大型科技网络系统安全方案设计

朱亚兴

(广东科学技术职业学院 软件工程学院,广东 珠海 519010)

摘 要:研究了基于某大型科技信息应用网站的安全管理解决方案的设计与实现。介绍了网络系统的安全体系设计、网络安全保证以及网络安全管理措施。着重介绍了双重防火墙保障技术以及非军事区结构模式,硬件安全保障措施以及先进的网管系统,严格的认证、授权机制,并采用防病毒软件和入侵监测系统等一系列安全技术和保障措施,形成了一个较完整的基于 Internet 信息系统应用的安全解决方案。

关键词:网络内容提供商;网络服务提供商;防火墙;非军事区模式;定制攻击描述语言

中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2010)13-0040-04

Major science and technology network security design

ZHU Ya Xing

(Department of Software Engineering, Guangdong Vocational Institute of Science and Technology, Zhuhai 519010, China)

Abstract: This paper studies the security design based on science information system. The security architecture design, network safeguard and security management method are introduced. It weightily introduces the firewall technique and DMZ structure, hardware safeguard and advanced network management system, firm authentication and authorization, anti-virus and access monitor system etc. They form a good integrated secure design method based on internet information system.

Key words: ICP; ISP; firewall; DMZ; CASL

目前,大中城市科技网得到了迅猛发展,已成为国家和省、市、地区信息基础设施的组成部分,是城市科技管理与科技工作现代化的重要基础。某市科技信息网的建设以专业化为特征,以科技、科管信息为采集重点,以统筹规划、统一标准、分布建库为建设方针,建设面向所属市及全国科技界的内容丰富、辐射面宽、实用性强、手段先进的网上科研信息资源。本文研究和建设的某市科技信息网定位为一个专门提供所属城市及全国科技信息的 ICP(Internet Content Provider),同时兼任 ISP(Internet Service Provider)的功能。

作为地区国民经济信息化的重要工程之一,某市科技信息网络系统的建设目标是:成为国际科技信息网和省科技信息网的地区主干网;成为城市与国内外科技信息交流的平台;成为市科技信息开发、应用与服务的平台和反映地区科技信息的主要窗口;面向科技管理职能部门,面向公众,加强科技服务的力度;通过网络的运作提高城市科技水平,为科教兴市作出贡献。本系统的建设目标为系统的总体安全方案设计提出了严格的要求,如何确保系统的安全,如何构建一个坚实的网络系统及安全体系已成为本系统的一项的重要任务。本文主要从双重防火墙过滤、入侵检测技术、防病毒技术、子网间网络协议互联及安全等几方面重点阐述。

1 网络总体规划及功能

系统网络平台和网络管理系统的建设总体规划是:

(1)构建外部连接网络平台。通过与一些主要信息网的 Internet 连接,使本系统成为一个城市内的科技信息主干网,为市内用户提供 Internet 入网和科技信息资源的综合利用服务。

(2)构建内部网络平台,为本系统各类网络应用提供网络支撑平台和完善安全的网络管理系统。

根据上述的系统总体规划目标,本系统网络平台提供以下网络功能服务:

(1)用户接入:提供拨号接入、Internet 接入、本系统局域网连接 Internet,域名解释、路由、文件传输、邮件收发。

(2)应用支持:为网上数据库提供网络支撑平台。本系统网络主干达到 1 000 MHz 的带宽,提供了 Oracle 数据库服务器/Lotus Domino R5/全文检索工具等结构化及非结构化的数据库平台,并提供相应应用开发工具,这样的带宽及数据库平台保证了软件的开发和运行。

(3)网络设备管理:提供网络设备管理支持平台、网络设备管理系统。

(4)网络互联支持:提供系统局域网内部各子网互联系统及协议系统支持。本系统配有代理服务器/IP 三层交换路由协议/防火墙等提供网络互联的支持。

2 网络体系结构

本系统网络体系分为外部互连结构与内部互连结构。

外部互连结构实现本系统与市公共多媒体信息交换网、市信息中心网及省科技信息网的网络互连。实现方法是:与市信息中心通过 100 MHz 单模光纤连到 Cisco 7204 边界路由器上,与省内科技网及公众多媒体信息网通过 128 K 帧中继连接。同时在 Cisco 7204 上留有 ISDN 接口,作为光纤的备用线路。把访问市科技信息网的路由直接指在 CISCO 7204 上。

