一种虚实融合、智能随需的安全服务平台研究

卢　凯,于增明,黄　兵
(中国电子信息产业集团有限公司第六研究所,北京 102209)

摘　要:随着云计算技术的发展以及社会信息化进程的加快,在信息安全防护领域出现了一种新的业务模式,即基于云计算环境的安全服务提供模式。针对现有安全服务平台存在的服务对象以及需求响应程度方面的局限性,设计了一种安全服务平台,将虚拟安全产品和实物安全产品相结合,为各类用户提供动态、按需的安全服务,并对平台关键技术和应用模式进行了详细阐述,使得安全作为一种服务,其所面向的用户群体以及提供的服务产品种类都有了很大的扩展,为安全服务新业务模式的推广应用提供了支撑。

关键词:安全服务;虚实融合;智能随需;云计算
中图分类号:TP309　　**文献标识码**:A　　DOI: 10.19358/j.issn.2096-5133.2020.04.004
引用格式:卢凯,于增明,黄兵. 网络与信息安全一种虚实融合、智能随需的安全服务平台研究[J]. 信息技术与网络安全,2020,39(4):19-23.

A requirement-aware security service platform based on virtual-physical integration

Lu Kai, Yu Zengming, Huang Bing
(The 6th Research Institute of China Electronics Corporation, Beijing 102209)

Abstract: With the development of cloud computing technology and the acceleration of social informatization, a novel business model has emerged in the field of information security protection, namely, a security service-providing model based on the cloud computing. Based on the limitations of the existing security service platforms in the service objects and the degree of demand response, we propose a sophisticated platform to provide security services. In order to provide dynamic and personalized services to diverse users, we combine virtual security products and physical security products to construct our security service platform. In addition, we illustrate the key technologies and available modes providing security as a service. In this paper, our platform extremely extends the group-oriented of user and service product, supporting the development of new business model.

Key words: security service; virtual and physical integration; intelligent on demand; cloud computing

0　引言

随着云计算技术、物联网技术的快速发展和应用以及“两化融合”工作的不断深化,人们可以切实地感受到生产效率的提高和生活品质的提升,线上购物、远程诊疗、数据云端存储、个性化定制家电等基于云计算技术的应用正在进入和影响着人们的生活。近年来,随着工业和信息化部《工业互联网发展行动计划(2018—2020 年)》的颁布,工业企业也迎来了一次“上云”的热潮。云计算成为了互联网产业和工业支柱产业发展的推动力。

伴随着制造、交通、能源、市政、医疗等各行业信息化进程的加快,服务化成为产业发展的必然趋势,各种生产活动的成果逐渐开始以服务方式向用户进行交付,即最终的交付成果是一种基于网络和信息平台的服务[1]。安全防护作为各行业信息安全领域的重要需求,以服务的形式向用户提供安全防护保障必然也会成为一种新的方式。本文将研究一种基于云计算环境的安全服务平台,使得用户只需按需定制即可快速便捷地获得信息安全防护服务,而不用考虑安全产品的升级维护、更新换代,同时服务平台采用虚拟安全产品与实物安全产品相结合的方式来降低用户的服务成本和满足用户的多样化需求。

1　研究现状

随着各产业信息化程度的提高,面临的网络安

全威胁也越来越严峻,传统的安全防护方式是在系统的物理边界和关键区域部署安全设备,这种方式存在如下这些问题。

(1)是否能正确进行产品配置关系着安全设备是否能真正具有防护的能力。

(2)病毒库、特征库是否能及时更新直接影响安全设备的防护效果。

(3)用户防护方案的逐步完善,可能会导致安全设备的需求变更。

(4)安全设备的功能细分为用户提供更多样的部署选择[2],增大部署难度。

(5)随着企业的发展及系统规模的增大,安全设备的备件库存会给企业造成不小的经济负担。

(6)安全设备对维护人员素质的要求越来越高,而企业安全人员的数量和能力都存在严重不足。

有别于传统的安全防护方式,基于云计算环境的安全服务作为一种新的业务模式,已经得到了越来越广泛的关注。国内外一些互联网企业、电信运营商以及安全企业已经纷纷推出了各自的云平台安全服务产品[3-5]。比如:美国 AT&T 公司,对采用其云安全服务企业的上网流量进行检查,保障用户访问网站以及邮件系统的安全;北美电信巨头 Verizon 拥有包括 DDoS 攻击防护、网络威胁监测与分析等品类丰富的安全服务产品,具备云安全产品的全球服务能力;国内中兴通讯在其 Cocloud 云计算平台基础上推出移动云计算安全服务,阿里、腾讯等运营商也都将安全产品与其云平台结合,为用户提供线上交付的安全服务。

