



专题:业务平台安全

构建集约化的运营商业务平台安全域防护体系 ——业务平台安全域划分及边界整合思路浅析

邱贤奕¹, 李 洪²

(1. 中国电信股份有限公司广东分公司 广州 510020;

2. 中国电信集团公司网络运行维护事业部 北京 100032)

摘 要:随着运营商网络规模和各类业务系统的不断扩大和发展,如何提升业务平台的安全防护能力,保证系统的安全稳定运行,确保数据的安全性与保密性,成为通信网络运行维护工作的重点。对于运营商来说,提高业务平台安全性最有效的方法,就是实施安全域划分,进行层次化、有重点的保护。在此基础上,对不同业务平台的安全域边界进行整合,并通过虚拟防火墙等方式,实现集约化防护。结合中国电信业务平台维护的实际情况及业界相关实践经验,分析业务平台安全域划分及边界整合方法,讨论如何构造集约化的业务平台安全域防护体系。

关键词:安全域;边界整合;业务平台;集约化安全防护

doi: 10.3969/j.issn.1000-0801.2013.08.009

Construction of Intensive Security Domain Protection System for Service Platform

——Discussion of Security Domain Division and Boundary Integration

Qiu Xianyi¹, Li Hong²

(1. Guangdong Branch of China Telecom Co., Ltd., Guangzhou 510020, China;

2. Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China)

Abstract: With the continuous expansion of network scale and the development of service platform, how to improve the safety protection ability of service platform has become the focus of communication network operation and maintenance for telecom operators, in order to achieve the effective and intensive protection of service platforms, the most effective way is security domain division and boundary integration. Reference to the maintenance of China Telecom service platforms and the experience of the industry, the method of security domain division and the boundary integration was analyzed, and the construction of a intensive security domain division system for service platform was discussed.

Key words: security domain, boundary integration, service platform, intensive security protection

1 实施安全域划分及边界整合的意义

当前运营商业务平台实施安全防护的难点,主要在于

业务平台的外部接口较多,网络边界、协议复杂多样,导致安全性难以控制。为解决上述难点,需要在满足业务平台正常业务互联需求的前提下,对业务平台实施安全

域划分。

业务平台安全域是指在同一个业务平台内,具有相同安全保护需求的子网或网络,这些子网或网络间彼此相互信任,一般配置相同的安全访问和边界访问控制策略,同一平台相同的安全域共享同样的安全策略。

为了简化业务平台安全域的防护边界,实现集约化防护,使其便于管理、强化控制、节省投资,达到提高安全防护效率、实现业务平台安全防护的目的,还需要实施业务平台的安全域边界整合,对平台网络接口进行整理,将相同的网络出口进行归并,在不影响业务正常需要的情况下,尽可能地减少接口的数量,提高接口的可控性和规范性,实现对各业务平台安全域的集中安全防护,以达到统一接入、统一管控、控制成本、集中防护的效果。

2 安全域划分方法

2.1 安全域划分流程

结合运营商业务平台的安全需求特点以及目前各主流业务平台普遍采用的安全措施,从平衡安全成本支出、控制安全风险的角度,一般采用“同构性简化”的安全域划分方法,对业务平台网络进行简化后设计防护体系,以便进行有效的安全管理,基于“重点系统、重点防护”的安全域划分和防护策略,综合实现业务平台的保护。安全域的划分流程如图1所示。

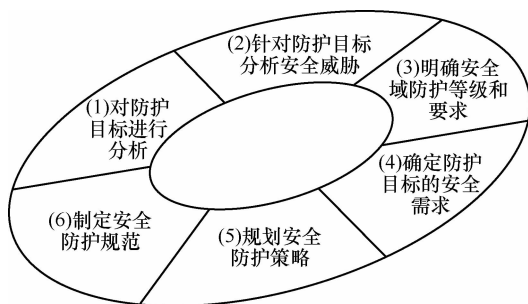


图1 业务平台安全域划分流程

2.2 安全域划分思路

安全域的划分应遵循业务保障、结构简化、等级保护和生命周期原则。实施安全域划分的根本目标是更好地保障平台承载的业务,在保证平台安全防护的同时,必须保障业务的正常运行,即遵循业务保障原则。

