Cloud Infrastructures Protection Technique Based on Virtual Machines Live Migration

Jan Fesl[1], Vineet Gokhale[1], Marie Doležalová[1], Jiří Cehák[1], Jan Janeček[2]

1. Institute of Applied Informatics, Faculty of Science, University of South Bohemia, CZECH REPUBLIC, České Budějovice, Branišovská 31a, email: {jfesl,vgokhale,dolezm01,jcehak}@prf.jcu.cz

2. Department of Computer Systems, Faculty of Information Technology, Czech Technical University in Prague, CZECH REPUBLIC, Prague, Thákurova 6, email: janecek@fit.cvut.cz

Abstract: **Cloud computing and virtualization are very popular research areas of the last years. The rising count of running virtual machines brings new opportunities for the malware or intrusion tools. Nowadays, there exist various ways how to detect the potential attack activities. Our paper evaluates such techniques and provides an efficient solution how to link the anomality detectors and hypervisors. This solution provides the way how to eliminate the problems without having to shutdown the running virtual machines.**

Keywords: **IDS, IPS, hypervisor, cloud, security, live migration, virtual machine.**

I. Introduction

The distributed virtualization infrastructures (DVI) are the engines of powerfull data centres, which create the executive parts of cloud environments. The typical virtualization architecture, which is depicted in figure 1, consists of the management node (MN), virtualization nodes (VN), data storage (DS) and interconnection networks (IN). Virtual machines (VM) run on the virtualization nodes, which contain the hypervisors. Hypervisor is the abstract layer between the physical and virtual hardware. There are more principles of virtualization techniques and their detail description can be found in [1]. Nowadays, the most power efficient hypervisors are based on direct cooperation with the hardware using dedicated instruction set.

$$DVI = \{MN, VN, DS, IN\} \quad (1)$$

The virtual machines can be moved during the runtime between all infrastructure nodes. The motion of the virtual machines allows the live migration technique. The detail info about it, can the reader find in [2]. The virtual machines have some limitations like allowed count of CPUs, size of operating memory, size of virtual hard drive or maximal network throughput. All parameters are managed by the hypervisor. The virtual machine lives in its own world and shares its resources with other virtual machines. The level, on which the physical and virtual computers are the same, is the network level, because both types communicate with outer world via the same packets. The virtual computers contain the same operation system like the physical, therefore they can suffer from the same security issues. The virtual machines are interconnected at the same virtualization nodes by virtual networks. The virtual networks can bridge some virtual machines with others or fully separate the network traffic between them.

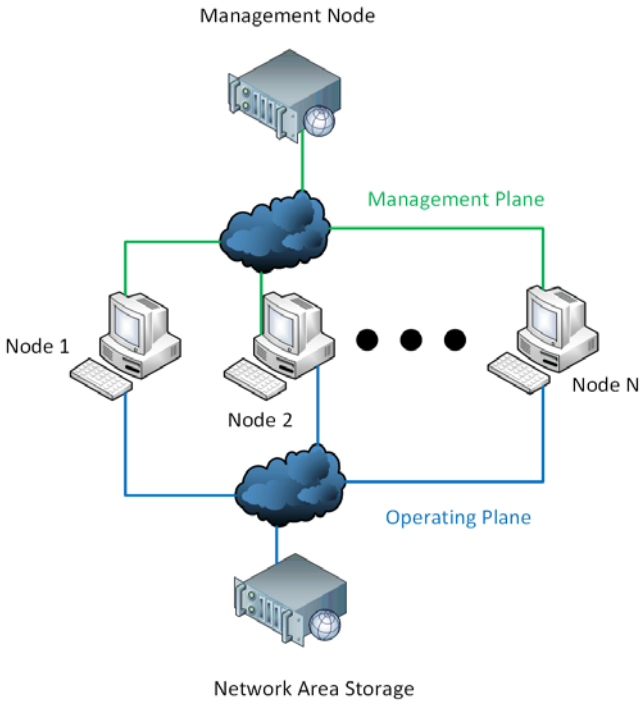

Fig. 1. Typical environment of the distributed virtualization infrastructure.

