Journal of Computer Applications
计算机应用,2015,35(5):1284 - 1289
ISSN 1001-9081
CODEN JYIIDU
2015-05-10
http://www.joca.cn

文章编号:1001-9081(2015)05-1284-06
doi:10.11772/j.issn.1001-9081.2015.05.1284

云计算平台异常行为检测系统的设计与实现

于红岩[1*],岑凯伦[2],杨腾霄[3]
(1.上海海事大学 交通运输学院,上海 201306; 2.上海海事大学 信息工程学院,上海 201306;
3.上海纽盾科技有限公司 研发部,上海 200092)
(*通信作者电子邮箱 yuersuc@163.com)

摘 要:针对传统网络安全设备对云计算平台中虚拟机内部发生的蠕虫病毒、地址解析协议(ARP)广播攻击等异常行为失效的问题,设计了基于VMware的云计算平台下异常行为检测技术架构,提出了云计算下有特征码的蠕虫病毒异常行为检测,和基于突变理论的无特征码的异常行为检测,并针对两种异常行为提出了"侦测—隔离—治愈—恢复"智能处理云安全机制。系统融合云计算下异常行为检测,云计算下事件与防卫管理,和云计算下ARP广播检测三种功能于一体。实验结果表明,系统能实时提供云计算环境下异常行为的采集及分析,每隔5秒自动刷新实时流量资料,且吞吐量可达到640 Gb的处理能力,能够将被保护链路中异常流量所占用带宽降至总拥有带宽的5%以下,解决了云计算下的异常行为检测和防护问题。

关键词:云计算;异常行为检测;事件管理;地址解析协议异常侦测;云安全
中图分类号:TP393.08 **文献标志码**:A

Design and implementation of abnormal behavior detection system in cloud computing

YU Hongyan[1*], CEN Kailun[2], YANG Tengxiao[3]
(1. *College of Transport and Communications, Shanghai Maritime University, Shanghai* 201306, *China*;
2. *College of Information Engineering, Shanghai Maritime University, Shanghai* 201306, *China*;
3. *Research and Development Department, Shanghai Newdon Technology Company Limited, Shanghai* 200092, *China*)

Abstract: Worm, Address Resolution Protocol (ARP) broadcast and other abnormal behaviorS which attack the cloud computing platform from the virtual machines cannot be detected by traditional network security components. In order to solve the problem, abnormal behavior detection technology architecture for cloud computing platform was designed, abnormal behavior detection for worms which brought signature and non-signature behaviors based on mutation theory and "Detection-Isolation-Cure-Restore" intelligent processing for cloud security was proposed. Abnormal detection, management of event and defense, and ARP broadcast detection for cloud computing platform were merged in the system. The experimental results show that the abnormal behavior inside the cloud computing platform can be detected and defensed with the system, the collection and analysis of the abnormal behavior inside cloud computing platform can be provided by this system in real-time, the traffic information can be refreshed automatically every 5 seconds, the system throughput can reach to 640 Gb and the bandwith occupied by abnormal flow can be reduced to less than 5% of the total bandwith in protected link.

Key words: cloud computing; abnormal behavior detection; event management; Address Resolution Protocol (ARP) anomaly detection; cloud security

0 引言

云计算因其虚拟化的特性,能够将计算机资源,逻辑抽象成资源池,实现资源共享、弹性分配、按需服务等功能[1-2]。企业用户通过将自身服务架设在云计算平台,显著降低维护成本;个人用户通过将自身数据和计算放在云端,降低了自身存在的存储和计算机性能有限带来的诸多约束。由于云计算带来的诸多好处,使得云计算逐渐成为一个全新的互联网服务模式。与此同时,用户对云计算的安全性提出了更严格的要求。

为了保证云计算下数据的安全,首先需要确保云计算平台的安全性。云计算平台和传统的网络相比,引入了大量虚拟化技术,虚拟机之间的网络流量对于网络安全设备是不可见的[3]。因此传统的安全保护手段不再适应云计算的安全需求,传统网络中存在的安全攻击如蠕虫传播、地址解析协议(Address Resolution Protocol, ARP)广播攻击等,均将对云计算平台的安全性产生巨大的威胁。

国内外学者首先针对传统网络发动的安全攻击进行了相关研究,Lockwood等[4]提出采用可编程逻辑设备对抗网络蠕虫的防范系统,这种检测方法需要提取蠕虫的特征码,但无法对未知蠕虫进行有效的检测;辛毅等[5]提出一种基于通信特征分析的蠕虫检测与特征提取技术,在解析蠕虫传播通信模式的基础上,通过评估通信特征集合间的相似度来检测蠕虫;朱晖等[6]提出一种基于节点行为的主动点对点(Peer-to-

