



## 基于云安全技术的智慧政务云解决方案

章谦骅<sup>1</sup>, 章坚武<sup>2</sup>

(1. 中国联合网络通信有限公司杭州市分公司, 浙江 杭州 310003;

2. 杭州电子科技大学, 浙江 杭州 310018)

**摘要:** 国家“十二五”规划提出要“加强信息共享, 厉行节约”, 政务云以规划为导向, 全国各地政府都在整合软/硬件资源, 共同构建公共电子政务平台。随着政务云的推广, 实施问题也随之而来。政务云建设需要解决政府职能部门间的“信息孤岛”问题, 同时考虑云计算技术的各种安全风险。从安全继承性角度, 电子政务云业务仍然是政务业务系统, 需要高度安全保护; 从安全合规性角度, 政府各局委办需要根据其重要性进行分等级保护。结合目前的云安全技术, 提出了一种电子政务云解决方案, 为安全体系规划、安全自动化部署及安全监管提供全面的安全方案。

**关键词:** 政务云; 电子政务平台; 云计算技术; 安全自动化部署; 安全监管

中图分类号: TP393.08

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017063

## Solution for smart government cloud based on cloud security technology

ZHANG Qianhua<sup>1</sup>, ZHANG Jianwu<sup>2</sup>

1. Hangzhou Branch of China United Network Communication Co., Ltd., Hangzhou 310003, China

2. Hangzhou Dianzi University, Hangzhou 310018, China

**Abstract:** The national Twelfth Five-year Plan have proposed to strengthen information sharing and austerity, government cloud development are planning this plan. Governments across the country are integrating hardware and software resources to jointly build a public e-government platform. With the promotion of government cloud, the implementation of the problem will follow. Government cloud construction needs to solve the problem of information islands among government departments, while taking into account the security risks of cloud computing technology. From the point of view of security inheritance, e-government cloud business is still a government business system, which need a high degree of security protection. From the point of view of security compliance, the government bureau of the commission need to be classified according to its importance. Combined with the current cloud security technology, a kind of e-government cloud solution was put forward, which provided a comprehensive security scheme for security system planning, security automation deployment and security supervision.

**Key words:** government cloud, e-government platform, cloud computing technology, security automation deployment, safety regulation

收稿日期: 2017-02-15; 修回日期: 2017-03-02

基金项目: 国家重点研发计划经费资助项目(No.2016YFB0800201); 浙江省自然科学基金资助项目(No.LY16F020016); 浙江省重点科技创新团队资助项目(No.2013TD03)

Foundation Items: The National Key Research and Development Program of China(No.2016YFB0800201), Zhejiang Provincial Natural Science Foundation of China(No.LY16F020016), Zhejiang Province Science and Technology Innovation Program(No.2013TD03)



## 1 引言

经过多年的发展,云计算已开始逐步从云端落地,越来越多地在实际应用场景中被使用。随着应用的部署,其系统和数据向云计算集中,开始发挥出云计算资源集中、高效率、低成本及个性化等优势。但系统和数据的集中也意味着风险的集中,并给信息安全的保障带来了更大的挑战。

云计算作为一个新兴的技术平台,在我国尚处于起步阶段,除了电信运营数据中心服务提供商和大型互联网公司外,政府也在积极地推动电子政务云的建设,试图通过集中建设,节约资金和资源,为各级电子政务应用和跨部门业务协同提供一个公共的平台,同时也为智慧城市建设、大数据分析等提供更为高效的数据支撑环境<sup>[1]</sup>。云计算技术的引入,云平台、虚拟化技术的使用以及资源和数据的集中为信息安全带来了前所未有的难题。除了云计算技术的共性安全问题外,在政务云特殊的环境下还包括以下需要解决的难点。

### (1) 业务系统隔离

传统网络中所有的政务业务都是部署在各自的独立业务区,安全防护自成体系,而在云计算环境下,网络、安全、计算、存储等资源共享,如何为每个政府单位、业务系统提供有效的隔离机制,是政务云安全需要解决的首要问题<sup>[2]</sup>。

### (2) 内/外网安全隔离

电子政务网络根据业务职能,一般包括对外提供互联网服务的互联网业务区、对内提供纵向互联的部门业务区(即电子政务外网)和横向互联的公共业务区<sup>[3]</sup>。政务云中,如何在保证这些区域有效隔离的同时,为不同的租户提供有效的安全防护,这也是一大难点。

