Research on Application of Idc Virtualization Security Technology Based on Host Whitelist Protection

Jianfeng Jiang1,*

1Suzhou Industrial Park Institute of Services Outsourcing, China, 215123

*Corresponding author e-mail: jiangjf@siso.edu.cn

Abstract. In recent years, virtualization technology has been widely used in various operators, but in the IDC virtual resource pool exists malicious scanning, DOS attack, SQL injection, virus Trojan, and based on various vulnerabilities of the invasive behavior. Therefore, there is an urgent need for a virtualization security protection software for IDC. Based on the development and utilization of host whitelist active defense technology, this paper firstly briefly explains the significance of IDC virtualization security technology of host whitelist protection, and at the same time discusses the security method, technology, and implementation scheme of IDC virtualization security technology of host whitelist protection, for the reference of readers.

Keywords: Cloud Security, Dc Virtualization, Virtual Diversion, Network

1. Introduction

With the wide application of cloud computing, the security of virtualization technology, as its core technology, has become the focus of the industry. In this case, the firewall is needed to improve the security performance of IDC virtualization technology, to ensure that IDC virtual resource pool in a secure environment [1-3]. Therefore, this paper introduces the APPLICATION of IDC virtualization security technology for host whitelist protection.

2. The significance of IDC virtualization security technology for host Whitelist protection

At present, the security protection of virtualized resource pools mainly relies on traditional monitoring and protection means, which makes it difficult to detect malicious network behaviors in cloud resource pools and lacks the ability to detect and monitor suspicious behaviors [4-6]. Meanwhile, the Ministry of Industry and Information Technology (MIIT) and the state require more and more operators' Internet access services to be assessed. In order to effectively implement the inspection requirements,
effectively solve the virtualization security protection, combining with the characteristics of virtual system, under the condition of host white list protection (as shown in figure 1 to host white list protection work normally under the picture), and put forward the related virtualization diversion, virtual security product deployment technology and actual case studies, aims to improve the supervisory ability of the operator safety, to further consolidate and improve users share.

![Figure 1](image)

**Figure 1.** Normal operation status of host whitelist protection

Therefore, through the application of IDC virtualization security technology, improve the security of network information.

3. **Host whitelist protection OF IDC virtualization security methods and technologies**

3.1. **Host whitelist protection virtualization diversion technology**

Virtualization diversion technology includes policy control center and diversion virtual machine. The policy control center is the management control center of the virtualized network monitoring system and the interactive interface between the system and users. Users can obtain information from V Center and ESXi through the interactive interface provided in the policy control, and can add and manage network security devices to the system. The policy control center can also divide and manage the virtual whole domain, formulate and lower security domain diversion policy, view the diversion virtual machine statistics, and so on [7].

The diversion virtual machine is the datagram processing component of the virtualized network monitoring system. The diversion virtual machine receives the virtual security domain policy from the policy control center. Grab network packets from the virtual switch, filter the packets according to the policy, and forward the packets to the designated target location; The diversion virtual machine receives control from the policy center and feeds back statistics to the policy center.

3.1.1. **Configure VLAN isolation diversion through port groups.** Because VLAN port groups of a virtual switch have independent VLAN domains, different VLAN port groups are isolated on the second layer of the switch, that is, they cannot be interconnected between different VLAN port groups.

3.1.2. **Capture east-west flow through VDS port mirroring** When configuring. VDS port mirroring traffic, you only need to select the source virtual machine (VM1, VM2...) to mirror the traffic during
configuration. VTAP and destination virtual machine port (VTAP) do not need to open the hybrid mode of the virtual switch port group, so the tunnel messages sent by VTAP diversion virtual machine will not be captured back again and will not form a flow loop [8].

3.1.3. Use VEPA to mirror diversion flow. The cuterbox switch board is used to image the specific network port traffic and send it to another network port on the switch panel, which is directly connected to the VEPA control center, or the network port is directly connected to the SDN switch, and the traffic is acquired and summarized through the virtualized threat detection system.

3.2. Host whitelist protection virtualization security product technology

Virtualization security products will be traditional security products of the functions of many products, such as: intrusion prevention IPS system, WEB application security gateway, database audit system, etc., through the way of virtualization deployment, to achieve the security monitoring, detection and protection of data flow in virtualization. In the virtualization security management platform, can be implemented [9].

Centralized deployment and management of various types of test products, audit products and gateway products.

Therefore, under the condition of host white list protection, the management control Center of the network monitoring system can obtain information from The V Center and can add and manage network security equipment to the system, thus improving the security performance of the network system. In addition, the diversion virtual machine receives the virtual security domain policy from the policy control center and feeds back statistical information to the policy center.

4. Host whitelist protection of IDC virtualization security technology implementation plan

4.1. Construction Ideas

4.1.1. Build an independent virtualization security platform. Build independent virtualization security platform, software-oriented security capabilities, and build virtualization security as a platform. Virtualization security is independent of cloud resource pool deployment, and the weak coupling between virtualization security and business resource pool is realized to ensure that the security is not affected when the cloud platform is upgraded and switched [10].

4.1.2. Realize the distributed collection of traffic. According to the application characteristics of network structure and platform software deployment, the method of "traffic distributed collection, security virtualization and autonomous distribution" should be adopted.

