Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.532 – 537

Secured Structural Design for Software Defined Data Center Networks

Reshmi. S[1], Dr. M. Anand Kumar[2]

[1]Department of Information Technology & Karpagam University, Coimbatore, India

[2]Department of Information Technology & Karpagam University, Coimbatore, India

[1] reshmismca@gmail.com; [2] anand2kumarm@gmail.com

Abstract— Research work provides efficient security which protects network resources from internal and external threats. Network virtualization is used to provide users with well-organized, controlled, and safe sharing of the networking resources. It also ensures privacy of data and integrity in Software-defined data center (SDDC) whose infrastructures is virtualized and distributed as a service. SDDC helps to broaden the virtualization concept which makes it more secure. The complete infrastructure is distracted from hardware and implemented via software. One of the core components of SDDC is SDN (Software defined networking) that includes network virtualization. SDN requires the method named Open Flow for the Control plane to communicate with data plane (forwards those incoming packets to the destination). SDN and Open Flow with Virtual LAN are used to concentrate on security issues in data centers. An integration of Software Defined Networking and Open Flow (SDNOF) with VLAN Virtual Server Security (VVSS) architecture is presented to address distinct security issues in virtualized network. The Software defined networking and open flow with VVSS is introduced for more secured protection and to maintain compliance integrity of servers in DCN.

Keywords – SDDC, Virtual LAN, Virtualization, SDNOF, VVSS, Virtual Server

I. INTRODUCTION

In recent times, data center networks (DCNs) have attracted a lot of interest in the enterprise networking industry. DCNs are used to provide data storage and files transfer where end stations are interconnected as clusters and bladed systems [9]. A data center represents the heart of any organization's network [6]. Companies rely on the data stored in the data center to interact with its employees and customers. The proliferation of the Web-based technologies makes the data center more vulnerable to security attacks. Any security attack on the data center can destroy the whole organization's network and data [6]. Besides throughput and low latency needed in DCNs, the security issues of endeavour data centers are also very critical. Several researches were dedicated to the security issues and the design constraints of large scale data centers from different points of view [6]. The papers [6], [7], [13], [2], [8] data center problems are conferred technologies which involves security strategies such as repositioning, exodus, growth and evaluation of asset management policies. The authors of [13] carried out an overview of the communication network design problems that arise with large numbers of nodes, links and switch costs. Some layered security models for addressing complex security issues are discussed in [2] and [8]. With fast changing technologies and service demands in DCNs, the need for an effective open platform secure model becomes very imperative.

© 2016, IJCSMC All Rights Reserved

In this paper with detailed study on the security proposals existing in literature, and having considered all the requirements of network security management for a virtualized data center model, this research work propose an effective secured model: Software Defined Networking and Open Flow (SDNOF) with VLAN Virtual Server Security (VVSS) [11]. The design is based on layered security architecture for virtual servers and open flow switch architecture. Operational mechanism is presented in section V with other details. In DCN, MAC controllers in the virtual open flow switch in DCN to house the flow tables for each virtual port; this work creates lines of defense against any security threat. Link buffer characterized and monitored unicast, broadcast and multicast traffic [16]. The paper is organized as follows. In Section II, we discussed virtualization in data center network, data center security problems as presented in [6]. In section III, the proposed security model (SDNOF) is shown with the Virtual server system.

II. VIRTUALIZATION IN DATA CENTER NETWORKS

Running multiple applications on a single server makes server virtualization more popular in data center [14]. Virtualization helps with server consolidation and provides flexible resource management mechanisms [14] in DCNs particularly. Virtualization is more popular in current years because of the promise of improved resource utilization through server consolidation. According to [10], a Data Center is the consolidation point for provisioning multiple services that drive an Enterprise business. In [6], the authors enlist the data center hardware and software components. The hardware components are: firewalls, Intrusion Detection Systems, contents switches, access switches and core switches. The software components are: IPSec and VPN, antivirus software, network management systems and access control server. However, for effective security implementation in a virtualized DCN [18], this work goes further to propose a more secured data center design that is programmed, protected, and supple using the SDNOF approach in our context.