收稿日期:2014-12-10;**修回日期**:2015-01-14。 **基金项目**:上海市教育委员会科研创新项目(11YS142);2014年上海市科技型中小企业技术创新基金资助项目(1401H164800);2012年上海海事大学校基金资助项目(20120080)。

作者简介:于红岩(1979 -),女,山东文登人,讲师,博士,主要研究方向:电子商务、云计算安全; 岑凯伦(1991 -),男,上海人,硕士研究生,主要研究方向:云计算安全; 杨腾霄(1977 -),男,山西长治人,工程师,硕士,主要研究方向:云计算安全。

Peer,P2P)蠕虫检测方法,设计和实现了一个主动 P2P 蠕虫检测系统,此系统可以实现 P2P 节点出站短连接的实时监控。对于网络故障异常和瞬间大量访问异常等无特性攻击行为的检测,也有学者进行了相关研究; Su[7] 采用非参数的累积和方法检测观测时间序列中的突变,以检测握手信号(SYNchronous,SYN)防洪攻击; Shah 等[8] 建立网络异常行为分析系统能够有效地分离出短期的和长期的异常流量; 在此基础上,Guan 等[9] 进一步研究了网络中路由器出口处的 IP 包头数据,当分析信号超过了历史阈值,诊断网络出现了异常行为。

由于云计算平台核心技术虚拟化的特性,需要有特定的安全防护手段去保护虚拟化平台的安全。项国富等[10] 提出在虚拟机中加载内核模块拦截目标虚拟机中的内部事件,通过直接还原操作系统级语义实现监控虚拟机状态,从而保护虚拟机的运行安全。刘谦等[11-12] 通过访问控制机制保障虚拟机之间的通信安全,只有被信任的用户才能够访问虚拟机。

目前云计算平台下的异常行为检测研究仍在起步阶段,与以往研究不同,本文提出了一种基于虚拟化管理器和策略处理引擎实现的云计算异常行为检测系统,通过将虚拟机之间的流量导入外部的策略引擎,针对传统网络下存在的蠕虫病毒攻击、未知攻击事件以及 ARP 广播攻击,提出了相应的检测方法。实验结果表明,本系统可以对云计算平台下出现的异常行为作出有效的检测和防护。

1　系统架构设计与关键技术

1.1　系统体系结构设计

1.1.1　设计思想

本文的设计思想是将云计算平台部署到虚拟化软件平台上,通过威睿虚拟交换机(Virtual Machine ware, VMware)取代传统交换机,实现虚拟机内部流量的转发。在虚拟机交换机上层,加入虚拟网关层,基于 VMware 流量拦截模块实现,将虚拟机之间的流量拦截在虚拟机交换机之前。传统的监控技术,是将监控点植入在被监控虚拟机内部,该方法可以有效获知虚拟机的状态,但由于和内核紧密相关,缺乏通用性。本系统基于虚拟机自省技术,将异常行为检测系统从虚拟机中转移至外部,通过虚拟网关的重定向,将分好类的异常流量传入策略引擎进行处理,实现云计算下事件与防卫管理,云计算下异常行为检测和云计算下 ARP 广播检测。最后在策略引擎的上层提供图形用户管理界面,用户可以通过图形用户界面(Graphical User Interface, GUI)进行管理,实现了系统的友好交互以及易操作性,具体如图 1 所示。

1.1.2　系统结构设计及部署

基于上述设计思想,本文设计并实现了云计算平台下异常行为检测系统,其体系结构如图 2 所示。

图 2 中云计算下异常行为检测系统通过旁路接入云计算下的骨干交换机。系统检测云计算下每一个虚拟局域网(Virtual Local Area Network, VLAN),并且启用骨干交换机网络流(Network Flow, NetFlow)和会话流(Session Flow, SFlow)机制,将骨干交换机的流量导入异常行为检测系统进行分析和处理。异常行为检测系统可以检测云环境中 VLAN 内第 2 层的封包及 VLAN 之间的第 3/4 层的网络异常行为,使管理员得以随时掌握云计算的安全状况。针对云计算平台中的虚拟机安全,借助虚拟机自省技术,即在虚拟机外部对虚拟机进行安全监控,将虚拟机内部状态拦截,传递至外部的策略引擎,通过上层的图形界面观察虚拟机的安全情况。最后针对应用层第 7 层的外部威胁,第三方安全设备将系统日志(System log, Syslog)导入到云计算异常行为检测系统中,系统通过设定第三方安全设备接口的接收端速率、发送端速率、临界值及触发异常(发送 Syslog)报警,从而保障云计算的安全。

