

基于 CloudStack 的网络攻防虚拟实验云平台

史建焘, 李秀坤, 张兆心

(哈尔滨工业大学 计算机科学与技术学院, 哈尔滨 150001)

摘要:网络安全实验通常需要复杂的实验环境,网络攻防本身具有一定破坏性和不可逆性,为教学而在系统中设置安全漏洞会产生巨大风险,环境搭建和维护具有较高成本。因此,使用虚拟化和 SDN 手段搭建虚拟实验教学平台具有重要意义。基于 CloudStack 开源云架构和 XEN 虚拟化技术,以 IAAS 为服务模式所搭建的网络攻防虚拟实验云平台,能够解决当前网络安全实验教学环境存在的问题。通过对 snort 与 Iptables 联动搭建防护墙实验的介绍和分析,实验表明,实验云平台在提升实验教学质量,培养学生工程实践能力和工程创新能力方面已经起到了效果,云平台本身具有广阔的发展和应用前景。

关键词:CloudStack; 云计算; 虚拟仿真; 网络攻防实验

中图分类号:TP 393.08

文献标志码:A

文章编号:1006-7167(2017)05-0075-04



CloudStack Based Virtual Simulation Cloud Platform for Network Attack and Defense Experiment

SHI Jiantao, LI Xiukun, ZHANG Zhaoxin

(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)

Abstract: Network security experiments often require complex experimental environment. The network attack and defense technology is destructive and irreversible. Setting network security vulnerabilities for teaching will produce huge risk. The setup and maintenance costs for experimental environment are very expensive. Therefore, it is of great significance to use virtualization and SDN technology to build the simulation platform. The virtual experiment platform of network attack and defense is constructed based on CloudStack, open source cloud architecture, and XEN virtualization technology. The platform solves the problems in the network security experiment teaching and can provide IaaS cloud services. The introduction and analysis of a specific experiment show that the cloud experiment platform can effectively improve the quality of experiment teaching and cultivate students' engineering practice ability and innovation ability. The cloud platform itself has broad prospects for development and application.

Key words: CloudStack; cloud computing; virtualized simulation; network attack and defense experiment

0 引言

目前,计算机网络与信息安全专业的实验课,主要还是以传统的单机编程方式来模拟实现,致使一些需

要复杂环境的实验无法开展,如大规模组网实验、网络协议开发实验、网络安全攻防实验等。由于网络攻防技术本身具有破坏性,为教学而在系统中设置网络安全漏洞会造成巨大风险,而在真实环境中进行网络攻击和病毒注入等实验还会产生不可逆的灾难性后果,因此需要借助虚拟仿真技术和手段开展该类实验。除此之外,攻防实验对实验环境的要求也具有特殊性,如网络攻防实战实验涉及网络搭建、环境配置、攻击目标定制、数据处理、防护及综合渗透测试等过程,实验环

收稿日期:2016-08-15

基金项目:国家自然科学基金项目(61402137)

作者简介:史建焘(1980-),男,黑龙江哈尔滨人、博士、工程师,主要从事计算机网络、云计算,信息安全等方面的研究。

Tel.: 13009877883, 0451-86413844; E-mail: shijiantao@hit.edu.cn

境的搭建和维护成本很高。因此,构建基于云计算技术的虚拟仿真实验平台具有重要意义^[1-3],可较好地克服大规模网络环境缺乏、实验对现有网络环境的破坏、多种实验不能实施等问题。通过 XEN 虚拟化技术^[4-5]提供底层虚拟机通过 CloudStack^[6-8]搭建系统架构提供基础设施即服务(简称 IaaS)模式的实验教学平台。基于云平台设置 Snort^[10]与 Iptables^[11]联动构建防火墙的典型实验,根据云平台提供的环境模板构建虚拟机和网络环境,然后学生可用 SSH 或远程桌面连接到虚拟机上进行相关扫描攻击,验证防火墙效果。本文介绍的云平台既满足学生进行复杂和有破坏性网络攻防实验的需求,又简化了实验环境的搭建过程,具有重要的现实意义。

1 相关技术

(1) IaaS。云计算具有 3 种典型的服务模式,分别是基础设施即服务(IaaS)、软件即服务^[12](SaaS)和平台即服务^[13](PaaS)。其中,IaaS 是其他两种服务模式的基础,通过对资源的最终抽象,为他们提供虚拟的硬件资源服务。该环境下用户可以通过服务直接请求硬件设备资源,如同直接使用裸机和外存设备一样,可以完成任何物理主机能够完成的事。IaaS 的资源是公用的,使用效率会很高,因此在 IaaS 中需要考虑的问题就是如何使多台机器协同工作。目前市场上存在的开源云平台,如 CloudStack 就是用来搭建云环境并提供 IaaS 云服务的。