III. DATA CENTER SECURITY PROBLEMS

There are different security threats in data center networks. The work carried out in [10], [11]and[12] discussed some of these problems, viz: Unauthorized Access, MAC Flooding, ARP Spoofing, IP Spoofing, Denial of Service (DOS) [15], Viruses, Worms, Trojans, and internal Security threats. However, sampled solutions to these problems were given in [6]. We still argue that these solutions do not completely eradicate security vulnerabilities in contemporary data center networks. A reorganized architecture which will address the possible lapses in addition to the outlined remedies in [6], will serve in securing today's enterprise networks.

IV. DATA CENTER SECURITY TECHNOLOGIES

It is very important to protect the stored information at the data center from any security threat that may destroy or modify it in any unwanted way [6]. These security threats can originate from hackers outside or from inside the data center network. Different solutions to the security threats can be used together to achieve the highest possible data protection [19]. Some of these technologies are:

- Firewalls.
- Detecting interference in network and preventing
- Virtual Local Area Networks (VLAN).
- Virtual Private Network (VPN) and IPSec.

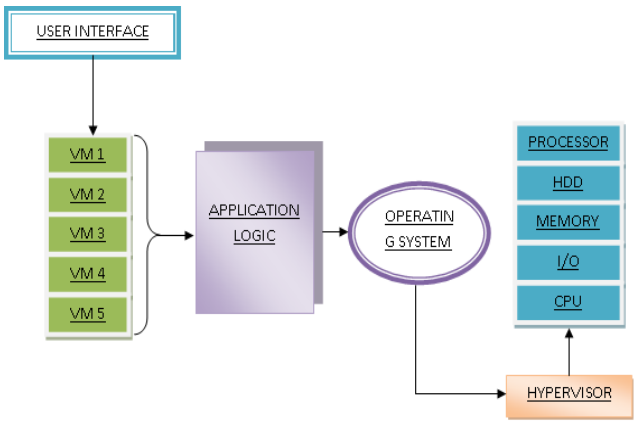

Fig. 1 VLAN Virtual Security System Model

© 2016, IJCSMC All Rights Reserved

Leveraging on these four technologies, our contribution is shown in the Open Flow Software Defined Network model in Fig. 2. SDNOF is a layer 2 protocol in the virtual Software Defined Network (SDN) switch that allows for policy control via its open flow visor (virtualization layer) [13]. This model creates multiple layers of security for the virtualized DCN controlling unicast, broadcast and multicast traffics. Section IV and V discussed in details the security models for highly scalable and secure virtualized DCN.

V. VLAN VIRTUAL SERVER SECURITY SYSTEM

To protect Virtual data center, VLAN Virtual Server Security (VVSS) system is proposed in this work for the server VM which provides multi-layered workgroup segmentation. The VVSS solution is a generic purpose-built framework proposed for large scale enterprises. The virtual environment at the core of the infrastructure is the Vm server running on ESX platform with its VMware [12]. Fig. 1 shows the VVSS model. Again, in our architecture shown in Fig. 2, MAC controllers were assigned to all the network entities to house their flow tables.

For active participation in the network, the open flow visor must uniquely identify and authenticate the client node else, the terminal is dropped for access. As shown in Fig. 1, VLAN virtual security model was modeled to be deployed on a virtualized server for various applications (Vm1…Vm5). The kernel utilizes the hypervisor API to inspect and control the virtual switch network and VM behavior. Virtual Security Service (VSS) utilizes a subnetted IP mapping, which is provided as VMsafe for various user groups.

For demonstration in this work, each VM server on virtualized server is managed and configured through packet tracer environment. A VLAN backbone which hosts the Vm server is the central manager for the applications. VVSS has the following functions:

- Hypervisor generator [17]
- Network Access Control (NAC)
- Discovery and Broadcast Isolation
- License and Update Management (LUM)

