ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Review on Network Security Virtualization Schemes

Dharmesh Ghelani, Prof. Vikas Maral

Student, Department of Computer Engineering, K.J. College of Engineering Management Research, Savitribai Phule Pune University, Pune, India

Asst. Professor, Department of Computer Engineering, K.J. College of Engineering Management Research, Savitribai Phule Pune University, Pune, India

ABSTRACT: there are various stakeholders having similar goals as well as policies due to which modification to the present internet is restricted to incremental updates; implementation of every novel fundamentally extraordinary innovation is beside inconceivable. To deal with this issue, the concept of network virtualization has designed as a diversifying attribute without having restriction of any system. By permitting multiple heterogeneous system structures to live together on a shared physical substrate, network virtualization gives flexibility, promotes diversity, and promises security and increased manageability. This survey present some previous work done related to above topic.

KEYWORDS: Network virtualization, Security; Threats, Countermeasures.

I. INTRODUCTION

When we consider security for networks, the circumstance is much more complicated. The extra security devices/middle-boxes fundamentally complicate network configuration/ management. Furthermore, security devices have numerous assorted security capacities to fill diverse needs. For instance, we can utilize a firewall to control network access, a network intrusion detection system (NIDS) to perform monitoring of exploit attacks in network payloads, and a network anomaly detection framework to identify DDoS attacks. Thusly, the network administrator should pick sensible security functions/devices and deploy them into reasonable places. Be However, it is a tough task for the administrator, since it is difficult to predict possible network threats of various network tenants and the administrator is not ready to know about requests of various tenants in advance. In this manner, those introduced security functions/appliances/devices may not be in the best areas that can best serve the different security needs of various network clients. Clearly, there is an urgent need to boost the resource use of those existing pre-installed devices/boxes, as well as abstract these security resources to give a straightforward interface for network tenants to utilize.

Software-Defined Networking (SDN) is an emerging architecture that is manageable, dynamic, adaptable and cost-effective, making it ideal choice for the high-bandwidth, dynamic modern day applications. This architecture decouples the network control and forwarding functions allowing the network control to become directly programmable and abstracting the underlying infrastructure for both applications as well as network services. The OpenFlow protocol is a foundational element for building SDN solutions. The SDN architecture is shown in figure:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

