A Fuzzy-Based Dynamic Provision Approach for Virtualized Network Intrusion Detection Systems

Bo Li[1,*], Jianxin Li[1], Tianyu Wo[1], Xudong Wu[1], Junaid Arshad[2], and Wantao Liu[1]

[1] School of Computer Science and Engineering,
Beihang University, Beijing, China
{libo,lijx,woty,wuxudong,liuwt}@act.buaa.edu.cn
[2] School of Computing, University of Leeds,
Leeds UK LS2 9JT
sc06ja@leeds.ac.uk

Abstract. With the increasing prevalence of virtualization and cloud technologies, virtual security appliances have emerged and become a new way for traditional security appliances to be rapidly distributed and deployed in IT infrastructure. However, virtual security appliances are challenged with achieving optimal performance, as the physical resource is shared by several virtual machines, and this issue is aggravated when virtualizing network intrusion detection systems (NIDS). In this paper, we proposed a novel approach named *fuzzyVIDS*, which enables dynamic resource provision for NIDS virtual appliance. In *fuzzyVIDS*, we use fuzzy model to characterize the complex relationship between performance and resource demands and we develop an online fuzzy controller to adaptively control the resource allocation for NIDS under varying network traffic. Our approach has been successfully implemented in the iVIC platform. Finally, we evaluate our approach by comprehensive experiments based on Xen hypervisor and Snort NIDS and the results show that the proposed fuzzy control system can precisely allocate resources for NIDS according to its resource demands, while still satisfying the performance requirements of NIDS.

Keywords: Network intrusion detection systems, fuzzy control, virtualization, dynamic provision.

1 Introduction

Virtual security appliances have recently emerged in the network security market and virtual appliance market, and have become a new trend for security appliances distribution and deployment. A Virtual Security Appliance is a computer appliance that runs inside virtual environments [1]. It is pre-packaged with a hardened operating system and a security application and runs on a virtualized platform such as VMware,

* This work is partially supported by grants from China 863 High-tech Program (Project No. 2009AA01Z419), 973 Fundamental R&D Program (No. 2005CB321803), and National Natural Science Funds for China (Project No. 60703056, 60903149).

T.H. Kim and H. Adeli (Eds.): AST/UCMA/ISA/ACN 2010, LNCS 6059, pp. 115–128, 2010.

Xen and Virtual PC. Virtual security appliances allow users to consolidate and manage security and networking products in a virtualized way which can, therefore, greatly reduce hardware costs and simplify IT management. Virtual security appliances are challenged with achieving optimal performance due to the fact that, in virtualized environments, physical servers are shared by all the virtual machines running on them whereas those resources are dedicated for physical security appliances. Furthermore, workloads are often consolidated in virtualized environments for the efficient use of server resources. However, server sharing will result in resource competition between virtual security appliance and the workload VMs running on the same physical server.

The issues described above are aggravated when virtualizing network intrusion detection and prevention systems due to multiple factors. Firstly, a network intrusion detection system (NIDS) often has a sensor that is required to analyze network packets at or near wire speed. However, a failure in this respect can lead to intrusion or malicious behaviors going undetected. Secondly, in order to comprehensively examine network traffic, NIDS need to analyze entire packet and also the payload, thereby consuming large amount of CPU cycles and memory pages. Finally, NIDSs often face varying network traffic; therefore, the resource consumption will fluctuate accordingly. If NIDS is virtualized, the performance of the other virtual servers which share the same physical resource with the NIDS virtual appliance will be affected. Moreover, resource competition will also degrade the performance of NIDS and affect its detection accuracy.

To guarantee the performance of virtualized NIDS, one common approach is allocating enough resources to IDS VM according to its maximum resource demand. However, the resource consumption of NIDSs varies with varying network traffic, which leads to resource idleness and waste thereby violating the objective of server consolidation. This, therefore, reflects a tradeoff between resource utilization and accuracy of security appliances in general and NIDS in particular. The emphasis of this paper is to present our efforts to achieve an effective tradeoff with the objective to preserve the performance of security appliances such as NIDS. To improve resource efficiency without sacrificing the performance of NIDS, one way can be to establish a mathematical model to characterize the relationship between workloads[1] and resource requirement of NIDS virtual appliance. Consequently, resource allocation can be done dynamically to allocate appropriate resources for NIDS to match the varying network traffic in a real-time manner.

Unfortunately, the complex nature of NIDS poses great challenges to accomplish this objective. Firstly, the detection mechanism of NIDS is complex. It involves analyzing every packet based on a number of matching rules which often requires varying processing times. Secondly, a NIDS's resource usage also depends on the characteristics of network traffic it analyzes. For example, the CPU cycles consumed for inspecting UDP and TCP packets are different; traffic containing more malicious packets will require more processing times than normal traffic for performing alerting and logging. Finally, for a NIDS virtual appliance, the resource usage includes resource consumption by both the NIDS application and the virtual machine hosting the NIDS application. For example, when handling network traffic, the frequent network

[1] The workloads of NIDS are usually referred to as network traffic that NIDS analyzes.