新的云安全解决方案及其关键技术

徐迎迎 高 飞 尚锋影 朱君礼
(北京邮电大学网络与交换技术国家重点实验室,北京 100876)

摘要 为了融合当前主流的云安全解决方案的优点并弥补不足,提出一种包括服务器和客户端,更全面、高效的云安全框架.服务器端包括基于信誉服务的主动防御模块和基于病毒行为分析的被动查毒杀毒(简称查杀)模块,两模块共享数据、协同工作;客户端采用多层次访问控制模型完成病毒本地查杀、威胁预防和可疑病毒发现.通过服务器集群和海量客户端的共同合作,使得此云安全框架集主动防御和被动查杀于一体,具有全方位、强有力的病毒查杀能力.

关键词 云安全;病毒防范;杀毒;云计算;入侵检测
中图分类号 TP309.5 **文献标志码** A **文章编号** 1671-4512(2012)S1-0074-05

New cloud security solutions and its key technologies

Xu Yingying Gao Fei Shang Fengying Zhu Junli
(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract Traditional signature-based detection solution for viral diversification and the complexity of the malicious attacks has been increasingly unable to meet the requirements. Therefore, the antivirus vendors had proposed the concept of cloud security. The prevalent cloud security solutions was introduced. In order to integrate the advantages of them and make up for their shortcomings, a more comprehensive and efficient cloud security architecture including server clusters and mass clients was put forward. The server-side has two core modules. One is responsible for the active defense based on reputation of resources, and the other completes positive defense by using technology of virus behavior analysis. They cooperate and share information with each other to improve accuracy of reputation service and the effectiveness of virus analysis. The multi-level access control model in client was designed to complete local defense, threat prevention and the discovery of suspicious virus. The server clusters and mass users work together and finish both active prevention and positive defense, so this solution gets the capabilities of comprehensive and powerful virus defense.

Key words cloud security; virus prevention; anti-virus; cloud computing; Intrusion detection

在云计算和云存储等技术得到普遍研究和应用的今天,云安全的概念同样得到了广泛关注,其有2层意思:a. 云计算的安全,包括云端数据存储安全和云端服务器之间数据传输等安全;b. 云计算作为服务应用到杀毒领域,即利用并行计算、网格计算和未知病毒行为分析判断等先进技术和概念,通过互联网把用户和全球各地的杀毒软件厂商的服务器集群[1].本研究讨论的云安全概念属于后者.病毒防范技术是网络安全领域关注的焦点,也是保证网络安全,保护互联网用户的社会、经济利益不可或缺的关键技术,然而,传统的基于主机的静态特征码比对技术多年来一直走的是解毒路线,即当部分用户中毒并反馈时,杀毒企业才能给出病毒特征码,供客户端下载完成本地查杀防护.这种静态查杀方式有2个明显缺点:第一,从病毒的产生到安全厂商提供病毒特征码这

收稿日期 2012-08-20.
作者简介 徐迎迎(1987-),女,硕士研究生,E-mail: a0651128xuyingying@126.com.

段空窗期内，大量互联网终端处于无保护状态，而且随着病毒隐藏和变异技术的发展，只有少数病毒能被及时发现并产生查杀方案；第二，用户端保存庞大病毒特征库，并需不断与厂商的防毒数据中心连网更新，占用大量客户端网络带宽和系统资源，影响用户终端性能. 另外，基于 Web 的网络威胁可以将看似无害的恶意代码组成恶意攻击的感染链，传统的杀毒方法对这种采用多层次、多协议的复合式攻击显然无能为力[2].

为了解决传统杀毒技术无能为力的问题，国内外安全厂商结合云计算技术的发展，提出了云安全的概念，即从单机版的解毒转换成基于网络的主动防毒，不再以用户计算机作为杀毒的“战场”，而是使互联网本身成为一个巨大的杀毒软件[3]，通过部署海量的服务器集群和借助云计算相关技术把病毒查杀作为一种服务提供给互联网用户.