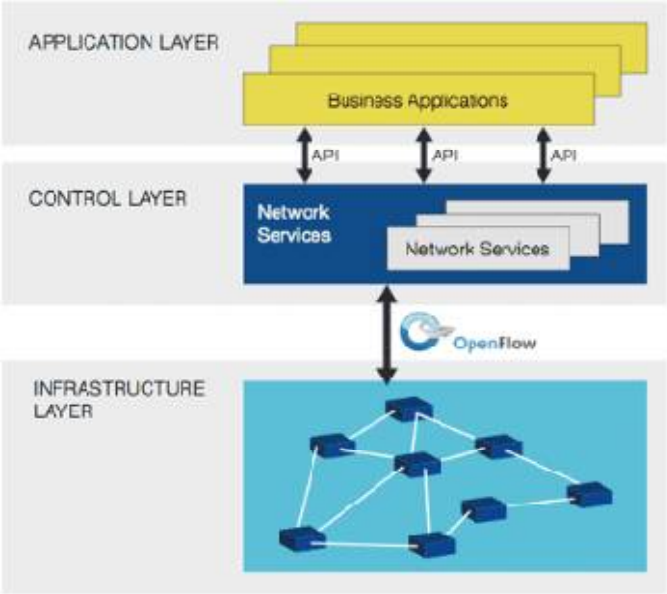

Fig. 1: SDN architecture

A "Network intrusion detection system (NIDS)" monitors network traffic looking out for any suspicious activity, which could be unauthorized activity or an attack. A scaled up NIDS server can be set up on a network backbone, to monitor all traffic; or smaller systems can be set up for traffic monitoring on a particular server, switch, gateway, or router. In addition to monitoring ingress and egress network traffic, a NIDS server can also scrutinize system files checking for unauthorized activity and to maintain file and data integrity. The NIDS server can also detect changes in the server's core components. In addition to traffic monitoring, NIDS server can additionally scan server log files and look for suspicious traffic or usage patterns that match a typical network compromise or a hacking attempts. The NIDS server can also perform a proactive role instead of a reactive function. Possible uses include scanning local firewalls or network servers for scanning live traffic or potential exploits to infer what is going on. Keep in mind that a NIDS server does not replace primary security such as firewalls, encryption, and other authentication mechanism. The NIDS server is a fallback network integrity device. Neither system (primary or security and NIDS server) should replace common precaution (building physical security, corporate security policy, etc.)

In this survey, Section II gives the Literature review for Network Monitoring and Trust Routing systems and also list there pros and cons**.**

II. RELATED WORK

This paper [1] present a new concept of network security virtualization, which virtualizes security functions/resources to network users/administrators, and thus maximally utilizing existing security devices or middle-boxes. In addition, it provides protection to configured networks with minimal management cost. To verify this concept, we further design and implement a prototype system, NETSECVISOR, which can utilize existing pre-deployed (fixed-topology) security devices and leverage software-defined networking technology to virtualize network security functions.

This paper [2], propose OpenSAFE, a system for enabling the random direction of traffic for security monitoring applications at line rates. Additionally, they describe ALARMS, a flow specification language that hugely simplifies management of network monitoring appliances. Finally, they describe a proof-of-concept implementation that they are currently undertaking to monitor traffic across their network.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

In this paper [3], authors present the design and implementation of an innovative cloud networking system called CloudNaaS. Customers can leverage CloudNaaS to deploy applications augmented with an extensible and rich flnetwork functions sets such as virtual network isolation, custom addressing, service differentiation, and flexible interposition of numerous middleboxes. CloudNaaS primitives are implemented within the cloud infrastructure directly using high-speed & programmable network elements, making CloudNaaS highly efficient. They evaluate an OpenFlow-based CloudNaaS prototype and find that it can be used to instantiate various network functions in the cloud, and that its performance is highly robust even in the times of large scale provisioned link/device and services failures.

.

This paper [4] propose FlowTags, an extended SDN architecture in which middleboxes add Tags to outgoing packets, to provide the necessary causal context. These Tags are used on switches and middleboxes for systematic policy enforcement. They discuss the early promise of minimally extending middleboxes to provide this support. They also highlight open challenges of south-bound and north-bound FlowTags APIs design; new controllayer applications for enforcing & validating policies and automatically modifying legacy middle-boxes to support FlowTags.

This paper [5] presents architecture for adding functionality to networks via outsourcing. In this model, enterprise network just forwards data; any further processing is performed via external Feature Providers (FPs). FPs provide & manage features, moving them in response to customer's demand and providing automated recovery for failures. Benefits to enterprise include cost reduction & management complexity, improved features via FP specialization, and better choice in services.

The paper [6], present the first large-scale analysis of failures in a data center network. Through our analysis, we seek to answer several fundamental questions: which devices/links are highly unreliable, how do failures impact network traffic, what causes failures & how effective is network redundancy? They answer these questions using multiple data sources commonly collected by network operators. The key findings of this study is that (1) data center networks show high reliability, (2) commodity switches such as ToRs and AggS are highly reliable, (3) load balancers leads in terms of fault occurrences with many short-lived software related faults, (4) failures have potential to cause loss of many small packets such as keep alive messages and ACKs, and (5) network redundancy is only 40% effective in minimizing the median impact of failure.

This paper [7] proposed a general NIDS architecture to leverage three opportunities: offloading processing to other nodes on a packetˆas routing path, traffic replication to off-path nodes (e.g., to NIDS clusters), and aggregation to split expensive NIDS tasks. As shown in table 1, literature review of various papers has been listed, giving possibility of research gap. We implemented a lightweight shim that allows networks to realize these benefits with little to no modification to existing NIDS software. Their results on many real-world topologies show that this architecture reduces the maximum compute load significantly, provides better resilience under traffic variability, and offers improved detection coverage for scenarios needing network-wide views.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

As shown in table 1, literature review of various papers has been listed, giving possibility of research gap.