II. Systems for Intrusion Detection and Prevention

The infected virtual machines can be the sources of potential network attacks. From the network OSI model point of view, the attack types can be divided into L2 and L3 groups. The first group is targeted on the computers and devices placed in local segments, the second group can affect all local and remote devices, which are connected to the computer network.

In the data center environment, the greatest problem for the administrator is, that it is not possible to permanently apply strict firewall rules like limit TELNET, SSH, RDP etc. services, because the users require to install and use various network services. The data centers can't also require from an user a paid antivirus/antimalware protection or firewall. The only one acceptable solution is to suppress the potential issue, but not to drop all other services. The traditional firewalls are

highly efficient, but strictly static and are not very good suitable for the data centers. The efficient way is to use more intelligent intrusion detection (IDS) and intrusion prevention (IPS) systems. Intrusion detection systems (IDS) are an essential component of protecting computer systems and network. To detect computer attacks and provide the proper response this is the main aim of IDS. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network. There are mainly two categories of DSs, network based and host based. IDS is key to detect and possibly prevent malicious activities. In the case, that the issue has been discovered, the administrator is informed by sending the message. Such systems have had the long tradition, but were primary proposed for the common computer networks. The basic structure of such system is depicted in figure 2.

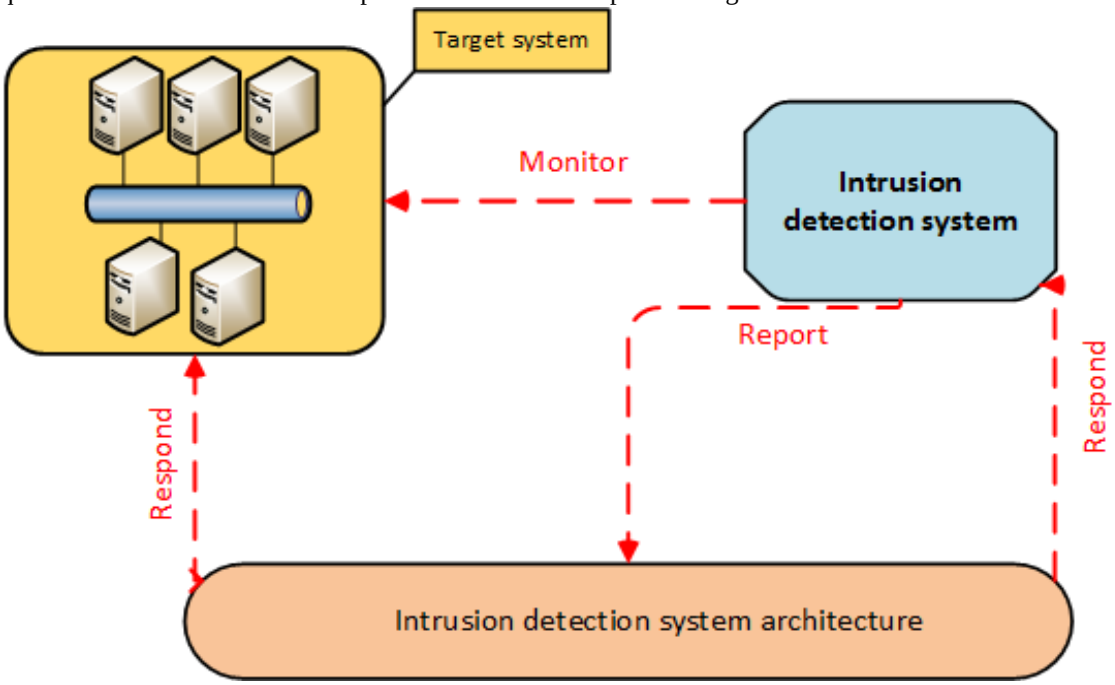

Fig. 2. Main components of the IDS system, which could be used as data center protection system.

The really comprehensive overview of this problematics including algorithms description is listed in [2] and some other in [3]. The basic detection techniques used in IDSs are as follows.

