Effective Security Architecture for Virtualized Data Center Networks

[1]Udeze Chidiebele. C, [3] Okafor Kennedy .C
[1,3] R & D Department, Electronics Development Institute
(FMST-NASENI), Awka, Nigeria.

[2]Prof. H. C Inyiama,[4]Dr C. C. Okezie,
[2,4] Electronics and Computer Engineering Department,
Nnamdi Azikiwe University, Awka, Nigeria

Abstract—**This work presents a candidate scheme for effective security policy that defines the requirements that will facilitate protection of network resources from internal and external security threats. Also, it ensures data privacy and integrity in a virtualized data center network (VDCN). An integration of Open Flow Software Defined Networking (OFSDN) with VLAN Virtual Server Security (VVSS) architecture is presented to address distinct security issues in virtualized data centers. The OFSDN with VVSS is proposed to create a more secured protection and maintain compliance integrity of servers and applications in the DCN. This proposal though still on the prototype phase, calls for community driven responses.**

Keywords- Infrastructure; Virtualization; VDCN; OFSDN; VVSS; VLAN; Virtual Server.

I. INTRODUCTION

Recently, 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 [1]. A data center represents the heart of any organization's network [2]. 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 [2]. Besides throughput and low latency required in DCNs, the security considerations of enterprise data centers is 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 [2]. The authors in [2], [3], [4], [5], [6] discussed on the data center security problems, technologies, security strategies such as consolidation, relocation, migration, expansion and review of asset management policies. The authors of [4] 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 [5] and [6]. With fast changing technologies and service demands in DCNs, the need for an effective open platform secure model becomes very imperative.

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, we propose an effective secured model: Open Flow Software Defined Networking (OFSDN) with VLAN Virtual Server Security (VVSS). 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. By allowing the MAC controllers in the virtual open flow switch in our DCN to house the flow tables for each virtual port, this work creates lines of defense against any security threat. Unicast, broadcast and multicast traffic are characterized and monitored by the modeled switch architecture which serves as an aggregation link buffer.

The paper is organized as follows. In Section II, we discussed virtualization in data center network, data center security problems as presented in [2]. In section III, the proposed security model (OFSDN) is shown with the Virtual server security system. Section IV gives the experimental setup for VLAN open flow switch. The paper ends with conclusions and future directions

II. VIRTUALIZATION IN DATA CENTER NETWORKS

Server virtualization has become popular in data centers since it provides an easy mechanism to cleanly partition physical resources, allowing multiple applications to run in isolation on a single server [7]. Virtualization helps with server consolidation and provides flexible resource management mechanisms [7] in DCNs particularly. We quickly add that Virtualization is not a new technology, but it has regained popularity in recent years because of the promise of improved resource utilization through server consolidation. According to [8], a Data Center is the consolidation point for provisioning multiple services that drive an Enterprise business. In [2], 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, this work goes further to propose a more secured data center design that is programmable, secured with strong isolation, and flexible using the OFSDN approach in our context.

III. DATA CENTER SECURITY PROBLEMS

Data center networks usually have its security threats. The work carried out in [8], [9]and[10] discussed some of these problems, viz: Unauthorized Access, MAC Flooding, ARP Spoofing, IP Spoofing, Denial of Service (DOS), Viruses, Worms, Trojans, and internal Security threats. However, sampled solutions to these problems were given in [2]. We still argue that these solutions do not completely eradicate security vulnerabilities in contemporary data center networks.

For a virtualized data center domain, a restructured architecture which will address the possible lapses in addition to the outlined remedies in [2], will serve in securing today's enterprise networks.

IV. Data Center Security Technologies

Information stored at the data center must be protected from any security threat that may destroy or modify it in any unwanted way [2]. 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. Some of these technologies are:

- Firewalls.
- Network intrusion detection and prevention systems.
- Virtual Local Area Networks (VLAN).
- Virtual Private Network (VPN) and IPSec.