1　主流云安全解决方案

1.1　方案 A：轻客户端＋主动防御

云安全解决方案 A 的核心在于超越了拦截 Web 威胁的传统方法，转而借助威胁信息汇总的全球网络[4]，其基于云计算强大的并行处理能力，构建了庞大的服务器集群来保存网络资源的信誉信息，并可以完成客户端快速的查询，提供了一种更快更全面的及时保护. 趋势科技为首的安全厂商提出方案 A，陆续推出云安全 1.0，2.0，3.0 方案来不断完善资源信誉服务技术，云安全 1.0，2.0方案重点实现如何通过多项指标给出网络资源安全级别，来阻挡用户对不安全信息的访问. 网络资源的信誉分值是用历史统计结果来决定的，不会根据某一时刻的表现来判断某个网站或者邮件的安全程度，而是历史的、动态的、加权的判定，这种方式极大地避免了误判的情形，并能在威胁到达网络终端之前予以防护.

云安全 3.0 则在原有技术方案的基础上提出从云安全到安全云的转变，不但用云计算服务来保护互联网安全还提供云计算环境本身的安全保护，从而丰富了云安全的概念，也拓展了趋势科技云安全解决方案的应用领域.

1.2　方案 B：互联网就是杀毒软件

云安全解决方案 B 主要包括 3 部分：数以亿计的客户端、与数百家互联网公司合作、高性能云安全服务器[2]. 目前瑞星及其合作公司的终端软件都集成了“云安全探针”，可以监控软件异常行为信息，如访问带有病毒的网页，木马开始运行文件并对注册表关键位置修改的动作，截获互联网中的木马、恶意程序的最新信息，然后推送到服务器端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端，其他客户端就可以对这种危害防患于未然，这样就切断了病毒通过互联网应用进行传播的途径. 海量客户端和高效病毒分析能力服务器组成轻量级的行为检测系统，它把互联网本身变成了巨大的杀毒软件，并渗透到了从服务器、路由器到用户电脑的互联网上的每个角落，从而极大提高病毒查杀效率和覆盖率，有效地阻止病毒入侵网络.

方案 B 须要解决 4 大难题：海量的云安全探针；专业的反病毒经验以及技术；大量资金以及技术投入；系统具有开放性并允许合作伙伴加入.

2　2 种方案面临的问题

方案 A 的云安全中的“云”指的是部署在全球的服务器集群[2]，快速高效地处理来自客户端对网络资源信誉的查询请求；但在方案 B 中安装了“云安全探针”的海量用户终端组成庞大的云[5]，而负责病毒识别的服务器反倒成了“云”客户端. 下面分析两种方案的优缺点.

方案 A 是主动防御，能在网络威胁到达主机之前对其进行拦截、监控、处理，但不能对通过 U 盘、移动硬盘等其他渠道已经进入到终端的未知病毒、木马等实行有效检测和查杀，而且还面临庞大网络资源信誉值如何广泛、实时采集的问题；

方案 B 属于被动防御，只能对已经进入到用户终端并开始异常行为的未知的病毒、木马实行防护，却不能应对复杂网络威胁[5]. 它不但对海量的“云安全探针”有很大的依赖性，而且存在处理可疑病毒查询的速度问题，此方案实则为传统解毒模式的互联网化.

另外，随着当前病毒技术不断更新发展，病毒种类越来越复杂，入侵方式也越来越多样，病毒隐藏技术也越来越高深，目前的云安全处理方案，单单是主动防御或者单单被动查杀都不能最好地扭转病毒威胁越来越严重的局面，也不能让云计算带来的处理优势在杀毒领域发挥到极至.

3　新的云安全解决方案

为了弥补主流云安全处理方案的弊端，思考能否以融合两种方案为基础，提出一种融合两者

优点又解决其面临问题的新方案,答案是肯定的,但不是机械式的组合. 本文将提出一种新的云安全解决方案,并阐述适用于新方案下的服务器和客户端关键技术.

3.1 方案整体架构

新方案的总体结构就是融合服务器集群组成的"云"和海量客户端组成的"云"来组成一个集主动防御和被动查杀于一身的杀毒"云". 服务器端借助并行处理、虚拟化、分布式计算等云计算技术完成病毒智能化分析和网络资源信誉服务;海量客户端安装在网络各个角落实现终端保护. 新方案整体架构和处理流程如图1和图2所示.

