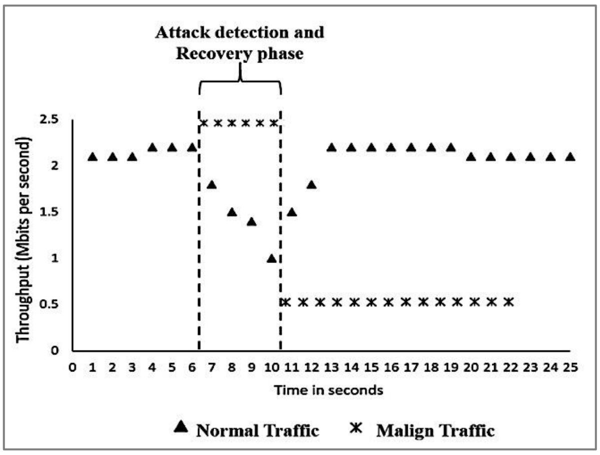

Fig 8.Attack Detection Efficiency

In the Fig 8, the attack traffic started closer to 7th second, within 3 seconds attack-detection mechanism from our SDN-firewall was triggered and the controller installed the blocking rule to drop these attack packets in the switch itself.

VII. CONCLUSION

In cloud environments, it is desirable to view global security events and respond to threats/attacks as soon as possible. It would be even more desirable if this ability was programmable and able to perform in bigger, spatially distributed cloud networks. Through our research, we were able to achieve this vision. We have integrated SDN with cloud computing and tackled various network attack scenarios and DDoS/botnet attack attempts. Our proposed SDNFV based security framework incorporates multi-plane security surveillance, threat analytics and attack detection/prevention through a large-scale application for cloud-computing. With the use of lightweight detection and prevention network functions residing in the data plane, and a novel control plane anomaly detection technique, we were able to create an efficient Network Intrusion Detection and Mitigation system for OpenStack cloud infrastructures.

REFERENCES

1. “*What is Software-Defined Networking (SDN)?”* https://www.ciena.com/insights/what-is/What-Is-SDN.html
2. McKeown et al. : “OpenFlow: Enabling Innovation in Campus Networks,” SIGCOMM Computing and communication. Rev., 2008
3. Patel, P., Tiwari, V., Abhishek, M.K.: “SDN and NFV integration in openstack cloud to improve network services and security”, 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). 656–656 (2016).
4. Scott-Hayward, S., Ocallaghan, G., Sezer, S.: “Sdn Security: A Survey”, 2013 IEEE SDN for Future Networks and Services (SDN4FNS). 1–7 (2013).
5. Son, J., Buyya, R.: “A Taxonomy of Software-Defined Networking (SDN)-Enabled Cloud Computing” ACM Computing Surveys. 51, 1–36 (2018).
6. Krishnan, P., Achuthan, K.: “CloudSDN: Enabling SDN Framework for Security and Threat Analytics in Cloud Networks”, Ubiquitous Communications and Network Computing, Springer Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 276, pp. 151–172, 2019. https://doi.org/10.1007/978-3-030-20615-4_12
7. Xing, T., Xiong, Z., Huang, D., Medhi, D.: “SDNIPS: Enabling Software-Defined Networking based intrusion prevention system in clouds”, 10th International Conference on Networks and Services

Management (CNSM) and Workshop. 1–4 (2014).

8. R. C. Diovu and J. T. Agee, “A cloud-based openflow firewall for mitigation against ddos attacks in smart grid ami networks,” in PowerAfrica, 2017 IEEE PES, 2017.
9. P. Rengaraju, S. S. Kumar, and C. H. Lung, “Investigation of security and qos on sdn firewall using mac filtering,” in International Conference on Computer Communication and Informatics, 2017, pp. 1–5.
10. Kumar S et al. “Open flow switch with intrusion detection system”, International Journal of Scientific Research Engineering & Technology ,2012,1(7):1-4.
11. Chi, Y., Jiang, T., Li, X., Gao, C.: “Design and implementation of cloud platform intrusion prevention system based on SDN” 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)(. 1–6 (2017).
12. Shin, S., Gu, G.: “CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?).” 2012 20th IEEE International Conference on Network Protocols (ICNP). 1–6 (2012).
13. Tkachova, O., Salim, M.J., Yahya, A.R.: “An analysis of SDN-OpenStack integration”, Second International Scientific-Practical Conference Problems of Info communications Science and Technology (PIC S&T). 1–3 (2015).
14. F.Foresta,et al.:“Improving OpenStack Networking: Advantages and Performance of Native SDN Integration”, 2018 IEEE International Conference on Communications (ICC).
15. Yan, Q., Yu, F.R., Gong, Q., Li, J.: “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges.” IEEE Communications Surveys & Tutorials. 18, 602–622 (2016).
16. Patel, P et al..: “SDN and NFV integration in openstack cloud to improve network services and security.” 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). 657–658 (2016).
17. Cheng, Q., Wu, C., Zhou, H., Zhang, Y., Wang, R., Ruan, W.: “Guarding the Perimeter of Cloud-Based Enterprise Networks: An Intelligent SDN Firewall” 2018 IEEE 20th International Conference on High Performance Computing and Communications.Corero DDoS Trends Report,2017 http://info.corero.com/DDoS-Trends-Report.html
18. Krishnan, Prabhakar, Jisha S. Najeem, and Krishnashree Achuthan. "SDN Framework for Securing IoT Networks." In International Conference on Ubiquitous Communications and Network Computing, pp. 116-129. Springer, Cham, 2017
19. B. Pa Poornachandran, Premjith and K. P. Soman, “A distributed approach for predicting malicious activities in a network from a streaming data with support vector machine and explicit random feature mapping,” in IIOAB Journal, 2016, pp. 24–29.
20. Krishnan Prabhakar, Achuthan Krishnashree , "Managing Network Functions in Stateful Application Aware SDN", 6th International Symposium on Security in Computing and Communications (2018), Springer Communications in Computer and Information Science Series(CCIS), ISSN: 1865:0929