VI. OPEN FLOW SOFTWARE DEFINED NETWORK MODEL FOR DCN

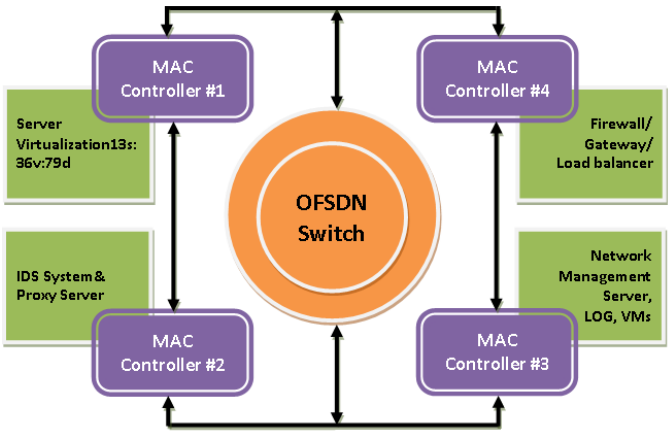

Fig. 2 SDN and OF security model for DCN

An open flow protocol (OFP) which can be enabled in the switch carries out control policy (CP), reaction execution (RE) and history tracking (HT). The Open flow software defined networking switch in figure 2 is a speed redundant device with isolated MAC controllers [20] housing the flow tables shown in Fig. 4. Once OFP is enabled on the switch, any device interfaced with the switch is actively monitored as a software robot, thereby securing the overall network against any form of threat. This is proposed for virtualized data center in context. The key security metric is the MAC ID of the interfacing devices.

© 2016, IJCSMC All Rights Reserved

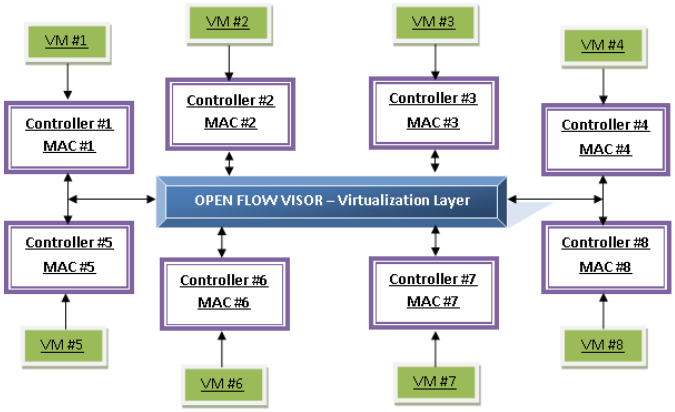

Fig. 3 A Open Flow Visor Switch in Virtualization Layer

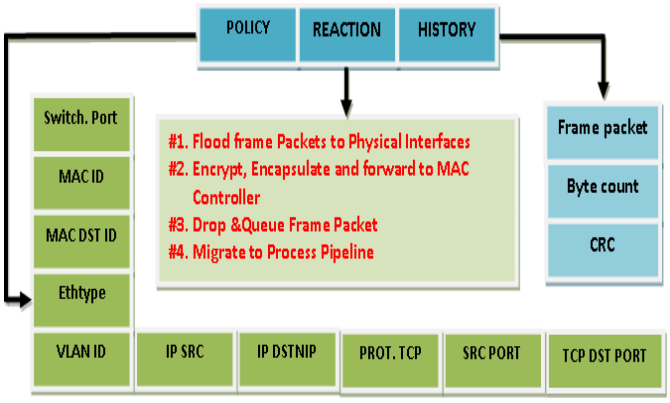

Fig. 4 The Entrance of Open Flow Switch Model Flow Table

The security policy of the flow table in Fig. 4 controls activities that is handled by conventional VLAN and Access control list (ACL) [14] such as traffic denial or flow allowance, routing, broadcast isolation flow, flow detection and suppression in the SDNOF switch. All servers, etc shown in Fig. 2 are mapped in the MAC controllers. Fig. 3 shows the open virtual isolation in the SDNOF switch. This model offers a highly secured security layer to existing security approaches in literature.

VII. EXPERIMENTAL SETUP

Engrossing virtualization of server test bed consisting of one standard HP machine with a dual-core Intel Xeon processor connected to a rack-mounted disk enclosure with a Small Computer Scale Interface (SCSI) backplane running on ESX linux sever is the first phase in this setup. For the purposes of trace security, six VLANs were created for the server and simulated with packet trace tool. In the server, a Seagate model 15,000RPM disks: of size 1TB was considered with a RAM of 6GB. The server was connected via a switched (SDNOF) 1Gbps Ethernet link. The experimental setup includes 3 basic services in security for protection against unauthorized access:

- Data authentication
- Integrity of data
- Confidentiality of data

Software-defined data center ensures privacy and integrity of data. The above 3 services are meant for protecting against any unauthorized access because SDDC acts a vital role by broadening the infrastructure to secure from intruders.

