



发电企业信息安全保障体系建设

余 颖

(国电成都金堂发电有限公司 成都 610404)

摘 要:为了满足当前信息化安全建设的要求,在保证现有业务系统可用的基础上,实现信息化安全保障体系建设目标,通过对发电企业代表单位——国电成都金堂发电有限公司现有的网络部署结构、系统访问模式、用户使用习惯等进行分析,确定了发电企业从网络管理、边界安全防护、移动接入安全、主机安全、应用系统安全 5 个层次对其业务系统进行安全加固的设计方案。通过介绍国电成都金堂发电有限公司先进的安全保障体系的建设过程,为其他发电企业信息化安全建设提供了参考。

关键词:身份认证;网络管理;安全防护;数据泄密;终端检查

doi: 10.3969/j.issn.1000-0801.2014.01.023

Construction of Information Security System of Power Generation Enterprise

Yu Ying

(Guodian Chengdu Jintang Generation Co., Ltd., Chengdu 610404, China)

Abstract: In order to meet the current demands of building information security, while ensuring existing business systems available, based on information technology to achieve the goal of building security system, the existing network deployment structure system access mode, user habits of Guodian Chengdu Jintang Generation Co., Ltd., on behalf of units of power generation enterprises, were analyzed. Based on this analysis, a five-level business system, as the network management, border security protection, mobile access security, host security, application security, was designed for power generation enterprise security reinforcement. By introducing the construction process of advanced security system of Guodian Chengdu Jintang Generation Co., Ltd., the references were provided for other power generation enterprise information safety construction.

Key words: identity authentication, network management, security protection, data leak, terminal check

1 现状

国电成都金堂发电有限公司(以下简称金堂公司)目前有一条带宽为 30 Mbit/s 的光纤接入到互联网,在互联网出口处部署了防火墙。金堂公司有两个不同的网络,一个是生产业务网,一个是互联网,由于终端数量有限,目前两个网络共用一套物理网络,用户在同一台计算机上可以访问互联网和业务数据,具体网络结构如图 1 所示。业务

系统集中在服务器区域,业务系统的结构有 C/S 类型和 B/S 类型。按照要国家电网建设要求和内部需求,需要将两网隔离,同时对用户的访问行为和系统安全进行有效的防护。