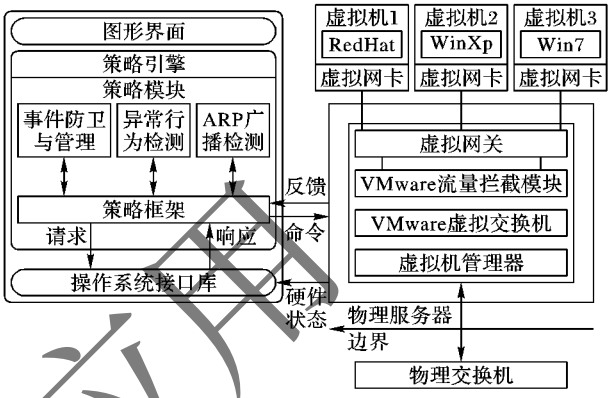

图 1　云计算下异常行为检测系统架构

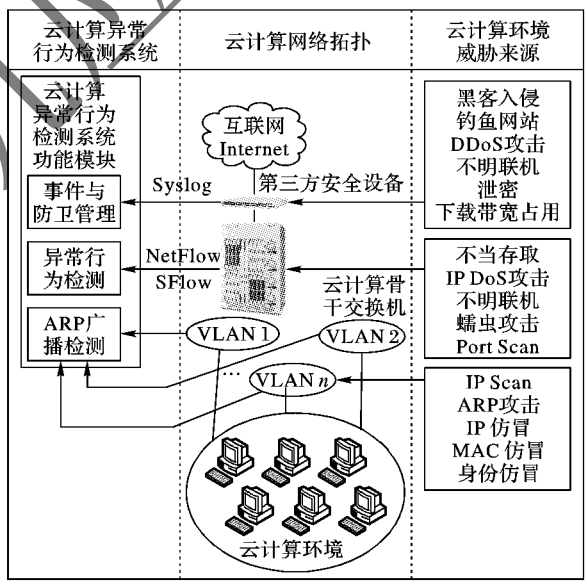

图 2　云计算下异常行为检测系统部署

1.2　系统关键技术

1.2.1　云计算下的蠕虫病毒分析

云计算不仅给用户带来超强的计算能力,同时也带来了蠕虫类病毒的超强攻击能力,因此云计算下具有特征信息的蠕虫病毒智能分析显得尤为重要。与传统网络环境不同,云计算下异常行为检测系统实现了蠕虫病毒特征码从客户端采集向云计算采集的迁移,云计算环境下服务器群收集大量的可疑信息和网络流量来实时监控网络,蠕虫对易感个体的探测和具有特征信息的感染注入数据均可能被云计算异常行为检测系统发现,这样不安全的链接或者恶意数据在云计算中直接被扼杀,阻止进入用户端,从而减少蠕虫病毒的扩散。云计算下蠕虫病毒检测逻辑框架具体如图 3 所示。

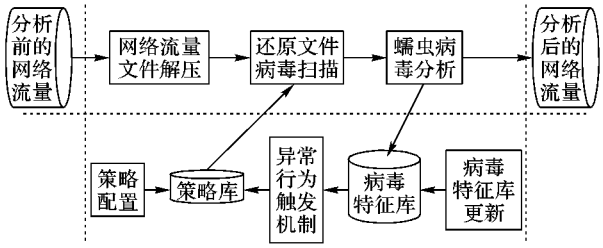

图3 云计算下蠕虫病毒检测逻辑框架

在图3中,云计算下蠕虫病毒行为智能分析依赖于特征码库的逐条逐包比对,如果比对成功则启动异常行为触发机制,对病毒实现实时处理。蠕虫病毒特征存储于云计算下的蠕虫病毒库,加入云计算环境下的个体都可以通过实时升级蠕虫病毒特征库来增强云环境下服务器和虚拟机的防御能力。由于云环境下强大的计算能力,本系统能更准确地分析得出蠕虫特征加以遏制,但是云计算平台的基石是虚拟化,每一台虚拟主机都要对进入的文件进行检测,如果将传统的主机防病毒方式直接移植到虚拟机上,势必要在每台虚拟机上安装病毒匹配软件,将直接导致防病毒软件过多地占用宿主机的物理资源,造成计算资源的浪费,这显然会大大降低云计算平台的效能。

针对虚拟化的架构,传统的安全防护措施已经无法有效地对虚拟机的安全进行防护,通过基于虚拟机管理器的安全技术手段才是增强虚拟化安全的重要途径。在云计算异常检测系统平台中引入了虚拟网关,其会定期与VMware控制中心通信,当虚拟机状态发生变化时第一时间得知,调用VMware提供的负责虚拟机安全的应用程序编程接口(Application Programming Interface, API)为虚拟机提供最高级别的安全防护,保证了云计算平台中虚拟机系统的安全,并将异常流量扼杀在用户端之前。

