应用于云计算中心的虚拟主机安全防护系统

王 茜[1],朱志祥[2],葛 新[1],杜 迟[1]
(1. 西安未来国际信息股份有限公司,陕西 西安 710063;
2. 西安邮电大学,陕西 西安 710121)

摘 要:针对云计算环境下的安全防护问题,文中提出了一种云计算中心虚拟主机安全防护系统。系统以“安全即服务”为出发点,以虚拟机为核心,针对虚拟化计算无边界的特点,以虚拟机群为单位,提供统一的安全防护。为云平台下的不同应用、租户、虚拟主机提供定制化的安全服务,以安全防护模板的形式对不同的安全性需求进行量身定制,将安全防护措施软件化、安全功能组件化、部署方式动态化、配置管理自动化,使安全处置手段不断更新,从而建立起了集各种安全措施为一体的自适应云平台安全防护体系。

关键词:云计算;虚拟主机防护;云安全;安全域
中图分类号:TP302.1 **文献标识码**:A **文章编号**:1673-629X(2014)03-0134-04
doi:10.3969/j.issn.1673-629X.2014.03.034

A Virtual Host Protection System Applying to Cloud Computing Center

WANG Qian[1], ZHU Zhi-xiang[2], GE Xin[1], DU Chi[1]
(1. Xi'an Future International Information Co., Ltd., Xi'an 710063, China;
2. Xi'an University of Posts & Telecommunications, Xi'an 710121, China)

Abstract: A virtual host protection system applying to cloud computing center is constructed in this paper to guarantee the security of cloud computing. Virtualization calculation has the characteristics of being no boundary. According to this, the virtual host protection system provides a unified security for cloud computing by taking security-as-a-service as a starting point, the virtual machine as the core, and the virtual cluster as a unit. Customized security services are provided for different applications, multi-tenancy, and virtual hosts on the cloud computing platform. The security template is tailored to satisfy the different security needs. The security protection measures are realized by software, the security function is achieved by components, the deployment method becomes dynamic, the configuration management becomes automatic, and the security disposal means are updated constantly. Then the adaptive security protection system integrating with a variety of security measures for cloud computing platform is built.

Key words: cloud computing; virtual host protection; cloud security; security domain

1 概 述

云计算是信息技术领域的一次变革,是信息技术发展的必然趋势和信息技术深度应用的必然结果,也必然对信息安全保障产生重大影响[1-3]。

在电子通讯时代,为了实现通讯保密,信息安全技术的主要研究内容以密码技术为主。进入计算机时代后,信息安全的理念有了新变化,主机安全成为信息安全的主要研究目标,以安全模型分析与验证为理论基础,以信息安全产品为主要构件,以安全域建设为主要目标的安全防护体系思想逐渐成为主流[4-7]。

在云计算时代,计算资源、存储资源、数据资源等高度共享,使其成为真正的基础资源,从而使得普通用户能够享用更高端的 IT 服务。云计算这一创新模式,也给信息安全带来了挑战和机遇,因此急需实现云计算环境下的数据安全与隐私保护,实现多租户环境的安全计算,实现涉及关键技术、标准、法规建设、国家监督管理制度等多层次、全方位的变革[8-12]。

1)传统安全防护模式。

(1)在传统网络安全防护模式下,各种硬件安全设备一层又一层地对网络计算环境进行安全防护,但各个安全设备之间缺乏协同防护及统一管理;

(2)云平台下安全防护的粒度越来越细,并且需

收稿日期:2013-05-21 **修回日期**:2013-08-26 **网络出版时间**:2014-01-07
基金项目:陕西省自然科学基金(2012JM7017)
作者简介:王 茜(1966-),女,博士,高级工程师,研究方向为电子政务;朱志祥,博士,教授,研究方向为网络与信息安全技术。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140107.1720.040.html

要及时对所面临的安全威胁做出统一的策略响应,传统的网络安全模式实施起来工作量非常大,这对安全管理水平提出了较高的要求;

(3)传统网络安全防护模式所针对的安全防护对象与云平台下虚拟化对象有很大不同,现有的安全手段已经不能满足云平台的安全性需求,尤其是在云平台下引入了多租户概念,对安全管理和安全措施的量身定制提出了更高要求;