2 信息系统安全风险和安全需求

安全风险分析和需求分析是有效保证系统安全的前提条件,只有从业务系统数据可能存在的风险进行详细

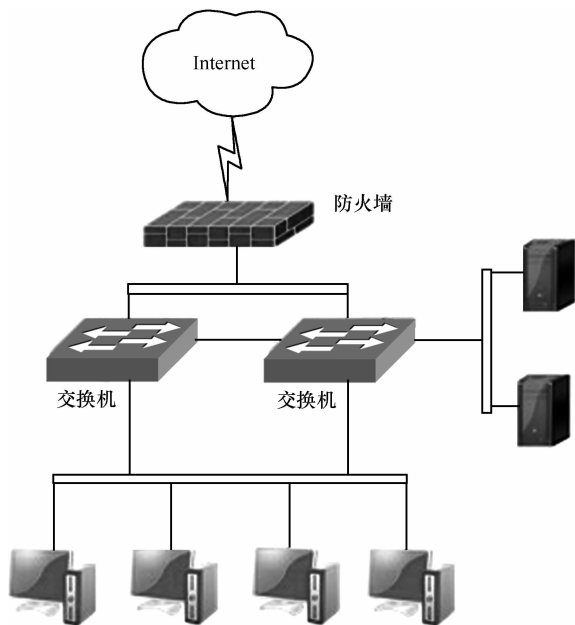


图1 原有网络结构

分析,准确地了解用户的安全需求,才能制定正确的建设方针。

2.1 存在的风险

- 缺乏有效的认证手段。没有有效的认证手段会导致上网人员没办法控制。
- 无法对上网用户的行为进行控制。金堂公司的互联网出口带宽只有 10 Mbit/s,如果内部用户在线观看电影或下载会严重影响其他用户的使用。
- 无法追踪非法访问。互联网的内容越来越复杂,内部用户有可能在互联网中干一些非法的事情,公安部会追查到相关部门,如果内部不能找到具体的人员,整个部门将受到影响。
- 移动用户无法安全接入。用户出差到外地时需要接入内部网络,如果将业务系统发布到公网整个系统将不安全,如果不发布用户在外部将不能访问系统。
- 存在终端隔离的安全风险。发电企业有内网和外网,两个网络需要隔离。
- 数据被窃听。终端用户使用 B/S 模式访问系统,由于采用 HTTP 部署,客户端和服务器的通信没有加密,容易造成被窃听。
- 数据泄密。发电企业内部有很多敏感信息,一旦这些数据泄密出去会对内部造成严重影响。
- 无应用层攻击防护。B/S 结构的应用系统存在如 SQL 注入、跨脚本攻击(XSS)、跨站伪造(CSRF)、

cookie 篡改及应用层 DDoS 等风险。

- 终端的安全风险。不安全终端接入网络时可能将一些风险带入到网络中,没有部署终端安全检查设备,无法对接入的终端进行安全检查。

2.2 建设思路和调研

2.2.1 建设思路

以上风险问题可通过以下建设来解决。

- 在互联网出口部署上网行为管理,用于解决用户接入互联网的认证、带宽管理、审计等几个问题。
- 部署 SSL 实现移动办公的安全接入。
- 部署应用层防火墙对 L2~L7 的攻击进行防护。
- 部署隔离设备实现双网隔离。
- 部署终端安全检查和终端安全管理实现终端的管理和防护。

2.2.2 建设对比

实现双网隔离有 3 种方式,一种是桌面云,一种是虚拟安全桌面,还有一种是隔离卡,3 种方式都有自己的特点,具体如下。

(1) 桌面云

在共享的工作模式下,所有的软件均安装在服务器上,并且均在服务器上运行,运行的结果送往云终端显示,云终端只负责显示及键盘、鼠标输入,不运行软件。当不同的终端登录时,服务器会为它开辟一片空间,所以不同的终端运行同一个软件,也不会冲突。软件运行的效果取决于服务器。其特点如下:

- 对接入终端硬件配置几乎没有要求,使用现有 PC、笔记本电脑、平板电脑以及智能手机都可以;
- 网络带宽要求较小,理想情况下每个接入终端占用几十到几百 kbit/s 带宽不等(需看传输内容情况);
- 维护工作量较小,桌面云的维护主要是数据中心的服务器和存储设备以及账户维护管理工作,终端的维护工作量较小;
- 关于数据安全、防泄密等要求,主要将服务器的数据安全、防泄密做好即可,因为终端用户看到的仅仅为图像界面,不存在太多的泄密风险(除屏幕截屏),可以对本地打印的功能进行限制,但是对互联网外发信息无法限制;
- 桌面云属于云计算的一种应用,其需要在数据中心建有大量的高端服务器、大规模存储以及较高的带宽。



(2) 桌面虚拟化

通过强认证、SSL 加密传输、权限划分等技术来控制整个网络和服务器的用户安全访问,再通过对本地系统资源的底层重定向的虚拟化安全桌面来解决终端层面遇到的各种泄密风险(如外设管理、网络隔离、数据加密等),其特点如下:

- 对接入终端硬件配置几乎没有要求,使用现有 PC、笔记本电脑等 Windows 平台系统可以直接支持,对于智能终端(平板电脑、智能手机)可以使用应用虚拟化发布方式扩展支持;
- 网络带宽无要求,与现有软件对服务器访问带宽一致,如果尽在本机操作,无流量;
- 维护工作量较小,仅需要将中心端的虚拟化桌面平台设备维护好即可,部署时用户使用浏览器下载虚拟安全桌面的插件即可(需几 Mbit/s 带宽);
- 数据安全、防泄密等较为完善,在本机将所有业务数据运行在加密的安全桌面环境下,对于用户的外发互联网外发以及打印甚至是屏幕截屏都可以控制;
- 投入方面仅需要在数据中心部署虚拟安全桌面平台即可。