(2) CloudStack。CloudStack 是一个开源的云计算项目,可用来搭建公有云和私有云,具有高效和高伸缩性优势。CloudStack 由 Apache 基金会资助,符合 Apache2.0 协议,用 JAVA 开发,支持目前主流的虚拟化技术,包括 Xen、KVM 和 VMware。CloudStack 可用来整合现有数据中心的大部分硬件资源,并将资源以池化的方式进行管理,包括海量的网络、存储和计算资源,并在此基础之上搭建云平台,提供云服务。在部署上,CloudStack 具有便捷的资源管理方式,对虚拟资源的管理更接近现实环境,通过从大到小的树形结构进行划分,而且对数据进行独立存储,包括主存储(Primary Storage)和辅助存储(Second Storage)两种数据存储模式。CloudStack 作为一种很好的区域架构模式,在管理云平台上具有结构清晰,管理方便的优势。

(3) Xen。Xen 是一个基于 X86 架构的开源虚拟化技术,由一个剑桥大学的研究项目逐渐发展成一个开源驱动项目,具有性能稳定、发展迅速、资源占用少的优势。Xen 通过半虚拟化技术来获得高性能,其占用的计算和存储资源只占系统总资源的 2% 到 8%,与其他虚拟化产品相比具有明显的优势,可以通过一台普通的 4 GB 内存、4 核 CPU 的主机,也可以构建 20 台

以上的虚拟机。

2 系统设计

2.1 系统拓扑结构

网络攻防虚拟实验云平台的拓扑结构如图 1 所示,平台实现基于 CloudStack 的高级网络架构,配备有一个 CloudStack 管理节点并配置了 MySQL 数据库、XenServer 群集、群集中配置有若干可扩展的计算节点;另外还有 2 台存储服务器节点来提供 NFS 存储,配置目录供二级存储和群集的主存储使用。

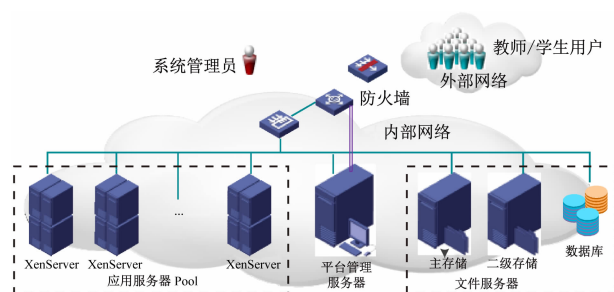


图 1 网络攻防实验云平台拓扑结构

XenServer 群集中配置了计算节点,用来产生平台所需的 Xen 虚拟机,平台使用 Xen 自身的管理机制来维护计算节点的物理可用性。主存储服务器用来保存虚拟机实例的卷,供虚拟机运行时使用,可被群集中所有节点访问,并支持存储分级功能。二级存储用来保存模板和快照等,具有一次写和多次读特点的数据,存储的数据量更大,需要配备较大存储容量的设备。全部的计算节点和存储节点仅通过内网访问,与外网完全物理隔离。平台管理服务器既是 CloudStack 管理节点,同时也要负责云平台的主要业务处理,因此通过双网卡接入了内部网络和外部网络。通过 CloudStack 管理节点,对主服务器及二级存储进行综合管理和配置使用,并为前端的业务逻辑层提供 API 调用接口。

网络攻防虚拟实验云平台主体位于学校内部网络,通过网络中心核心路由器连接到 ISP,外部对虚拟机节点的访问需要通过管理服务器提供的端口映射机制,① 防止了外部攻击,② 保证实验平台上的攻防流量不会对外部网络造成影响。在业务层还实现了用户权限管理,将平台用户分为学生、老师和管理员等不同权限级别,各个权限级别的用户须进行认证后方可进行登录及相关操作。管理员用户仅能通过内部网络登录,用来管理平台的参数设置,维护平台及物理主机的运行;教师和学生用户可以从外部网络登录平台前端页面,正常访问攻防实验用到的虚拟机;而对于非认证用户或非正常的访问,为保证平台正常运行会进行访问者来源记录。对于虚拟机自身的安全性,平台在保证不同用户的实验环境互相隔离的同时,还采用基于

