# *Security of Virtual networks in cloud computing for education*

Achraf Bousselham,
National School of Applied Sciences,
University Ibn Tofail,
Kenitra, Morocco
bousselham.achraf@gmail.com

Tayeb Sadiki,
Electronic, Logistic,informatics,and
Telecom Laboratory
Technopolis Rabat-Shore, Int. Univ. of
Rabat, Sala el Jadida,Morocco
tayeb.sadiki@uir.ac.ma

***Abstract***

***Cloud Computing emerge as new IT paradigm, which aims to provide applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services, by sharing resources to achieve coherence and economies of scale . However, one of the most important occupations of cloud computing today is to ensure the security of the infrastructure. This paper brings an introduction to the virtualization in a cloud environment. In the first place we will describe the principle of operation of a virtual network in the platform Xen, then we will discuss some possible attacks on these networks. In the end, we will introduce an analysis of some models of IDS applied to the cloud computing.***

***Keyword:*** ***Cloud computing, Security, IDS, Xen, Attack, Vulnerability, IAAS.***

## I. INTRODUCTION

Cloud computing is a delivery IT model, it is a computer service that allows to offer both software and hardware as a service on demand on the internet. It improve IT efficiency, agility and reliability, to reduce the cost of IT technologies. There are many companies that participated to deliver cloud solutions in various ways for example Amazon, IBM, Google, Oracle, Microsoft, HP and Salesforce.

The concept of cloud computing is very new in the computer field, It can be termed as the next evolution of computing, cloud computing can be defined as:

- A computing platform that allows sharing of resources in hardware and software infrastructure, and it offers a platform for application development.
- A technology, which uses service-oriented architectures which is based on virtualization offered by companies that have servers of high power with a large storage capacity.

It includes three categories of services: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

- Software as a service (SaaS): is any application or software that is running on the platform of the cloud provider, it is a service with access by permission. To access you can use a light client (for example: web browser) to send data a receive results. In addition the consumer has limited authority because he has the right to set up certain parameters so that it has no knowledge on the infrastructure used by the provider of the cloud.
- Platform as a service (PaaS): In this service model, the service provider provides basic accessories, which includes the operating system, network, servers, and development tools that allow different users this service to develop their applications.
- Infrastructure as a service (IaaS): in cases where a user of cloud computing has developed its own applications and he needs just to the hardware infrastructure to deploy. The service provider offers a complete infrastructure on demand with different components (processors, network, storage, etc.)

One of the main reasons for which the enterprises to are slow in accepting and moving towards the platform of cloud computing, is security issues and challenges associated with it.

Since these services are accessible via the internet this can be the cause of several attacks. However, the security must be integrated into all aspects of the cloud platform for users to trust the cloud.

One of the major challenges of security in the cloud is secure virtual networks that allow communication between different virtual machines of the IT infrastructure. By that there are several types of attack that cannot be controlled; however the attacker will have full access to the infrastructure.

In this article, we focus on the issues of security in virtual network and we select the open source Xen hypervisor project as a platform for research. Through this work, we discuss and analyze some attacks on networks and we present a model that allows IDS to detect certain attacks to secure the cloud infrastructure.

## II. VIRTUAL NETWORK

Network virtualization is an effective approach to solve the problem of ossification of the Internet. It has become a promising way to support many heterogeneous networks on physical ones.

The standard of virtual network is a process for creating a network independent by decoupling network services from the underlying physical network hardware.
Different tools can provide a virtual network for a virtual machines and which allows to always staying in the physical network.

### *A. Project "Xen" hypervisor*

The Xen hypervisor originally is a research project at the University of Cambridge; it is the powerful virtualization industry standard open source. Since the release of the Xen virtualization market has evolved.

Today, the Xen hypervisor is becoming the fastest solution and the most secure infrastructure virtualization [1].

Xen has the opportunity now to support different operating systems as guest (Windows, Linux, Solaris, and various versions of the free BSD).

A Xen system has multiple layers, the lowest and most privileged of which is Xen [2].

Xen runs different operating system in secure virtual machines. It creates several areas, the first is field 0 that is automatically created when starting the system with a special privileges.