(3) 隔离卡

隔离卡是以软件切换方式将一台计算机虚拟为两台计算机,计算机在物理隔离的状态下既可连接内部网络(内网),又可连接外部网络(外网),其特点如下:

- 对接入的终端有较高的要求,用户数据调取在本地,本地计算机的硬件配置较高,另外需要 2 个硬盘,每个硬盘用于不同的网络;
- 用户体验效果较差,用户只能同时使用一个网络,当用户需要切换到另一个网络时先需要重启计算机,并通过切换开头或切换选项实现两个网络的切换;
- 数据防泄密方式差,用户在使用内部网络或外部网络时可以直接通过打印、U 盘复制、截图等方式将数据泄密出去;
- 终端维护工作大,每个用户都是独立的终端,当终端出现问题时都需要管理员协助用户处理问题。

(4) 对比小结

桌面云在数据防泄密方面较差,用户可以通过互联网直接将数据外发出去,另外,桌面云需要在服务器区域部

署高性能的服务器来满足用户的需求,因此从数据防泄密安全和服务区域高成本投入等方面综合考虑,桌面云不适合当前的业务发展需求。使用隔离卡用户每次切换桌面时都需要重启计算机,影响用户使用,同时隔离卡不能对终端的打印、U 盘复制、截图等进行限制,需要另外投入产品来满足防泄密的要求,因此从用户使用体验、数据防泄密的安全、资金投入等方面考虑,虚拟桌面都要占优势,因此采用虚拟安全桌面来实现网络隔离更为合适。

3 安全设计与实现

从网络管理、边界防护、移动接入安全、主机安全、应用系统安全 5 个层次进行安全防护设计,保障数据在各方面的安全,达到安全、管理、易用的效果。

3.1 网络管理、边界安全防护、移动安全接入设计与实现

网络管理、边界安全防护、移动接入安全主要分如下几步进行建设,具体如下。

- 在出口部署上网行为管理。通过配置上网行为管理上的策略配置,实现对用户的流量管理、上网行为管理、非法控制、访问审计等,另外通过配置上网行为管理的安全桌面,让用户在安全桌面下上网,保护上网的安全。
- 部署认证系统。通过部署认证系统,用户接入互联网时需要先通过认证。认证系统可以通过上网行为管理上的认证系统,也可以通过上网行为管理调用专业的认证系统进行用户上网认证。
- 在出口部署防火墙。通过对防火墙的配置进而有效防护攻击,如防御 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、CC、SYN Flood、ICMP Flood、UDP Flood、DNS Query Flood、ARP 欺骗攻击防范等,另外在防火墙上配置地址转换和端口控制,实现内部信息的隐藏。
- 部署移动接入安全设备。虚拟专用网(virtual private network,VPN)指的是在公用网络中建立专用的数据通信网络的技术,实现低成本、高安全地解决数据传输及应用发布平台。移动用户通过 VPN 接入,保证了用户可接入内部网络,同时降低了接入风险。

3.2 主机安全防护设计与实现

主机的安全设计主要从以下几个方面进行。

- 使用专业漏洞扫描仪(漏洞库为最新的)对主机系统进行全面扫描,确保主机系统只开启应用系统所需要的服务,关闭系统非必需的服务,并根据漏洞扫描结果进行主机系统安全加固。
- 部署系统补丁分发系统,时时更新补丁分发系统,同时对终端系统的补丁进行升级,减少终端系统漏洞,保障终端的安全。
- 安装正版防病毒和防木马软件,并确保安全软件系统能正常升级。
- 安装终端接入检查机制,对接入终端的安全进行检查,通过检查用户终端的进程、注册表、操作系统版本及系统补丁等内容,对不符合安全要求的终端不