(4)在大规模云计算平台下,如果只是依靠传统的网络安全防护模式,依靠大量的网络安全设备的投入,那么高额的投入成本将使企业难以承受,而且安全设备的使用效率也是个问题。

2)云计算安全防护模式。

根据云平台的特点,文中提出的虚拟主机安全防护方案变革了传统网络安全防护手段,解决了云计算环境下虚拟化和多租户所产生的安全问题。

(1)以一体化机柜为基本单元,一体化机柜既是云平台部署和运维管理的基本单元,也是安全防护的基本单元,同一机柜中的主机属于同一安全域;

(2)以组件化的形式提供安全设备,可以根据需求不断扩展新的安全组件;

(3)以安全组件为基础建立安全措施库,根据不同的安全需求类型,定制不同的安全措施模板;

(4)引入 Secaas(Security-as-a-service)“安全即服务”,使不同的租户专享个性化的安全服务;

(5)针对云平台下的安全性需求,设计开发加解密引擎、密钥管理等安全组件。

2　虚拟主机防护系统总体结构

针对大规模云计算数据中心的特点,文中研究开发了云计算中心虚拟主机安全防护系统(以下简称“虚拟主机防护”),虚拟主机安全防护系统以“安全即服务”为出发点,以虚拟机为核心,针对虚拟化计算无边界的特点,以虚拟机群为单位,提供统一的安全防护。为云平台下的不同应用、租户、虚拟主机提供定制化的安全服务,以安全防护模板的形式对不同的安全性需求进行量身定制,将安全设备组件化,可以不断地更新安全处置手段,最终建立集各种安全措施为一体的自适应云平台安全防护体系。其核心思想是将安全防护措施软件化、安全功能组件化、部署方式动态化、配置管理自动化,为不同的应用、不同的租户提供可定制的按需安全服务,并做到安全防护服务按需配置、按需部署和按需监管。

图 1 为虚拟主机防护系统总体结构,虚拟主机防护系统由虚拟主机防护管理中心、虚拟主机防护组件库、虚拟主机防护策略模板库、安全防护节点组成。其中,安全管理中心通过收集安全节点的日志信息能够动态监控云计算中心的安全状态信息。

系统采用分布式部署方式,在云计算中心的每个机柜中部署安全节点,安全节点使用透明模式进行部署。安全节点中运行安全防护组件,所有的安全节点由虚拟主机防护管理中心统一管理控制。

