International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-10, October 2014

Software Defined Networking with Intrusion Detection System

Yogita Hande, Aishwarya Jadhav, Achaleshwari Patil, Rutuja Zagade

***Abstract*— SDN and network programmability have emerged to address trends in IT by providing greater automation and orchestration of the network fabric, and allow dynamic, application-led configuration of networks and services. networks must be open, programmable, and application aware in order to deliver these requirements,. Networks must evolve to meet the emerging trends without compromising their current resiliency, service richness, or security, and without disrupting previous organizational investments. Software Defined Networking (SDN) is an emerging network architecture where network control is decoupled from forwarding and is directly programmable. This migration of control, formerly tightly bound in individual network devices, enables the underlying infrastructure to be abstracted for applications and network services, which can treat the network as a logical or virtual entity. Security is a challenge in future networks. Future Internet proposals rely on virtualization to provide multiple types of networks sharing the same physical infrastructure. This proposal takes advantage of the programmability offered by Software Defined Networks (SDN) to provide architecture for an Intrusion Detection System.**

***Index Terms*— Software Defined Networking, Network Virtualization, OpenFlow.**

I. INTRODUCTION

The proposed system is basically designed for Intrusion detection system in campus networks using a new concept called SDN (Software Defined Networking). The ability to detach networks based on software defined networking (SDN) has risen in popularity. Intrusion detection is one of the main challenges of internet security today. If in real time the campus system gets intruded then what helps is the SDN.SDN will solve this problem through the use of Openflow. Presently, Openflow is a new network technology. It is an open standard for SDN in which the control plane and data plane of network equipment is separated. Thus, Openflow provides an open protocol to program the flow table in different switches and routers. Network administrator, researchers, students along with people using the campus network for their purpose can define their own flow table and use the system accordingly. Everyone gets their slice of bread without affecting others network.

Today, there is almost no practical way to experiment with new network protocols (e.g.: routing protocols) in sufficiently realistic settings to gain the confidence needed for their widespread deployment. The new ideas from the networking community go untried and untested. There is a need of virtualized programmable network. Virtualized programmable networks could lower the barrier to entry for new ideas, increasing the rate of innovation in the network infrastructure. Commercial switches and routers do not typically provide an open software platform, let alone provide a means to virtualize either their hardware or software.

The proposed system will contain virtually created network with few virtual switches and virtual hosts (PCs) which will be high end LINUX PCs. And then the Openflow controller will communicate with the virtual network. Then our system will detect the bad packets generated by Packet generator. The packets will be captured and viewed through the use of software called Wireshark.

Manuscript received October 03, 2014.

II. EXISTING SYSTEM

Today, there is almost no practical way to experiment with new network protocols in sufficiently realistic settings to gain the confidence needed for their widespread deployment. The result is that most new ideas from the networking research community go untried and untested; hence the commonly held belief that the network infrastructure has “ossified”. The existing switches and routers have inbuilt protocols that the device will be using. If there is a need to change the protocol then the switch/router is to be changed. Thus changing of the protocol is very hard and costly as all the hardware is needed to be replaced accordingly.

III. PROPOSED SYSTEM

A. ***Why SDN:*** Traditionally, network architectures within corporate and government networks use network devices that combine control plane and data plane functions in a single device, typically a router or switch. The control plane is an element of a router or switch that determines how one individual device within a network interacts with its neighbors. Examples of control plane protocols are routing protocols, such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Spanning Tree Protocol (STP). These protocols determine the optimal port or interface to forward packets (that is, the data plane). While these control plane protocols scale very well, and provide a high level of network resiliency, they pose limitations. For example, routing protocols may only be able to determine the best path through a network based on static metrics such as interface bandwidth or hop count.

Likewise, control plane protocols do not typically have any visibility into the applications running over the network, or how the network may be affecting application performance. Data plane functionality includes features such as quality of service (QoS), encryption, Network Address Translation (NAT), and access control lists (ACLs). The features directly affect packet forwarding, including being dropped. However,

many of these features are static in nature and determined by the fixed configuration of the network device. There is no mechanism to modify the configuration of the above features based on the dynamic conditions of the network or its applications. Finally, configuration of these features is typically done on a device-by-device basis, greatly limiting the scalability of applying the required functionality.

IV. SYSTEM ARCHITECTURE

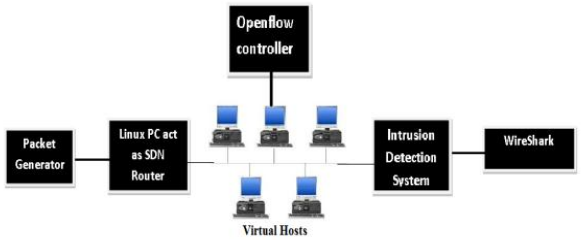

Fig 1: SDN in Campus with IDS system diagram

V. OVERALL DESCRIPTION

Network layer is divided into three different planes: Data plane, control plane and management plane.

A. ***Data plane*:** The data plane (user plane, forwarding plane) is the part of a network that carries user traffic. The data plane enables data transfer to handle multiple conversations through multiple protocols, and manages conversations with remote peers. The conventional networking and SDN networking differs in such a way that in the former all the planes are implemented in the firmware of routers and switches whereas in later case the data and control planes are decoupled. Thus network administration becomes more flexible.