沙盒的设计,保证用户数据在沙盒内运行,实验结束即自动销毁。

2.2 系统框架

网络攻防虚拟实验云平台的系统架构如图2所示,包括:基础设施、后端服务和前端应用。

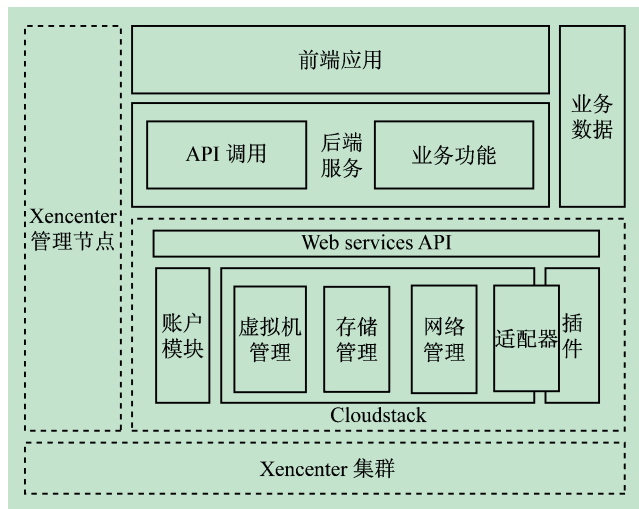


图2 云平台系统架构图

平台系统最下层的基础设施由一组高性能服务器基于Xen虚拟化技术构建,管理员可以通过XenCenter工具,来管理和配置集群节点的物理设备和网络连接。并且可以检测所有虚拟机的运行状态。

云虚拟实验平台的其它服务基于CloudStack提供的基础架构和API进行二次开发实现,具体功能模块包括:虚拟机管理模块、账户管理模块、存储模块和网络管理模块。虚拟机管理模块作为云服务的核心,负责虚拟机整个生存周期的管理,包括生成、运行、迁移和销毁。模块可以根据当前CPU、内存、带宽等因素进行综合评定,选择合适的宿主机分配虚拟机实例,避免物理节点的负载不均衡,保证了平台的服务质量。系统账户的管理由账户管理模块负责,通过权限设置和访问控制策略,控制不同用户对虚拟机资源、网络资源和存储资源的访问,保证了平台的安全性。存储模块采用基于两级存储模式分别管理虚拟机实例所需的静态主机模板和运行时所需的镜像文件,这种层次性的存储能够更好的维护存储资源,确保平台运行效率。网络管理模块采用Cloudstack的高级网络模式,基于虚拟VLAN技术构建实验网络环境,使得虚拟机物理隔离。每个用户创建的实验环境可能包含多个虚拟机节点,会被分配一个统一的VLAN ID,构成了该用户的私有虚拟网络。为了给私有网络提供远程访问等公有网络服务,为每个虚拟网络配置了基于系统虚拟机的虚拟路由器,作为不同网络间的公共接口,提供了包括NAT、源NAT、DHCP、DNS、数据转发和防火墙等功能。

CloudStack平台本身为外部调用和二次开发提供

了API调用,可以实现对云数据库和服务功能的访问、对虚拟机资源和存储资源的操作等等。在系统后端,云平台通过实现一个守护进程,调用CloudStack的API接口,为前端业务逻辑模块提供服务。

2.3 系统功能模块

实验平台通过图3所示的前端页面功能提供服务。

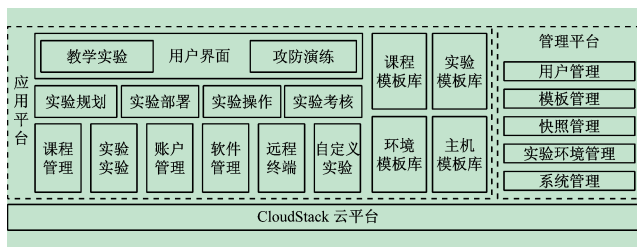


图3 云平台前端功能

与传统的实验室相比,云平台对几乎所有系统资源进行了虚拟化,包括操作系统、网络资源等。可以对实验内容、实验环境以及网络拓扑进行定制,并且提供了对复杂攻防实验的支持。界面分别提供了教学实验入口和攻防演练入口,配置虚拟实验环境所需的模板包括主机模板,环境模板,实验模板和课程模板。