Table 1: Survey Table

Sr no.	Title	Publication/ year	Techniques	Advantages	Research gap
1.	A First Step Toward Network Security Virtualization: From Concept To Prototype	IEEE, 2015	Mininet	Provides network security virtualization to network users/administrators	adds a very small overhead
2.	Extensible and scalable network monitoring using OpenSAFE	USENIX Internet Netw. , 2010	OpenFlow	makes monitoring large scale networks easier	has a rich area for future work
3.	CloudNaaS: A cloud networking platform for enterprise applications	ACM, 2011	uses a policy that enables point-to-point reachability between VMs 1-3	robust	---
4.	Enforcing network-wide policies in the presence of dynamic middlebox actions using Flow-Tags	NSDI, 2014	FlowTags-enhanced Middleboxes	overhead of FlowTags is comparable to traditional SDN mechanisms	automating DPG generation via model refinement techniques can be performed
5.	Understanding network failures in data centers: Measurement, analysis, and implications	ACM SIGCOMM, 2011	---	analysis on haracterizing failures of network links and devices, estimating their failure impact, and analyzing the effectiveness of network redundancy in masking failures	correlating logs from application-level monitors

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

III. PROPOSED WORK

A SYSTEM ARCHITECTURE

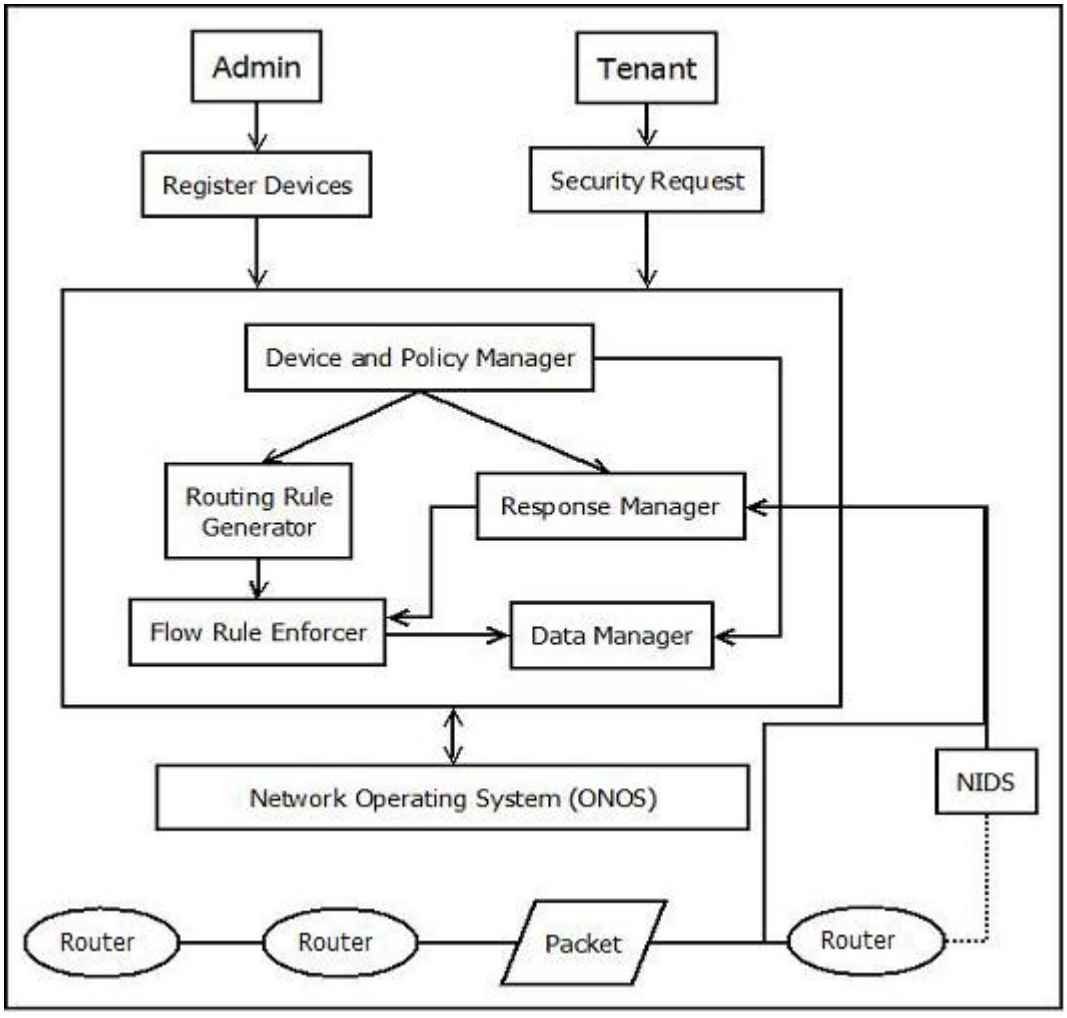

Fig.1. System Architecture

Figure 2 shows the system architecture of proposed system. A typical operation of NETSECVISOR works as follows. A network administrator registers network security devices (both physical devices and virtual appliances) to NETSECVISOR. After registration, cloud tenants need to create their security requests and submit them into NETSECVISOR. Then, NETSECVISOR parses the submitted security requests to understand the intention of tenants and writes the corresponding security policies to policy table. Next, if NETSECVISOR receives a new flow setup request from a network device, it checks whether this flow is matched with any submitted policies. If it is, NETSECVISOR will create a new routing path and corresponding flow rules for the path. At