1.2.2 基于突变理论的云计算下异常行为检测

以往采用特征码识别技术的云计算异常行为检测系统,依赖于经常更新病毒特征库,因此只能被动识别病毒特征库中已经存在的病毒和攻击,对于无病毒特征的攻击行为,没有防范能力。而无特征威胁也是云计算的另一大安全隐患。安全领域里主要采用的模型有尖点突变、燕尾突变。在突变理论中最容易观察到的特性是突跳性,在异常行为检测中,突变模型的测量指标包括审计事件的数量、间隔时间、资源消耗等。图4描述了云计算下由瞬间大量数据拥塞引起的异常行为,其中横坐标代表时间,单位是秒;纵坐标表示云计算下骨干交换机吞吐量(数据包)的观测值。

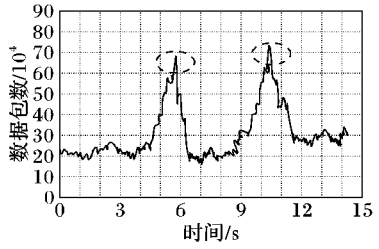

图4 瞬间大量数据拥塞引起的异常

从图4可以看出,当云计算中出现异常行为时,骨干交换机吞吐量将在瞬间发生迅速增长,导致云计算骨干交换机出现拥塞。在图4中,吞吐量观测值在6 s左右发生了突跳性的变化,由20万包/s瞬间激增为75万包/s;在11 s左右也发生了突跳性的变化,由35万包/s瞬间激增为80万包/s。

通过对云计算下异常行为的数据观察,观测到了数据的突跳性,能够对云计算下异常流量进行分析,包括:IP主机流量记录、分析与稽核;主干线路流量速率分析与警示。本文选择尖点突变模型来描述云计算环境下的异常行为,设计云计算下基于突变理论的异常检测算法。该算法利用了分叉集曲线各区域网络行为的突变特性以及遵从理想延迟约定,能准确判断云计算环境的网络状态,以判断是否启动异常行为触发机制。云计算下基于突变理论的异常检测流程如图5所示。

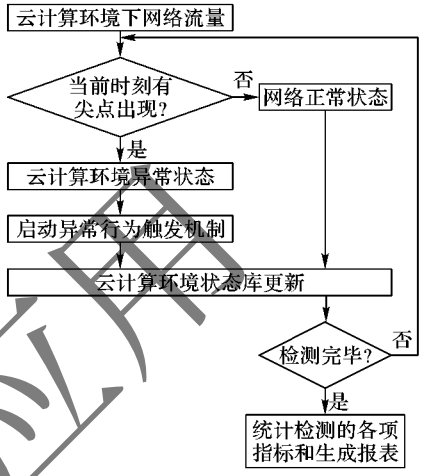

图5 云计算下基于突变理论的异常检测流程

云计算下基于突变理论的异常行为检测,实现了对无病毒特征比对的异常行为检测,具有以下特点:

1)无需逐包检查,只对云计算下异常行为进行审计和管理,简单高效,无需升级病毒库,使用简便,无需维护;

2)强大的数据处理能力,适合云计算环境部署,极大地提高云环境的安全性;

3)主动进行云环境下异常监测和隔离管理,从网络的第2层、第3层入手主动应对现有及未来的各种威胁,适用于识别云计算下无特征信息的攻击行为。

1.2.3 云计算下异常行为触发机制

云计算下异常行为触发机制不仅提供有特征信息的蠕虫类病毒进行隔离和治疗,也能对无特征信息的攻击行为进行及时隔离与通知,确保云计算环境下各种异常行为得到及时控制。设计思路如下:遇有威胁可立即将云计算环境设备与用户联机切断,降低端口流速,并记录日志,以防止云计算环境中由于主机被攻击或破坏而导致所有虚拟机都瘫痪;设计自动智能化的控制中心,将多种防护措施有机融合在云计算环境中,采用“侦测—隔离—治愈—恢复”智能处理安全机制,能够有效防御云计算下的各种威胁,保证云计算下的所有个体24小时运行。具体设计如下。