4.1.3. Realize the visualization of traffic in the security domain of the virtual environment. It presents the network flow connection of the virtual security domain, so that the network security manager can view the IP assets of the virtual security domain from different levels, and the topology of the actual traffic connection relationship between the assets, etc.
4.1.4. Realize the intrusion detection of virtualized environment traffic. Detect the threats in virtual traffic such as virus, worm, Trojan, DoS, scan, SQL injection, XSS, buffer overflow, spoofing hijacking, etc. to prevent the use of virtual machine as an attack springboard.

4.1.5. Realize database behavior audit of virtualized environment traffic. Analyze, analyze, record, and report the network operation behavior and database operation behavior under the virtualized environment to help users plan and prevent in advance, monitor real-time during the event, respond to violations, report compliance after the event, trace and trace the source of accidents, and promote the normal operation of core asset database and server.

4.2. Network Implementation

Between IDC virtualization security platform and cloud platform, virtual diversion technology is adopted to export the traffic. After the traffic is arranged on the circulation and distribution platform, all kinds of security units delivered to virtualization security are divided into tenants, and the security units analyze and deal with the traffic, to realize the security protection and visualization of east-west traffic. The deployment structure is simplified as shown in Figure 2 below. There are two traffic delivery models: load sharing of traffic and replication of traffic. The load sharing of traffic can be divided based on IP and distributed to different network interfaces. It can usually be used to decompose large traffic into small traffic, and multiple low-performance security components can jointly handle large traffic scenarios. Traffic replication is a scenario in which the flow scheduling platform can copy traffic to multiple network interfaces, which can usually be used to copy traffic to multiple security components and carry out multi-dimensional analysis of traffic at the same time.

![Figure 2. Schematic diagram of virtualization security protection system](image)

4.3. Cloud resource pool flow traction

The traffic that needs to be monitored is exported from the virtual network environment to the physical security equipment through the cloud diversion system, and the specific security business logic is handled by the physical security equipment. This approach has little impact on user business and
network; Using physical security devices to handle security business can achieve very high performance with only a small amount of virtual consumption

Just fit the resource. Cloud diversion system is the data packet processing component of virtualized network monitoring system. Cloud diversion system is essentially a virtual machine with special functions. The cloud diversion system receives the virtual security domain policy from the policy control center, grabs the network message from the virtual switch, filters the message according to the policy, and forwards the message to the designated target location. The cloud diversion system receives control from the policy center and feeds back statistical information to the policy center. When there is virtual machine migration, the security policy matched with virtual machine will be copied to the destination diversion virtual machine before and after virtual machine migration to ensure the same policy before and after virtual machine migration. The flow that needs to be monitored is diverted to the virtualization security platform through the virtual streamer. The deployment of the security platform system is fast and simple, and a small amount of virtualization resources are required. Products such as Flowey, IDS, and audit classes can be implemented in software form according to requirements on the security platform.

Therefore, the implementation scheme of IDC virtualization security technology for host whitelist protection is explained to improve the security of network operation and network database under the virtualized environment.

5. Conclusion

Based on host whitelist protection, the security performance of IDC virtualized resource pool has been further improved. At present, all established IDC virtual resource pools basically adopt physical conventional security products, without professional virtualization security detection and audit products, lack of real-time monitoring and protection technology means of cloud resource pools, cannot find malicious network behaviors in cloud resource pools, and lack the ability to detect and monitor suspicious behaviors. After the construction of this system, it is of great significance to effectively supplement the security protection means of cloud resource pool and improve the discovery and processing capacity to meet the national three-level protection requirements and do a good job in network information security.

Acknowledgments

Supported by the high-end training project for teachers of higher vocational colleges in Jiangsu Province. Qinglan Project of Jiangsu Province. The 13th Five-Year Plan of Jiangsu Province :Research and Practice of the New Generation Information Technology Talent Training Model under the "1+X" Certificate System( D/2020/03/20).

References

[1] Chen Jiaxing, sun Juan. Research on Virtualization security technology [J]. Tianjin Science and technology, 2020,47 (08): 21-23.

[2] Zheng Shaobo. Risk identification and security under virtualization technology system [J]. Digital communication world, 2020 (06): 153-154.
[3] Tang Jianjun, Liu Shuai Chen. Research on Application of IDC virtualization security protection technology [J]. China new communications, 2019, 21 (24): 134-135.

[4] Wang Jiazheng. Host based real-time suspicious website detection system [D]. Jilin University, 2016.

[5] Qing song. Analysis of core technology and development trend of industrial host white list products [J]. China electric power industry, 2018 (09): 94-95.

[6] Hu Haisheng. A code defense scheme for power monitoring host based on white name single machine system [J]. Computer applications and software, 2017, 34 (09): 114-119.

[7] Guan S Y , Fan Y , Lv H L . The Application Research of the University Human Resource Systems Based on Virtualization Technology[J]. Advanced Materials Research, 2014, 1046:449-452.

[8] Li Y , Sun J , Zheng Z , et al. Research of University Disaster Recovery System Based on Virtualization Technology[C]// International Conference on Information Computing and Applications. Springer Berlin Heidelberg, 2012.

[9] Gull D , Wehrmann A . Optimized Software Licensing – Combining License Types in a License Portfolio[J]. Business & Information Systems Engineering, 2009, 1(4):277-288.

[10] Park S W , Kim J N , Lee D G . SecureDom: secure mobile-sensitive information protection with domain separation[J]. The Journal of Supercomputing, 2016.10:3.