安全域划分的直接目的是简化网络结构,一个经过简化的网络结构,更有利于设计防护体系,即结构简化原则。安全域的划分还应根据信息资产价值,使得每个安全域具

有相同或相近的安全等级和安全环境,部署相近的安全访问控制策略,即遵循等级保护原则。

对于安全域的划分和边界防护的部署,还要遵循生命周期原则,考虑到业务平台的不断扩容变化、承载业务的更新发展,在安全域的设计、划分、建设、调整、维护过程中,都需要实行工程化的管理模式。

由于业务平台提供的业务服务一般比较灵活多样,与外部网元的交互性也比较复杂,进行安全域的划分,一定要基于对网络架构与业务需求的充分理解,在保证平台正常业务提供的同时,实现对安全域的有效划分和隔离。

根据业务平台安全域的数据分类,结合目前维护的实际需求,将每个业务平台划分为4个安全子域:交互网络域、计算域、维护域、服务域,具体划分情况如图2所示。

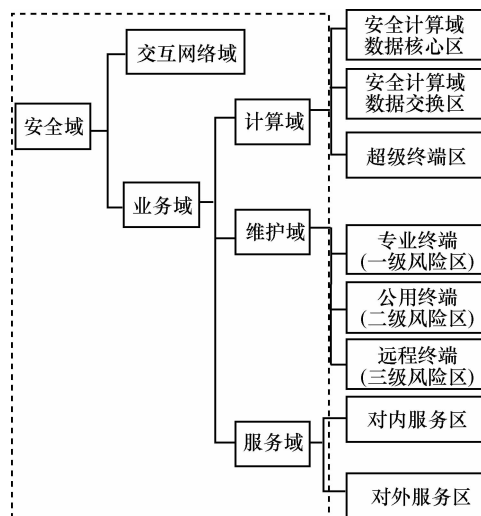


图2 业务平台安全域划分示意图

- 交互网络域:是安全子域与承载网络(如专线、CN2、DCN、公网等)的接口区域,按照不同的网络特性,一般可分为3个逻辑接入分区,即专线接入区、内网接入区、互联网接入区。交互网络域一般包括平台出口的网络设备,如出口防火墙、路由器、交换机、IDS、IPS等设备。
- 计算域:是指在业务平台中,负责平台核心数据的存储和传输,负责业务数据处理的服务器所组成的区域,具体包括业务处理主机、数据库服务器以及磁盘阵列等。
- 服务域:一般分为对外服务区和对内服务区。顾名思义,对外服务区是为业务平台提供统一对外服务的网络设备和服务器所组成的区域,如业务平台对



外提供的 Web 站点等;对内服务区则是为安全域提供日志审计、安全认证、事件管理、病毒及系统补丁更新管理、策略管理等统一服务的区域。

- 维护域,根据维护终端的物理位置及接入方式的不同,可分为本地维护区和远程维护区;根据使用维护主体的不同,又可分为外包厂商维护区和运营商维护区。业务平台安全域的划分应视相关网络及系统的实际情况,将以上各安全区域合并为其中的几类。

根据上述的安全域划分思路,对于典型的业务平台进行安全域划分时,可以参考如图 3 所示的划分方式。

2.3 安全域划分案例

以中国电信股份有限公司广东分公司(以下简称广东电信)某业务平台的安全域划分情况为例进行详细分析,安全域划分情况如图 4 所示。

其中,计算域包含该业务平台的应用服务器、数据库服务器,其不直接对外提供服务,在系统内承担计算、认证、存储的功能;服务域包含 Web 服务器,负责处理终端发出的各种请求,并将处理结果以 Web 的方式返回;维护域由所有需要登录该平台进行日常维护的终端构成,以 DCN 接入(包括直接接入和 VPN 接入)为主,私网接入为辅。网络域