1)设置触发条件。触发防卫动作的“特定条件”,这些条件通常包括“严重等级”,或事件说明内“特定关键词”等,处理方式有隔离、告警、封锁三种。

2)隔离管理。隔离对云计算环境造成威胁的攻击源,当Syslog服务器接收到“特定条件”的安全事件记录时,会立即启动防卫隔离机制。

3)告警。针对异常事件可提供E-mail通知机制。

4)封锁方式。当安全事件符合触发条件时,便会启动封

锁的动作,方式分别有“自动”与“手动”两种。可封锁交换机接口,或物理地址(Media Access Control, MAC)联机阻断。

1.3 系统模块设计

云计算下异常行为检测系统将云计算下异常行为检测,云计算下事件与防卫管理和云计算下 ARP 广播检测功能融为一体。通过海量终端的分布式处理能力进行安全事件采集,上传到云计算异常行为检测系统进行智能分析和检测,极大地提高了云计算下安全事件搜集、病毒防范等方面能力。云计算下异常行为检测系统 3 个核心功能模块主要利用了 VMware 提供的负责保护虚拟机安全的 API,实现功能如下:1)云计算下异常行为检测——病毒防护、DPI 深度包检测、第 3/4 层流量分析、TCP 服务效能、异常行为分析子系统;2)云环境下事件与防卫管理——审计系统事件和应用程序事件,攻击源追踪协助防御管理;3)云计算下 ARP 广播检测子系统——第 2 层 ARP 的数据封包检测。

1.3.1 云计算下异常行为分析与检测

云计算下异常行为分析检测模块实现蠕虫病毒检测和无特征信息攻击行为的检测。蠕虫病毒检测规则设定:系统内建的 SFlow 分析器随时收集云计算环境下骨干交换机导入的 Layer 3/4 flow 流量信息,且每 5 ~ 10 min 就会实时依据“蠕虫病毒检测规则设定”作分析,检查内部网络是否有蠕虫攻击行为、病毒活动的迹象。并配合防卫触发条件,启用异常行为触发机制进行处理。除了系统默认的最知名蠕虫的流量行为特征,本系统实现了病毒特征码从客户端采集向云计算环境采集的迁移,可以不断添加到云计算下蠕虫病毒特征库中,进行蠕虫病毒特征比对,从而判定是否启用异常行为防卫管理机制进行处理。

针对无特征信息异常行为的定义,包含超流、异常规则、超过目标主机数及超过目标端口数,如果发生超流、异常规则、超过目标主机数及超过目标端口数的情况,则启用异常行为触发机制进行处理。云计算环境下无特征信息异常行为规则字段说明如表 1 所示。

表 1　基于突变理论的异常行为规则设定

参数	异常行为规则字段说明
通信协议	设定该规则检查的协议,代号 0 为全部,1 为 ICMP,6 为 TCP,17 为 UDP
来源 IP	联机来源的 IP 地址
目的 IP	联机目的的 IP 地址
来源端口	联机来源端使用的端口
目的端口	联机目的端使用的端口
封包数量	产生的封包上限
封包长度	封包的长度上限
发生次数	该规则判断为异常的上限

1.3.2 云计算下事件与防卫管理

云计算下事件管理主要目的是收集本系统与其他配合信息安全厂商的 Syslog,并配合信息安全的严重等级或者定制的触发条件以防卫、隔离威胁来源。通过将事件截获模块嵌入虚拟器管理器中,事件截获模块对虚拟机中客户操作系统发生的系统调用进行拦截。云计算下事件管理设定有 3 个步骤:

1)信息安全设备建档。ReVirt[13] 提出在虚拟机管理器层将客户操作系统的行为记录到系统日志中。它主要记录了影响进程运行的非确定性事件:外部输入和定时器。它根据日志记录来进行系统重放,从而分析攻击行为。本系统中设定云计算下异常行为检测系统连接的第三方安全设备的 IP 地址。信息安全设备建档设定本系统处理的 Syslog 信息安全设备来源品牌与 IP。目前可以支持信息安全设备的种类包括思科、华为、飞塔等,如表 2 所示。

表 2　信息安全设备建档

设备 IP	设备种类
127.0.0.1	思科
192.168.10.254	飞塔
110.118.25.154	华为

2)Syslog 格式定义。设定云计算下异常行为检测系统支持的第三方安全设备 Syslog 格式,其中包括设备名称、栏位属性、等级、日志来源、消息类源、状态、协定、来源 IP、源 MAC、来源端口、目的 IP、目的 MAC、目的端口、封包数量、长度、时间、消息等各项属性。Syslog 格式设定如表 3 所示。

表 3　Syslog 格式设定

设备属性	设备 1	设备 2	设备 3
设备名称	思科	飞塔	华为
栏位属性	关键词	关键词	关键词
等级	pri	pri	
日志来源	rmsw		
消息类型	type	type	type
状态	status	status	
协定	proto	proto	PROTO
来源 IP	src	src	SRC
源 MAC	smc		
来源端口	sport	src_sport	SRC
目的 IP	dst	dst	DST
目的 MAC	dmc		
目的端口	dport	dst_port	DPT
封包数量	packets	sent_pkt	
长度	octets	sent	LEN
时间	time	time	
消息	msg	msg	