### (3) 分等级的安全服务

传统网络中各业务单位按照不同业务系统的重要性和安全等级,划分安全域,提供如防火墙、VPN、负载均衡、Web 安全防护等能力。而在云计算环境下,资源统一供给,如何为不同的政府单位和不同安全防护需求的业务系统

提供个性化的分等级安全服务,并满足信息安全等级保护相关条款,对政务云安全架构设计提出了较高的要求<sup>[4]</sup>。

### (4) 安全资源自动化部署

政务云的创建就是为了解决原有政府各类业务建设和维护的问题,提升政府办事效率,而在计算资源、网络资源等能够实现自动化部署的前提下,安全能力也要实现自动化的部署交付,这就要求政务云能够实现全业务的自动化管理。

## 2 政务云安全体系设计规划

政务云在安全方面需考虑很多因素,主要有如下几点。

- 按政务网业务划分的要求进行政务云安全区域划分,并在各区域内提供相应的云安全服务。
- 实现政府多租户隔离和个性化的安全服务,确保不同市(或县、区)政府下属的各局、委员会、办公室(以下简称政府局委办)等的业务在迁移到政务云后能够享受云安全等级保护符合规范的安全服务。
- 借助先进的安全自动化部署服务,提供云安全服务的自动化部署功能。

### 2.1 各业务区域安全规划及隔离设计

政务云按所承载业务的不同划分为不同的区域,面向互联网的门户网站和相关信息系统区域、部门自身的业务系统区域和跨部门共享的信息系统区域。各区域之间应采用 VPC 等技术进行隔离,区域内部系统按不同的安全要求确定安全等级保护并按相应要求进行保护。跨区域数据的访问或数据同步应有相关的控制手段。政务云 IaaS 平台需按照等级保护三级标准进行建设,各租户业务系统根据等级保护定级要求实施不同安全级别的保护,具体见表 1。各区域具体的安防规划介绍如下。

#### (1) 互联网业务区

一般部署政府各职能部门对外门户网站和公共服务,不同业务单位需要进行有效的隔离,同时还要应对来自互联网的各种可能风险,安全防护内容将主要以 Web 安全防护为主。

表 1 政务云业务区安全需求分析

|      | 互联网业务区                            | 部门业务区               | 公共业务区                      |
|------|-----------------------------------|---------------------|----------------------------|
| 业务描述 | G2B:对外发布;政府门户网站;对公众服务             | 政府局委办的纵向业务          | 政府统一规划横向互访业务行政审批、办公系统、综合治税 |
| 形式   | 依托电子政务外网,对 Internet 开放服务          | 依托本部门业务专网,统一的电子政务外网 | 依托电子政务外网,政府局委办统一规划         |
| 安全需求 | 多租户隔离、多租户分等级保护、VPN 接入认证审计、互联网风险防护 | 多租户隔离、多租户分等级保护      | 多业务安全隔离、基础访问控制、Web 门户安全防护  |

### (2) 部门业务区

主要部署各部门专属业务,为部门内部服务,主要防护需求为租户间的隔离,同时业务分等级保护。

### (3) 公共业务区

主要为政府部门公共服务及跨部门、跨地区业务的协同应用系统,此类应用仅能在电子政务网内部访问,仅被授权的业务部门具备访问权限。

政务云业务区域隔离设计如图 1 所示。由图 1 可知,按照各分区安全要求构建安全防护网络,主要考虑以下几个因素。

- 政务云基础设施资源划分为 3 个独立的区域,分别为互联网业务区、部门业务区、公共业务区,3 个区域间不能直接访问,仅能通过跨网数据交换区进行数据交换。
- 为满足等级保护合规需求,每个业务区内还需要划分二级等级保护区和三级等级保护区两个区域,两者的计算资源不允许共享,即二级业务和三级业务应用系统不得同时部署在同一台物理服务器上。每个等保区域内不同租户应用间通过 VLAN/VxLAN 隔离,租户应用间通过访问控制设备进行访问控制,禁止非授权访问。
- 管理区域与业务区域网络要实现隔离。管理平台(网管平台、安管平台、云管理平台)仅允许通过管理区域内的管理终端本地访问,避免远程管理可能引入的系统风险;远程安全接入区提供 VPN 接入服务,满足政务应用(移动报税、公安执法等)。