方面,由于该平台与 DCN、城域网和各合作商专线都具有网络互连的需求,网络域作为平台与 DCN、城域网和各合作商专线的统一接口区域,防火墙、核心交换机、接入交换机、路由器、负载均衡、VPN 等设备均属于网络域的范畴。

3 边界整合方法

业务平台边界整合就是在安全域划分的基础上,对不同的业务平台或区域基于相同或相似的保护等级、功能、网络需求进行整合,减少或简化系统边界,以便于进行安全防护、访问控制和监控。安全域的边界整合必须在保障平台业务顺畅运行且性能满足要求的前提下进行。

3.1 逻辑整合

安全域边界整合一般包含逻辑整合和物理整合两方面。其中,逻辑整合是指对单个安全域的逻辑边界进行整合,使其具有清晰、完整的逻辑边界,便于进行安全管理、安全防护和安全控制。如对于特定安全域,根据要求明确其出口边界,统一整合成互联网接入区、专线接入区和内网接入区。

一般来说,经过安全域划分后,各系统的边界已经较为清晰(如图 5 所示),安全域的交互网络域与互联网、专

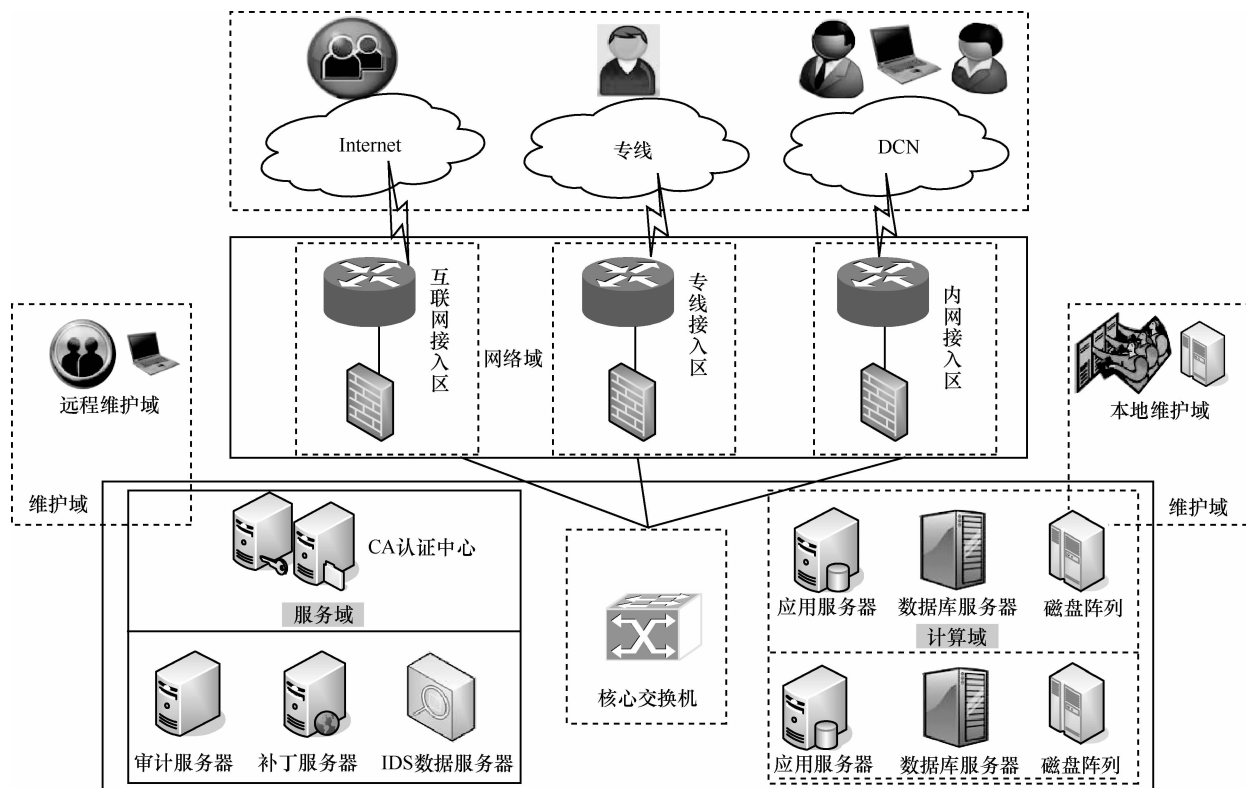


图 3 典型业务平台安全域划分示意