内部体系结构由各子网组成,确定子网划分的依据是子网应用职能及子网应用(或应用部门)的独立性;确定子网互连结构的依据是子网互联运行的安全要求,以及系统的对外服务性能优先原则。子网互连体系结构如图 1 所示。子网划分方案如下:

外部网:与本系统连接的所有远程网络、ISP 网和拨号网。

对外服务子网:包括本系统内与一切外部网直接连接的系统,是本系统与 Internet 连接和图 1 系统内部互连结构图对外服务的唯一子网,也是本系统分隔外部网和内部网的子网。

内部网和内部公共网:只与对外服务网互连,但内部网与对外服务子网的连接需通过内部防火墙过滤。内部分共网与对外服务子网的连接需通过外部防火墙的过滤。

3 安全性整体解决方案

3.1 安全性原则

为保证安全性本系统采取以下措施:

(1)采用双重防火墙系统,即硬件和软件防火墙,针对不同的服务和数据安全性满足不同的数据过滤要求和协议支持。

(2)接入设备、路由器和中心交换机均有冗余插槽和端口,提供接入通道、接入端口的备份,保证了对外连接和内部数据交换的高可用性。

(3)提供对 VPDN 的支持扩展,以保证楼外内部用户的安全接入。

(4)内部网支持 VLAN,可以随时针对不同的部门重新划分网段。

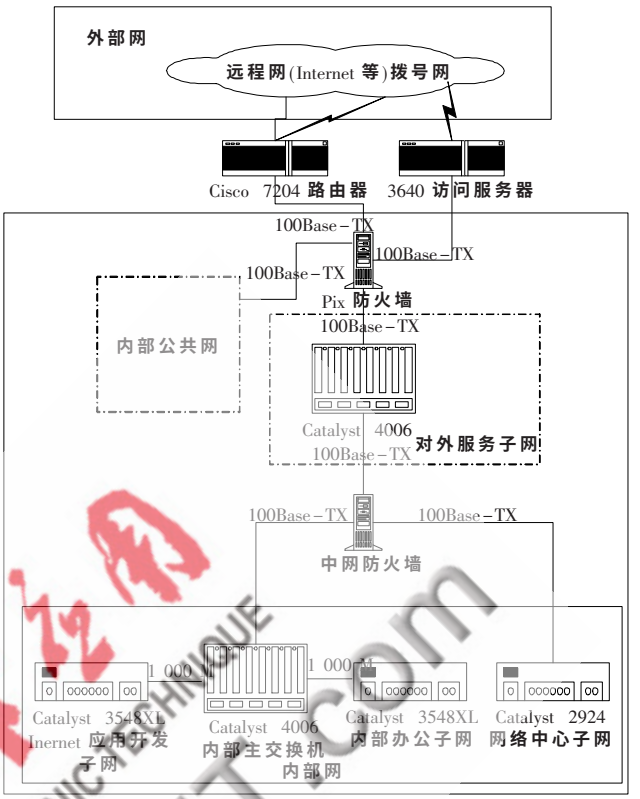

图 1 系统内部互连结构图

(5)采用先进的防病毒技术。

(6)采用先进的防入侵检测技术。

(7)比较完整的安全性管理措施和 IP 规划。

(8)由于本网站与市信息中心采用 100 MHz 单模光纤连接,因此可以借用这个高速通道,对数据进行远程备份,这也是一个提高本系统安全性的措施。

3.2 网络安全设计

本系统通过操作系统配置、路由器、防火墙、代理服务器、防入侵检测系统、硬件设备安全保证措施等多种手段,保证只有合法的、经授权的用户才能上网,才能登录到服务器[1-2]。