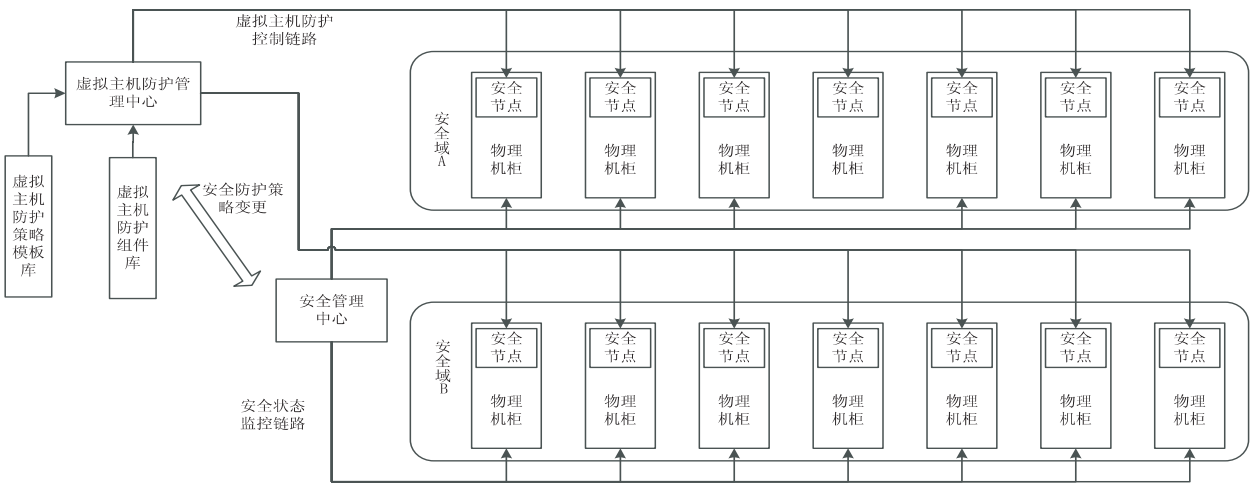

图 1　虚拟主机防护系统结构图

3　安全防护节点

虚拟主机安全防护节点是一个网关类型的安全防护设备。系统使用 Linux 系统内核组件获取网络通信流量,通过对网络流量的分析、处理达到安全防护的效果。安全节点中运行着以组件方式存在的安全防护组件,这些组件主要包括入侵检测/防御组件、防火墙组件、防病毒组件等,根据不同安全域的安全防护需求,安全防护组件由虚拟主机防护管理中心统一下发到各个安全节点中,同时针对不同的需要进行防护的安全事件与不同的安全防护组件,虚拟主机防护管理中心从虚拟主机防护策略模板库中提取防护策略模板,根据安全域内实际的网络和虚拟主机情况编译成为安全防护组件能够执行的安全防护策略,并把这些策略下发到对应安全节点的安全防护组件中。

安全防护节点示意图如图 2 所示。

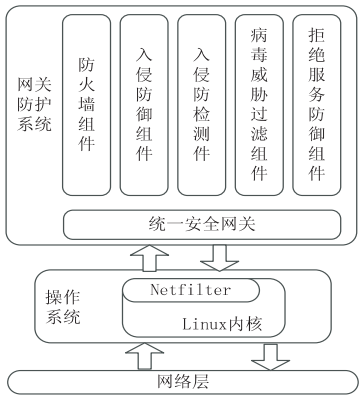

图 2 安全防护节点示意图

4 安全防护组件

4.1 入侵检测/防御组件

入侵防御可以拦截所有网络流量,通过基于已知攻击模型的特征码检测技术,能够检测出网络内部的恶意行为。在阻断恶意用户的同时,入侵防御功能对于用户完全透明,对网络性能也没有任何影响。入侵防御组件逻辑框架如图 3 所示。

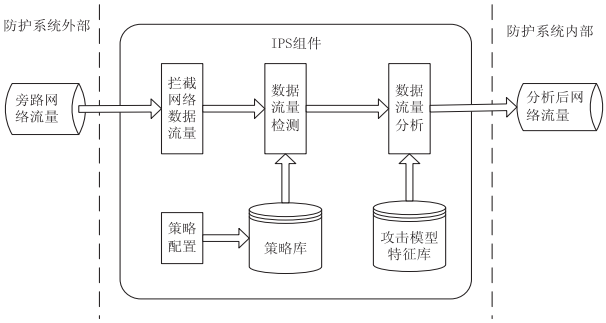

图 3 入侵防御组件逻辑框架图

入侵防御组件关键技术点:

1)可设定特定的特征码阻止并记录攻击行为。

2)使用自定义规则和变量来创建新的特征码。

4.2 防病毒组件

网关防病毒技术主要有两部分,一是如何对进出网关的数据进行查杀;二是对要查杀的数据进行检测与清除。

网关防病毒通过文件解压,将数据包还原成文件进行病毒扫描。防病毒网关能够检测进出网络内部的数据,对 HTTP、FTP、SMTP、IMAP 四种协议的数据进行病毒扫描,一旦发现病毒就会采取相应的手段进行隔离或查杀,在防护病毒方面起到了非常大的作用。网关防病毒组件逻辑框架如图 4 所示。

网关防病毒组件关键技术点:

1)可配置的控制策略,根据配置策略对进出网络内部数据流量类型进行扫描。

2)HTTP:通过文件扩展名或 MIME 类型进行可配置的扫描。

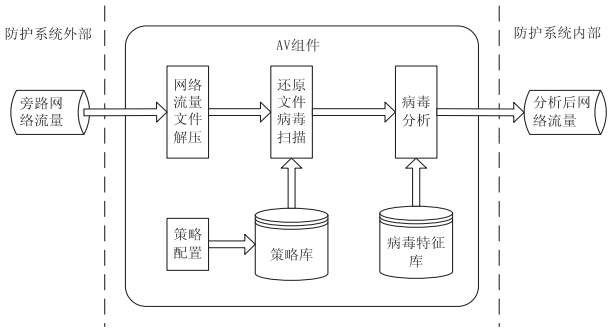

图 4 网关防病毒组件逻辑框架图

3)SMTP:查杀病毒并可设定为清除感染、阻止或允许、包含或不包含发送者/接收者。

4)POP 和 IMAP:查杀病毒并可设定为清除感染或放行(POP 和 IMAP 的协议特性使邮件不能够被阻止,但可被扫描并被清除)。

5)FTP:可以禁止 FTP 下载。

4.3 防火墙组件

防火墙组件通过划分内外网的界线,在网络边界处搭建第一道安全防线。虚拟主机防护的防火墙基于简单、灵活的规则来监控和阻止网络流量,通过用控制网络协议、源地址或源端口,目的地址或目的端口等手段来实现网络流量的控制。防火墙组件逻辑框架如图 5 所示。

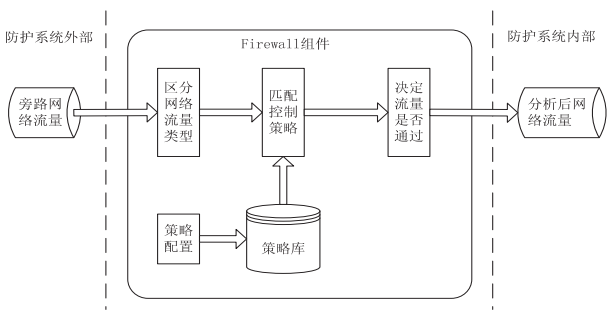

图 5 防火墙组件逻辑框架图

防火墙组件关键技术点:

1)建立防火墙策略控制的数据库,方便维护防火墙策略。

2)用户可以根据协议、源地址、目的地址、源端口、目的端口定义防火墙策略。

3)用户可以自定义防火墙策略匹配命令。

5 虚拟主机认证

虚拟主机认证是为了保证用户与虚拟主机之间的身份互信,为了完成这种互信机制引入了基于公开密钥体系的身份认证机制。在虚拟主机建立时为虚拟主机发放一对身份密钥,最终用户的身份也是使用一对密钥进行标识,用户登录虚拟主机时,用户身份,虚拟主机身份均通过多级跨域认证系统进行认证,完成虚

拟主机与最终用户之间的身份互信。

虚拟主机认证框架图如图 6 所示。

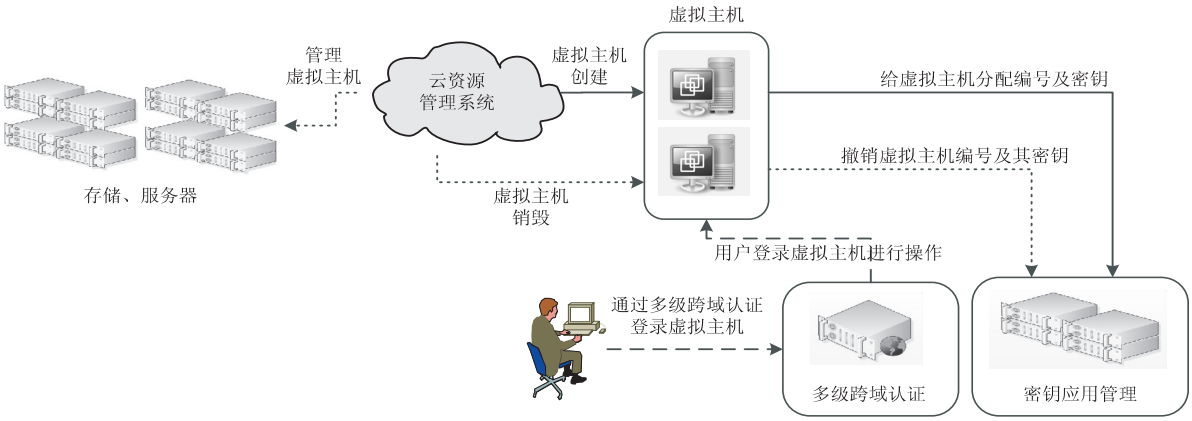

图 6　虚拟主机认证框架图

6　应用案例

虚拟主机防护系统已经在陕西省信息化综合服务中心及榆林市信息化综合服务平台等系统中上线部署运行,在实际运行中,虚拟主机采用物理主机部署方式,在数据中心的每个机柜中部署一个安全防护节点,该防护节点通过桥接或路由模式串联接入机柜网络中。每个安全防护节点中运行统一安全网关,各个安全防护组件如入侵检测组件、防病毒组件、防火墙组件等运行在统一安全网关中。

