New Security Perspective for Virtualized Platforms

Abdelmajid Lakbabi, Said El hajji, Ghizlane Orhanou, Kaouthar Chetioui

***Abstract*— Recently, an important transition in IT infrastructure and delivery services occurs, based on the virtualization technology, cloud computing becomes the key for any successful information technology solution.**

Unfortunately, This success will brings fundamental changes in the classic network security concepts and implementation, since in virtualized environment, components are no longer considered as a separate systems, but resources, data and applications, are seen as services with no visible security perimeter, from this perspective, new adapted security approach to protect such environment is needed; Each physical security solution, like firewalls, intrusion prevention system and network access control, will have a corresponding that fits in the virtual platform, with automation capabilities to monitor, assess network traffic and stop threats accurately.

The perspective of this paper is to propose a deep study of the virtualized platform, especially the hypervisor and the inter-virtual machines communications enumerates some of its important security concerns, then propose a solution to secure it.

We will present the virtualized architecture, analyze its vulnerabilities and integrate it with virtual Firewall, virtual Intrusion Prevention Systems, and add NAC capabilities to protect the entire virtual environment.

***Index Terms*— Hypervisor, virtual Firewall, virtual IPS, virtual Switch, vulnerability exploit, NAC**

I. INTRODUCTION

The virtualization [1] consists of the creation of many virtual resources from one physical resource. It materializes the use of virtual machines to let multiple network subscribers maintain individualized desktops and servers on a single, centrally located hardware machine that is generally located at a data center. Users may be geographically scattered but are all connected to the central machine by a proprietary local area network (LAN) or wide area network (WAN) or the Internet.

a. Virtualization concept

From an IT point of view, it is the ability to run multiple operating systems on a single physical system and share the underlying hardware resources.

Abdelmajid Lakbabi is a Doctoral Student of Laboratory of Mathematics, Computing and Applications , Faculty of sciences, University of Mohammed V-Agdal, BP.1014 RP. Rabat, Morocco
(Author's e-mail: lakbabi@gmail.com,
Coauthor's e-mail: elhajji@fsr.ac.ma, ghizlane.orhanou@gmail.com, kaoutharchetioui@gmail.com)

b. Virtualization components

Host or hypervisor: the machine that hosts other virtual machines using virtualization software. It can run virtual machines whose operating systems differ from that of the host machine.

It manages multiple operating systems (or multiple instances of the same operating system) on a single computer system. The hypervisor manages the system's processor, memory, and other resources to allocate what each operating system requires.

VMs: A virtual machine (VM) is a software implementation of a computing environment in which an operating system (OS) or a program can be installed and run.

VMM: Virtual Machine Monitor, a software layer that creates and maintains the Virtual Machine environment.

Virtual Switch (vSwitch): A virtual switch is simply a core L2 forwarding engine that does VLAN tagging, stripping, filtering, L2 security, checksum, segmentation offload units, and many other tasks that are done by Physical Switchs (pSwitches) in Physical networks (pNetworks), essentially:

- Models a physical Ethernet switch
- Connects VMs (Virtual machines) to Uplink adapters
- Combines the bandwidth of multiples network adapters and balances traffic among them and handles physical NIC failover.
- Forward traffic between VMs and links to external networks.

There are two types of virtual Switchs:

- Virtual standard Switch: A software-based switch that resides in the virtualized host kernel and provides traffic management for VMs; Administrators must manage vSwitchs independently on each virtualized host.

- Virtual Distributed Switch: A software-based switch that resides in the virtualized host kernel and provides traffic management for VMs. Distributed vSwitchs are shared by and managed across entire cluster of virtualized hosts.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

vNetwork: Virtual Network that contains all the VMs, vSwitchs, and virtual systems connected all together using virtual network interfaces.

II. Virtualization and Networking Environment

Virtualization is revolutionizing the data center, delivering capacity escalation and flexible utilization when improving productivity. It is also changing the network by adding a rapidly growing "virtual network" of virtual machines (VMs) connected to each other and to the physical network through virtual switches. Then, local switching is required between different VMs within the same server, with other hypervisor's VMs and with the physical network as well. This feature is provided using a software-based virtual switch.

From a security perspective, we need to study the vulnerability vectors and surface attacks to understand the risks and propose solution when connecting such virtualized network to the physical network and the cloud [2].