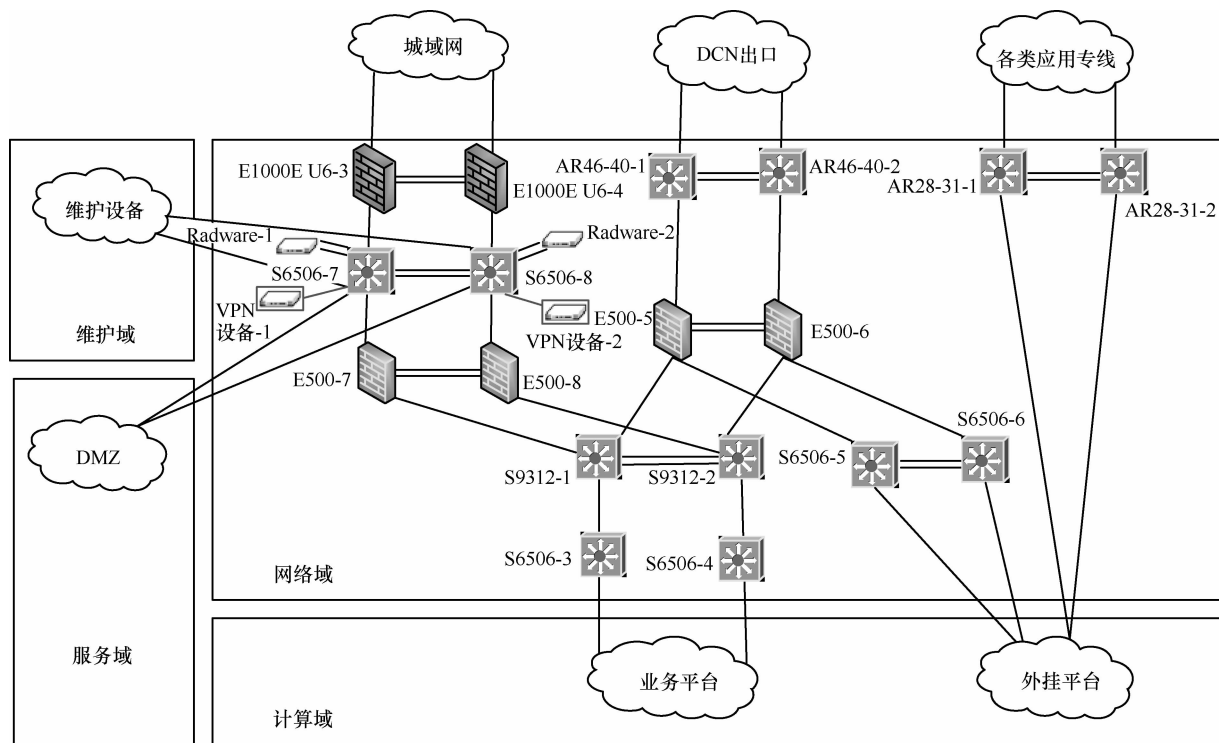


图 4 广东电信某业务平台安全域划分案例

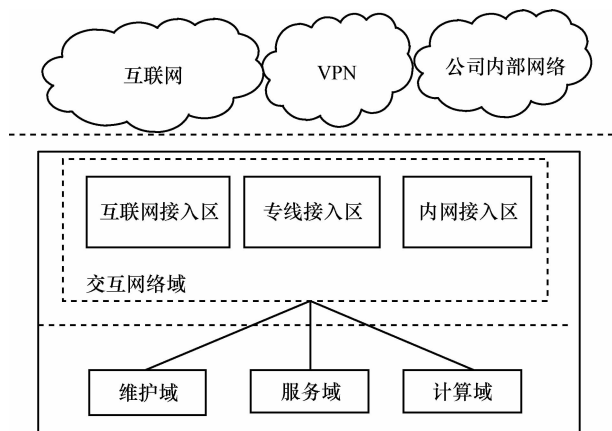


图 5 安全域边界逻辑整合示意

线和内网的边界为网络边界,是安全域的重要边界。

3.2 物理整合

安全域的物理整合是指对同一物理地址多个安全域的多个边界进行物理调整,使其共用相同的设备,或使用相同的通信端口进行通信。如某业务平台中,有多个系统与互联网络有互联需求,在安全等级保护要求相似的基础上,将这些系统的出口统一整合到“互联网接入区”,再与互联网进行互联。

当同一系统中的多个节点需要与外网进行互联时,为避免网络设备的重复投资建设,节省投资成本及后续的维

护成本,应使其共用相同的设备或使用相同的通信端口,将不同系统的相同类型安全域进行整合,形成一个大的安全域。通过实施边界整合,各安全域以及外部接口实现集中的安全防护,可以共享 IDS、IPS、防火墙等安全防护手段。具体如图 6 所示。

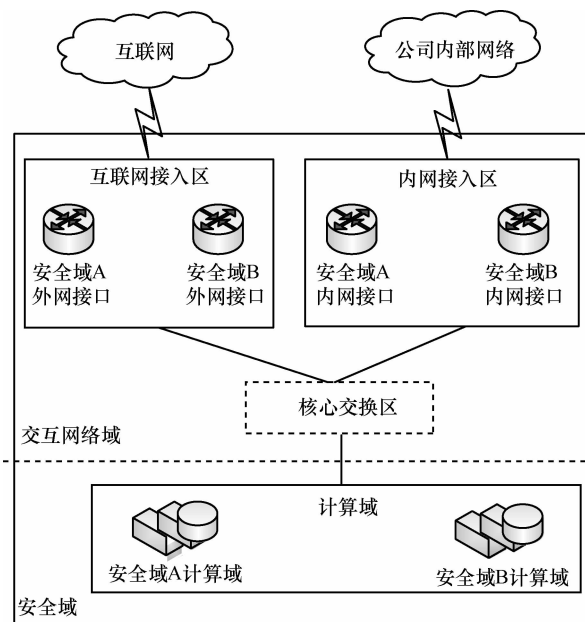