Xen provides two modes for users to configure the virtual network [3].

1. Bridge (bridge mode)

In this mode, Xen fixed the interface of the virtual machine directly to software Ethernet Bridge connected to the physical network.

The administrator can manage the demands of virtual machines in DHCP network in the same way that the processing of applications for common network DHCP request.

The below figure illustrates the structure of a network and bridge virtual interface (VIF) Bridge Xen [4].

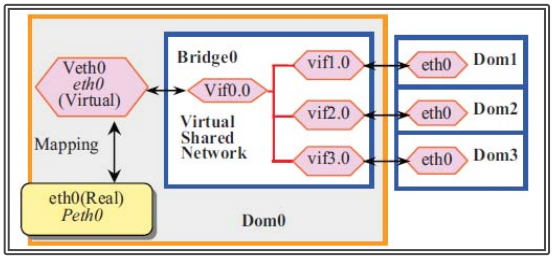


Fig 1 : Structure of a network bridge and the bridge VIF Xen [1]

2. Route

The 'Route' virtual network configuration mode allows the administrator to create a peer-to-peer connection between the privileged domain dom0 and each virtual machine.

A MAC and IP addresses must all be defined in advance by what routes to each virtual machine must be added to the routing table of dom0 before a virtual machine is started.

Thus, in this mode, each instance of virtual machine created by Xen she will assigned a free couple of address (MAC/IP) and released when the virtual machine is completed. DHCP does not work in Route mode. The below figure represents a structure of mode Route in Xen.

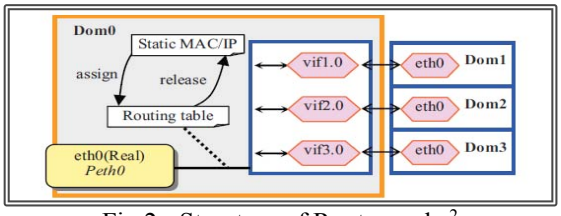


Fig 2 : Structure of Route mode [2]

*B. Vulnerability of virtual networks*

The virtual network significantly affects the interconnectivity of VMS, which is one of the greatest security challenges in the design of Cloud Computing Platform. Which raises a number of security issues.

However the safest is to isolate each virtual machine and use a physical channel dedicated for each host-VM link. However, as we have already described ways of configuring virtual networks of the Xen hypervisor, as there are other hypervisors (VMware ESXi, Virtual-box) that offer virtual networks to connect virtual machines with either the road or Bridge mode.

The problem in these two modes, when virtual machines are running on the same physical machine finds that the performance of inter-VM communication is near-native. Consequently, the mechanism of isolation can be quickly broken through various existing vulnerabilities in virtual networks:

- Sniffing a virtual network: in the mode of bridge (Bridge), the bridge plays the role of a "virtual Hub". All machines virtual use the 'virtual hub' to communicate with the network, in which a virtual machine is able to sniff the virtual network using the tools of sniff as "Wireshark" [5].
- Spoofing the virtual network Route mode, this last plays the role of a "virtual switch". The virtual switch uses a virtual interface dedicated to connect each virtual machine. In this case the virtual machine can make an "ARP spoofing" attack spoofing of the address resolution protocol, all packages will be redirected to the attacker as he will be able to sniff all packets going or coming from other machines, [6].

As can illustrate the process of spoofing a virtual network as follows:

The switch starts and initializes the routing table and sends an ARP command to other startups machines. The routing table collects the necessary information (port, IP address, MAC address) based machines.

Generally, the application of a security mechanism depend the network technology and network topology, and the network perimeter.

Include security equipment as (firewalls and IDS / IPS) is always placed on the edge of the network to keep the protected system. With virtualization, virtual machines located within the same server can be assigned to different

[1] Source : Network Security for Virtual Machine in Cloud Computing

[2] IDEM

areas of logical security; however virtual machines belonging to different servers can be on the same logical security domain.

However traditional security policies that are adapted to physical machines cannot be applied to a virtualized environment.

However, we must develop a new security policy that can be much more suited to the virtual environment (virtual machines, virtual network computing), to ensure the safety of the physical and virtual network simultaneously.