## 2.2 多业务安全资源池创建

政务云中,针对不同的租户可以提供隔离和个性化的安全服务,但是为每个租户单独部署一套安全设备是不现实的。因此,和计算资源虚拟化一样,可以将安全资源进行虚拟化。等级保护多业务安全资源池设计如图 2 所示,采用安全设备虚拟化技术建立安全资源池实现多业务能力。在政务云中,因为等级保护的需求,通常需要具备以下几种能力:云防火墙提供区域隔离能力、云入侵防御提供攻

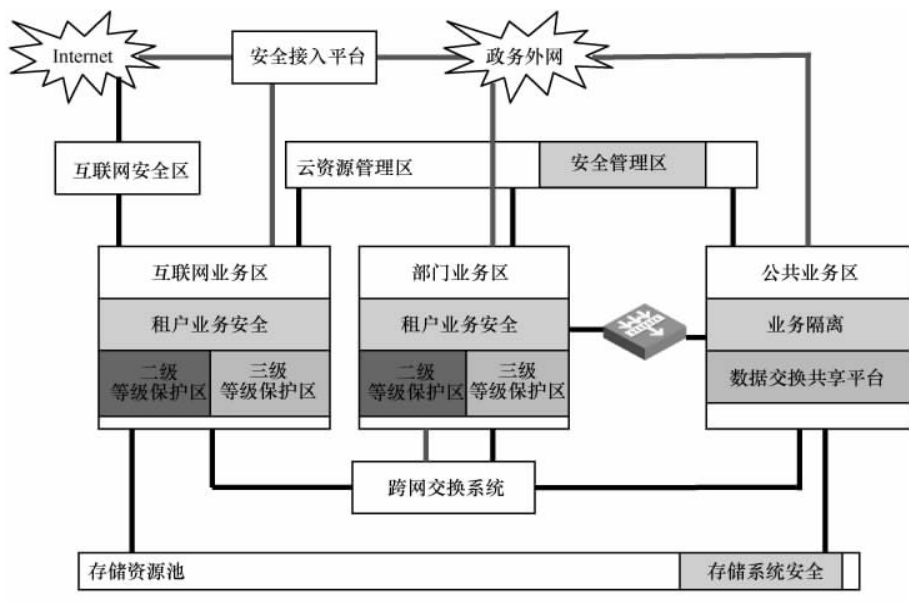


图 1 政务云业务区域隔离设计

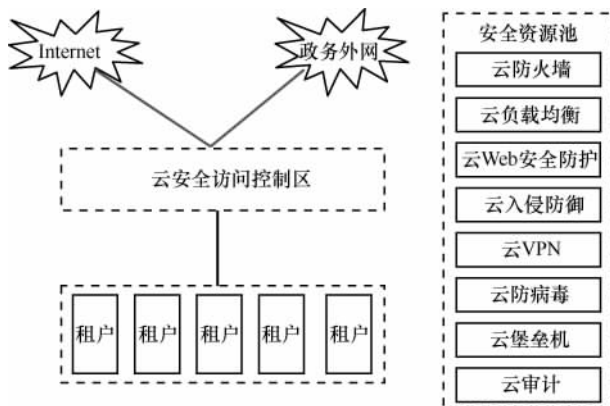


图 2 等级保护多业务安全资源池设计

击防御能力、云负载均衡提供应用优化和流量调度能力、云 Web 安全防护(云 WAF)提供 Web 攻击防护能力、云 VPN 提供租户 VPN 接入能力、云防病毒提供针对租户的网络防病毒能力、云堡垒机提供租户网络安全运维审计能力、云审计提供对租户的业务访问审计能力等。所有的安全防护资源根据业务类型和等级保护可以从资源池中按需调用,从而构建出云安全等级保护立体防御矩阵。

虚拟化技术是实现基于多业务隔离和访问控制的重要方式,且该虚拟化技术是要求完全实现虚拟化的。要完全实现虚拟化,需让每个虚拟化的安全设备能够通过唯一的 OS 内核对系统硬件资源进行管理,每个虚拟安全设备作为一个容器实例运行在同一个内核上。多台虚拟安全设备相互独立,对外呈现为一个完整的安全设备。该系统业



