Research and Implementation of Network Security Management Based on Virtualization Technology

Zhimin Ni*, Fan Zhao
Gansu Institute of Scientific and Technological Information, Lanzhou 730000, Gansu, China

*Corresponding author: zhimin@gisti.edu.cn

Abstract. With the rapid development of the Internet application, virtualization technology and network security management, combining the resources of science and technology information has become one of the network security management subject, because the information system is becoming increasingly complex, software and hardware not compatible, the network security and the waste of resources seriously influence the efficiency of the information office, at the same time also increased the complexity of the network operation and maintenance and cost and energy consumption. This paper, by using virtualization technology to construct the virtual network, optimize the integration of existing server resources, saving operation and maintenance costs, reduce energy consumption, improve equipment utilization. Using the virtual firewall, virtual routing and virtual intrusion detection and other new technology was used to construct the network security system.

1. Introduction
At present, the more types of servers, firewalls, and routers, the more complex hardware failures, natural disasters, planned maintenance, deployment architectures, and environments become. This leads to difficulties in network security management and affects normal business operations.

Use virtualization technology to integrate existing physical servers and build virtual network environments such as virtual gateways and virtual firewalls. Build a virtualization management platform to centrally manage, analyze and monitor server utilization and availability. Reasonably allocate server resources to ensure data security and improve business continuity. Establish network security strategies and licensing strategies for virtual environments to ensure efficient and stable operation of the network and improve network management.

2. Current technology
2.1. Actual physical equipment application technology
First of all, the actual physical equipment cannot detect threats such as illegal occupation of network resources and illegal control, which reduces the stability of the physical equipment. Secondly, as the number of servers’ increases, resulting in reduced performance and increased power consumption, deployment architectures and environments have become more and more complex, resulting in resource manag...
element difficulties. Finally, there is no guarantee for the security of mutual access between internal servers.

2.2. Virtualization technology
Existing server virtualization can be implemented in two ways: hosting virtualization and native virtualization. Hosting virtualization realizes network security management. Because the virtual machine monitor runs on the host operating system to realize the management of virtual machines, it cannot effectively reduce the number of concurrency and cannot meet the access control of a large number of users. The system resource occupancy rate is high and the network is safe. Protection ability is low.

Native virtualization realizes network security management, which is better than boarding virtualization. But it reduces the security access and management capabilities of the virtual machine.

3. Design
First, establish a research on the key technologies of server virtualization based on VMware ESX technology, allocate an independent hard disk partition and specify an independent network interface card for each virtual server, ensure the network performance of each virtual server, and physically isolate the network connection. Complete the virtual server deployment.

Secondly, build a virtualization management platform and establish a virtualization platform management based on VMware vSphere to achieve dynamic load balancing of server resources.

Third, build virtualized security management. Use additional network security policies and embedded management tools to closely monitor the operating status of the virtual server.

Finally, deploy virtual firewalls and virtual routers in a virtual environment to build a virtual intrusion detection system.

4. Realize
The network security management system structure of this content adopting virtual machine technology is mainly composed of three parts: security management controls connecting WAN and LAN networks, LAN virtual network security management platform controls, and LAN virtual machines. The realization is shown in Figure 1.

First of all, through the security management controls connecting WAN and LAN networks, the client user first realizes safe access to the LAN network from the WAN network through physical firewalls, physical routers, and switches that support redundancy.

Secondly, through the LAN virtual network security management platform control, the user accesses different virtual machines in the ESX host to perform security access settings, permission settings, routing settings, filtering settings, and intrusion detection and scanning. The process is:
Figure 1. Network security management topology diagram based on multiple virtualization technologies
Figure 2. Network security management flowchart based on multiple virtualization technologies

a). First, after WAN users enter the LAN network, they first isolate the virtual machine through the virtual firewall module, provide control area, external network and parameter protection, etc., and perform access rights and malicious information and malicious third-party programs in the driver model. Filter settings and block settings.

b). Second, the virtual router module assigns routes to virtual machines requesting access to different resources, that is, according to actual needs, routes are set to different forms of bridging in VMware vSphere to establish virtual routes.

c). Finally, the virtual intrusion monitoring module is used to monitor the access in real time. Finally, the secure access client requests virtual machines with different resources in the ESX host. Thereby greatly improving the ability of network security management.

5. Conclusion
The research and implementation of virtualized technology network security management can not only improve the efficiency and availability of science and technology information network resources and
applications, but also cultivate talents in the field of network security and virtualization technology, and provide a strong guarantee for the construction of e-government network.

References
[1] Muli Ben-Yehuda. IBM Research Report The Turtles Project: Design and Implementation of Neted Virtualization[R].Computer Science, January9, 2012. H_0282 (H1001-004)
[2] Ding Zuoshan. Research and analysis of server virtualization deployment [J]. Computer CD-ROM software and applications .2012(5):43-P44
[3] Feng Hua, Tang Hongwei, Lu Kai. A new Hypervisor logic domain channel design [J]. Computer Engineering and Science .2011(9).P52-56.
[4] Zhu Haitao, Construction and Application of VMwar Virtualization System in University Library [J]. Modern Library and Information Technology .2012(001).TP393.09