We illustrate other types of vulnerability and attacks that can be launched on the virtual network:

- Network Infrastructure attack on virtual network: The network infrastructure providers can move to management practices break by introducing monitors network traffic virtual networks, through this management we will violate privacy and violation privacy.
- Virtual Network attack on virtual network hosted jointly: In the case where a network hosts a set of virtual network, the proposed increase network security solution is used logical isolation between them. However, isolation of resources may result in a set of network attacks. An attacker can take advantage of shared infrastructure resources to assess vulnerabilities el features virtual networks hosted jointly. Vulnerable virtual network could be a competitor of the virtual network running a specific service. Once the attacker virtual network is instantiated, it benefits from the implementation and launches an attack in order to steal information from the network vulnerable.

## III. ATTACK ON VIRTUAL NETWORK

### *A. DOS attack*

The attack of denial of service (DOS) in a virtual environment is a serious threat for virtual machines. This attack may be the result of a misconfiguration of a hypervisor that allows a single virtual machine to consume all available resources, so to deny other machine running on the same machine physical and disturbed the operation of hosts on the network due to the shortage of material resources. However, hypervisors to prevent any VM to win 100% usage of all shared hardware resources, including CPU, RAM, network bandwidth, etc. In addition, an appropriate hypervisor configuration allows extreme resource consumption to detect and take the solution, for example, automatically restart the virtual machine.

### *B. DDOS attack*

A denial of service DOS attack is an attempt to malicious purpose, which can be operated by one or more persons. When this attempt is derived from a single host on the network, it is a DoS attack. In addition, it is also possible that many malicious computers coordinated to flood the victim with a DOS attack, so the attack takes place simultaneously from several points. This type of attack is called an attack denies distributed service, or DDoS attack [7].

The DDOS attack can be performed using automated tools. There are several automated such as Trinoo, TFN, TFN2K, Stacheldraht, Shaft attack tools, Knight etc.

Those tools are based on the knowledge of the identity of the other in IRC (Internet Relay Chat). Long ago, the transport layer was the main target of the exhaustion of the resources of liaison between network devices.

However today the most answered target is web applications. The use of DOS attacks require the same traffic characteristics, syntax and network level as a legitimate user, making it much more difficult to detect attacks. Attacks at the application level are http GET floods, etc. SQL Injection Attack. DDOS attacks are difficult to distinguish them from facing web applications traffic. In addition, the target system can be affected the performance of the equipment, because the target server can be damaged by small connections and traffic.

## IV. INTRUSION DETECTION SYSTEM (IDS)

### *A. Principle of IDS*

The intrusion detection system acquires information on system to perform a diagnosis of system security. Using this type of system to discover various security breaches, flaws and the different possible threats that can lead to a violation of the system.

This system includes a set of information used to detect intrusions is a kind of knowledge base attack, for example the configuration information of the current system status and information audit of writing events that occur on the system.

Nevertheless systems available intrusion detection cannot detect the attack which may include for example distributed DDOS attacks all types.

### *B. Existing technique*

In order to implement an IDS model dedicated for use in cloud computing to improve the security of the latter and detect various possible threats to the cloud. In this section we will exhibit two models using the IDS in the cloud.

#### 1. Cloud IDS

In the first model of distributed cloud IDS uses a technique called "multi-therad" which improves the performance of IDS in cloud infrastructures. In addition, the distributed IDS is a "Network Intrusion Detection System" NIDS that uses multiple sensors to monitor network traffic and to check the malicious packets. The system sends alerts to the monitoring intrusion by third parties, it can provide instant reporting system management system of the organization of the cloud user with an advisory report to the service provider cloud computing.

There is also the possibility of deploying IDS at the hypervisor that allows the administrator to monitor virtual machines and the hypervisor at the same time. In contrast

with the large volume of data flowing through the cloud, a problem of performance management will arise as the overhead of virtual machine that hosts the IDS and drops packets. In addition, if the machine that hosts the HIDS "Host Intrusion Detection System" itself is attacked HIDS will be neutralized.