(1)双重防火墙

本系统根据需要划分了若干子网,其安全保障措施是通过双重防火墙技术实现。其中内部网的安全性要求最高,所有系统的审计信息、计费信息以及所有最重要的信息都存储在这个网段的服务器中。本系统内部体系结构如图 1 所示。

系统选用两道防火墙。外部防火墙选用 Cisco PIX Fire Wall 520,内部防火墙采用中网公司开发的国产硬件软件一体的防火墙[3]。

Cisco Pix FireWall 满负荷时运行速率超过 45 Mb/s,具有专用链路加密插件,可以用数据加密标准(DES)算法对数据加密,同时引入了 IETF 的鉴别标题(AH)和封闭安全性负载(ESP)协议。

这两个防火墙针对不同的应用和不同的网段进行了不同的包过滤。对内部网和外部网的数据包过滤系统(即内、外防火墙系统)进行分布式配置,内、外防火墙系统均具有地址过滤和服务过滤功能,还具有有关的过滤控制方面的能力[4]。所有内部网段内几个子网都要通过这个防火墙才能访问到对外服务网,再通过 Pix 访问 Internet[5]。

在本系统中,外部网与内部网互连采用了非军事区结构模式,如图 2 所示。

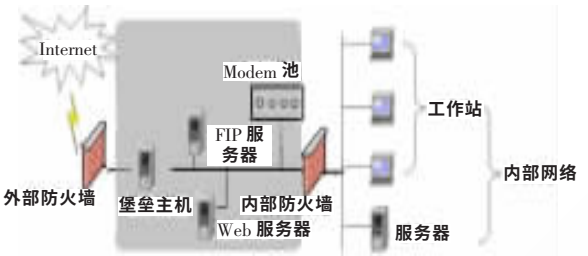

图 2 非军事区结构模式示例图

非军事区(DMZ)通常是一个过滤的子网,DMZ 在内部网络和外部网络之间构造了一个安全地带。DMZ 防火墙方案为要保护的内部网络增加了一道安全防线,同时,它提供了一个区域放置公共服务器,从而又能有效地避免一些互联应用需要公开而与内部安全策略相矛盾的情况发生。在 DMZ 区域中通常包括堡垒主机、Modem 池以及所有的公共服务器。在这种防火墙方案中,包括两个防火墙、外部防火墙抵挡外部网络的攻击,并管理所有外部网络对 DMZ 的访问。内部防火墙管理 DMZ 对于内部网络的访问,内部防火墙是内部网络的第三道安全防线(前面有了外部防火墙和堡垒主机),当外部防火墙失效的时候,它还可以起到保护内部网络的功能。

本系统中外部网与内部网互连需要由对外服务子网分隔,其目的是禁止外部网与内部网的直接互连);对外服务子网是外部网与内部网的隔离区,即 DMZ 非军事区,也称周边网络,此防火墙系统采用的是被屏蔽子网结构的防火墙。

(2)用户接入安全

对于用户接入功能,也提供了非常安全的保证措施。漫游用户首先需要通过 Cisco 7204 的数据过滤,拨号用户需要首先通过 Cisco 3640 上的数据过滤、Radius Server 安全认证,如果访问对外服务子网,要通过 Cisco Pix FireWall 520 上的安全管理及安全检测,如果要访问内部网则还要通过中网防火墙的安全过滤,同时在对外服务子网安装了 NAI 的 Cybercop Monitor 防入侵检测系统,最大限度地保证网络安全。

(3)防病毒软件

采用防病毒软件对服务器、工作站进行保护,防止病毒侵袭。防病毒的安全解决方案实现包括对服务器的保护、网关的保护、桌面的保护。

(4)入侵检测系统

采用入侵检测系统,提供实时的入侵检测及采取相应的防护手段,可记录证据用于跟踪恢复和断开网络连接等。实时入侵检测能力还能够对付来自内部网络的攻击,并能够缩短黑客入侵的时间。该系统可检测网络配置方面的安全漏洞;可检测网络系统日志或系统审计记录,发现用户的异常活动;有对上述的安全漏洞和异常活动进行定义的入侵检测管理系统;具有开放性的系统结构,可为以后增加检测功能提供检测功能开发接口和检测功能调用;具有模块化的跨平台检测能力,能通过增减功能模块达到对 NT、Netware 和各 UNIX 平台的动态支持;可定时运行和由系统管理员执行运行。此外,系统还配置了安全扫描工具 CyberCop Scanner,测试潜在的网络漏洞,评估系统安全配置,以提前主动地控制安全危险。