3)防卫触发条件定义。Syslog 触发云计算下异常行为检测系统“防卫管理”机制。触发条件默认值为异常条件发生的 Syslog,包括 ARP 传感器与流量分析器所设的异常分析。流量分析器使用标准的 netflow 和 sflow 格式,其中对流分析是对该 IP 对外通信的交叉分析;协议分析是指该 IP 对外的通信使用的 TCP 服务分析。

云计算下防卫管理设定:①云计算中各个 VLAN 内广播总数及各类广播的统计图、临界值及触发异常(发送 Syslog)示警;②云计算中计算各网络设备接口的接收端速率、发送端速率、临界值及触发异常(发送 Syslog)示警;③整合云计算下各交换机的侦测环路、CPU 及内存使用率与私接路由器等的侦测,当异常发生时,可以纳入云计算下异常行为检测系统告警与标准处理程序;④云计算下事件追踪——通过指定日期与时段,针对发生异常告警的设备与事件的追踪。

云计算下事件管理和防卫管理架构如图 6 所示。

在图 6 中,不同的形状(例如椭圆、矩形、菱形)分别代表了不同类型和版本的客户操作系统。语义恢复模块植入在管

理域的内核中,与虚拟机中客户操作系统的类型相对应,因此用不同的形状来表示。语义恢复模块以内核模块的方式进行加载,从而动态地对新的虚拟机进行有效的监控,因此也被称为监控驱动。调度管理模块只是对各种监控驱动进行管理,例如加载、卸载等[10]。

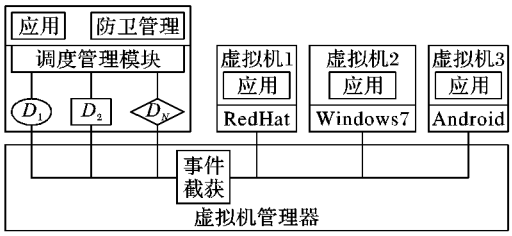

图 6 云计算下事件防卫架构

1.3.3 云计算下 ARP 广播检测

云计算下 ARP 广播检测模块设计了自动学习云计算下设备的 MAC/IP 地址模块、实时检测非法入侵云计算下的网络设备、云计算内部的 ARP 异常侦测、云计算内设备的 MAC/IP/Port 在线列表。

1)攻击源位置追踪。

云计算下攻击源位置追踪最主要的用途是协助管理员确定攻击者的来源,当异常行为检测系统从交换机接收到网络攻击时,管理员最需要的就是根据 IP 或 MAC 地址来搜寻攻击者的位置,加以处理以阻止云计算下的危害蔓延扩大,实时侦测用户并阻断。ARP 广播检测模块可以依据 IP 或 MAC 逐一搜寻比对云计算环境下网络组织设备表内交换机,找出该 IP 或 MAC 来自哪台交换机的哪个端口,并确定设备的空间位置。

2)ARP、MAC/IP 管理。

云计算下 ARP 广播检测模块提供一套 ARP、MAC/IP 安全管控子系统,以透过 IP 与 MAC 相互比对功能,当 IP 与 MAC 无法对应时会将该端口立即锁定关闭,可以确实针对云计算内部每台主机的联机机制实现严格安全管控。云计算下 ARP 安全管控策略字段定义如表 4 所示。

表 4 云计算下 ARP 广播检测各字段含义

参数	云计算下 ARP 广播各字段含义
目的主机分析	访问目的主机数是否超过限制
目的端口数分析	访问 TCP 端口数是否超过限制
规则分析	可限制 IP/MAC/PORT 的时间
ARP IP 扫描分析	IP Scan 是否超过临界值
ARP 异常分析	ARP 封包是否异常
ARP 广播分析	ARP 广播是否超过临界值
IP-MAC 分析	IP/MAC 绑定是否吻合