不过,现有这些云平台安全服务产品存在着以下几点不足。

(1)云安全服务产品是为其云平台本身业务服务的,具有天然的局限性。

(2)云安全服务的用户局限于其云平台的租户上,无法向云租户之外的用户(如普通工业企业用户)提供服务。

(3)云安全服务的产品局限于可虚拟化和软件化的安全产品上,无法满足用户的多样化需求。

2 平台架构设计

针对现有云安全服务产品的不足,本文设计了一种虚实融合、智能随需的安全服务平台,服务平台基于云环境构建,整合虚拟化安全产品以及实物安全产品资源,面向各类用户,提供动态随需的安全服务。平台由硬件资源层、虚拟网络层、安全服务层、服务平台层和安全管理体系这五部分组成,总体架构如图 1 所示。

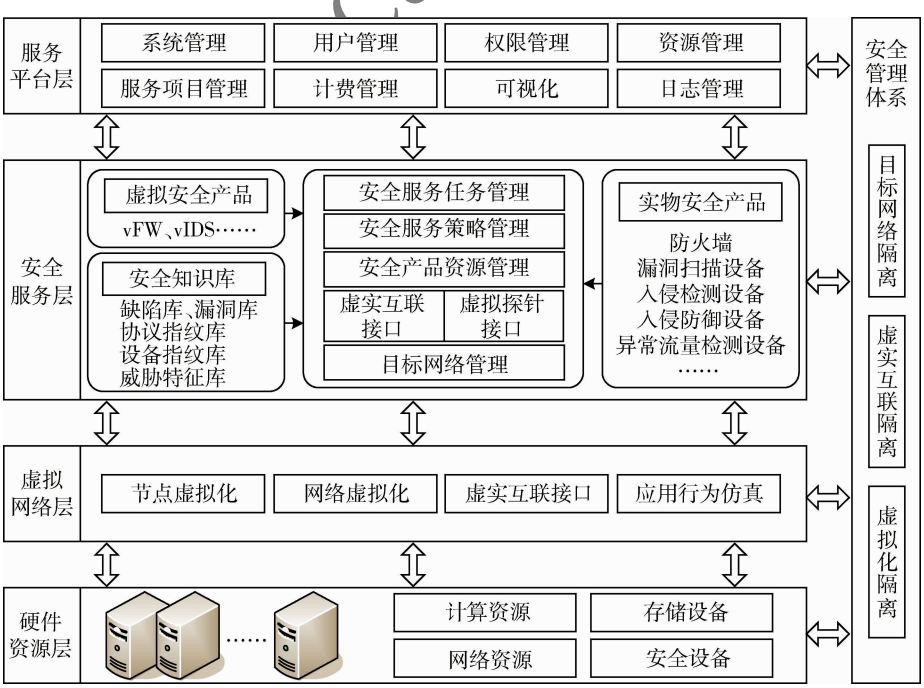

图 1 安全服务平台总体架构

硬件资源层:提供云计算平台运行的硬件资源,包括计算资源、网络资源、存储设备和安全设备等。

虚拟网络层:提供节点虚拟化支撑、网络虚拟化支撑和虚实互联的接口。虚拟化支撑负责生成虚拟机节点和容器节点,网络虚拟化支撑负责生成虚拟网络节点,并通过 SDN 技术实现数据流量交换和链路特性仿真,虚实互联接口实现安全防护目标网络与防护对象的连接。

安全服务层:实现安全服务任务管理,根据用户定制化需求生成安全防护目标网络,对虚拟安全产品资源、实物安全产品资源和安全知识库进行管理和分配,下发安全防护策略。安全防护目标网络包括该用户需求的所有虚拟和实物的安全防护设备,实物安全产品通过虚实互联接口接入。防护策略包括安全产品的功能设置、服务对象加载以及与安全知识库匹配的规则等。

