



中国电信云计算业务平台安全建设浅析

李 洪,渠 凯,伍思源,周文红

(中国电信集团公司网络运行维护事业部 北京 100032)

摘 要:基于中国电信集团公司业务平台的特点,研究了在迁移到云计算环境后的新增安全问题,建立了云计算业务平台安全防护框架,提出了云计算业务平台的安全防护体系建设方案。

关键词:业务平台;云计算;安全体系

doi: 10.3969/j.issn.1000-0801.2013.04.028

Cloud Computing Security Construction Analysis of China Telecom Business Platform

Li Hong, Qu Kai, Wu Siyuan, Zhou Wenhong

(Network Operation and Maintenance Department, China Telecom Corporation, Beijing 100032, China)

Abstract: The new security problems in the cloud computing environment were studied based on the characteristics of China Telecom business platform. On the basis of these studies, the security protection framework and construction scheme of cloud computing business platform were put forward.

Key words: business platform, cloud computing, security framework

1 引言

云计算为电信运营商带来了良好机遇,为实现精细化运营、推进转型深化提供了利器,作为承载中国电信集团公司增值业务的业务平台系统逐步迁移到云计算环境,也将是今后发展的趋势。

安全性是客户选择云计算时的首要考虑因素之一,也是在建设云计算业务平台时所重点考虑的关键问题。本文首先分析了在迁移到云计算环境后新增的安全问题,进一步提出了云计算业务平台的安全防护体系和部署方案建议。

2 云计算业务平台的安全重点

2.1 云计算业务平台新增的安全问题

当业务平台迁移到云计算环境后,由于虚拟化技术的

引入,原本运行在物理服务器上的业务系统转而运行到虚拟机上,因此出现了新的安全需求和问题。云计算业务平台 and 传统业务平台相比,新增的安全问题主要包括以下几个方面。

- 主机层安全:基于以虚拟化技术为核心的云资源池,使得主机层安全需要重新考虑。一方面要考虑运行在虚拟机之上的操作系统、数据库系统等的安全问题,同时还要考虑虚拟机管理程序(VMM)的安全问题。
- 网络层安全:虚拟化技术的引入使得传统的基于物理服务器为单元划分网络安全域的方法发生了改变,与传统的基于安全域隔离的模型不同,云计算模型不再有物理机的隔离,测试虚拟机可能与生产虚拟机在同一台物理机上,相应的网络隔离也不再存在。

- 数据层安全:在虚拟化环境下,由于云计算平台的多租户特性,数据安全将更为复杂,需要考虑虚拟环境的用户数据隔离、镜像文件存储、残留数据处理等安全问题。

2.2 云计算业务平台安全框架

基于上述对于云计算业务平台的新增安全问题的分析,设计的迁移到云计算平台后的业务平台安全体系架构如图1所示。

云计算业务系统重点需要考虑的安全问题主要包括以下内容。

- 网络层安全:除传统的安全问题之外,需重点考虑虚拟安全域的问题,包括虚拟安全域划分方式、虚拟安全域访问控制以及相应的虚拟防火墙部署和配置等。
- 主机层安全:主要分为虚拟机管理程序(VMM)安全和用户虚拟机(Guest OS)安全两个层面的问题。VMM安全是云计算系统新增的安全问题,主要包括VMM安全漏洞检测、VMM用户身份鉴别、VMM物理和网络访问控制、VMM安全审计等问题。Guest OS安全与传统的主机安全需求基本一致。
- 数据层安全:除了传统业务平台的机密数据保护和数据备份恢复之外,还需要重点考虑虚拟环境下的

用户数据隔离、用户镜像文件保护、残余数据的销毁和处理等问题。

- 物理安全、应用安全、安全管理方面与传统的业务平台安全需求基本相同。

3 云计算业务平台安全防护体系建设方案建议

3.1 云计算网络安全防护体系建设重点

3.1.1 网络安全防护体系建设整体思路

网络架构建议采用云中心(cloud center)架构,可以将传统的网络安全技术和基础设施平滑地转移到云中。网络安全防护建设的重点是分区规划和分层部署。

分区规划就是以VLAN为基础,按照不同业务需求和安全需求划分安全域,此部分与传统安全防护手段基本相同,本文中不再赘述。

分层部署是在每个区域的边界处,根据实际情况进行相应的安全需求部署,包括防DDoS(distributed denial of service, 分布式拒绝服务)攻击、虚拟防火墙、流量分析与控制、VPN、入侵防御以及负载均衡等需求。考虑到云计算的特点,在分层部署时应重点考虑虚拟防火墙和抗DDoS攻击设备的策略配置以及边界安全设备的性能指标、可靠性和扩展性。

