ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 146

2nd International Conference on Artificial Intelligence: Technologies and Applications (ICAITA 2018)

The Research for Virtualization Network Security on Cloud Computing

Junjun Sun, Ying Zeng, Guowei Shi, Wei Li and Zhihong Li

Xinjiang Oilfield Data Company of Petrochina, Xinjiang Karamay 834000, China

***Abstract*—The paper describes the benefits of cloud computing for enterprise cost reductions, rapid deployment and dynamic extensions, while the virtualization technology brings some potential hazards and risks to network security. According to the characteristics of cloud computing technology, we put forward the ideas and methods of strengthening network security. The fine-grained control strategies on the virtual machine level and the security domain level improve the security of the virtual network environment.**

***Keywords*—cloud computing, virtualization, access control, security policy**

I. INTRODUCTION

Cloud computing provides users with safe, fast and convenient data storage and network service as an emerging computing model based on the Internet while computing resources can be dynamically deployed and shared in a scalable data center. Compared with the traditional software architecture, cloud computing has obvious advantages of low cost, quick deployment and flexible adjustment, thus these characteristics make it well suited to supply the hardware services, infrastructure services, platform service, software and storage services and so on.

It is the primary characteristics of cloud computing to provide the dynamic computing services with flexible "service contract" as the core business model. However, cloud computing is currently facing many new security threats due to the characteristics of virtualization, no-boundary and dynamic migration, which can threaten the personal privacy, enterprise interests and even state security. Those cloud computing incidents such as the service outrage of Amazon's Simple Storage Service and the documents leakage of Google users have raised concerns over the security of cloud computing technology. In fact, the security problem has become an important factor of restricting the development of cloud computing. The healthy sustainable development of cloud computing can be ensured only if we construct the complete information security system of defense based on the comprehensive analysis of all kinds of security problems.

The virtual computing environment is the biggest difference between cloud computing and traditional IT environment, which makes security problem become more difficult[2]. The different levels of application system can be separated from each other through the virtualization technology including server, software, data, network and storage and so on, which removes the dependency to the physical devices for traditional IT architecture and transforms infrastructure into virtual resources that can be dynamically adjusted on demand. However, the traditional security techniques and strategies begin to fail in the virtual environment and this brings new security issues, such as the attack between the virtual machines or between the VM and the host, the DDoS attack, anti-virus, security isolation of data or application and so on[3,4]. Therefore, this paper proposes the ideas and methods to solve the network security problems of virtualization.

II. OVERVIEW OF VIRTUALIZATION

Virtualization is a resource management technology which can break down non-cutting barriers between physical entities by abstraction and transformation of various computer resources such as server, network, memory, storage and so on, that brings more effective ways of configuration to use these resources[5,6]. The virtual parts of these resources are not limited by the existing architecture, location or physical configuration.

The appearance and application of virtualization technique have been around for more than decades and mainly used on server and mainframe at early stage. However as the capability of PC improved, virtualization also gradually became popular on X86 architecture. Virtualization technology can transform the traditional IT architecture into a more powerful, more flexible and more dynamic one. By integrating multiple operating systems into one high-performance server to maximize the utilization of all the resources, it can simplify IT infrastructure and reduce the difficulty of resources management and also can achieve more with less investment so as to avoid the unnecessary expansion of existing IT infrastructure. The running-time migration of virtual machine provided by virtualization can realize true uninterrupted operation to maintain the business sustainability without paying the big price for buying high availability platform[7,8].

Hypervisor is the most popular approach to virtualization which establishes an abstraction layer between the virtual server and the underlying hardware. There are several representative commercial products such as VMware ESXi and Microsoft Hyper-V, while kernel-based virtual machine KVM is the open source product for Linux system.

Hypervisor can capture CPU instructions and act as the agent for these instructions to access hardware controller and external device. Therefore full virtualization technique can make almost any operating system installed on the virtual server without any change while the virtual environment is transparent for them. Hypervisor works as the host operating

system running on the bare hardware while the guest operating system running on a virtual server managed by the hypervisor.

The application of virtualization technique changes the fixed boundary of business systems, which brings about the necessity of protection and isolation between virtual machines according to business needs. It's necessary to prevent the attacks among virtual machines or between virtual machine and the host, so the network traffic should be monitored and detected effectively to prevent sabotage or virus and so on.