服务平台层:提供人机交互界面,实现系统管理、权限管理、资源管理等平台层面维护管理以及用户管理、服务项目管理、计费管理等服务业务管理。

安全管理体系:包括目标网络隔离模块、虚实互联隔离模块和虚拟化隔离模块。目标网络隔离模块负责在部署目标网络时保障不同用户服务任务的节点和链路是逻辑隔离的。虚实互联隔离模块负责实现系统网络与外部网络之间的隔离。虚拟化隔离模块负责实现虚拟化的安全性,隔离虚拟机和宿主机运行环境。

3 主要技术

本文从安全产品虚实融合技术、安全资源按需保障技术和服务平台安全保障技术三个层面来阐述安全服务平台的实现路径。

3.1 安全产品虚实融合技术

3.1.1 安全产品虚拟化

以 pfSense 防火墙、Snort 入侵检测、FreeWAF Web 应用防护系统等为代表的开源安全产品率先实现了虚拟化,同时基于类 UNIX 操作系统的安全产品在进行虚拟化方面有着先天的优势。开源安全产品在实际使用中有大量用户,在开源社区所有人都可进行使用、测试,针对产品的测试力度超过一般的商业产品,其功能丝毫不亚于甚至高于商业版的安全产品。此外,国内一些安全厂商像绿盟、天融信等也都将各自安全产品进行了一定的修改,支持虚拟化。虚拟化的安全产品在与云计算结合后,更能够方便地实现自动部署、快速启动、按需编排。以 pfSense 为例,它是一个基于 FreeBSD 系统、专为防火墙和路由器功能定制的开源版本,它以可靠性著称,并且提供往往只存在于昂贵商业防火墙才具有的特性。pfSense 通常被部署作为边界防火墙、路由器、无线接入点、DHCP 服务器、DNS 服务器和 VPN 端点。

3.1.2 安全产品虚实互联

虚实互联功能是将在虚拟网络环境中无法通过虚拟网络设备提供的服务,通过接入物理设备,使之与虚拟网络融合,采用物理设备提供的服务来实现服务的可扩展接入。对于安全服务平台来说,物理设备即是各种不同类型的安全防护产品,如防火墙、IDS/IPS 等。图 2 为实物安全产品接入虚拟安全防护网络的结构图。

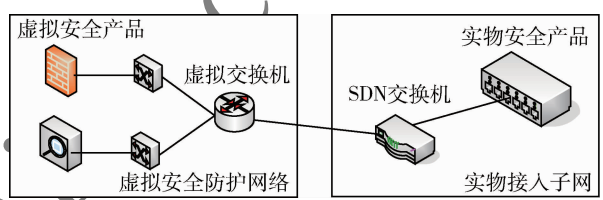

图 2 安全产品虚实互联结构图

实物接入子网络使用 SDN 交换机将流量接入安全防护目标网络的虚拟交换机,由虚拟交换机和 SDN 交换机两者的共同作用,形成了安全防护目标网络。在此过程中,两种交换机起了流量接入导出的作用,通过配置流表使虚拟网络与实物设备在逻辑上形成一个网络。

安全服务平台通过安全产品的虚拟化来获得更丰富的虚拟安全资源,通过虚实互联技术来实现虚拟安全产品和实物安全产品的融合,以适应更广泛的用户安全需求。

3.2 安全资源按需保障技术

3.2.1 安全资源的按需保障

安全服务层的安全产品资源管理模块负责整合虚拟安全产品资源和实物安全产品资源,形成一个安全产品资源池,采用自研、外购、合作等方式完善安全服务平台的产品体系。

用户提交安全服务需求,由安全服务平台来进行安全资源的分配管理和部署管理。安全服务平台的虚实互联功能使得平台具有高可扩展性,可根据用户需求动态增加新的安全防护产品,扩充资源池。而当用户需求发生变更或服务期满时,空余的

安全产品也会被回收进资源池。这种安全资源的弹性管理能降低成本并提高产品的使用效率。

安全产品资源池的构建以及安全资源的弹性管理保障了用户端到端的安全需求。

3.2.2 安全服务的快速重构

安全防护目标网络通过虚拟网络拓扑的构建来实现安全产品的编排,实物安全产品也是通过虚实互联功能接入到虚拟网络拓扑中的。安全服务平台支持虚拟网络的链路仿真,为虚拟网络节点间建立通信链路,链路仿真是构建虚拟网络的核心支撑技术,通过虚拟链路仿真可灵活构建虚拟网络的拓扑结构。