Leveraging on these four technologies, our contribution is shown in the Open Flow Software Defined Network model in Fig. 2. OFSDN 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). 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

VLAN Virtual Server Security (VVSS) system proposed in this work for the server VM provides multi-layered workgroup segmentation while utilizing the underlying hardware technology to protect the virtual data center. 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.

Fig. 1 shows the VVSS model while Fig. 5 and Fig. 6 show the packet tracer simulation. 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.

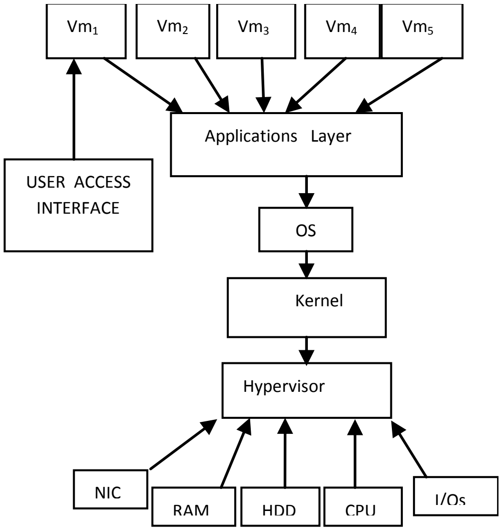


Figure 1. VLAN Virtual Security System Model.

A VLAN backbone which hosts the Vm server is the central manager for the applications. VVSS has the following functions:

- Inter-VM migration of Applications and services for compatibility issues
- Virtual Machine generator and monitor
- Network Access Control (NAC)
- Discovery and Broadcast Isolation
- License and Update Management (LUM)

VI. Open Flow Software Defined Network Model For DCN

The Open flow software defined networking switch in figure 2 is a speed redundant device with isolated MAC controllers housing the flow tables shown in Fig. 4. An open flow protocol (OFP) which can be enabled in the switch carries out control policy (CP), reaction execution (RE) and history tracking (HT). 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.

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

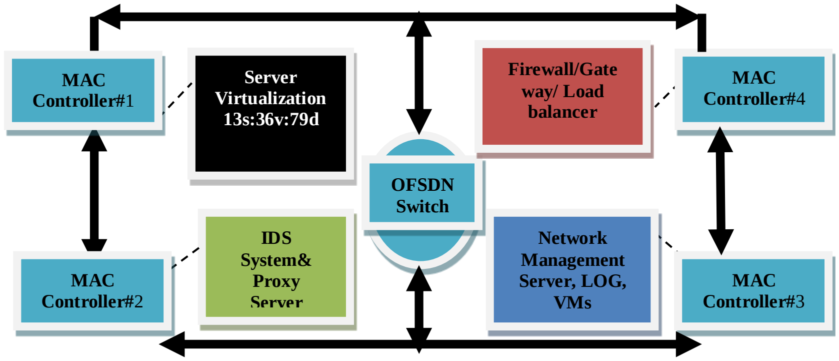

MAC Controller#1
Server Virtualization 13s:36v:79d
Firewall/Gate way/ Load balancer
MAC Controller#4
OFSDN Switch
MAC Controller#2
IDS System& Proxy Server
Network Management Server, LOG, VMs
MAC Controller#3