2 实验分析与结果

云计算异常流量检测系统 V1.0,安装于云计算服务器 IBM System x3650 M3 上,节点数量约 100 个的 VLAN、1 600 个 IP 主机,配合设备,华为 3Com S9512E 核心交换机和思科 4506 和接入交换机,配合操作:核心交换机 H3C S9512E:设定 1 个 VLAN 聚合接口、1 个流量镜像接口;思科 4506R 及接入交换机:开启简单网络管理协议(Simple Network Management Protocol,SNMP)功能,提供只读共同体。实验网络由核心、汇聚和接入三级架构组成,全网 IP 节点数量约 1 600 个,交换路由设备约 30 余台。表 5 给出了云计算下异常流量检测系统的实验分析(部分数据)。系统基于统计学原理,能实时提供云计算环境下异常行为的采集及分析,实现实时流量资料每隔 5 s 自动刷新,且吞吐量可达到 640 Gb/s 的处理能力,能够将被保护链路中异常流量所占用带宽降至总拥有带宽的 5% 以下,解决了云计算下的异常行为检测和防护问题。系统通过对云计算下网络事件的异常行为设定,以及状态检测、连接数管理和流量控制等功能,从带宽和连接数等多个纬度,能够精准实现对云计算资源的合理分配和对异常行为的有效控制,从而达到对外进行异常流量清洗,对内实现流量优化的全面功能,能够解决云计算平台下异常行为的检测与防护问题。

表 5 云计算下异常流量检测系统实验分析(2014-08-07)

序号	用户主机	异常	原因分析
1	132.146.101.3	非法 ARP 封包	中毒虚拟主机或恶意的 ARP 攻击软件如 NetCut 等,发动虚假的 ARP 请求
2	Vlan 220	ARP 广播数量超过警戒范围	云计算下平台大量广播包易造成风暴,耗尽虚拟主机性能
3	132.146.223.254	IP 端口扫描	当黑客攻击前会先扫描本网段在线的主机,然后再实施攻击

截取的云计算异常流量检测系统运行界面如 7、图 8。

图 7 侦测到非法 ARP 封包

从多次仿真运行的情况来看,云计算异常流量检测系统完成了 IP 流量异常分析(目的主机数、目的端口数、会话数);私接设备(非法 DHCP 设备),ARP 行为异常分析(扫描、欺骗、广播)。云计算下异常流量检测系统协助云计算环境实现主动防御机制,监视网络设备的运行状态、分析用户通信的异常行为、追踪可疑用户所在的位置并自动封锁。此外,还可以整合网络中的其他安全设备(如防火墙)、交换机等,构筑一道全网联动的主动防御体系。

上述实验结果验证了云计算异常行为检测系统可以快速定位网络故障,减轻网管工作量的网络故障定位器,实现网络监测和安全防御。云计算环境下有任何异动,即时预警、自动防御、化解危机,降低网络风险、避免网络事故发生,减少管理工作量。云计算异常流量检测系统实现了云计算下异常流量检测、故障排错、事件预警与资源记录等功能,运用云计算环境下网络动态监控、主动防御的管理机制,为云安全提供保障。

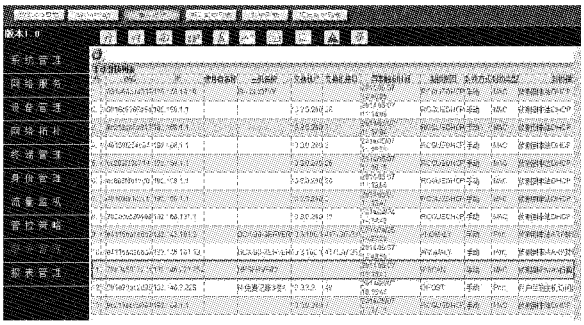

图 8　侦测到 IP Scan 扫描

3　结语

通过虚拟化技术,云计算平台实现了资源共享、弹性分配资源的功能。然而虚拟化的技术特性,使得传统的网络安全手段无法检测从虚拟机内部发动的异常攻击行为,传统网络中存在的蠕虫病毒、未知攻击行为以及 ARP 广播攻击会对云计算平台产生巨大安全威胁。本文设计并实现了融合事件与防卫管理、ARP 广播检测以及针对两种异常行为的异常检测机制的云计算异常行为系统,并且通过嵌入在虚拟机管理器的虚拟网关功能,将虚拟机之间的流量重定向外部的检测系统中进行处理,经实验表明,有效解决了云计算下异常行为的检测和防护问题。下一步的工作将针对云计算环境下越来越多变的异常行为,提升本系统的通用性。

参考文献:

[1] ARMBRUST M, FOX A, GRIFFITH R, *et al*. A view of cloud computing [J]. Communications of the ACM, 2010, 53(4): 50 – 58.

[2] FENG D, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2012, 22(1): 71 – 83. (冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71 – 83.)

[3] SHAO G, CHEN X, YIN X, *et al*. Design and implementation of virtual machine traffic detection system based on OpenFlow [J]. Journal of Computer Applications, 2014, 34(4): 1034 – 1037. (邵国林, 陈兴蜀, 尹学渊, 等. 基于 OpenFlow 的虚拟机流量监测系统的设计与实现[J]. 计算机应用, 2014, 34(4): 1034 – 1037.)