当用户的业务应用场景发生状态变化(如规模、功能、成熟度等发生变化)时,必然会产生防护方案的变化,也必然导致安全服务需求的变更,这就要求安全服务平台具有快速重构网络拓扑的功能。

当目标网络拓扑发生变化时,目标网络管理模块对虚拟链路、虚拟交换机、转发表进行增量重构。目标网络拓扑中安全产品的添加或删除,体现为相关虚拟链路的添加或删除。

安全服务平台通过对安全资源的按需保障以及服务业务的快速重构技术来达到为用户提供智能随需安全服务的目的。

3.3 服务平台的安全保障

3.3.1 服务对象的安全接入

云租户的安全服务需求,对于安全服务平台来说,相当于是对云平台的虚拟主机和应用软件等的防护需求,只需将流量从网络中抓取和引导出来,在平台内部进行安全防护网络的构建即可提供相关服务[6]。

而向云租户之外的用户提供安全服务,需要建立用户网络与安全服务平台之间的连接。从安全性和经济性方面来综合衡量,安全服务平台采用虚拟专用网络(VPN)的方式,通过虚拟网络层的虚实互联接口来建立与用户网络之间的连接。通过设置代理,打通安全防护目标网络和用户网络之间的连接,用户网络与互联网之间的交互流量被引入到安全防护目标网络进行审查,实现安全防护的目的。

虚拟专用网络是一种在公用网络上架设专用网络进行加密通信的技术[7-8]。通过 VPN 传输数据,可以对数据包中的数据、验证包、源 IP 地址以及目标 IP 地址进行重新封装,使得数据包可以通过公网传输,且保障了连接的安全和高效。

3.3.2 服务平台的安全管理

服务平台自身的安全性是制约安全服务业务推广与发展的重要因素之一,只有平台的安全措施能保障用户使用云服务的功能和数据安全,才能促使用户愿意将安全服务交付给服务平台来实施。

安全服务平台的基础云平台由硬件资源层和虚拟网络层构成,平台的物理架构采用双网结构设计,分为管控网和业务网,管控网支撑安全服务业务管控、目标网络构建、数据采集与展示等系统运行,业务网支撑目标网络自身业务的运行。

安全服务平台的安全管理体系实现服务业务目标网络之间、系统网络与外部网络之间、虚拟机与宿主机之间的安全隔离。

服务业务目标网络之间的安全隔离主要采用 VLAN 隔离和访问控制等措施。系统网络与外部网络之间的隔离主要由硬件资源层的安全设备来保障,最基本的配置是由 2 台防火墙和 1 台入侵检测设备组成,在管控网路由器前端以及虚实互联接口处各部署 1 台防火墙,在管控网内部部署 1 台入侵检测系统,实现与外部网络的隔离以及对网络异常状况的检测。虚拟机与宿主机之间的安全隔离主要由操作系统内核进行原生支持,配合硬件虚拟化共同完成虚拟化的安全隔离。

安全服务平台从服务对象网络的安全接入以及平台自身安全管理措施两个方面来保障用户安全服务业务的安全。

4 应用模式

安全服务平台可以为用户提供虚实互联、智能随需的安全服务。云租户的安全服务在平台内搭建安全防护网络即可,本文将描述一个非云租户的某企业的安全服务应用场景。

某企业信息系统分为核心服务区、用户办公区和分支单位接入区 3 个区域,核心服务区布置邮件系统、ERP 系统、OA 系统等服务器,用户办公区布置计算机终端,分支单位接入区提供外单位服务器接入接口。3 个区域的防护要求不同,核心服务区要求部署防火墙、IPS 和专用数据库审计产品,用户办公区要求部署防火墙和网络审计系统,分支单位接入区要求部署隔离网闸。