In this model, the network-based IDS would be most suitable for cloud deployment as infrastructure. NIDS will be placed outside the server virtual machines on the network points such as switch, router or gateway for monitoring network traffic for a global vision system. The NIDS will always be confronted with the volume of data through the access rate to the network cloud computing environments.

To manage this large number of packets flowing through a cloud environment can use the solution of an IDS "Multi-therading" this solution is capable of handling a large amount of data and it reduces the number of lost packets. After the IDS treats all packets it passes alerts to a monitoring service, which directly informs users of their cloud attacked system. In addition, there also with the monitoring service providers cloud services can have expert advice on the configuration and the towers of intrusion into the system. The figure below illustrates the proposed IDS model.

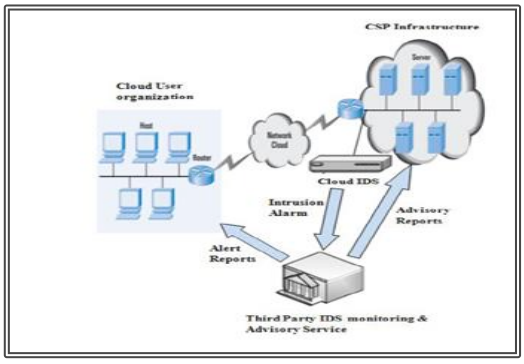


Fig 3 : Model cloud IDS

This cloud model IDS is proposed for distributed cloud environments is based on three modules:

- Module capture and queue
- Module for analysis and processing
- Module report

The capture module is used to capture the data packets to be sent to the queue for the analysis.

The analysis and processing unit in turn receives the data packets from the shared and to analyze it with the signature database and a set of predefined rules. Through analysis and effective treatment of bad packets will be identified and the alert is generated.

The reporting module will read the alerts queue shared as it prepares reports alerts. However, there is guarded by another party and a counseling service with experience and report user information cloud will be generated immediately at the end it sends a full report on consultants for the provider cloud services. The figure below illustrates the project organization multithreaded IDS.

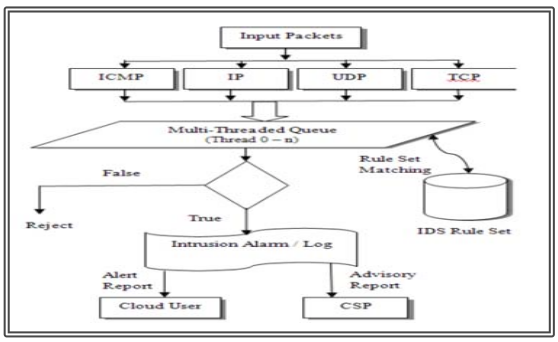


Fig 4 : the project organization multithreaded IDS

2. Virtual Machine ID (Intrusion detection)

The second model is a strategy IDS that can be reliable in cloud computing environments.

This model is proposed to deploy each virtual machine computing platform ID (Intrusion Detector) in order to divide the network traffic overload on different IDS. HOWEVER, with the implementation of an ID on the VM you will avoid the problem of strategy position of IDS. With this model we will ensure a reduction of attacks as possible.

There are several technical Proposals to use of the IDS in computing platforms all which include the following examples:

- The first is a theoretical model ID in the cloud, using a single controller ID, Which Creates a small single instance of IDS the for each user [8]. This instance can be used in several controllers and node, each node can contain multiple instances of IDS users. HOWEVER, the analysis stage of the Proceeding ID for each user is set in the controller of the IDS [9].

- By applying the ID for each virtual machine is an idea that was proposed by several researchers [8], this technique can increase the effectiveness of ID by assigning a detection system multi-level intrusion and log management in cloud computing. In this sense, users will receive an appropriate level of security, which will emphasize the degree of ID applied to the virtual machine and as well on the stage prioritization of log analysis documents. This model of multilevel security solves the issue of efficient use of resources.

- A cooperative IDS system has been proposed for detecting DOS attacks in the network cloud. As the proposed model is a distributed system where each IDS ID is composed of three additional modules: power, communication and cooperation, in addition to the Snort IDS system.