图 6 安全域边界物理整合示意



除了安全域的边界整合外,安全子域之间也存在相应的边界整合,如计算域、服务域、维护域之间的整合等;另外,与第三方的边界主要存在于各安全域的维护域中,在本地维护区和远程维护区中,都包括第三方厂商的现场技术支持和远程技术支持。针对各系统,应根据具体系统的安全等级要求,考虑设置连接出口。

3.3 通过边界整合实现集约化维护

不同的业务平台,根据物理布局及安全防护要求相近的平台,可以考虑进行出口边界整合,以中国电信股份有限公司广东分公司(以下简称广东电信)的主要业务平台为例,通过将短信中心、业务网关、彩信中心、WAP网关、ISAG、ISMP等结构相近、网络需求相似的平台边界进行整合,使用统一的机房汇聚交换机、防火墙接入CN2、DCN、163网络,并使用同一套入侵检测系统,达到集中化管理、集约化维护的目的,如图7所示。

在出口防火墙上,对于各平台相同的访问控制需求,配置相应的访问控制策略进行控制,配置NAT实现地址映射,并实现对常见漏洞端口或基于网络传播的恶意代码(如冲击波、SQL Slammer等)的拦截,随着后续虚拟防火墙等技术的使用,各平台的出口控制将更加灵活。