允许接入网络中,并告诉用户需要对终端安全进行升级,只有符合安全要求的终端系统才能接入网络中,保证接入网络的安全性。

3.3 应用系统安全设计与实现

系统隔离建设如图 2 和图 3 所示。

应用系统的安全设计主要从系统区域的安全防护、加密访问、系统加固、备份与恢复等多方面考虑,系统的防护如图 2 所示,应用系统专网隔离如图 3 所示。

在服务器出口处部署一台应用防火墙,通过对应用防护策略的设计实现 L2~L7 的防护,如 SQL 注入、跨脚本攻击(XSS)、跨站伪造(CSRF)、口令爆破、弱口令探测、应用信息探测、非法上传威胁文件、cookie 篡改及应用层 DDoS

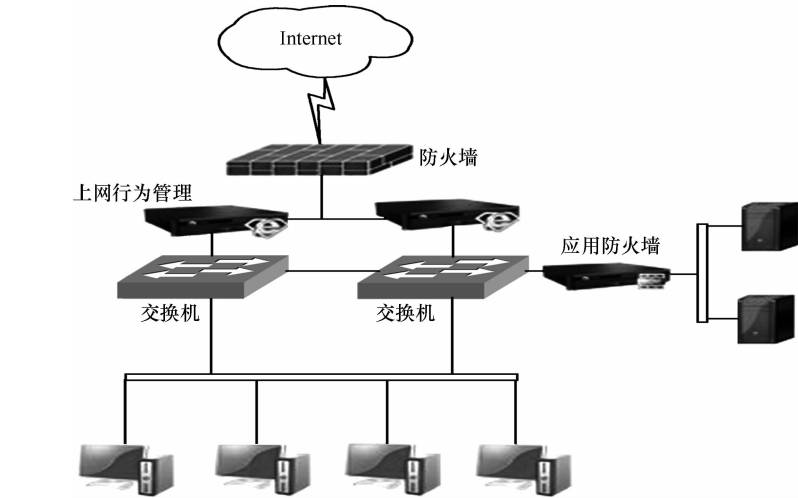


图 2 应用防护

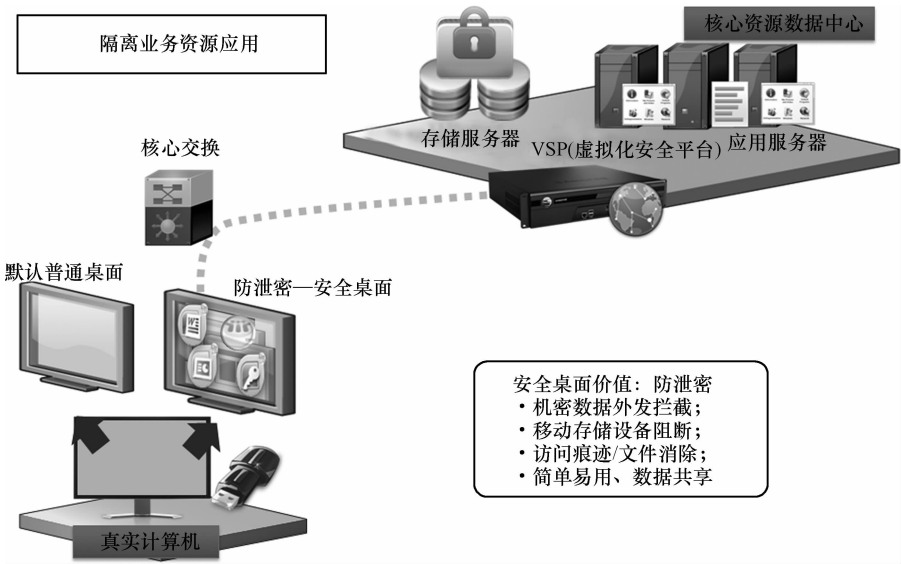


图 3 虚拟安全桌面



等方面的防护,另外在应用层防火墙上配置服务器隐藏、Web 隐藏将服务器区域的信息隐藏起来,保障内部应用的安全。

(1)业务系统采用 SSL 加密访问

SSL 加密是一个安全通信通道,它可以在用户和服务之前建立一个安全的加密通道,用户通过加密方式访问业务数据,最大程度地降低系统遭受会话监听和劫持攻击的风险。要实现业务系统的 SSL 加密访问,可以在服务器区域前部署 SSL 加密设备,也可以将业务系统结构改成 HTTPS 形式。

(2)强化口令策略

增加口令强度自检模块,检测系统用户口令长度、强度等是否符合强口令要求。如果修改的口令不符合口令策略要求时,系统阻止用户登录,并提示用户重新更改密码,直到口令强度符合要求。系统登录时设置登录次数限制,防止遭受暴力攻击风险。

(3)网络应用隔离

应用系统数据需要与互联网隔离开,以防止信息泄密出去,保证内部数据的安全。通过建设虚拟桌面的方式将整个物理网络隔离成两个不同的网络,用户访问互联网的数据在本地网络中,用户访问业务系统数据在加密的专网中,并且通过策略控制,禁止在虚拟桌面中使用外设(USB、打印机、COM 等),禁止虚拟桌面与本地桌面通信,实现两个网络的隔离。