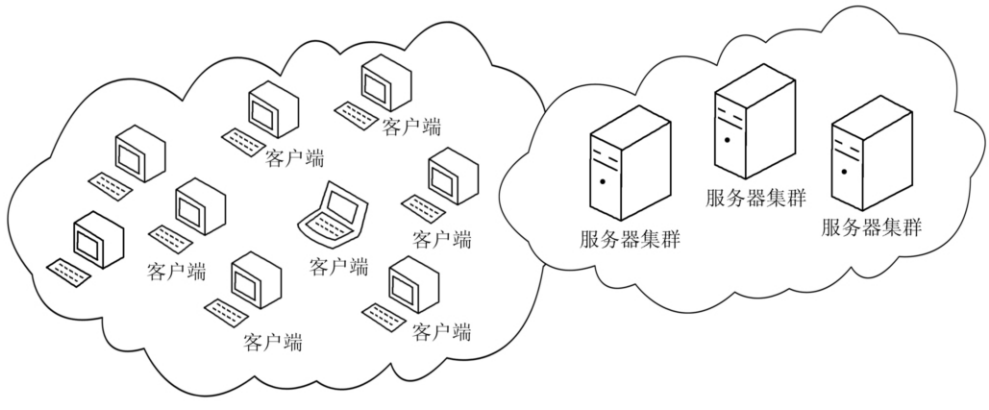

图1 新方案整体构架

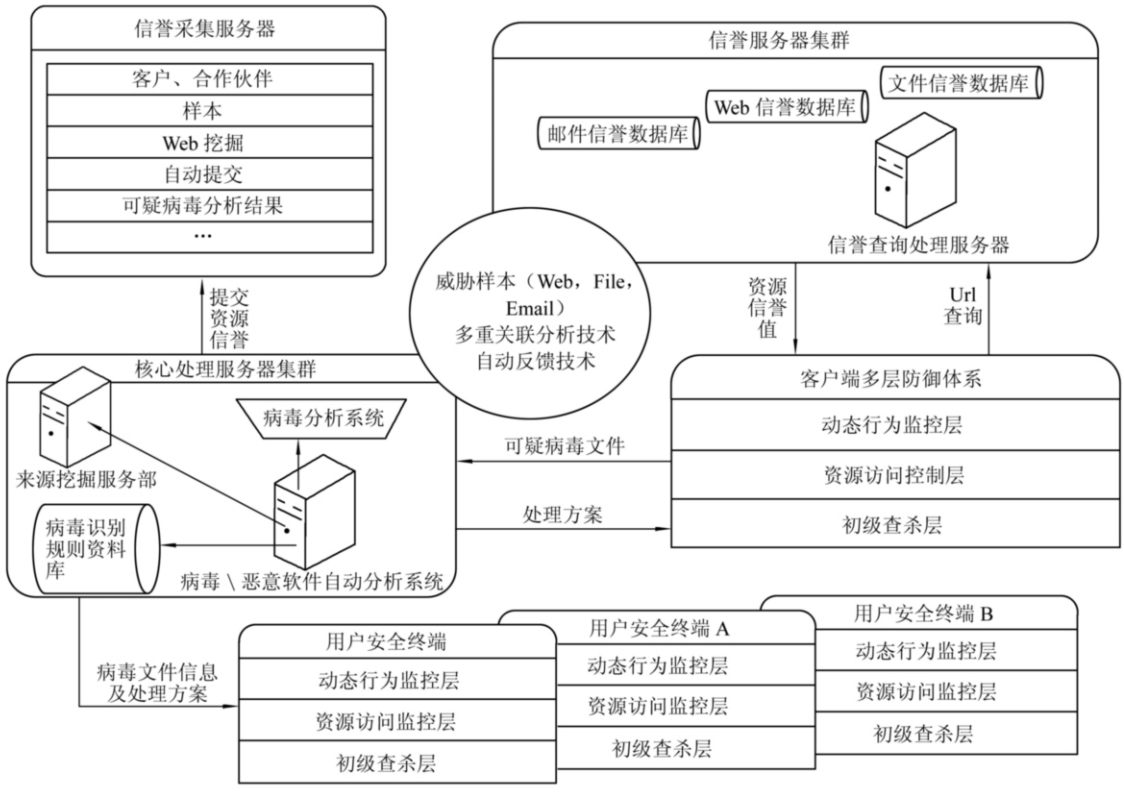

图2 新方案处理流程图

下面介绍新的云安全解决方案总体构架.