III. NETWORK SECURITY OF VIRTUALIZATION

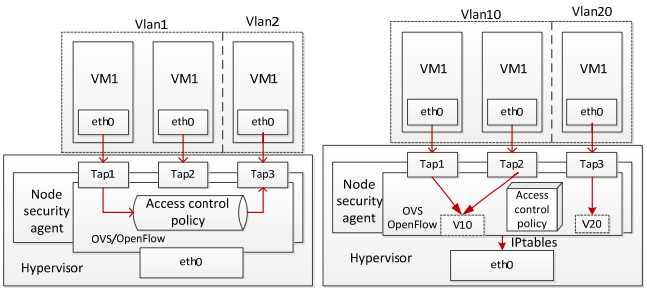
The feature of dynamic boundary for virtualized network in comparison with traditional physical network brings about new challenges to network security control mechanism based on fixed boundary. The traditional physical security devices can restrict and detect the network traffic in and out by deploying the device at the clearly defined network boundary. However, the virtual machines are linked together through the virtual switch and the virtual interface provided by virtual machine monitor layer, as a result, the virtual network can cross the traditional physical network boundary. In order to ensure the security, the fine-grained control strategy over the virtual network should be deployed based on the virtual machine level and the security domain level.

A. Access Control for Virtual Network

The access control mechanism for virtual network can be realized by Open vSwitch(OVS)technique, which would inspect network data packets passing in and out through security agent. The security agent supported by kernel driver layer enables the virtual ports in the route of data flow to load control function and corresponding security policy. This security agent mode can achieve some functions such as security control optimization, policy synchronization and so on. In addition, the Open vSwitch technique can be used to realize many functions such as the access control among vLANs or security domains or virtual machines, the dynamic development and migration for security policies and so on.

B. Access Control Among Virtual Machines

There are two conditions for the communication with each other among virtual machines, the first one is the case when a virtual machine communicates with others residing on the same host, the other one is that residing on different hosts. The access control mechanism can be implemented by estimating security attributes of the security domain or vLAN for these virtual machines combined with the control policies lying in the virtual ports or virtual switches. The following figure demonstrates the access control principle for the above two communication modes.



FINGER I. THE ACCESS CONTROL PRINCIPLE FOR COMMUNICATION AMONG VIRTUAL MACHINES

C. Security Group

Users can create security groups according to the virtual machine security demands and specify a set of access rules for each group. The virtual machine would be protected by the access rules when it added into the security group. So this mechanism enable user to carry out security isolation and access control by creating virtual machines and then selecting specific security group for each of them.

Virtual machines assigned in the same security group would respectively reside on multiple distributed physical hosts, and these machines can communicate with each other. However, these virtual machines in the different security groups were not allowed to communicate with each other by default unless they get the permission through the configurability.

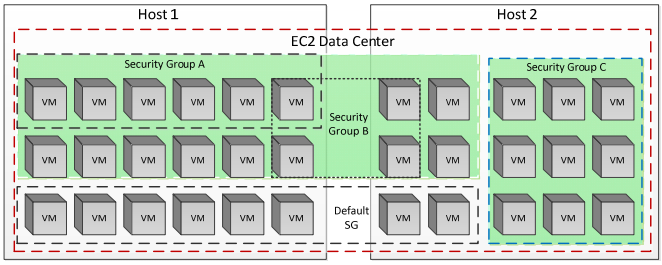


FIGURE II. SECURITY GROUP

D. Dynamic Migration for Security Policies

The dynamic shifts of virtual machine and the dynamic changes of virtual network make the deployment and maintenance for security strategies become more complicated, which would bring the inconsistency causing the risk of failure for these security strategies. The function of dynamic migration for security strategy provided by virtual network protection system ensures the consistency of corresponding security policy in combination with dynamic shift of virtual machine or dynamic change of virtual network. The security agent bands with the management interface of virtual machine can monitor the above shift status and the network configuration change. The cloud security operation center would centrally update the security policy repository and the specific network security policy for the targeted virtual machine that changes, and then all the updated information would be sent to the network control point for that virtual machine so as to retain the consistency of security policies before and after shift.

E. Virtual Network Traffic Monitoring

Compared with the traditional network traffic monitoring it can fully monitor the traffic flowing in the virtual network and among virtual machines in cloud computing data center in addition to the physical network traffic. Differing from traditional monitor systems cloud security monitoring tends to focus on the operation status of cloud data center thereby user can control the general operating situation from a global perspective.