务功能完整、管理独立、具备精细化的资源限制能力。只有这样,才能做到每个虚拟安全资源独立自主地为不同租户提供互不干扰的服务。如果某个虚拟安全设备因访问量过大,侵占了整个物理设备的资源,那么在同一台物理设备上的其他虚拟安全设备将无法正常工作。

### 3 政务云安全自动化部署

#### 3.1 基于 SDN/overlay 架构搭建自动化安全调度网络

政务云对自动部署的要求很高,除了计算、存储等传统业务的自动化部署外,网络安全的自动化部署也非常重要。因此在整个政务云中引入云计算、网络、安全的一体化自动调度方案很有必要。本文采用了一种基于 SDN/overlay 的技术实现对网络安全的改造,通过对业务流量的自动化调度,并结合服务链技术定义安全防护的类型和顺序,将流量按需引入安全防护资源池中进行“清洗”,从而进行灵活的安全防护调度。

#### 3.2 构建可编程的安全服务

通过云平台的统一门户,实现多租户安全资源自助申请和个性化安全服务。为租户在申请云主机、云存储等服务时提供配套的安全防护服务,安全策略定义也要与租户的云服务行为相一致,主要为外部用户对政务云内部资源的安全威胁防御,使租户通过政务外网、公有云、互联网等对政务云内部资源的风险过滤,有效保证政务云基础资源的安全性。

从自助门户上申请的安全服务,基于软件编排的安全服务能够自动形成转发路径表并下发到底层硬件设备,实现自动化的业务配置和部署,具体流程介绍如下。

- 需要通过自助门户进行租户身份认证。
- 租户在登录自助门户后,根据自身的业务需要,选

择或定义差异化的安全需求和资源带宽要求。

- 在完成申请确认后,这些安全服务和策略进行自动化的配置下发。
- 如果租户选择多个安全服务,如云防火墙、云防病毒等,则需为租户的业务流生成匹配的安全服务转发路径并实现流量自动化牵引,提升业务部署效率。
- 管理平台需要具备针对不同租户的安全资源和策略进行监控的能力,并将监控的分析报告提交给租户,使得租户可以根据分析结果对资源和安全策略进行调整。

### 4 政务云安全监管中心设计

政务云除了做到基础的安全隔离防护外,还需根据政务业务的特点,在安全监管上进行规划设计。例如,政务外网群集中部署到云端后,需要提供对网站群的集中监管能力;此外,政务云作为一个庞大的政务业务服务体系,整网安全监控显得更为重要,这也需要运维人员能够具备对整网安全可视化和安全态势监控的能力。安全监管中心有别于单点安全产品,应广泛收录基础架构设施中与安全存在关系的日志,并进行融合分析的集中化安全产品,还能够实时展示云内各种安全状况,并结合大数据技术预知风险,协助管理员做出有效的管控措施。

#### 4.1 安全服务管理

安全服务管理如图 3 所示。由图 3 可知,安全服务管理的主要作用是 FW、IPS 等安全设备的安全策略配置管理和部署、安全设备软件及配置文件管理等,确保关键安全节点自身的正常运行。