主机模板包括不同的操作系统版本和实验所需的基础软件,并针对攻防演练的需求定制了多种系统和软件漏洞。模板可以由管理员通过配置的虚拟机实例的镜像制作,也可通过外部导入。环境模板根据实验要求设定主机数量和主机模板类型,并定制静态或动态登录密码,配置网络环境。实验模板中设置了实验指导书和需要的环境模板,实验指导书包括实验准备、实验步骤、实验预期结果等。课程模板根据实际课程教学需要,定制课程所需实验,选择实验模板,设定实验学时,制定考核标准等。

实验平台分别提供了应用平台和管理平台,应用平台主要为教师用户和学生用户提供实验规划、实验部署、实验操作和实验考核的入口,支持课程管理、实验管理、个人账号管理、远程管理、远程终端连接和定制实验的功能。管理平台主要是为了方便管理员维护基本的平台环境和平台资源,包括用户管理、模板管理、虚拟机快照管理、实验环境和系统管理等功能。

实验的具体流程。管理员分配教师和学生账号,并为不同账号设置访问权限;教师用户用自己的账号登录系统后,可对自己的课程进行设置,选择课程所需的实验项目,上传实验指导书和实验报告模板,配置主机模板和环境模板,选择选课学生;实验开始前点击构建实验环境按键,系统会根据目前选课人数创建相应的虚拟实验环境。学生登录后,根据对应的实验项目获得环境中所有可见虚拟机的IP/端口、登录密码(静

态或动态),通过 Telnet、SSH 或者远程桌面的方式进入自己的实验环境。

实验过程中,教师可以随时查看学生的实验情况,进行实验指导。平台的实验过程具有可视化优点。实验数据也可多次回放,实验环境可以随时恢复。通过这样统一集中管理方式,所有实验资源能够集中恢复和一键销毁。对于一些不可逆的攻防实验,学生也可在实验过程中重置实验环境,反复体验某些实验步骤。实验平台由于具有高度的扩展性,因此能够支持复杂的大规模网络实验,保证多层次学生的实验需求。

3 实验案例

3.1 实验准备

现以“信息安全概论”课中一个具体实验为例,实

验是通过 Snort 与防火墙进行联动来构建一个轻量级的入侵检测系统。其中,Snort 入侵检测系统,可将网络上的恶意外行为和恶意代码制成规则库,与实际数据源进行匹配,从而判断入侵行为。但 Snort 只能发现入侵,并不能阻断攻击,而 Iptables 规则是常用的阻断网络数据包的方式,因此本实验通过 Snort 与 Iptables 的联动,综合二者优点,互补对方的缺点,达到检测攻击并切断攻击的目的。实验利用一个简单的脚本实时读取告警日志,根据记录的 IP 和端口,创建对应的 Iptables 规则,加入远程或对应主机的防火墙规则中。

在传统环境中由于大量用户同时进行扫描等攻击行为,会造成局域网的流量阻塞,影响网络正常使用。因此,本实验选择在虚拟实验云平台下进行,实验的环境模板配置如图 4 所示。

系统概况

主机模板管理

环境模板管理

部署资源管理

测试管理

首页

环境模板管理

环境模板视图

Snort与单台防火墙联动构建轻量级IPS

主机

+ 添加主机

主机名称	主机模板名称	动态密码	固定IP地址	是否返回	是否按部署	主机台数	修改时间	状态
snort-host	centos6.5	否	10.1.1.12	否	否	1	2014-07-15 15:26:06	正常
test	winxp-32-ccl	是	不固定	是	否	1	2014-07-15 15:25:33	正常
host	winxp-32-ccl	是	不固定	是	否	1	2014-07-15 15:25:09	正常

图4 实验主机及网络配置

实验环境有 3 台虚拟机构成,其中 snort-host 主机只可在环境内部登录,不提供远程登录接口。另 2 台主机可通过远程桌面连接,host 主机为实验操作机,用来远程登录、安装和配置 snort 主机,test 主机则用来远程探测。通过实验平台可以按实验人数,载入对应数量的实验环境,由于采用了 CloudStack 的高级网络模式,不同实验环境的主机之间被物理隔离,实验结果不受外界影响。环境搭建成功,学生登录后看到的实验平台的界面。

3.2 实验步骤

(1) 通过 host 主机登录 snort-host,安装并配置 snort 环境,包括 snort 依赖包、Snort 规则库、DAQ、libdnet、guardian 等。Guardian 是一个开源的 perl 程序。通过读取和分析 Snort 日志,自动执行自己的 shell 脚本来配置 Iptables 下的规则,将恶意 IP 地址加入 Filter 表中的 INPUT 链下,并将其数据包丢弃。