this time, NETSECVISOR guarantees that the routing path includes required security devices that are defined in a matched policy. After this operation, it enforces flow rules to each corresponding network device to forward a network flow. If any of security devices detects malicious connection/content from monitored traffic, they will report this information to NETSECVISOR. Based on the report and submitted policies, NETSECVISOR enables a security response function to respond to malicious flows accordingly.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

IV. CONCLUSION

This paper analyses various techniques used for Network Monitoring and Trust Routing. Also given the advantages and drawbacks present in the different studies performed by various researchers. To deal with drawbacks in present systems we presented an idea of the new system.

REFERENCES

1. Seungwon Shin, Haopei Wang, and Guofei Gu, "A First Step Toward Network Security Virtualization: From Concept To Prototype", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 10, OCTOBER 2015.
2. J. R. Ballard, I. Rae, and A. Akella, "Extensible and scalable network monitoring using OpenSAFE," in Proc. USENIX Internet Netw. Manage. Conf. Res. Enterprise Netw., 2010, p. 8.
3. T. Benson, A. Akella, A. Shaikh, and S. Sahu, "CloudNaaS: A cloud networking platform for enterprise applications," in Proc. 2nd ACM Symp. Cloud Comput., 2011, Art. ID 8.
4. S. K. Fayazbakhsh, L. Chiang, V. Sekar, M. Yu, and J. C. Mogul, "Enforcing network-wide policies in the presence of dynamic middlebox actions using Flow-Tags," in Proc. 11th USENIX Symp. Netw. Syst. Design Implement. (NSDI), 2014, pp. 533-546.
5. G. Gibb, H. Zeng, and N. McKeown, "Outsourcing network functionality," in Proc. ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN), Aug. 2012, pp. 73-78.
6. P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers: Measurement, analysis, and implications," in Proc. ACM SIGCOMM, 2011, pp. 350-361.
7. V. Heorhiadi, V. Sekar, and M. K. Reiter, "New opportunities for load balancing in network-wide intrusion detection systems," in Proc. ACM CoNEXT, 2012, pp. 361-372