在汇聚交换机上,通过划分不同的VLAN,实现业务平台之间的隔离,通过接入IDS实现入侵检测功能,及时发现攻击、渗透行为,以便进行相应的处理。

下联的各个业务平台,可根据实际需要配置防火墙,用于实现平台之间的访问控制及部分个性化访问控制需求,对于安全防护需求较低的平台,也可以将交换机直接接入汇聚交换机,不设置防火墙,以控制投资建设及后续的维护成本。

4 安全域防护策略

结合业务平台的组网特点,综合平衡成本和风险,基于“重点系统、重点防护”的策略,综合实现业务平台安全域防护。安全域的防护建议以“预防为主,检测为辅”,采用通用防护设备或技术,如在网络边界部署防火墙、IDS、安全监控系统,通过在核心交换机设置访问控制策略、划分VLAN等技术手段对安全域进行安全防护。

4.1 安全域防护需求设计的总体思路

在安全域划分和边界整合完毕后,需要进行安全域防护的设计。安全域防护设计一般按照如下思路进行。

(1) 对防护目标进行分析

明确各安全域所提供的业务后,需要全面、深入地分析各种服务所对应的数据流及其数据活动情况。同时,还需要识别出进行安全域防护的目标所包含的网络设备、服务器、应用及与其系统或网络互联的现状,分析各业务在网络、系统、应用层的承载情况,重点是跨边界通信与业务平台接口互联的情况。

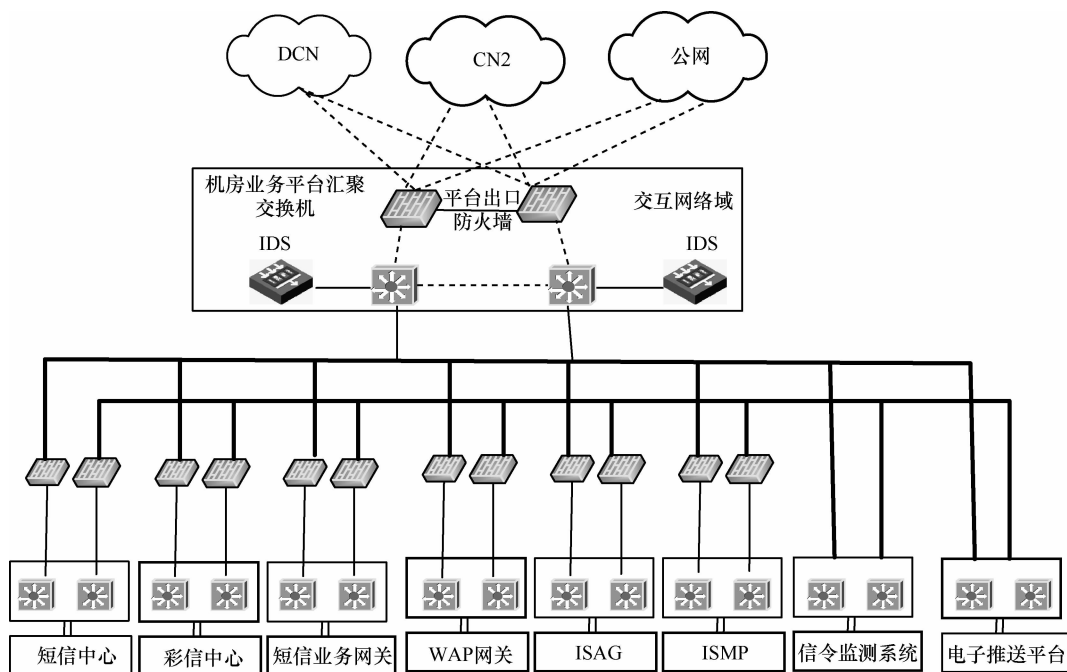


图7 不同平台边界整合案例

(2) 对防护目标分析安全威胁

以业务所对应的各种数据、数据流以及数据处理情况为防护对象,全面识别并梳理各要素在网络、系统、应用、内容等层次受到的安全威胁及脆弱性情况,并对防护目标进行评估,分析其可能受到的威胁、侵害和影响。