[4] LOCKWOOD J W, MOSCALA J, KULIG M. Internet worm and virus protection in dynamically reconfigurable hardware [C]// Proceedings of the 2003 ACM CCS Workshop on Rapid Malcode. New York: ACM, 2003: 1 – 8.

[5] XIN Y, FANG B, HE L, *et al*. Worm detection and signature extraction based on communication characteristics [J]. Journal on Communications, 2007, 28(12): 1 – 7. (辛毅, 方滨兴, 贺龙涛, 等. 基于通信特征分析的蠕虫检测和特征提取方法的研究[J]. 通信学报, 2007, 28(12): 1 – 7.)

[6] ZHU H, LI W, SHI H. Peer behavior based proactive P2P worm detection[J]. Computer Engineering and Applications, 2013, 49(7): 93 – 97. (朱晖, 李伟华, 史豪斌. 基于节点行为的主动 P2P 蠕虫检测[J]. 计算机工程与应用, 2013, 49(7): 93 – 97.)

[7] SU M. Using clustering to improve KNN-based classifiers for online anomaly network traffic identification[J]. Journal of Network and Computer Applications, 2011, 34(2): 722 – 730.

[8] SHAH B, TRIVEDI H B. Artificial neural network based intrusion detection system: a survey[J]. International Journal of Computer Applications, 2012, 39(6): 13 – 18.

[9] GUAN X, QIN T, LI W, *et al*. Dynamic feature analysis and measurement for large-scale network traffic monitoring [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 905 – 919.

[10] XIANG G, JIN H, ZOU D, *et al*. Virtualization-based security monitoring[J]. Journal of Software, 2012, 23(8): 2173 – 2187. (项国富, 金海, 邹德清, 等. 基于虚拟化的安全监控[J]. 软件学报, 2012, 23(8): 2173 – 2187.)

[11] LIU Q, WANG G, WENG C, *et al*. A mandatory access control framework in virtual machine system with respect to multi-level security I: theory[J]. China Communications, 2010(4): 137 – 143. (刘谦, 王观海, 翁楚良, 等. 一种虚拟机系统中关于多级安全的强制访问控制框架 I: 理论[J]. 中国通信, 2010(4): 137 – 143.)

[12] LIU Q, WANG G, WENG C, *et al*. A mandatory access control framework in virtual machine system with respect to multi-level security II: implementation [J]. China Communications, 2011(2): 86 – 94. (刘谦, 王观海, 翁楚良, 等. 一种虚拟机系统下关于多级安全的强制访问控制框架 II: 实现[J]. 中国通信, 2011(2): 86 – 94.)

[13] DUNLAP G W, KING S T, CINAR S, *et al*. ReVirt: enabling intrusion analysis through virtual-machine logging and replay[C]// Proceedings of the 5th Symposium on Operating Systems Design and Implementation. New York: ACM, 2002: 211 – 224.

(上接第 1283 页)

[8] CHEN L, XIAO M, GAO F. Artificial bee colony algorithm for parallel test tasks scheduling [J]. Computer Measurement and Control, 2012, 20(6): 1470 – 1472. (陈利安, 肖明清, 高峰. 人工蜂群算法在并行测试任务调度中的应用[J]. 计算机测量与控制, 2012, 20(6): 1470 – 1472.)

[9] LI X, SHEN S, LU H. Algorithms of tasks scheduling in parallel test based on graph coloring theory [J]. Journal of Beijing University of Aeronautics and Astronautics, 2007, 33(9): 1068 – 1071. (李昕, 沈士团, 路辉. 基于图染色理论的并行测试任务调度算法[J]. 北京航空航天大学学报, 2007, 33(9): 1068 – 1071.)

[10] PU B, TAO S. Coloring problem in solving graph with genetic algorithm[J]. Computer Development and Applications, 2001, 14(2): 26 – 27. (蒲保兴, 陶世群. 遗传算法求解图的染色问题[J]. 电脑开发与应用, 2001, 14(2): 26 – 27.)

[11] LIU Y, WU Y, DENG X. Parallel test of advanced avionics system based on timed Petri net and artificial bee colony algorithm [J]. Measurement and Control Technology, 2014, 33(11): 37 – 41. (刘云周, 吴勇, 邓雪杰. 基于时延 Petri 网和人工蜂群算法的航电系统并行测试研究[J]. 测控技术, 2014, 33(11): 37 – 41.)

[12] FANG Y, XUE H, XIAO M. Parallel test tasks scheduling and resources configuration based on GA-ACA [J]. Journal of Measurement Science and Instrumentation, 2011, 2(4): 321 – 326.