Signature matching

This techniques identify attacks by matching network packet contents against specific attack signatures. These signatures are created using already identified and well-described attack samples, which is time consuming and can take from couple of hours up to several days, which gives attackers plenty of time for their criminal activities. The biggest weakness of this solution is that it is detecting only known attacks, which can be due to smart evasion techniques used by malware limiting. With the growing proportion of encrypted traffic, use of self-modifying malware, and other evasion techniques, the use of a detection technique tailored to catch predefined known set of attacks is becoming irrelevant.

Anomaly-based detection

This concept tries to decrease the human work (e.g. manual creation of signatures) by building a statistical model of a normal behavior and detect all deviations from it. This enables to detect new, previously unknown attacks provided that their statistical behavior is different from that of the normal traffic. While anomaly-based methods are attractive conceptually, they have not been widely adopted. This is because they typically su#er from comparatively higher false alarm rate (not every anomaly is related to the attack) rendering them useless in practice, since network operator can analyze only few incidents per day [3]. That is why the signature based IDS are still widely used even they are not able to detect new types of attack nor to find anomalous behavior of the network users.

In the literature [4], there are known five types of IDS systems, which can be used in the cloud computing.

Host based intrusion detection system (HIDS)

Such system is an intrusion detection system that monitors and analyzes the information collected from a specific host machine. HIDS running on a virtualization node detects intrusion for the virtual machine by collecting information. HIDS observes modification in host kernel, host file system and behavior of the program. Upon detection of deviation from expected behavior, it reports the existence of attack. The efficiency of HIDS depends on chosen system characteristics to monitor. Each HIDS detects intrusion for the machines in which it is placed. With respect to Cloud computing, HIDS can be placed on a host machine, VM or hypervisor to detect intrusive behavior through monitoring and analyzing log file, security access control policies and user login information.

Network based Intrusion Detection System (NIDS)

It is an intrusion detection system that tries to detect malicious activity such as DoS attacks, port scans or even

attempts to crack into computers by the network traffic monitoring. The information collected from network is compared with known attacks for intrusion detection. NIDS has stronger detection mechanism to detect network intruders by comparing current behavior with already observed behavior in real time. NIDS mostly monitors IP and transport layer headers of individual packet and detects intrusion activity. NIDS uses signature based and anomaly based intrusion detection techniques. NIDS has very limited visibility inside the host machines. If the network traffic is encrypted, there is really no effective way for the NIDS to decrypt the traffic for analysis. NIDS can be deployed on edge node interacting with external network. However, it has several limitations. It can't help when it comes to attack within a virtual network that runs entirely inside the hypervisor. In cloud environment, NIDS must be installed by the service provider.

Distributed Intrusion Detection System (DIDS)

This system consists of many IDS over a large network, which communicate together or with a central server that enables network monitoring. The intrusion detection components collect the system information and convert it into a standardized form to be passed to the central analyzer. Central analyzer is a machine that aggregates information from multiple IDS and analyzes the same. Combination of anomaly and signature based detection approaches are used for the analysis purpose. DIDS can be used for detecting known and unknown attacks since it takes advantages of both the NIDS and HIDS, which are complement of each other. In cloud environment, DIDS can be placed on the virtualization nodes.

Hypervisor based intrusion detection system (HIDS)

The proposal of such system is still more in theoretical surface then in some real implementation. From the real world, Hyper-V hypervisor [5] contains the L3 firewall, which can be used for blocking of some attacks. The principle is depicted in figure 3. The greatest trouble is its implementation, which can cause the rapid virtualization technology performance decreasing.