(4)访问审计

审计是保障信息系统安全的重要手段,而且应用系统的跟踪、监控及灾难恢复都依赖于日志系统。通过部署数据库审计系统和行为审计系统可以有效地记录访问应用

的行为和数据。

(5)数据备份及恢复

为了防止人为的失误或破坏,应在异地建设灾备中心,一旦主数据中心出现故障,异地数据中心可以正常工作,保障业务不中断,数据不丢失。

4 结束语

随着信息安全形势的日益严峻,对信息安全的高度重视,业务应用系统的建设和使用已经不能仅停留在系统可用性功能上。应用系统的设计、开发、运行都必须确保网络与信息的安全。本文以一个发电公司——金堂公司的信息安全为例,在现有的网络和信息化建设情况下,开展了详细的分析与安全设计。本文对发电企业业务系统的安全加固建设、双网隔离、用户管理、移动接入安全有一定的参考价值。

参考文献

- 1 国家电力监管委员会 5 号令. 电力二次系统安全防护规定, 2004
- 2 国家电力监管委员会电监安全 34 号文件. 电力二次系统安全防护总体方案, 2006

[作者简介]



余颖,女,国电成都金堂发电有限公司高级工程师、信息中心主管,主要研究方向为信息化安全及系统建设。

(收稿日期:2013-08-01)

(上接第 147 页)

参考文献

- 1 侯延湘. 数据质量管理及在数据仓库实现探讨. 吉林大学硕士学位论文, 2007
- 2 刘涛. 青海移动数据仓库数据质量控制方案设计与实现. 北京邮电大学硕士学位论文, 2011
- 3 付威. 金融行业数据仓库项目的数据库质量管理应用. 北京邮电大学硕士学位论文, 2006
- 4 杨凡涛. 关于省级数据集中后税收数据质量管理与应用研究. 中国海洋大学硕士学位论文, 2009
- 5 宋敏, 覃正. 国外数据质量管理研究综述. 情报杂志, 2007(2)

[作者简介]



张瑜,女,内蒙古电力公司信息通信中心工程师,主要从事电力信息化网络及数据建设、管理和规划方面的工作。

潘红芳,女,内蒙古电力公司信息通信中心工程师,主要从事电力信息化建设、发展和规划方面的工作。

(收稿日期:2013-08-01)