为了确保系统的安全,硬件设备等也采取不同的措施[6],主要有:

(1)所有设备具有非常可靠的性能。

(2)设备的适当冗余,以满足高峰时间的访问,同时由于网管系统的监视,当出现非正常的访问接入时,可以放弃某些请求,以保证整个系统的正常运行。

(3)主要服务器系统具有硬盘热插拔能力和热备用系统,当某些系统出现故障时,可以不间断服务,更换有问题的硬盘。

(4)主要网络设备和服务器具有热备用系统或备用插槽。

(5)大容量的磁盘阵列,这些磁盘阵列本身具有信息备份和磁盘备份能力。

(6)在综合布线系统中,通信线路留有一定的余量。

(7)机房装修符合国家标准,采用标准的通风、电源和防雷措施,所有重要的服务器和网络系统均有 UPS 电源保护。

另外,网络安全措施还采用了先进的网管系统,网管系统是系统安全性的重要保障手段;采用严格的 IP 地址规划,对内部网的 IP 采用保留地址,使入侵者看不到内部重要的服务器及工作站,限制了入侵者可能攻击的范围;采用认证、授权、审计和计费管理,包括各种接入的认证、各种操作的授权,所有的网络设备和服务器均设有审计措施。对服务器、数据库和网络设备实现审计日志的统一管理,对不同的用户类型进行严格的计费管理和监视管理。

3.3 安全管理措施

当前,人们对网络安全已经有一个共识,即网络安全不只是技术问题,更是管理问题[7]。建立日常安全管理规章制度,任何优秀软件都需要人掌握和使用,因此对所有的信息备份管理、审计信息集中管理、IP 地址的

分配管理、网段的划分等除提供管理软件外，还要针对不同的内部人员(如系统管理员、管理人员、信息管理员、一般内部人员等)建立一系列管理的规章制度，对信息备份、设备的使用范围、帐号的建立、更换和销毁等都要做详细的规定，并制订一系列检查、监督跟踪措施，以保证这些规章制度的执行。在这些制度中，针对系统管理员的制度尤为重要，主要有：帐号管理、权限分配、系统运行的监视；针对信息管理员的制度有：信息的录入、销毁、备份、变换、传送等。

本文详细介绍了一个大型科技信息网络系统的安全体系设计、安全保证以及管理措施。着重介绍了双重防火墙保障技术以及非军事区结构模式，硬件安全以及先进的网管系统，严格的认证、授权机制，并采用防病毒软件和入侵监测系统等一系列安全技术和保障措施，形成了一个较完整的基于 Internet 科技信息系统应用的安全解决方案。该系统运行两年多，有效地满足了用户需求，用户反映良好。

参考文献

[1] ARBAUGH W A. An inductive chosen plaintext attack against WEP/WEP2. IEEE Document 802.11-01/230,2001-05.

[2] CCIMB-99-031. Common Criteria Security Evaluation for Information Technology, V2.1.1999-08.

[3] 谢希仁.计算机网络[M].大连:大连理工大学出版社,2000.

[4] 刘淼,李鹏,陈康民,等.综合网络安全系统的研究与设计[J].计算机工程与设计,2009,30(13).

[5] 张国情,曹重英.一种 Intranet 信息保护系统的设计和实现[J].计算机工程与应用,2003(39):157-158.

[6] 杨卫东.网络系统集成与工程设计[M].北京:科学出版社,2002.

[7] 李晓明.从整合管理开始.中国计算机报,2005(1380):12.

(收稿日期:2010-01-05)

作者简介：

朱亚兴，女，1972 年生，高级工程师，主要研究方向：网络信息系统与数据库。