对 Snort 的配置文件 snort.conf 修改如下:

```
#实验环境配置的子网段
ipvar HOME_NET 10.1.1.0/24
ipvar EXTERNAL_NET any
#配置 snort 规则
varRULE_PATH /etc/snort1/rules
varSO_RULE_PATH /etc/snort1/so_rules
varPREPROC_RULE_PATH /etc/snort1/preproc_rules
varWHITE_LIST_PATH /etc/snort1/rules
```

```
varBLACK_LIST_PATH /etc/snort1/rules
#检测端口扫描,不去注释也可以,去掉注释用 nmap 扫描即可看到扫描日志
preprocessor sfportscan: proto { all } memcap { 10000000 }
sense_level { low } include PREPROC_RULE_PATH/preprocessor.rules
include PREPROC_RULE_PATH/decoder.rules
include PREPROC_RULE_PATH/sensitive-data.rules
```

对 guardian 的配置文件 guardian.conf 进行如下修改:

```
Interface eth0
LogFile /var/log/snort/guardian.log
AlertFile /var/log/snort/alert //alert 文件的位置
IgnoreFile /etc/snort/guardian.ignore //白名单
targetFile /etc/snort/guardian.target //黑名单
TimeLimit 120 //阻断时间,以秒为单位
```

用如下命令启动 guardian:

```
/usr/bin/perl /usr/local/bin/guardian.pl -c /etc/snort/guardian.conf
```

(2) 联动测试。登录 host 主机,打开 x-scan 扫描软件,将扫描参数中指定 IP 搜索范围设置成 snort 主机的 IP 地址:10.1.1.12。全局设置选项卡中的扫描模块选则“全选”,插件设置选项卡下的所有设置均全部选中。

(下转第 147 页)

参考文献 (References):

- [1] Peter Tiernan. Enhancing the learning experience of undergraduate technology students with LabVIEW software [J]. Computers & Education, 2010(55):1579-1588.
- [2] Faraco G, Gabriele L. Using LabVIEW for applying mathematical models in representing phenomena [J]. Computers & Education, 2007(49):856-872.
- [3] 李祖明, 郑对元. 精通 LabVIEW 虚拟仪器程序设计[M]. 4 版. 北京: 清华大学出版社, 2012.
- [4] 张兰勇, 孙 健, 孙晓云. LabVIEW 程序设计基础与提高[J]. 5 版. 北京: 机械工业出版社, 2013.
- [5] 郝 丽, 赵 伟, 王 坤, 等. 利用 LabVIEW 提高电气工程专业本科生教育质量[J]. 实验室研究与探索, 2016 (35):217-219.
- [6] 李 欣, 谢 宏. 虚拟仪器技术在通信原理教学中的应用[J]. 实验室研究与探索, 2014(33):155-159.
- [7] 马 蕾, 王金城, 王 尧. 基于虚拟仪器的自动控制原理实验系统[J]. 实验室研究与探索, 2005, 24(增):210-212.
- [8] 刘 中, 袁少强, 张军香. 自动控制原理实验课的改革与实践[J]. 实验室研究与探索, 2013(32):403-406.
- [9] 刘瑞歌, 宋 锋. 基于虚拟仪器技术的自动控制原理教学实验平台[J]. 自动化与仪器仪表, 2011(4):171-173.
- [10] 刘 宝, 孟令雅, 王 钊, 等. “自动控制原理”课程特色教学研究[J]. 电气电子教学学报, 2013(35):66-68.
- [11] 蔡周春, 缪妹妹, 王 辉, 等. 基于 LabVIEW 的自动控制原理实验系统的设计[J]. 工业控制计算机, 2012(25):39-40.
- [12] 王 娟, 胡文军, 王培良. 基于 LabVIEW 的多物理量测量实验系统[J]. 实验室研究与探索, 2016,35(4):121-124.
- [13] 顿爱波. 远程教学用虚拟电子实验室系统研究[D]. 大连:大连理工大学, 2005.
- [14] 严 浩. 基于 LabVIEW 的网络虚拟仪器在实验教学中的应用研究[D]. 武汉:华中科技大学, 2007.
- [15] 吕桂云, 吴晓蕾, 高洪波. “无土栽培学”实践教学的改革与实践[J]. 河北农业大学学报(农林教育版), 2012(14):55-58.
- [16] 章铁军, 高洪波, 吴晓蕾. 网络教学与课堂理论教学相结合—无土栽培学课程教学模式的试验研究[J]. 河北农业大学学报(农林教育版), 2010(12):85-88.