虚拟防火墙技术是实现云计算中心的安全域边界防



图1 云计算业务平台安全框架示意



护的重要手段。所谓虚拟防火墙就是在—台物理防火墙上虚拟出多台逻辑上的防火墙,具有各自的管理员,并可以根据需要配置出完全不同的安全策略,各虚拟防火墙的安全策略互不影响。虚拟防火墙支持 VPN 实例绑定和 VLAN 实例绑定,提供相互隔离的安全服务,具备私有的区域、ACL (access control list, 访问控制列表) 规则组和 NAT (network address translation, 网络地址转换) 地址池,并且能够将绑定接口加入私有区域。同时由于虚拟防火墙功能可将资源分别独立分配给各个虚拟的系统,彼此之间互不干扰,因此当一个虚拟系统因抵御黑客攻击耗费大量资源时,另一个虚拟系统的资源却不受任何影响,从而有效保证网络其他应用的正常运行。

对于云计算,其最大需求是实现计算、存储等 IT 资源灵活调度,让资源得到最充分利用,而实现这一需求的基础是以数据中心的虚拟机作为主要的计算资源为客户提供服务。较传统网络,云计算网络的流量模型发生了两个变化:一是从外部到内部的纵向流量加大;二是云业务内部虚拟机之间的横向流量加大。

为保证未来业务开展,整个云计算数据中心必须具有高的吞吐能力和处理能力,在数据转发和控制的各个节点上不能存在阻塞,同时具备突发流量的承受能力。对于安

全设备选择具体体现在以下两个方面。

- 安全设备接入数据中心,应具备 10GE 级接入、10GE 级性能处理为基础,并且要具备根据业务需求的灵活扩展能力。
- 随着服务器的虚拟化及多租户业务部署,云计算环境下的网络流量无序突发冲击会越来越严重,为保证云计算服务的服务质量,安全设备必须具备突发流量时的处理能力,尤其是一些对时延要求严格的业务。

3.1.2 网络安全防护体系部署示例

图 2 给出了一个业务系统云平台的网络安全防护体系的网络部署示意。建议在云数据中心边界部署专业的抗 DDoS 攻击设备,防火墙建议采用旁挂式设备部署在核心交换机之上,启用双机模式。防火墙设备和抗 DDoS 攻击设备在选型时要充分考虑云数据中心的业务类型、业务容量、业务扩容性预期等,从而对设备架构、功能、性能指标、可靠性、扩展性等进行严格的遴选和测试。建议将云平台中的每个业务系统单独划分为一个安全域,启用硬件防火墙上的虚拟防火墙功能,通过 VLAN ID 将不同安全域绑定到不同的虚拟防火墙,这样每个业务系统可以有独立的安全边界和管理员,通过虚拟防火墙可以设置独立的安全

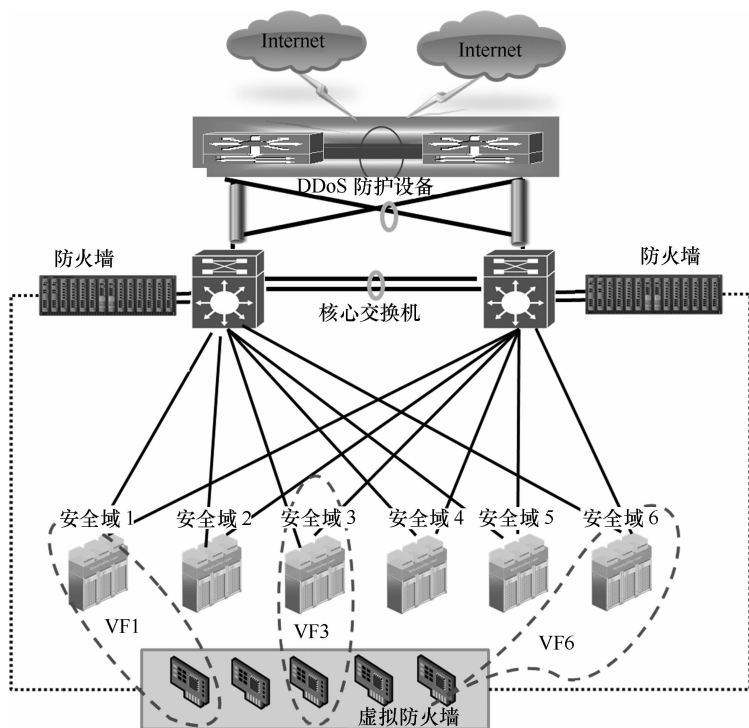


图 2 云平台网络安全防护体系部署示意

访问控制策略。对于虚拟防火墙和虚拟主机安全产品的选择,要重点考虑启用安全特性之后的性能损耗和产品的集中配置管理能力。

3.2 虚拟主机安全防护体系建设

在云计算数据中心中,由于虚拟化技术打破了物理边界,使得传统的基于物理服务器和物理边界的主机安全防护体系难以有效地应用在虚拟主机的安全隔离和防护上。虚拟主机安全防护体系建设需要重点考虑的问题包括以下几点。