3.1.1 部署高性能的云端服务器

信誉服务器完成Web资源、Email和File的动态信誉评价,快速响应客户端对网络资源安全性的查询;病毒分析处理服务器根据可疑病毒文件的行为信息确定查杀方案,并推送给海量云安全客户端. 2类服务器还须进行如病毒来源和资源信誉评价指标等数据的交互,从而提高其性能.

3.1.2 安装海量杀毒客户端

新方案要求互联网上尽可能多的终端安装杀毒客户端,它不但根据终端状态动态地、分层次地请求云杀毒服务完成保护,还负责采集病毒样本并将其作为资源信誉评价的参考.

海量客户端分布在互联网每个角落的网络设

备上，云杀毒服务模块可以部署在多家安全厂商的高性能服务器集群中，让每个互联网计算机都为网络安全贡献一份力量，实现杀毒互联网化.

3.2　服务器端关键技术

3.2.1　网络资源信誉采集、动态评定与快速查询

信誉采集服务器通过诸如客户、合作伙伴、样本采集、Web 挖掘、可疑病毒分析结果等多种渠道结合行为关联分析技术、自动反馈机制、威胁信息汇总技术提供 Web 信誉服务、电子邮件信誉服务、文件信誉服务. 具体来说，就是根据网站页面的历史位置变化和可疑活动迹象等因素来动态指定 Web 信誉分值；根据邮件源 IP 地址的“行为”、“活动范围”以及历史分值进行不断地分析而加以细化产生邮件信誉等级；根据已知的良性文件清单和已知的恶性文件清单等多项指标确定文件信誉分值[8].

服务器端通过并行计算、分布式计算等技术高效、快速地完成多种网络资源的安全分析，并根据多种指标动态、准确计算，还需要借助虚拟化技术存储大量信誉资料. 其核心查询引擎负责快速处理来自客户端对资源安全性的查询请求.

3.2.2　病毒样本智能分析、存储与分发

云端服务器部署“病毒/恶意软件自动分析系统”能够对客户端提交的可疑病毒样本进行自动分类、家族特征提取、病毒工程师分析等流程完成海量病毒的自动分析，并产生处理方案推送给所有客户端. 在病毒识别分析过程中，借助来源挖掘服务器找到可疑病毒来源，使得信誉服务器提供的病毒源信誉值成为病毒识别的一个标准，并且病毒分析系统的分析结果也将实时影响该资源信誉值. 这样，云端服务器病毒识别和资源信誉服务器相互协作，提高病毒识别覆盖率、减少误报率.

3.3　客户端关键技术

云安全客户端进入到用户终端，并近距离和病毒进行“肉搏”，需要全方位、多层次、智能化的主动防御体系.

3.3.1　第 1 层：初级查杀层

客户端可以下载部分典型或者简单病毒特征码，按照传统的杀毒方式在本地完成初级查杀. 这样，不但过滤出一部分病毒减少网络请求和处理，也保证了即使在断网状态下也能对系统进行简单的应急保护. 这也体现了新的云安全技术需要和传统杀毒方案进行结合的思想.

3.3.2　第 2 层：资源访问控制层

资源访问控制可分为网络资源访问控制和本地资源访问控制. 其中网络资源包括 Web 访问、邮件和文件等，在主机对这些资源进行访问之前，信誉查询触发器能够及时向云端发起资源信誉查询请求，根据返回的资源信誉等级确定是否阻断访问；另外，客户端需要检测系统资源（如注册表、文件、系统 API、引导区等）进行规则化控制[6]，控制木马、病毒等恶意代码对他们的访问，杜绝攻击的发生. 由此可知，资源访问控制层在病毒进入主机和产生危害之前进行主动防御；

本层控制还需考虑提高用户体验，可以根据用户对安全的要求程度定制阻断级别，对于可疑资源访问控制，用户也是可以参与进来的.

3.3.3　第 3 层：动态行为监控层

一旦病毒通过变异、隐藏技术逃过以上两层的检测，开始进行攻击，动态行为检测层也会采用“智能网页脚本行为判断”和“本机程序行为判断技术”等防御技术来感知可疑行为[7-9]，并把检测到的可疑病毒信息迅速上传给云服务器，利用服务器端强大的分析处理能力，得到解毒方案，完成病毒查杀[10]；

另外，除了这 3 层防御体系，云安全客户端需要提供旁路接入不影响终端正常业务，防护级别用户可定制，感知危险形成危险报告等服务.