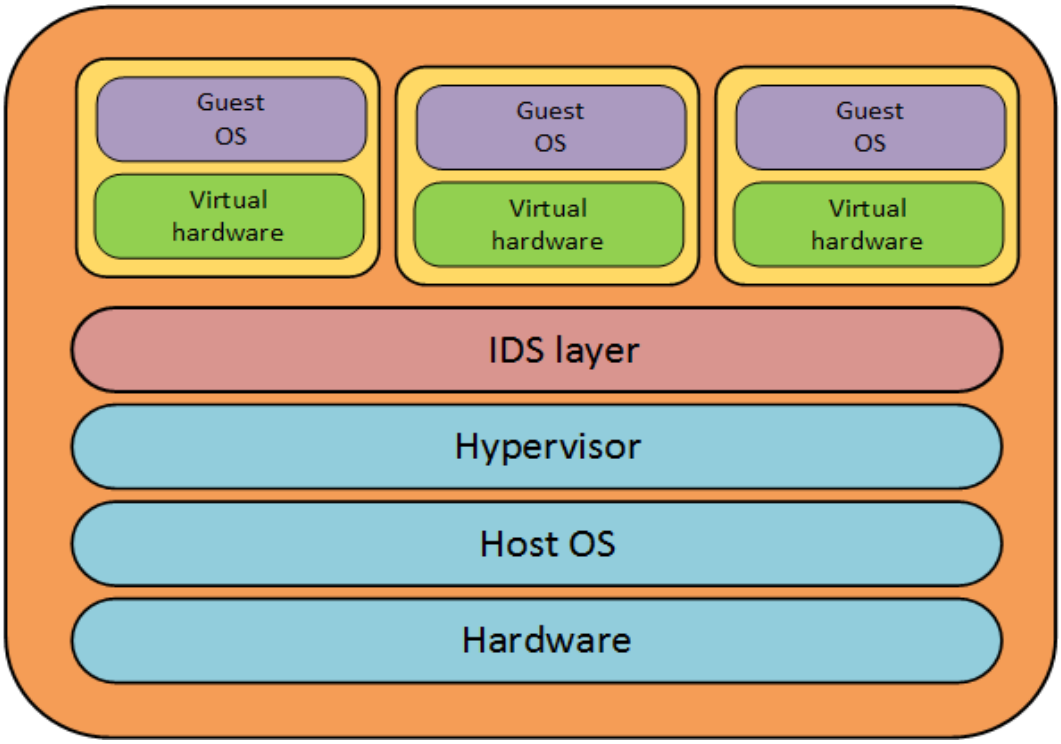

Fig. 3. Hypervisor based IDS, integration with the operating system.

Virtual machine introspection (VMI) based IDS

VMI is the main idea behind out-of-box intrusion detection. VMI is a technique of inspecting VM state by moving the inspection module outside of the VM. The software running inside the guest system is analyzed externally to detect any intrusion. One advantage of this technique is that malware detection continues to work unaffectedly even in the presence of an intrusion. This capability is missing in HIDS and NIDS. In the case of a compromise, HIDS starts reporting falsely while NIDS has limited visibility. More info can be found in [6] or [7] and [8].

III. Protection Technique Based on Virtual Machines Live Migration

The basic idea behind this technique is as follows. The virtualization infrastructure with an active IDS can be divided into three smaller elastic independent groups. The groups differs by the level of network traffic filtering – {A,B,C}. The group A contains virtualization nodes with VMs with no traffic filtering. The group B contains virtualization nodes, which are L3 protected for some outgoing L3 attacks e.g. SSH, TELNET or SMTP. The type of the supressed traffic for concrete VM is strictly evaluated by the IPS. The group C is

called “Quarantine” and has at L2 strictly separated and filtrated traffic off all virtual machines. The specific outgoing L3 traffic is filtered as well - it can be the most of the L3 outgoing traffic, depends on IPS decision. The users, who manage VMs in the group C, can connect to them via the specific terminal service. The IDS directly cooperates with the hypervisors of all virtualization nodes. If the IDS detects some issue, it gives a command to the specific hypervisor which migrates the affected VM to the virtualization node, which is the member of other more secured group. Before the migration of VM, all restrictions proposed by IPS are activated on the destination node. Live migration serves for isolation of potential malicious and health virtual machines. The principle is depicted in figure 4. This principle is further summarized in he following 5 step algorithm.