- 虚拟机安全隔离:传统的基于物理边界建立安全域的方法只适用于物理主机,对于虚拟主机如何实现有效的安全隔离,是安全防护体系需要重点考虑的问题。
- 虚拟机安全监控:同一物理主机中的虚拟机之间的数据交互是通过虚拟交换机(vSwitch)实现的,这部分流量不会出现在物理交换机上,因此传统的安全防护设备无法监控虚拟机之间的数据流量,也无法察觉虚拟机之间的攻击行为。
- 虚拟机自身安全保护:客户虚拟机与传统主机一样,面临病毒、木马、恶意入侵等安全威胁;而对于VMM的安全防护,包括VMM的身份鉴权、访问控制、安全漏洞修补、防止虚拟机逃逸等也是主机安全防护体系的重点。

对于解决虚拟主机的安全隔离和安全监控问题,目前业内主要有两种技术方案。

(1)将虚拟主机网络管理的范围从服务器内部转移到网络设备

将虚拟机内部的不同VM之间网络流量全部交由与服务器相连的物理交换机进行处理,这将使得安全部署变得同传统边界防护一样简单。

这种思路目前有两种解决方案,分别是基于VN-Tag(虚拟网络标签)的IEEE 802.1Qbh和基于VEPA(虚拟以太网端口聚合)的IEEE 802.1Qbg。目前这两个标准还处于草案阶段,尚未正式发布。

这种解决思路的最大优点是:将复杂的控制功能重新交给技术成熟的网络设备,可以继续沿用传统的网络安全控制机制。但目前相关产品的技术成熟度和商品化程度不够,VN-Tag由思科一家独大,VEPA的支持厂商虽多,但成熟的产品尚未投放市场。因此该解决方案目前尚不适用,需要根据后续产品的成熟度而定。

(2)在虚拟化层实施安全隔离和安全监控

由于虚拟机之间的通信在虚拟化层可见,因此虚拟化软件公司可以将虚拟化层接口开放给合作公司,由第三方开发虚拟化安全防护软件。如VMware公司在虚拟化层提供了vShield安全套件,可提供虚拟安全边界、防火墙、流量监控、防病毒等安全功能。

此方案不仅解决了虚拟主机的安全隔离和安全监控问题,也提供了客户虚拟机的安全保护能力,同时实现了安全策略配置的自动迁移,应该说提供了虚拟主机安全防护体系的一揽子解决方案。但此方案也存在一定的缺点,一方面,安全套件在虚拟化层实现,没有备份,存在单点故障;另一方面,安全套件以软件形式实现,处理能力相对有限,而且会影响虚拟化层的性能。

综上,基于虚拟化层的安全套件目前有较为成熟的商业产品,并且提供了针对虚拟主机安全防护体系的一揽子解决方案,因此是目前较为合适的选择。但由于虚拟化安全套件有单点故障和性能影响等方面的缺陷,因此应与传统的安全设备和技术手段相结合,建立纵深的安全防护体系。

3.3 数据安全防护体系建设

对于云数据中心的数据安全核心需求主要包括以下几点。

- 数据传输安全:数据在传输过程中不被泄露、篡改,以保障数据机密性、完整性、可用性。
- 数据存储安全:不同用户数据在共享存储介质中应安全隔离,并对访问权限进行控制,用户数据应保障隐私。
- 数据可靠性:具备容灾备份能力,当存储设备发生故障时,可快速恢复。

具体到业务系统云平台,建议对于不同业务系统单独划分安全域,不同业务系统的数据存储在各自的安全域存储系统中,这样可以通过网络边界访问控制实现数据存储安全。在每个安全域的虚拟防火墙中制定相应的数据访问控制策略,主要包括以下两个方面。

- 用户级权限控制:定义不同的用户和权限,通过权限控制限制不同权限用户访问和操作不同的数据。
- 定义数据存储对象的ACL控制:所有的对象都存储于指定的存储容器中,限定数据存储对象的访问IP列表、角色、用户等ACL控制。