Figure 2. OFSDN Security Model for DCN

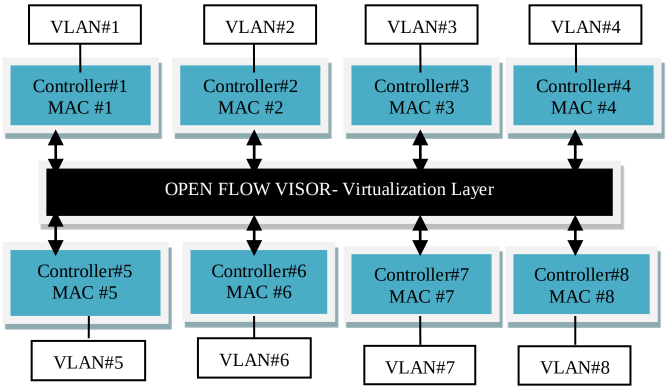


Figure 3. A Virtualized Open Flow Switch

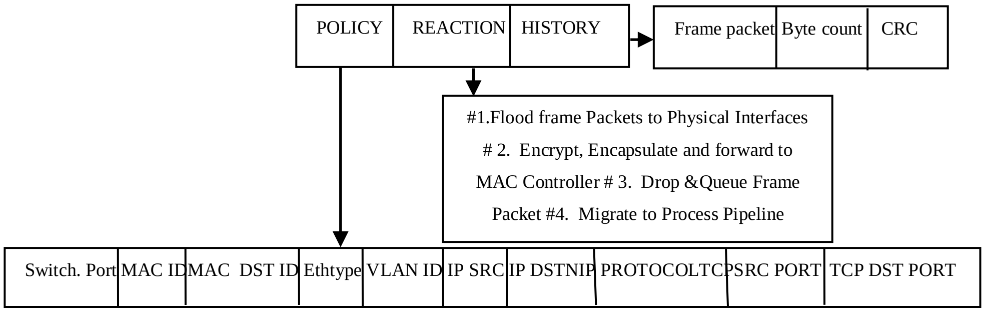

POLICY
REACTION
HISTORY
Frame packet
Byte count
CRC
#1.Flood frame Packets to Physical Interfaces
# 2. Encrypt, Encapsulate and forward to
MAC Controller # 3. Drop &Queue Frame
Packet #4. Migrate to Process Pipeline
Switch. Port
MAC ID
MAC DST ID
Ethtype
VLAN ID
IP SRC
IP DSTNIP
PROTOCOLTC
PSRC PORT
TCP DST PORT

Figure 4. Flow table Ingress in Open Flow Switch Model

VII. Experimental Setup

The first phase experiment involves virtualizing the 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.

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 (OFSDN) 1Gbps Ethernet link.

This work provides three fundamental security services:

- Data confidentiality: protecting against unauthorized access to data being transmitted.
- Data integrity: protecting against alteration or future replay of traffic.
- Source authentication: network addresses are authenticated as part of the protocol.

We deployed Classless Inter-domain Routing (CIDR) approach to generate usable IP for the VM server and users on the network. For valid IP range for 200 users with 128Vm servers, we used a class valid host range: 192.168.10.1 to 192.168.10.199 with a subnet mask of 255.255.255.0. For effective security and broadcast isolation, virtual IP mapping on the Vm server enables the hosts, guests and clients to communicate with each other. Fig. 5 and Fig. 6 show the packet flow in the packet tracer integrated development environment (IDE).

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
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%
NETWORK I/O	<5%
DISK I/O	<5%

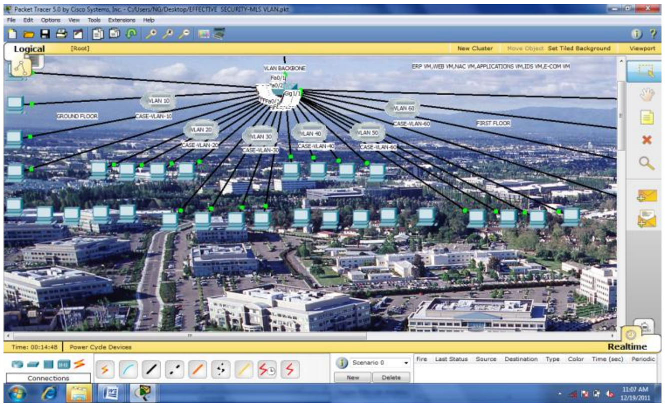
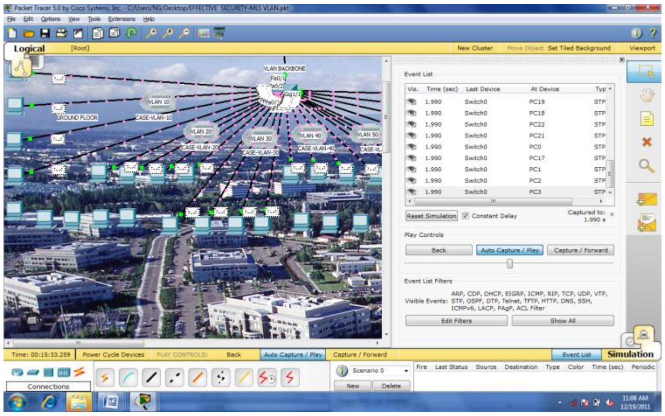