虚拟主机防护系统统一管理数据中心内所有安全防护节点,虚拟主机防护组件库存储所有组件化、模块化的安全防护组件,根据不同的安全防护需求通过虚拟主机防护管理中心将安全防护组件下发到各个安全防护节点;同时将虚拟主机防护模板策略库中不同的安全防护策略经过编译后下发到各个安全防护组件。

实际运行过程中可向安全防护模板策略库增加新的防护策略模板以应对不同的安全防护需求。

7　结束语

文中提出了一种针对云计算环境下虚拟主机的安全防护方案,根据该方案已经开发出了实际系统,并在一些数据中心投入正式运行,目前该数据中心根据承载业务系统的特点划分了不同的安全域,每个安全域执行不同的安全防护策略。虚拟主机防护系统管理不同的机柜中的安全防护节点,根据安全域的划分将多个安全防护节点从逻辑上划归为一个有着相同安全防护要求的安全域,为每个安全域中的多个安全防护节点部署同样的安全防护组件,在这些安全防护组件上执行相同的安全防护策略。同时,对单个安全域中的某个安全节点可以增加更多的安全防护策略。这样就能形成基于安全域并针对虚拟主机的整体安全防护,同时又可以针对特定的需求提高单个安全节点的保护强度。针对云计算虚拟化环境中安全防护边界模糊的实际情况,文中提出的虚拟主机防护方案通过依赖物理边界的分布式安全防护,为云计算数据中心构建出动态、安全、完善的信息安全防护体系。

参考文献:

[1] 林果园,贺　珊,黄　皓,等. 基于行为的云计算访问控制安全模型[J]. 通信学报,2012,33(3):59-66.

[2] 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] 梁　彪,曹宇佶,秦中元,等. 云计算下的数据存储安全可证明性综述[J]. 计算机应用研究,2012,29(7):2416-2421.

[4] 李春光,赵　彬,周保群. 一种基于行为的主机入侵防护系统设计与实现[J]. 计算机工程,2007,33(6):129-131.

[5] 初晓博,秦　宇. 一种基于可信计算的分布式使用控制系统[J]. 计算机学报,2010,33(1):93-102.

[6] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[J]. SIAM journal on computing, 2003, 32(3): 586-615.

[7] 柳晓春. 虚拟可视性:在虚拟环境中应对合法监听挑战[J]. 计算机安全,2012(6):84-87.

[8] 许　蓉,吴　灏,张　航. "云安全"检测技术安全性分析[J]. 计算机工程与设计,2012,33(9):3309-3312.

[9] 陈　全,邓倩妮. 云计算及其关键技术[J]. 计算机应用,2009,29(9):2562-2567.

[10] Mather T, Kumaraswamy S, Latif S. Cloud security and privacy[M]. [s. l.]: O'Reilly Media, 2009.

[11] 陈丹伟,黄秀丽,任勋益. 云计算及安全分析[J]. 计算机技术与发展,2010,20(2):99-102.

[12] Wu Hanqian, Ding Yi, Chuck W, et al. Network security for virtual machine in cloud computing[C]//Proceedings of 5th international conference on computer, sciences and convergence information technology. Seoul, Korea: [s. n.], 2010: 18-21.

应用于云计算中心的虚拟主机安全防护系统

作者： 王茜， 朱志祥， 葛新， 杜迟， WANG Qian， ZHU Zhi-xiang， GE Xin， DU Chi

作者单位： 王茜,葛新,杜迟,WANG Qian,GE Xin,DU Chi(西安未来国际信息股份有限公司,陕西 西安,710063)， 朱志祥,ZHU Zhi-xiang(西安邮电大学,陕西 西安,710121)

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(3)