(上接第 78 页)

点击开始按钮,开始扫描;登陆 snort-host 观察日志文件/var/log/snort,发现产生多条类似如下形式的告警日志,表示检测到外界扫描。

```
12/25-13:12:11.724778 [ * * ] [ 122:1:1 ] (portscan) TCP
Portscan [ * * ] [ Classification: Attempted Information Leak ]
[ Priority:2 ] { PROTO:255 } 192. 168. 101. 103 -> 192. 168.
101. 100
```

在 snort 主机上启动 guardian,并与 iptables 联动,之后在日志文件中,可以发现 block 脚本已经被执行。

```
Running '/usr/local/bin/guardian_block.sh 192. 168. 101. 107
eth0'
```

执行 iptables - L,观察是否有新规则被插入,如果有则证明实验验证成功。插入的 Iptables 规则格式如下:

```
Target port opt source destination
DROP all --192. 168. 101. 103 anywhere
```

至此,单台防火墙联动已成功实现,有效验证了通过虚拟仿真云实验平台进行网络攻防实验的可行性。

4 结 语

针对当前网络安全实验教学环境的问题,介绍了基于 CloudStack 架构的网络攻防虚拟实验云平台,平台既可满足日常实验教学的需要,也为网络安全技术爱好者提供了攻防演练的场所。平台具有的现实意义:① 大大节省了实验设备空间;② 能够快速搭建复杂网络,支持具有破坏性和不可逆性的网络攻防实验;③ 可以同时构建大量相同实验环境,实验环境物理隔离;④ 有利于实验内容的开放和共享;⑤ 大大减少了实验教师和管理者的劳动强度。目前,实验平台的

XenServer 集群包括 8 台双路 4 核、128 GB 内存的高性能服务器,可以同时建立 300 台以上的虚拟机。已经通过平台成功的开展了信息安全基础、信息内容安全等信息安全专业本科实验教学,取得了较好效果。今后可通过扩展底层的服务器,提升系统承载能力,将平台向外推广,让其具有更广阔的前景。

参考文献 (References):

- [1] 张朝昆,崔 勇,唐嵩祯,等. 软件定义网络(SDN)研究进展[J]. 软件学报,2015,26(1):62-81.
- [2] 宋 平,刘 轶,刘 驰,等. 一种支持细粒度并行的 SDN 虚拟化编程框架[J]. 软件学报,2014,25(10):2220-2234.
- [3] 龙艳军,欧阳建权,俞佳曦. 基于 GNS3 和 VMware 的虚拟网络集成[J]. 实验技术与管理,2013,30(2):90-93.
- [4] 石 磊,邹德清,金 海. Xen 虚拟化技术[M]. 武汉:华中科技大学出版社,2009.
- [5] 吴 迪,薛 政,潘 嵘. 基于 XEN 云平台的网络安全实验教学[J]. 实验室研究与探索,2013,32(7):62-66.
- [6] 吴常清,王慧敏,薛 涛. 基于 CloudStack 的私有云平台的构建与实现[J]. 西安工程大学学报,2014,28(2):220-224.
- [7] 彭 红. 基于 CloudStack 云管理平台的关键技术研究与应用[D]. 上海:华东理工大学,2013.
- [8] 余志涛. 基于 CloudStack 云平台的研究与自动系统的实现[D]. 大连:大连理工大学,2014.
- [9] 董健康,王洪波,李阳阳,等. IaaS 环境下改进能源效率和网络性能的虚拟机放置方法[J]. 通信学报,2014,35(1):72-81.
- [10] 孙 伟. Snort 轻量级入侵检测系统全攻略[M]. 北京:北京邮电大学出版社,2009.
- [11] Gregor N P. Linux iptables Pocket Reference [M]. California: O'Reilly Media, 2004.
- [12] 李晓娜,李庆忠,孔兰菊,等. 基于共享模式的 SaaS 多租户数据划分机制研究[J]. 通信学报,2012,33(S1):110-120.
- [13] 徐 鹏,陈 思,苏 森. 互联网应用 PaaS 平台体系结构[J]. 北京邮电大学学报,2012,35(1):120-124.