TABLE 1

DATA CENTER VM SERVERS (13 SERVERS, 36 VOLUMES, 79 DISKS)

Vmservers	Vlan	Volumes	Ip mapping
$UserV_M$	10	3	192.168.10.2
$ProjectV_M$	10	3	192.168.10.3
$PrtrV_M$	20	4	192.168.10.4
$HrdmV_M$	20	5	192.168.10.24
RDVm	20	1	192.168.10.20
$PrxyV_M$	30	2	192.168.10.22
$ScrV_M$	30	3	192.168.10.50

© 2016, IJCSMC All Rights Reserved

WebVm	40	2	192.168.10.24
MdSVm	40	4	192.168.10.23
ERPVm	40	2	192.168.10.68
NACVm	50	4	192.168.10.70
E-ComV_M	30	2	192.168.10.58
IntrantVm	60	1	192.168.10.78

TABLE 2

AVERAGE UTILIZATION RATES.

Resource	Utilization
CPU	6%
MEMORY	40%
INPUT / OUTPUT NETWORK	<5%
DISK I/O	<5%

The proposed mechanism uses OpenFlow Switches and a central controller to reduce network overhead and enable the switches to deal with network during traffic bursts. The central controller manages multiple openflow switches, which helps to store the database information as a slice and removes the drawbacks in VLANs & updates the network with its configuration. The analytical model and validation of the proposed models are defined in future work; however this work seeks to use the presented approaches to enhance the security design of a virtualized data center network.

The large scale service providers who deployed a SDN already in the data center, decided to extend it with WAN like CloudGenix which is based on cloud computing. For better development of SDDC approach VMware is used. The uses of CloudGenix are to connect the people across the world through application either in hybrid or private cloud. It is planning to bring the advantages of SDN to the WAN and manage it using VMware NSX in data center.

VIII. CONCLUSION

The more efficient security architecture discussed in this paper is envisaged to achieve the best possible solution for virtualized data center systems. Due to the progression in technology of virtualization, the security methodologies for traditional data centers which includes: firewalls, intrusion detection system/intrusion protection system, virtual local area network (VLAN) and virtual private network (VPN) cannot effectively handle security implications of a virtualized data center networks. This work presents an effective open flow software defined network switch with VVSS model and with emphasis on VLAN virtualization on ESX server to ensure total security of the critical data in the virtualized data center network.

REFERENCES

[1] Nachikethas A. Jagadeesan, and Bhaskar Krishnamachari, *Software-Defined Networking Paradigms in Wireless Networks: A Survey*, Journal ACM Computing Surveys (CSUR), Volume 47 Issue 2, January 2015, Article no: 27, Doi no: 10.1145/2655690.

[2] Wang K, Zhou H, Luo H, Guan J, Qin Y, and Zhang H, *Detecting and mitigating Interest flooding attacks in content-centric network*, Security and Communication Networks published online, Volume 7, Issue 4, April 2014, pp 685-699,Doi no : 10.1002/sec.770.

[3] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, *AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks*, CCS '13 Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Volume 1, Issue 1, November 2013, pp 413-424, Doi no: 10.1145/2508859.2516684.

© 2016, IJCSMC All Rights Reserved

[4] Qiao Yan, and F. Yu, *Distributed denial of service attacks in software-defined networking with cloud computing*, IEEE Communications Magazine, Volume 53, Issue 4, April 2015, pp 52–59, Doi no: 10.1109/MCOM.2015.7081075.

[5] S. Chowdhury, M. Bari, R. Ahmed, and R. Boutaba, *PayLess: A low cost network monitoring framework for Software Defined Networks*, Network Operations and Management Symposium (NOMS), 2014 IEEE, Volume 1, Issue 1, May 2014, pp 1-9, Doi no: 10.1109/NOMS.2014.6838227.

[6] Bin Wang, Zhengwei Qi, Ruhui Ma, Haibing Guan, Athanasios V. Vasilakos, *A survey on data center networking for cloud computing*, Computer Networks, Science Direct, Elsevier, Volume 91, Issue 1, November 2015, pp 528-547, Doi no: 10.1016/j.comnet.2015.08.040.

[7] Fabrizio Baiardi, Claudio Telmon, Daniele Sgandurra, *A simulation-driven approach for assessing risks of complex systems*, EWDC '11: Proceedings of the 13th European Workshop on Dependable Computing ACM, Volume 1, Issue 1, May 2011, pp 35-40, Doi no: 10.1145/1978582.1978590.