Figure 5. DCN VLAN workgroup Model with ESx server



Event List

Vis.	Time (sec)	Last Device	At Device	Typ
	1.990	Switch0	PC19	STP
	1.990	Switch0	PC18	STP
	1.990	Switch0	PC22	STP
	1.990	Switch0	PC21	STP
	1.990	Switch0	PC0	STP
	1.990	Switch0	PC17	STP
	1.990	Switch0	PC1	STP
	1.990	Switch0	PC2	STP
	1.990	Switch0	PC3	STP

Reset Simulation ☑ Constant Delay Captured to: 1.990 s

Play Controls

Back | Auto Capture / Play | Capture / Forward

Event List Filters

Visible Events: ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP, VTP, STP, OSPF, DTP, Telnet, TFTP, HTTP, DNS, SSH, ICMPv6, LACP, PAgP, ACL Filter

Edit Filters | Show All

Figure 6. Simulated Packet Flow for secured DCN

VIII. Conclusion

The effective security architecture discussed in this paper is conceived to achieve the best possible solution for virtualized data center networks. Owing to advancements in virtualization technology, 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.

The analytical model and validation of the proposed models in Fig. 2 and 3 will be clearly shown in the future work; however this work seeks to use the presented approaches to enhance the security design of a virtualized data center network.

REFERENCES

[1] Jinjing. jiang and R.Jain, " Analysis of backward congestion notification (BCN) for ethernet in datacenter applications. IEEE communications Society INFOCOM 2007 proceedings.

[2] Jalal Frihati, Florica Moldoveanu, Alin Moldoveanu , General guidelines for the security of a large scale data centre design, U.P.B. Sci. Bull., Series C, Vol. 71, Issue 3, 2009.

[3] Data centre services, URL, http://www.sun.com/service/storage/datacenterdatasheet.pdf

[4] Practical Large-Scale Network Design With Variable Costs for Links and Switches, URL:http://whitepapers.silicon.com/0,39024759,60304468p,00.htm

[5] Mitchell Ashley "LAYERED NETWORK SECURITY 2006: A best-practices approach",URL:http://www.stillsecure.com/docs/StillSecure_LayeredSecurity.pdf.

[6] Juniper networks layered security solution, URL:http://cn.juniper.net/solutions/literature /white _papers/2005.pdf

[7] Timothy Wood, "Improving data center resource Management, deployment, and availability with virtualization", PHD thesis June,2009,(Unpublished).

[8] http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a008073377d.pdf

[9] Data center: infrastructure architecture SRND,URL:http://www.cisco.com/application/pdf/en/us/guest/netsol/ns304/c649/cdccont_0900aecd800e4d2e.pdf

[10] Data Center: Securing Server Farms , URL:www.cisco.com/application/pdf/en/us/guest/netsol/ ns304/c649/ccmigration_09186a008014edf3.pdf

[11] Data center security topologies: www.cisco.com/application/pdf/en/ us/ guest/netsol/ns376/c649/cdccont_0900aecd800ebd1d.pdf