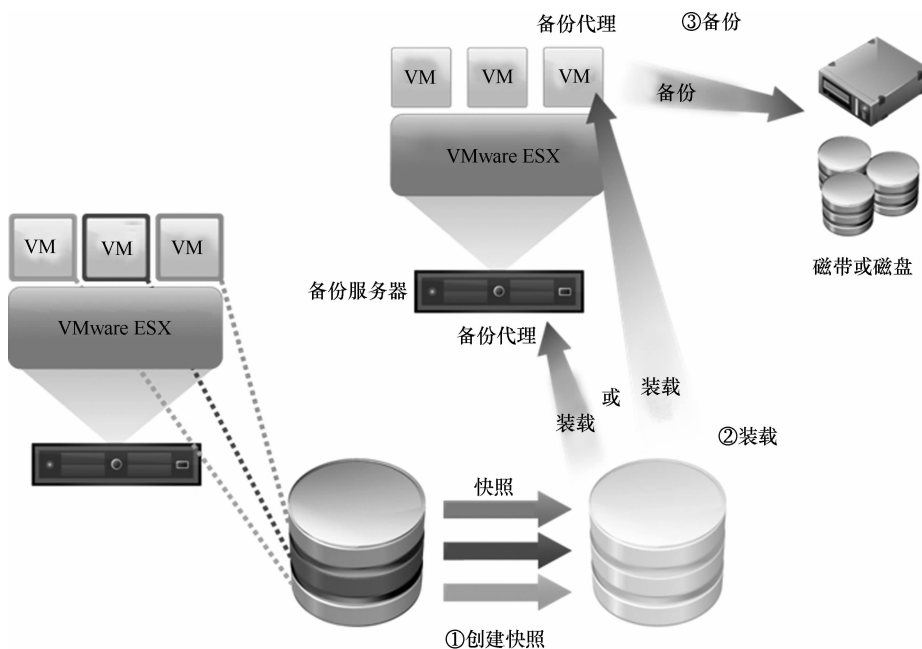


图3 VMware data recovery 示意

对于数据传输安全,主要应保证对于业务系统的管理维护以及数据传输使用加密通道,可以采用以下措施:

- 启用虚拟防火墙的 VPN 功能,实现从外网到业务系统云平台数据传输通道的安全;
- 对于业务系统设备的维护管理操作应采用加密通道,使用 SSH、HTTPS 等安全协议进行登录和操作。

而对于虚拟系统的数据备份和数据恢复也是云平台数据安全的重点,目前主流的虚拟系统都推出了相应的数据备份和恢复产品。

VMware 公司推出的 VMware data recovery 支持快速备份到磁盘,支持快速和完全的恢复,从而能够预防虚拟环境中的数据丢失,VMware data recovery 部署架构如图 3 所示,主要特点包括如下 3 个方面:

- 基于磁盘的备份和恢复,可实现快速的虚拟机恢复;
- 易于部署,VMware data recovery 是一个运行于 VMware ESX 和 ESXi 主机上的虚拟机;
- 根据需要恢复单个文件或整个镜像。

思杰系统公司也提供了虚拟机镜像备份恢复应用程序——VM protection and recovery (VMPR),可以基于策略对虚拟机做快照和归档,并为快照和归档分别设置计划选项,从而实现虚拟机的备份和恢复。

4 结束语

云计算作为电信运营商下一步发展的战略重点,同时其面临的安全挑战也是前所未有的。本文以业务平台为切入点,就云计算安全防护体系建设进行了探讨,阐述了云计算安全防护中的核心问题及对策,并提出了云计算业务平台安全防护体系的建设方案,希望能给今后云数据中心建设一定的借鉴和参考。

为了实现云计算的安全目标,还需要在具体云计算平台实现的基础上,深入研究各个安全关键技术,并且逐步建立健全云计算安全管理体系和安全运维体系,这也将是今后需要进一步努力的研究方向。

参考文献

- 1 中国电信集团公司. 中国电信新建业务平台安全验收管理办法, 2011
- 2 张建勋, 古志民, 郑超. 云计算研究进展综述. 计算机应用研究, 2010, 27(2): 429~433
- 3 Craig Balding. Biggest cloud challenge: security. <http://cloudsecurity.org/2008/10/14/biggest-cloud-challenge-security/>, 2008
- 4 CSA. Top Threats to Cloud Computing V1.0. <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>, 2010
- 5 林兆骥, 付雄, 王汝传等. 云计算安全关键问题研究. 信息化研究, 2011(4)

(收稿日期: 2013-03-11)