[8] D. Kreutz, F. M. Ramos, and P. Verissimo, *Towards Secure and Dependable Software-Defined Networks*, in Proceeding HotSDN '13 Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, Volume 1, Issue 1, August 2013, pp 55-60, Doi no: 10.1145/2491185.2491199.

[9] G. Vigna; F. Valeur; J. Zhou; R. A. Kemmerer, *Composable tools for network discovery and security analysis*, Computer Security Applications Conference, 2002. Proceedings. 18th Annual, IEEE Conference Publications, Volume 1, Issue 1, 2002, pp 14-24, Doi no: 10.1109/CSAC.2002.1176274.

[10] K. Argyraki, P. Maniatis, and A. Singla, *Verifiable network performance measurements*, in Proceeding Co-NEXT '10 Proceedings of the 6th International Conference, ACM, Volume 1, Issue 1, November 2010, pp. 1:1–1:12, Doi no: 10.1145/1921168.1921170.

[11] Wolfgang Braun and Michael Menth, *Software-Defined Networking Using Open Flow: Protocols, Applications and Architectural Design Choices*, Open Access, Future Internet May 2014, Volume 6, Issue 2, pp. 302-336; Doi no:10.3390/fi6020302.

[12] I. Ahmad, J. M. Anderson, A. M. Holler, R. Kambo, and V. Makhija, *An analysis of disk performance in VMware ESX server virtual machines*, Workload Characterization, 2003 IEEE International Workshop, 27 October 2003, Volume 1, Issue 1, pp. 65 – 76; Doi no : 10.1109/WWC.2003.1249058.

[13] Pascal Dauer, Rahamatullah Khondoker, Ronald Marx, and Kpatcha Bayarou, *Security Analysis of Software Defined Networking Applications for Monitoring and Measurement: sFlow and BigTap*, Proceeding CFI'15 The 10th International Conference on Future Internet, ACM, Volume 1, Issue 1, pp-51-56, Doi no: 10.1145/2775088.2775104.

[14] Ruxandra Trandafir,; Mihai Carabas, Razvan Rughinis and Nicolae Tapus, *FirewallPK: Security tool for centralized Access Control List management*, 2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference, IEEE, September 2014, Volume 1, Issue 1, pp 1 - 6, Doi no: 10.1109/RoEduNet-RENAM.2014.6955309

[15] R. R. Rejimol Robinson and Ciza Thomas, *Evaluation of mitigation methods for distributed denial of service attacks*, 7th IEEE Conference on Industrial Electronics and Applications (ICIEA), IEEE, July 2012, Volume 1, Issue 1, pp: 713 -718, Doi no: 10.1109/ICIEA.2012.6360818

[16] Jian Chen and V. C. M. Leung, *Applying active queue management to link layer buffers for real-time traffic over third generation wireless networks*, Wireless Communications and Networking, IEEE, March 2003, Volume 3, Issue 1, pp: 1657 – 1662, Doi no: 10.1109/WCNC.2003.1200635

[17] Johan Fornaeus, *Device hypervisors*, Proceeding DAC'10 Proceedings of the 47th Design Automation Conference, ACM, 2010, Volume 1, Issue 1, pp 114-119, Doi no: 10.1145/1837274.1837305

[18] Katherine Barabash, Rami Cohen, David Hadas, Vinit Jain, Renato Recio, Benny Rochwerger, *A case for overlays in DCN virtualization*, DC-CaVES '11: Proceedings of the 3rd Workshop on Data Center - Converged and Virtual Ethernet Switching, September 2011, Volume 1, Issue 1, pp: 30-37.

[19] Gurudatt Kulkarni; Rupali Shelk, Kiran Gaikwad, Vikas Solanke, Sangita Gujar, Prasad Khatawkar, *Wireless sensor network security threats*, Fifth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2013), Sept. 2013, Volume 1, Issue 1, pp: 131 - 135, Doi no: 10.1049/cp.2013.2225.

[20] In-Pyo Hong; Yong-Joo Lee; Sung-Jae Chun; Yong-Surk Lee; Jinoo Joung, *Multi-threading processor architecture for wireless LAN MAC controller*, Digest of Technical Papers. International Conference on Consumer Electronics, 2005. ICCE, January 2005, Volume 1, Issue 1, pp: 379 - 380, Doi no: 10.1109/ICCE.2005.1429876.

© 2016, IJCSMC All Rights Reserved