安全服务平台可按该企业需求提供专属安全服务,安全服务应用场景如图 3 所示。

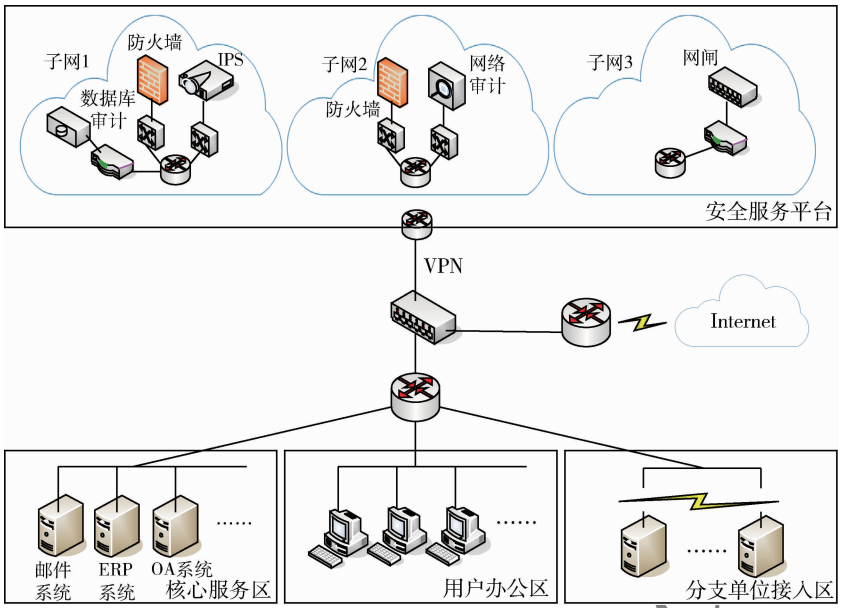

图 3　某企业云安全服务应用场景

安全服务平台与用户信息系统之间采用 VPN 连接,在平台内创建安全服务项目,任务管理模块根据需求创建 3 个子网,分别为用户 3 个区域提供安全防护服务。子网中的安全产品根据虚拟化成熟度采用虚实结合的方式部署,防火墙、IPS、网络审计产品使用虚拟安全产品,网闸和数据库审计系统使用实物安全产品。目标网络生成后,服务平台再进行安全产品的配置以及安全策略的生成与下发后,即可为用户提供所需的安全服务了。

5　结论

本文针对基于云计算环境的安全服务这一新的业务模式,分析了传统信息安全防护方式以及现有云服务平台的不足之处,设计了一种虚实融合、智能随需的安全服务平台,从安全产品虚拟化及虚实互联技术、安全资源按需保障的措施以及服务平台安全保障的手段等几个方面介绍了服务平台的实现路径,实现了安全服务平台在满足用户安全防护产品多样性需求以及服务对象广适性需求方面的功能,为安全服务新业务模式的推广应用提供了支撑。由于云服务场景下,检测和防护都需要大量数据的传输,容易形成瓶颈,后续将在提高平台性能和平台安全性方面继续开展研究。

参考文献

[1] 俞乃博. 云计算 IaaS 服务模式探讨[J]. 电信科学,2019(10A):39-43.

[2] 盖玲. 基于云计算的安全服务研究[J]. 电信科学,2011(6):97-100.

[3] 王海燚,樊宁,沈军. 电信运营商云平台安全服务产品发展思路[J]. 广东通信技术,2016(11):14-15,76.

[4] 石桂花,徐超,刘君,等. 基于云安全服务平台的等级保护测评方法[J]. 计算机工程与应用,2017,53(S3):130-133.

[5] 陈小华,董振江,金怡爱. 按需供给的移动云计算动态安全服务[J]. 中兴通讯技术,2015,21(2):4-9.

[6] 李杰. 云环境下一种基于软件定义安全服务的入侵检测算法研究[D]. 南京:南京邮件大学,2015.

[7] 张玉珍. VPN 在中小型企业 ERP 系统安全网络架构中的应用[J]. 计算机安全,2009(12):77-79.

[8] 山德鲁. 全方位解读 VPN 技术[J]. 电脑知识与技术,2015(5):106-109.

(收稿日期:2020-02-26)

作者简介:

卢凯(1977 -),男,本科,高级工程师,主要研究方向:工业控制、信息安全。

于增明(1985 -),男,硕士,高级工程师,主要研究方向:工业控制、信息安全。

黄兵(1983 -),男,硕士,高级工程师,主要研究方向:工业控制、信息安全。

版权声明