B. Control plane: the control plane is the part of a network that carries signaling traffic and is responsible for routing. Functions of the control plane include system configuration and management. In sdn control plane is moved on from hardware to software layer which enables easy programmatic access. It thus, allows dynamic access and administration. A network administrator can shape traffic from a centralized control console without having to touch individual switches. The administrator can prioritize, de-prioritize or even block specific types of packets.

C. ***SDN:*** Software-defined networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of lower level functionality. The architectural approach optimizes and simplifies network operations by more closely binding the interaction (i.e., provisioning, messaging, and alarming) among applications and network services and devices, whether they are real or virtualized. An SDN separates the data and control functions of networking devices, such as routers, packet switches, and LAN switches, with a well-defined Application Programming Interface (API) between the two.

D. ***SDN in campus:*** For conventional network in campus various native groups are working on same network. The network is equally distributed to all the communities using the network. But if a researcher wants to test his design or protocol, or if another person wants to work on his newly designed system what creates a problem is the network access. Since the protocols and network design for routers and switches are provided by the vendor, possibility of changes is very less or not found. Hence the concept of SDN in campus comes into picture wherein the various users of network can utilize their slice of network by allocation of resources and when the job gets over the resources can be de-allocated.

E. ***IDS:*** An intrusion detection system (IDS) is a software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. The function of the present system is detecting the intrusion in the system which will be virtually created by our packet generator which is responsible to generate bad packets which will be processed and captured by our system.

F. ***OpenFlow controller:*** An OpenFlow controller is an application that manages flow control in a software-defined networking (SDN) environment.SDN controllers functions according to OpenFlow protocol. The SDN controller acts as a sort of operating system (OS) for the network. All communications between applications and devices have to go through the controller. The OpenFlow protocol connects controller software to network devices so that server software can tell switches where to send packets. The controller uses the OpenFlow protocol to configure network devices and choose the best path for application traffic.

G. ***OpenFlow switch:*** OpenFlow provides an open protocol to program the flow table in different switches and routers. An OpenFlow Switch consists of 3 parts: A Flow Table, A Secure Channel, The OpenFlow Protocol.

VI. SYSTEM FEATURES

1. Software-Defined Networking transforms network architecture into traditional network backbones of rich service-delivery platforms.

   Software-Defined Networking focuses on three key features:

   - Separation of the control plane from the data plane
   - A centralized controller and view of the network
   - Programmability of the network by external applications

2. Intrusion detection is one of the main challenges of internet security today. In this system we will be generating the good and the bad packets. The user will be able to see the bad packets as well as other packets that are being captured by the intrusion detection system and can be able to analyze them though the packet analyzer Wire Shark.

VII. FUTURE SCOPE

Software Defined Network can be a useful tool for an Intrusion Prevention System, due to its capability to both mirror the network traffic and block the malicious flow as soon as the Intrusion Detection System notifies the controller. For future work, a study on the scalability of our proposal is intended, allowing multiple IDS virtual machines running in the same network. We will further study the characteristics of various malwares, investigate malware detection techniques and explore the possibilities of employing them in the context of SDN. In addition, we plan to take better advantage of infrastructure and test our system at a larger scale in order to optimize our system design.

VIII. ADVANTAGES

1. ***Operational Savings***: SDNs lower operating expenses. Network services can be packaged for application owners, freeing up the networking team.

2. ***Flexibility:*** SDNs create flexibility in how the network can be used and operated. Resellers can write their own network services using standard development tools.

3. ***Better Management:*** Managed Service Providers (MSPs) can use a single viewpoint and toolset to manage virtual networking, computing and storage resources.

4. ***Planning:*** Better visibility into network, computing, and storage resources means resellers can also plan IT strategies more effectively for their customers.

5. ***Infrastructure Savings*****:** Separating route/switching intelligence from packet forwarding reduces hardware prices as routers and switches must compete on price-performance features.

IX. CONCLUSION

An SDN come up to foster network virtualization, enabling IT staff to manage their servers, applications, storage, and networks with a common approach and tool set. Whether in a carrier environment or enterprise data center and campus, SDN adoption can improve network manageability, scalability, and agility. It provides interface with SDN controllers, helping better integration and coordination between them. The future of networking will rely more on software, which will accelerate the pace of innovation for networks as it has in the computing and storage domains. SDN promises to transform today's static networks into flexible, programmable platforms with the intelligence to allocate resources dynamically, the scale to support enormous data centers and the virtualization needed to support dynamic, highly automated, and secure cloud environments. With its many advantages and astonishing industry momentum, SDN is on the way to becoming the new norm for networks.

REFERENCES

[1] OpenFlow reference website "OpenFlow tutorial", 2014.
[2] Siamak Azodolmolky, "Software Defined Networking with OpenFlow controller", reference book, 2013.
[3] Open Networking Foundation "Software defined networking in campus networks" April 13, 2012.
[4] "The Internet Protocol Journal" Volume 16, Number 1, March 2013.
[5] Nick Mckeown, Tom Anderson, Hari Balkrishnan, "OpenFlow: Enabling Innovation in Computer Networks, 2008.
[6] SDN reference website, "www.sdn.ieee.org", 2006.
[7] IEEE Std 830-1998 IEEE Recommended, "Practice for Software Requirements Specifications", IEEE Computer Society, 1998.
[8] Richard Heady, George Luger, Arthur Maccabe, Mark Servilla, "The Architecture of a Network Level Intrusion Detection System", 1990.