1) Network traffic monitoring: The network traffic monitoring module takes charge of all-round, multi-grained, multi-layered collection, analysis and mining over both the virtual network traffic and the physical network traffic. Exceptions can be discovered for both virtual network appliances and physical network devices as well as server hosts by traffic analysis and application identification. Based on the global fine-grained traffic analysis and critical business performance real-time monitoring it can report the running state of physical and virtual network, which would assist users to identify and trace cyber-attacks as well as to finish fault location effectively. The following figure demonstrates the module of network traffic monitoring and analysis.

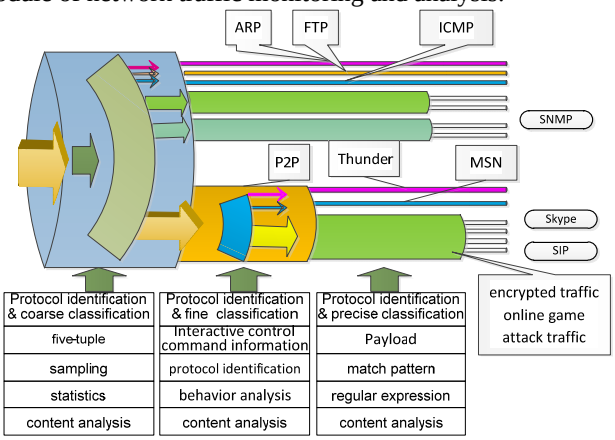


FIGURE III. NETWORK TRAFFIC MONITORING AND ANALYSIS

The above module provides visualized monitoring over virtual network traffic and comparative analysis for historical data baseline including the number of concurrent users, new TCP connections, connection average duration, application response time and throughput, TCP retransmission and reset ratio and so on for the cloud data center. Integrating raw data and message it provides the virtual network performance overall monitoring. Based on the build-in recognition characteristics it can identify various applications precisely. It also analyzes the correlation among services provided by the business applications in the data center. Based on the in-depth data mining technique for large scale traffic it also can draw the relation maps automatically to help users master the real-time dependency relationship among application services running on the internal virtual network.

2) Operating status monitoring: The visualization of data center based on cloud security monitoring system provides users with a means to sense the operating status of the cloud. It will monitor the usage condition of the three virtual resources including virtual nodes, virtual network and virtual storage by means of the unified cloud management platform. For virtual machines it primarily monitor these items including the on-off and exception events, the usage condition of CPU, Memory, traffic and storage. Users can customize the different monitoring dimensions such as time, metric and category and so on. Besides, users also can activate the warning function by setting the threshold parameters and the multiple alarm modes. For virtual network it mainly monitors the changes of network topology, the running state of virtual network appliances and the configuration of virtual ports. For virtual storage it chiefly monitors the capacity allocation, utilization factor and throughput rate.

F. Virtualized Agentless Anti-virus Mechanism

The cloud security solutions prevent virus intrusion by deploying the virtualized agentless anti-virus software in data center. Anti-virus software developers can carry out secondary development to create the virtualized anti-virus solutions based on the API provided by the visualization platform. The anti-virus mechanism can be achieved by deploying the antivirus engine on a specified security virtual machine while installing lightweight drivers on user's local virtual machine.

This agentless anti-virus mechanism only needs to manage the specified security virtual machine without management of virus library installation and updates for every virtual machine. The virus scanning results would share with each virtual machine residing on the host rather than sharing within only one machine so as to improve the scanning efficiency.

Hypervisor can realize the isolation between different virtual machines residing on the same physical host to avoid data theft and malicious attack from the other virtual machine. The isolation mechanism ensures that resources utilization for every virtual machine won't be affected by others. The end users were only allowed to access their own resources such as hardware, software and data while not allowed to access others resources thereby retaining isolation security.