(3) 明确安全域防护等级和要求

根据工业和信息化部等级保护要求,对运营商的业务系统进行定级备案;根据安全域定级备案结果,结合工业和信息化部等级保护要求,分析安全域安全防护是否符合等级保护的相关要求。

(4) 确定防护目标的安全需求

以安全域承载的业务为出发点,分析各种业务的功能、持续性以及安全防护要求,并从自身的安全威胁、脆弱性状况及安全趋势走向出发,分析、总结并提出安全改进需求。

(5) 规划安全防护策略

安全防护策略是为了满足防护目标安全需求而制定的一系列安全防护要求。通常需要对防护目标的总体安全需求进行整理,再按照一定的次序进行逐步细化,以明确各个安全域的边界和内部安全防护策略。

(6) 制定安全防护规范

根据防护目标及各个安全域的安全防护策略,明确相应的安全防护手段及其部署方式,明确防护目标中各个设备应部署的安全防护策略,并检查安全防护是否满足安全服务所需的性能和安全需求。

4.2 安全域防护方法

在安全域划分和边界整合完毕后,需要进行安全域防护的设计。安全域防护设计一般应遵循等级防护、集中防护和分层防护原则。

由于各业务平台安全区域的安全需求不尽相同,具体采用的安全方案也需要区别对待,原则上应根据各平台的等级保护要求对安全域进行安全防护。业务域的设备应按照其功能、业务、网络互联需求,相应地部署至合理的安全域。考虑到设备自身安全防护能力是系统安全防护的基础,业务平台设备也需要实施安全加固,提高自身的安全防护能力。

交互网络域是业务平台的重点访问控制区域,通过在交换设备上 VLAN 划分、根据“禁止所有除非被明确允许”的原则设置防火墙访问策略等技术手段,有效地实现对业务平台计算域和服务域的安全防护。

在安全需求方面,对于计算域,一般以防病毒、木马攻击、黑客篡改、维护人员误操作导致的数据丢失为主。在防护手段上,可以采用防病毒木马、设置合理的访问控制策略、加强补丁更新管理、账号口令和权限管理等手段,实现计算域资产的保护。

对于维护域,则通过加强认证和审计、权限管控以及制定严格的配置标准等手段,同时部署相应的安全防护及接入控制系统,如 4A 统一认证登录系统、防病毒系统、防木马系统等;另外还应强化维护终端的安全管控,实现维护终端的统一管理和敏感操作监控。

对于服务域,则以防病毒、木马攻击、DDoS 攻击、黑客入侵为主,并加强用户的权限管理和认证审计,同时需要进行 Web 服务器的软件版本管理,如进行 Web logic、Apache、Tomcat 等版本更新等,避免版本漏洞问题导致的被入侵;另外,还应注意 SQL 注入、XSS 等漏洞(可参考 OWASP 公布的十大 Web 漏洞列表)的排查和整改。在部署防火墙方面,一方面要实现最小化访问控制策略,另一方面也需要根据实际情况,适当地部署 IDS、IPS、Web 防火墙和防病毒系统。

4.3 安全域防护案例

在广东电信某业务平台安全域结构中,根据实际业务、维护需要及存在的威胁情况(病毒、蠕虫、黑客攻击、DDoS 攻击、口令猜测等),最终实现的该平台的安全域防护控制情况见表 1。

网络域原则上只允许维护域固定的源地址段访问特定的目的端口。

计算域的防护策略只允许服务域的固定源地址访问特定的目的端口,考虑到实际维护需要,对于来自维护域的访问,也需要相应进行放通。

服务域由于需要对用户提供 Web 服务,因此需要允许公网地址访问 Web 服务器的 IP 地址和目标端口(一般为 80 或 8080);由于服务域的服务器需要与计算域的核心服务器进行业务互通,也需要允许计算域内的核心服务器单向访问到服务域的特定 IP 地址和特定目标端口;根据维护需要,开放来自维护域网段的特定维护终端的访问。