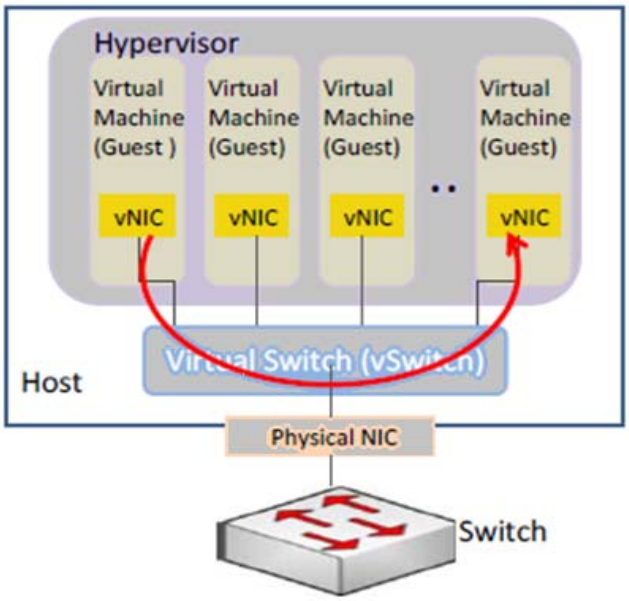


Fig. 1. Virtualized network architecture

A. *Virtualized plateform vulnerabilties*

Hosting multiple components on one physical system, leads to greatly increase the potential impact if an attacker gains physical access to that host system or lunch an arp based attack or a denial of service against it.

Since each Hypervisor held hudred of VMs with eachone has its own Operating System and its own vulnerabilities, each succefull attack againt the Hypervisor, will lead to compromise all the VMs inside it.

B. *The hypervisor attack surface*

Virtualized plateforms are vulnerable to all types of attacks for normal infrastructures. However, security is a greater challenge as virtualization adds more points of entry and more interconnection complexity.

The hypervisor present to the guest VM a view that appears as though the VM's operating system and applications are running directly on the hardware. The hypervisor achieves this by emulating the underlying hardware and arbitrating access to it. Realizing this functionality requires a complex software routines that require a frequent interaction between the guest VMs and the hypervisor. This interaction is a security threat which a malicious VM can utilize to attack the hypervisor and exploit bugs in the hypervisor or to attack another VM inside the hypervisor.
Unlike physical servers, virtualized systems have two boundaries:

1. Physical boundarie security

Within the Data Link layer of the TCP/IP protocol stack, Address Resolution Protocol (ARP) is used convert IP addresses to Media Access Control (MAC) addresses, to assure computers communication in a Local Area Network (LAN). When a node wants to send data, it refers to the ARP cache to find out the MAC address corresponding to the target IP address.
ARP implementations update their cache of ARP to IP mappings whenever a reply is received. If the MAC address reported in the packet for the given IP has changed, the new value will overwrite the old one.
That way makes possible many sorts of attacks based on the "man in the middle" attack technique, by sending an ARP reply packets to perform ARP cache poisoning against the VMM that represents the management channel of the hypervisor.

This attack scenario will start by sending an ARP reply to the VMM (the hypervisor managemnt interface) stating that management client's IP maps to attacker's MAC address, and another ARP reply to that management client stating that VMM's IP maps to attacker's MAC. Since ARP is a stateless protocol, the VMM and the management client B assume they sent a ARP request at some point in the past and update their ARP caches with this new information.

We propose at this point to use an ARP Poisoning that is the basis of more complex attacks, by sending an ARP reply packets to perform ARP cache poisoning against the VMM that represents the management channel of the hypervisor.

Many higher level protocols such as IP, TCP and even SSL depend on ARP. The inherent weakness in the ARP protocol directly affects the security of these higher level protocols. As we have seen, these attacks are relatively simple to employ, as there are a wide variety of automated tools available, while any defense against them is minimal. Security measures such as switched networks and hard coded ARP tables do not offer great protection against ARP poisoning attacks.

To deal with such attacks, a security layer should be added: EAP-TLS – Transport Layer Security.

EAP TLS is one of the most commonly implemented EAP type for securing LANs through a RADIUS Server. Each machine must have a certificate that a RADIUS server can validate. Likewise, the RADIUS server must have a

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

certificate that the server can validate. This is referred to mutual authentication. This is true if both parties can validate the other's certificate. This is typically done by having both certificates issued by one Certificate Authority (CA), and for each party to have the CA's certificate.

Pros:

- Client 802.1x is included in Windows and Linux operating systems
- EAP-TLS is resilient to man-in-the-middle attacks
- It provides explicit mutual authentication between the workstation and RADIUS server

Cons:

- Requires the complexity and expense of a CA to support the workstation and RADIUS server authentication
- Requires certificate distribution and administration

2. Virtual boundarie security

The biggest challenges after securing the Hypervisor is to maintain and secure all of the VMs, since many instances and configurations can be rapidly created or modified.
Hypervisors can allow VMs to communicate amongst themselves, and this communication will not even go onto the physical network and can't always be seen as it's carried by the hypervisor, then it is not easy to secure it.