同时,对网络和应用的管理是作为安全监管中心的重要辅助功能,主要用于:监控到的性能指标用于事件

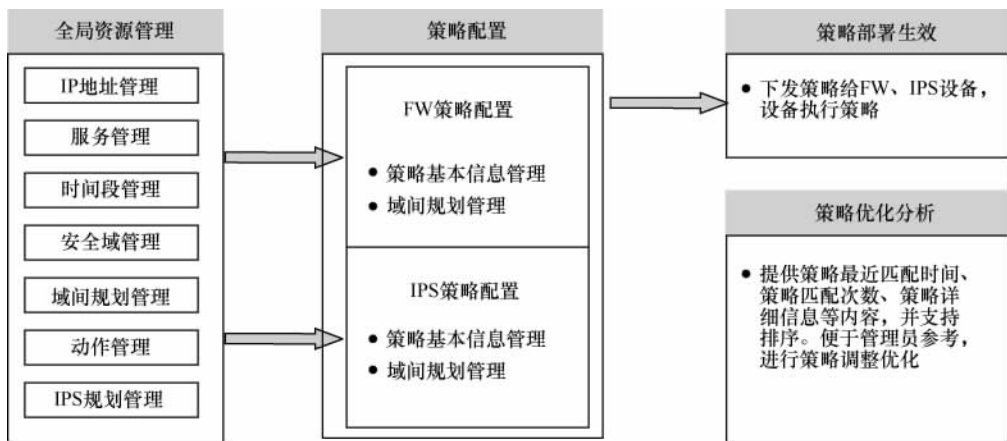


图 3 安全服务管理

关联分析、确保关键路径安全设备的正常运行、攻击拓扑溯源等。

#### 4.2 安全事件管理

安全事件管理是安全监控中心的基础功能,即对数据处理环节的日志及事件进行事件级的关联分析、多维度统计分析等功能。安全事件管理主要是收集和分析来自网络和安全设备产生的安全事件以及主机和应用系统的日志分析一体化事件。

将安全事件管理和安全信息管理整合在一起,其中安全信息管理聚焦于内控管理,安全事件管理更多地是关注内/外部的威胁及安全事故响应处理。具体设计时应考虑两种分析方法:事件关联分析法和事件统计分析法。事件关联分析能从海量的来自异构数据源的事件或日志进行相关性分析,找出其中的联系,从中提炼出需要运维人员关注的“关联事件”;事件统计分析要从攻击、漏扫、设备、主机、运行状态、综合等多维度分别给出数据分析报告,不留死角地对企业安全状态进行全面呈现,使安全监控中心的使用者更好地聚焦安全威胁。

#### 4.3 安全风险分析

安全事件分析是以事件为核心来进行安全分析的,属于微观层面的分析;而安全风险分析是站在资产和业务以及整个政务云的高度进行宏观的风险分析和安全风险评级。

##### (1) 资产风险监控

资产风险由指向该资产的攻击事件及漏洞组成。典型的漏扫应包括 Web 漏扫、主机漏扫和数据库漏扫,并提供漏洞风险情况的展现,以便及时进行漏洞修复。最终由攻击事件和漏扫结果进行计算,得到某个资产的安全评分。

##### (2) 业务风险监控

将具有相关性的资产通过建模,构成一个业务,业务的安全度数值由该业务下各个资产的安全度通过加权计算得出,可以反映出该业务面临的风险状况。

##### (3) 全局风险监控

全局风险由各个资产安全评分加权得到,还应提供高风险资产、安全告警、网络告警、安全事件趋势、攻击源和 IP 变化趋势等内容。从宏观角度评判整个企业的风险情况,快速做出安全运维管理方面的决策。

#### 4.4 安全响应管理

通过对安全时间和安全风险的分析,生成相应的告警

事件。通过安全响应管理对这些事件进行及时和规范的处理和解决。在响应方式上,可以通过邮件响应、短信、声音等方式通知租户,并发出响应动作,如用户下线、用户隔离、加入黑名单、执行设备命令脚本等。

## 5 结束语

本文结合目前的云安全技术,提出了一种电子政务云解决方案,给出了政务云安全体系规划、安全自动化部署要求及安全监管中心设计方案。一个完整的政务云安全系统还应包括云平台安全、租户业务系统主机安全、应用安全、数据安全等内容。安全监控中心是面向全 IT 资源的集中安全管理平台。通过对海量异构网络与安全事件的采集、处理和分析以及对安全设备、应用、服务器等日志数据的横向分析,帮助政务云管理部门实现高效的安全运维。

## 参考文献:

- [1] KAUFMAN L M. Data security in the world of cloud computing[J]. IEEE Security & Privacy, 2009, 7(4): 61-64.
- [2] FENG D G, MIN Z, YAN Z, et al. Study on cloud computing security[J]. Journal of Software, 2011, 22(1): 71-83.
- [3] PAQUETTE S, JAEGER P T, WILSON S C. Identifying the security risks associated with governmental use of cloud computing[J]. Government Information Quarterly, 2010, 27(3): 245-253.
- [4] SHIN D H. User centric cloud service model in public sectors: policy implications of cloud services[J]. Government Information Quarterly, 2014, 30(2): 194-203.

## [作者简介]



章谦(1990-),男,中国联合网络通信有限公司杭州市分公司创新业务支撑经理,主要研究方向为智慧城市、云计算、大数据等。



章坚武(1961-),男,杭州电子科技大学通信工程学院教授、博士生导师,主要研究方向为移动通信系统、多媒体通信技术等。