计算域的防护策略只允许通过维护人员使用的特定 DCN 的固定地址段进行访问,如果使用 4A 统一认证系统,则开放 4A 统一认证系统的堡垒机 IP 地址即可,由于维护域存在访问计算域、服务域的维护需求,因此也需要开放日常维护所使用的地址及端口。



表 1 广东电信某业务平台安全域防护策略

	公网	专线	DCN	服务域	计算域	维护域	网络域
网络域	只允许维护域固定源地址段和目的端口	禁止所有专线源地址段对网络域进行访问	只允许维护域固定源地址段和目的端口				
计算域				只允许服务域固定源地址段和目的端口		放通相应维护域网维护终端网段	
服务域	只允许公网访问服务域特定 IP 地址和特定目标端口		只允许 DCN 固定源地址段访问服务域特定 IP 地址和特定目标端口		允许计算域内的核心业务平台和外挂平台单向访问到服务域的特定 IP 地址和特定目标端口	放通相应维护域网维护终端网段	
维护域			固定地址段连接	服务域对来自维护域的访问,限制源 IP 地址和目的端口	维护域存在访问服务器维护需求,按需放通维护网段和端口		网络域对来自维护域的访问,需限制维护域的固定网段和目标端口

5 结束语

安全域的划分与边界整合是一项复杂的工作,需要在深入了解业务平台组网架构、网络接口、安全要求的基础上,有针对性、原则性地实施安全域划分,并根据不同业务平台的特点,实现分层次、分重点的保护,同时结合边界整合,简化系统边界,避免重复投资,达到统一接入、统一管控、控制成本、集中防护的效果。

实施业务平台的安全域划分与边界整合,推动安全防护技术体系的建设,提升安全防护效果,构建集约化的运营业务平台安全域防护体系,是解决当前业务平台安全问题的最有效手段。

参考文献

1 崔玉华. 对“信息安全等级保护”的探讨. Netinfo Security, 2005(2):72~74

2 吉增瑞. 信息安全等级保护浅析. 网络安全技术与应用, 2005(1): 55~57

3 林宁, 吴志刚. 我国信息安全标准化概况. 信息技术与标准化, 2006(8): 6~8

4 邱岚, 谭彬. 安全域划分研究与应用. 计算机安全, 2012(6): 39~42

5 赵立刚, 姚兴, 秦良斌. 运营业务系统安全域划分思路浅析. 计算机安全, 2012(9):30~38

(收稿日期:2013-08-01)



·简讯·

东信北邮中标江苏移动家庭
业务管理平台 HDC 一期项目

近日,东信北邮信息技术有限公司(简称东信北邮)成功中标中国移动江苏分公司家庭业务管理平台 HDC(home data center)一期项目。该项目为基于 IaaS 云平台基础上的家庭业务,提供接入统一管理与展现的综合性平台。

由东信北邮提供的家庭业务管理平台 HDC,通过接入 BOSS、网管系统,以帮助用户更好地营造良好的家庭业务生长环境,实现对家庭业务的统一控制管理和运营支撑。同时,家庭业务管理平台 HDC 建设也降低了移动家庭业

务的生成和接入门槛,在规范业务实施流程的前提下,更能满足移动用户业务快速上线的需要,避免了重复建设和资源浪费。据了解,东信北邮 HDC 家庭业务管理系统,支持包括家庭安防、健康守护、家信通、平安家庭等与家庭业务相关的绝大部分业务类型。

作为江苏移动家庭业务的第一门户,中国移动江苏分公司的家庭业务管理平台 HDC,已被定为中国移动重大课题。东信北邮通过对能力立体化和多维度的开放、组合,在推动移动业务产品的创新、促进家庭业务方面快速发展,被中国移动股份有限公司江苏分公司评为 2012 年优秀合作伙伴。