The contents of each guest OS is a virtual disk, stored as a file. If this file is accessed, copied, or modified on the host by an unauthorized party, then the privacy and integrity of the VM is compromised. Likewise, if an attacker accesses the host and directly modifies the hypervisor, then he will be able to run arbitrary code. The vulnerability in the hypervisor (or configuration) allows any virtual guest to "break out" into the host environment and affect other virtual guests.
Inter-VMs communication refers to connection between co-resident virtual machines in a physical machine. A efficient communication is expected because the hardware is shared including disks, memory and others.

Therefore, the hypervisor should strictly control communication between VMs and limit resource consumption of each VM to a finite bound and to prevent attacks on vulnerabilities of VMs. So, but it is absolutely essential to secure the host and each guest OS in order to create a secure virtual environment, Inter-VM communication traffic never touches the physical network, making it invisible to physical network monitoring tools and unprotected by physical network security.
Uncontrolled network with no enforceable security policies is a big concern. Since there is the potential for privilege escalation when VM workloads with different trust levels. This risk is amplified when VMs move from a host to another.

To resume, Virtual networks can be configured to be completely isolated from all other virtual and physical networks. Or, if necessary, they can be configured to have limited isolation on the network until the point of connection to the physical network as detailed below:

- ***Network isolation***

To configure a virtual machine to have complete network isolation, each virtual machine must be assigned to only one internal virtual network. This virtual network must be configured so that it does not use a physical network adapter. Once a virtual network is attached to a physical network adapter, it is exposed to the same security risks as that physical network adapter.

- ***Network packet isolation***

Virtual machines should not intercept network packets from the host operating system. Similarly, the host operating system should not intercept network packets from a virtual machine. This isolation is enforced by the virtual machine network services driver, which determines whether a network packet is routed to the host operating system or to a virtual machine

III. Network Access Control for Virtualized Network

Virtualization breaks traditional security models by creating new attack surfaces--guest-to-guest, guest-to-hypervisor, network/external-to-hypervisor.

It introduces another switch layer into the network topology, the vSwitch that is invisible to traditional network security techniques and products.

As detailed above, access controls and proper network segmentation are key requirements in many compliance mandates. Indeed, creating network boundaries and enforcing traffic flow among distinct network segments are a security best practice that should be considered fundamental to securing both physical and virtual environment.
Specific threat vectors include exposure of traffic to attackers and sniffers, as well as common network-based attacks such as spoofing and man-in-the- middle. We intend to virtual network components within virtualized network and a number of security settings impacting traffic flows among the host and virtual guests.
With the increasing use of the virtualization and the cloud computing concepts, it becomes necessary to think about efficient solutions to ensure the virtual environment security.

In this section, we will propose our vision to securing the virtual networks by using virtual security solution for virtual platforms.

We propose a distributed solution to add NAC[3] mechanism to protect the hypervisor itself and the VMs from network attacks, based on the Access control technology and deep inspection solution to inspect traffic inter VM and traffic between the hypervisor and physical switchs. This will allow us to:

- Manage flows
- Control the virtual and physical switches
- Manage and control access for users and machines
- Tracking malware source and locate it quickly

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The virtual firewall and IPS/IDS use adapteded technology to meet the virtual environment security challenges; by enforcing a rule-based policy for each VM, such virtualized network control, is based on a well designed security architeture, to inspect trafic inside virtual plateforms, and inter-VM traffic.

To achieve this high security level, Access Control features should be implemented to strengthen the isolation between virtual images, and allow VMs to run in a separate security context, with the appropriate policy.

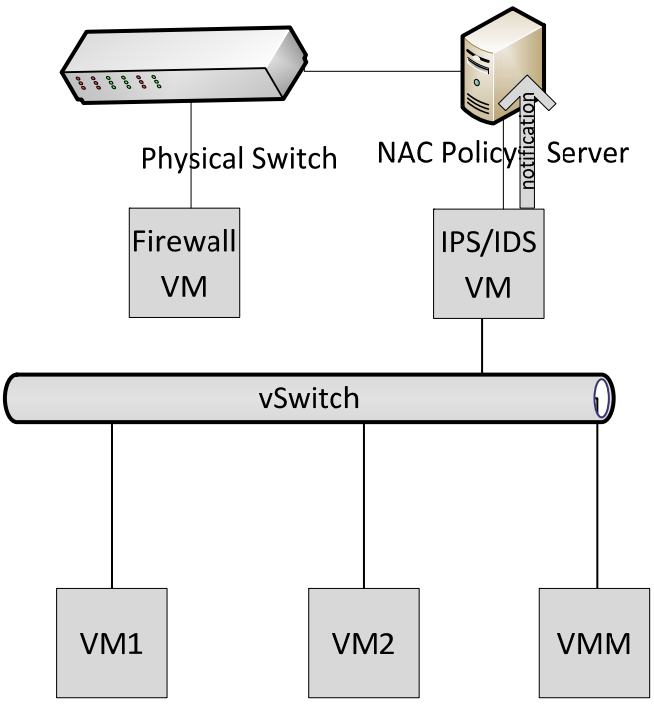
VLANs should be used to isolate traffic from one customer VM to another customer VM. This requires VLANs to be extended beyond the core switching infrastructure. There could be an issue with scaling VLAN capabilities to support very large clouds.