To detect and analyze the attacks in a cloud environment, we propose the following model is to install and configure Snort on each virtual machine. With this method we will avoid all the overloads and the impact of the attacks can be reduced. During an attack the IDS alerts will, which will be stored in MySQL placed in Cloud Fusion Unit (CFU) of the front server. However, a single database is

proposed to be used to reduce the risk of data loss, to maximize the use of resources within virtual machines and simplify the work of the administrator of the cloud, which will all alerts in the same location. Another idea is to add a management unit of IDS that can analyze the results using the Dempster-Shafer theory of evidence based on three values. Cloud Fusion Unit (CFU) consists of 3 elements: MySQL database, EPS calculation and evaluation of attacks.

### *V.* COMPARISON OF THE TECHNIQUES OF IDS IN THE CLOUD

Each of the approaches presented above tries to address the issues of security of virtual networks, each of which offers an advantage that differentiates it from the other and that can give good results in cloud security network. For this we quote below the different benefits of each model:

For the model which proposes to install IDS optimized for cloud computing this model offers the following advantages:

- It allows to manage a large volume of data in a cloud computing environment with a single node through a multi-threaded approach.
- There may be a reduction of the memory consumption and the rate of packet loss in order to improve the overall efficiency of the cloud.
- Another tracking service and advice that has been proposed to manage the intrusion data and generate reports aims to for cloud users and providers of cloud service.
- A final highlight of cloud is that IDS is capable of performing simultaneous processing of data analysis, which is an effective approach.

The second model IDS distributed across multiple virtual machines that is cloud computing. This model, in turn, offers the following advantages:

- Through this mechanism of distribution of IDS on the set of virtual machines, which is the cloud reduces the overhead and the impact of the attacks will be reduced.
- All alerts are stored in a MySQL database which facilitates the management tasks for the administrator of the cloud.
- It offers a management unit and analyzing the results of the IDS.

Through the various benefits mentioned above both IDS models we can conclude that both models can be beneficial for virtual networks and cloud computing if you combine the two models can have other much more interesting results.

## VI. CONCLUSION

Security is the biggest concerns about cloud computing, that takes a great importance among the cloud users. Through this article, we discussed the security of virtual networks in cloud computing and which is essential for its operation. Thus, we present some models of intrusion detection system IDS to compare them and expose the various benefits of each model of IDS applied to cloud computing. Our research can be extended in several directions.

The first to be much faster than we will for example implement patterns proposed IDs in cloud computing in the detected aim points of weakness of these models as well trying to propose a new model that combines between previous models and allows furthering improving the security of the cloud.

## REFERENCES


[1] «Xen Hypervisor goes Standard,» 9 2010. [En ligne]. Available: http://www.serverwatch.com/tutorials/article.php/3646516/Xen-Hypervisor-Goes-Standard.htm.

[2] Xen, «Xen Documentation Support,» Juillet 2010. [En ligne]. Available: http://www.xen.org/support/documentation.html.

[3] «Xen Networking,» 7 2010. [En ligne]. Available: http://wiki.xensource.com/xenwiki/XenNetworking.

[4] Y. D. W. Y. Hanqian Wu, «Network Security for Virtual Machine,» *Science Foundation,* pp. 19-21, 2013.

[5] «Wireshark,» 8 2010. [En ligne]. Available: http://openmaniak.com/wireshark.php.

[6] «An Introduction to ARP Spoofing,» 11 2008. [En ligne]. Available: http://www.cse.iitm.ac.in/~jvimal/cs410/arp-spoof.html.

[7] D. P. H. T. A.M. Lonea, «Detecting DDoS Attacks in Cloud Computing Environment,» *INT J COMPUT COMMUN,* pp. 70-78, 2013.

[8] S. N. e. a. Dhage, «Intrusion Detection System in Cloud Computing Environment,» chez *In International Conference and Workshop on Emerging Trends in Technology*, TCET, Mumbai, India, 2011.

[9] A. Haeberlen, «An Efficient Intrusion Detection Model Based on Fast Inductive Learning,» chez *Sixth International Conference on Machine Learning and Cybernetics*, Hong Kong, 19-22 August 2007.