4　方案分析

4.1　新方案优点

a. 云服务器端以并行处理、分布式处理、虚拟化、数据存储等云计算技术为基础，结合专业病毒查杀的安全经验，实现了集网络资源信誉服务和病毒分析、识别、处理能力于一体的目标. 服务器端两模块协同合作，数据共享，提高了云端服务器的性能.

b. 客户端采用 3 层访问控制模型，不同种类病毒分级处理，多种进攻全面覆盖，不但扩充了云端病毒样本库还为病毒源头网络资源信誉评价提供参考，在享受云安全保护的同时，也为互联网安全贡献一份力量. “云安全”客户端遍布在从服务器、路由器到用户电脑的每个角落，极大提高病毒查杀效率和覆盖率，有效地阻止病毒入侵网络.

c. 新方案集主动防御和被动查杀于一体，实现全方位、强有力的病毒查杀能力，充分体现了云计算应用到安全领域的高效性. 另外，组成“杀毒服务器云”和“用户云”让每个互联网用户都参与到病毒防范中来，真正实现了防毒杀毒互联网化.

4.2　待解决问题

a. 部署成本高、管理难度大. 此方案要求安

全厂商部署服务器集群和海量客户端探针,不但成本高,而且管理难度大.安全厂商有专业的安全知识,却不一定能较好完成服务器集群和海量数据高效的管理工作.

b. 安全厂商合作,标准统一.为了实现杀毒互联网化,需要安全厂商通力合作,新技术建立统一标准,改变目前安全厂商各自为战的局面,实现技术、人力、软硬件资源价值的最大化.

c. 云结构的细化与管理,提高杀毒服务质量.新方案要求几乎互联网上的所有网络设备都参与到杀毒防毒的工作中来,但由于处理不同业务的网络设备对安全性要求是不同的,因此应该在云安全的网络体系架构上进行优化设计,例如分层结构、区域划分等管理.

d. 安全问题.服务器集群由于其数据庞大和业务处理复杂、重要性等特点,必将成为恶意攻击的目标,因此需要利用云计算的安全技术,保证用户信息、病毒样本和资源信誉值等数据的安全和服务器运行的安全.

上述问题并不是伴随新方案产生,而是所有云安全解决方案都要面对和重点关注的问题,所以真正实现杀毒互联网化、提高全网安全是未来工作需要研究的重点问题.

参 考 文 献

[1] Oberheide J, Cooke E, Jahanian F. CloudAV: n-version antivirus in the network cloud[C]// Proceeding of the 17th USENIX Security Symposium. San Jose: [s. n.], 2008: 91-106

[2] 范伟. 一种基于云计算的病毒木马防护安全解决方案[C]//第二十一届全国信息保密学术会议(IS2011)论文集. 北京: 中国计算机学会, 2011: 164-168.

[3] 胡晓荷. 云安全——网页挂马的克星[J]. 信息安全与通信保密, 2009(2): 31-32.

[4] 赵鹏,齐文泉,时长江. 下一代计算机病毒防范技术"云安全"架构与原理[J]. 网络与通信, 2009, 10(6): 67-71.

[5] 肖珑,张翠,鹿凯宁. 基于趋势和瑞星云安全方法的改进设计[J]. 中国教育网络, 2011, 2: 86-87.

[6] 张茜. 云安全环境下的恶意代码前端检测技术研究[D]. 安徽: 合肥工业大学计算机与信息学院, 2011.

[7] 曾德明. 浅析杀毒软件中的"云安全"技术[J]. 电脑知识与技术, 2011, 7(11): 2538-2539.

[8] Casassa-Mont M, Pearson S, Bramhall P. Towards accountable management of identity and privacy: sticky policies and enforceable tracing services[J]. IEEE Computer Society, 2003, 10(5): 377-382.

[9] 潘剑锋. 主机恶意代码检测系统的设计与实现[D]. 安徽: 中国科学技术大学计算机科学与技术学院, 2009.

[10] 蒋国松,金徐伟,陈云志,等. 互联网病毒新趋势与防治策略研究[J]. 计算机时代, 2011(3): 20-24.