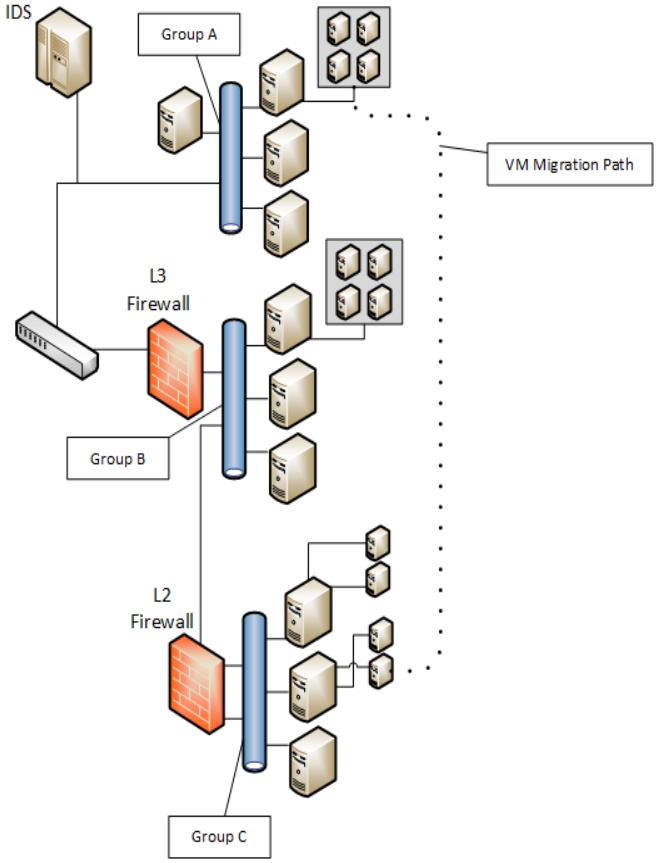

Fig. 4. Live migration protection technique principle.

The 5-step protection algorithm (managed by IDS)

V is the set of new potential affected virtual machines. R is the set of recommendations, which means the new running groups for V-contained VMs, e.g. VM runs in A, but has a security issue, than IDS recommends move this VM from A to B, R({VM,A→B}) .

1. Detect all possible problematic running VMs and store them in V and their recommendations in R.
2. For all VMs in V find the destination nodes (DN) according to R values for their migrations.
3. Apply all L2/L3 protection rules on DN for all VMs in V.
4. Give a command for live migration of all VMs in V to all involved hypervisors.
5. Give a message to all administrators of the affected VMs which VMs were migrated.

The algorithm can be more generalized for the positive reevaluation which means, that if some issue on the VM disappears, the VM can be back migrated to less strict group.

IV. Conclusion

We proposed the new technique which is able to help by the protection of the distributed virtualization network infrastructures. Its deploying depends on the election of the proper IPS element. The greatest benefit of such solution stands in the runtime protection without supressing more services, than it's necessary. The solution requires for the deployment such hypervisor type, which is able to migrate the VMs during the runtime. The advertised technique is suitable for all L2 or L3 network attack types.

References

[1] J. Fesl, "Virtual distributed systems and their application", dissertation thesis, Czech Technical University in Prague, 2017, pp. 10-27

[2] Fesl, J., et al., "Live Migration of Virtual Distributed Computing Systems",, *International Journal of Innovative Computing Information and Control. (IJICIC)* 2015, Vol. 11, Issue 3

[3] J.Grill, "Combining network anomality detectors", *dissertation thesis, Czech Technical University in Prague*, 2016, pp. 3-17

[4] F. Alruwaili, T. Gulliver, "CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services", *International Journal Latest Trens of Computing, Vol. 4, Issue 4*, 2014

[5] A. Lownds et al.,"Windows Server 2012 Hyper-V Installation and Configuration Guide”

[6] A. Riaz et al., "Intrusion Detection Systems in Cloud Computing: A Contemporary Review of Techniques and Solutions", *Journal of Information Science and Engineering, Issue 4*, 2016

[7] T. Hwang, Y. Shin, K.Son, H.Park, "Design of a Hypervisor-based Rootkit Detection Method for Virtualized Systems in Cloud Computing Environments", *AASRI Winter International Conference on Engineering and Technology*, 2013

[8] Y. Tayyebi, D. Bhilare, "Cloud security through Intrusion Detection System (IDS): Review of Existing Solutions", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol.* 4., Issue 6, 2015