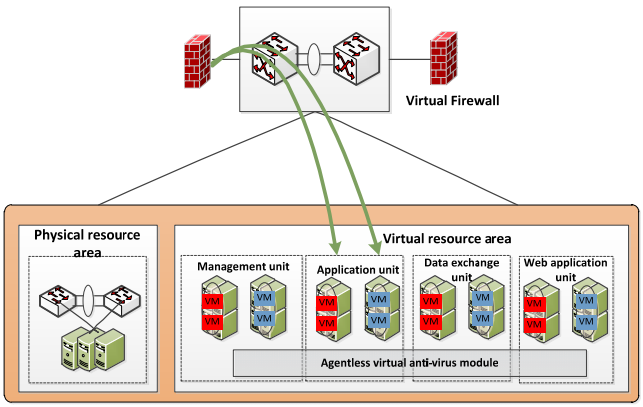


FIGURE IV. VIRTUAL MACHINE SECURITY SOLUTION

1) Traffic diversion solution: The standard VEPA traffic diversion scheme introduces the invisible flow in the

secondary layer of vSwitch into the physical security devices in order to realize the basic isolation and several advanced security features such as IPS, Anti-virus of layer 4 to layer 7. It will maintain the clear management boundary for network and servers through unloading host resources effectively.

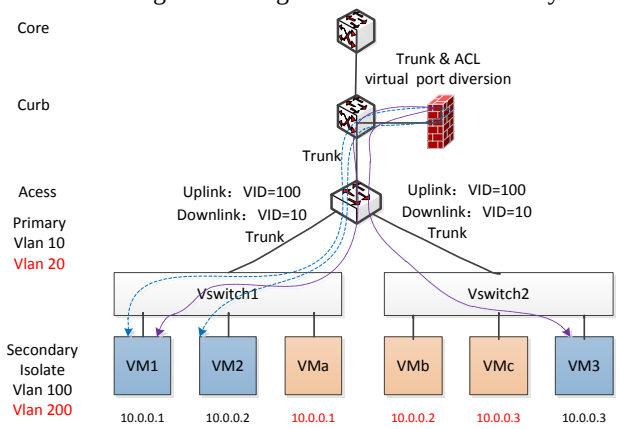


FIGURE V. TRAFFIC DIVERSION SOLUTION

2) Preventing mutual attacks solution for virtual machines: The key factor for avoiding mutual attacks between virtual machines is to prevent address spoofing which will be achieved by the flowing schemes in Hypervisor without extra configuration. In order to avoid IP and APR address spoofing the virtual switch binds IP address with MAC address of virtual machine thus it only send messages with its own address. In order to avoid malicious sniffing from virtual machine the hypervisor adopts exchanging virtual switch rather than sharing type to send messages respectively from different virtual machine to the specified virtual ports resulting in that the virtual machine can't sniff messages form the other one even in the same physical host.

IV. CONCLUSION

Virtualization is one of the most important techniques for cloud computing which changes the traditional IT security architecture. The paper primarily researches the virtualization security protection technology and later we will focus on the security issues on data security and application security and so on to promote the popularization and application of cloud computing.

REFERENCES

[1] Zhang Jian-xun, Gu Zhi-min, Zheng Chao. Survey of Research Progress on Cloud Computing[J].Application Research of Computers,2010,27(2):429-433.

[2] Fang Jing, Wu Hao, Bai Song-lin. Virtualization Security Issue in Cloud Computing[J], Telecommunications Science,2012,(4),135-140.

[3] Jasti A, Shah P, Nagaraj R, et al. Security in multi-tenancy cloud. Proceedings of 2010 IEEE International Carnahan Conference on Security Technology (ICCST), San Jose,CA, 2010:35~41

[4] Hanqian Wu, Yi Ding,Winer Chuck,et al.Network security for virtual machine in cloud computing. Proceedings of 5th International Conference on Computer, Sciences and Convergence Information Technology(ICCIT),Seoul,Korea,2010: 18~21

[5] Tim Mather, Subra Kumaraswamy, Shahed Latif. Cloud Security and Privacy.O'Reilly Media, 2009

[6] Yanfeng Zhang, Cuirong Wang,Yuan Gao.A QoS-oriented network architecture based on virtualization.Proceedings of First International Workshop on Education Technology and Computer Science,Wuhan,China,2009:959~963

[7] Sehgal N K, Ganguli M.Applications of virtualization for server management and security. Proceedings of IEEE International Conference on Industrial Technology(ICIT),Mumbai,India, 2006:2752~2755

[8] Xiaorui Wang, Yefu Wang.Coordinating power control and performance management for virtualized server clusters.IEEE Transactions on Parallel and Distributed Systems, 2011,22(2):245