At this point, we will study, in the following subsection, virtual network architecture to understand the security issues inside such environment. Then we will propose the implementation of such open source platform, based on a virtual Firewall, Virtual IPS/IDS and a NAC policy server in order to mitigate the attacks against the hypervisor end secure the communication inter-VMs.

A. The proposed solution components

Our proposed solution is based on the following security components:

- Virtual Firewall
- Virtual IPS
- NAC policy server



1. Virtual Firewall

It controls the access between security zones within the virtual or cloud environments using policy rules. For higher end workloads, there is quite a bit more architecture to be done to make use of a virtual firewall, as there are limits with nearly any technology.

2. Virtual Intrusion prevention/Detection system

The IDS mode is used for aggregating network traffic from multiple physical and virtual traffic sources, such as switches and Wire TAPs, into one centralized IDS sensor or IDS cluster. In such case, IDS is able to restrict traffic by sending resets or requesting a firewall or Inline IPS to isolate the segment from other networks using a blacklisting mechanism.
When we have to protect large Local Area Network (LAN) segments, IPS mode is good to block attacks, since it is able to identify a clear threat path, such the case of traffic from an Internet attacker to DMZ segment.

.

3. Virtual NAC Policy Server

The IPS/IDS system will observe the network traffic and notify the NAC server in case potential suspicious network activities are detected. For this reason, we use an IPS/IDS VM in such a way that it is acting as IPS virtual appliance. It sends alerts to the NAC server based upon malicious traffic that was observed, and then NAC server changes the corresponding switch port vlan to contain the potential risk.

B. How the proposed security solution works

Basically this is an open source solution, and each component handles a specific task in order to detect and prevent network attacks.

- The NAC policy server supervise, assure the correlation of decision based on the traffic inspection result, and administer the switch accordingly
- The Firewall implements the policy access rules to prevent unauthorized access.
- The open source IPS/IDS snort is composed of different components; each one is responsible for a particular task in the prevention and detection process:

1. Sniffer: Packet Sniffer Taps into network;
2. Preprocessor: examine packets for suspicious activity
3. Checks against plug-ins
4. Port scanner plug-in
5. Detection Engine: the snort intrusion detection process based on :
   - Snort signature-based
   - Implemented via rule-sets
   - Rules: the rules header contain some important information like “Action to take”, “Type of packet”, “Source, destination IP address”, etc.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

6. Alert Logging: this module is responsible to trigger warning and alert to the NAC policy Server that administer the Switch using snmp and order it to stop or limit the access for the suspected VM.

- ***LAB and experimentation***

The proposed solution is based on following free products:

- Snort [4]
- Vmware ESX [5]
- Iptables [6]

C. Cloud Security Identity-based Policy Enforcement

It is particularly challenging to define granular user roles, to do separation of network administrator from server administrator, and access policies across a distributed, virtualized environment. The risks of failing to properly define roles and access policies are significant because access to the hypervisor can potentially provide broad access to key infrastructure components (including switches, firewalls, payment applications, log aggregation servers, databases, etc.). Because of the increased accessibility to multiple virtual devices and functions from a single logical location or a user, monitoring and enforcement of appropriate separation of duties is crucial in a virtual environment.

IV. Conclusion

Our proposition aims to reduce the risk and the attack surface, but it doesn't fix all security issues, especially that related to users identity in the cloud. In addition to this, there is the lack of hypervisor-VM visibility, accountability, and consistency of the management model, to effectively troubleshoot roles and responsibilities inside virtualized platforms.

Such important security feature still presenting a security challenge for the virtualization and cloud technology.
As a perspective, we count to extend our future work to this security area.

References

[1] Dave Shackleford, Virtualization Security: Protecting Virtualized Environments book, Wiley, November 2012.
[2] David Newman, “Is Your Network Ready For Cloud Computing?,” Cisco, 2012.
[3] A. Lakbabi, G. Orhanou, S. El Hajji : “Network Access Control Technology - Proposition to contain new security challenges”, International Journal of Communications, Network and System Sciences, Vol. 5, No 8, August 2012.
[4] Open Source Network Intrusion Prevention and Detection System, http://www.snort.org, by Sourcefire April 2013.
[5] Ruest, Danielle and Nelson Ruest, “Virtualization: Beginner’s Guide”, McGraw Hill Books, 2009
[6] Open Source packet filtering software, www.netfilter.org, by Core Team, March 2013.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)