基于IPv6的中小企业防火墙设计与实现

张 媛
(太原大学 外语师范学院,山西 太原 030012)

【摘 要】目前网络服务日趋多元化,当服务数量已不是问题,我们就更需要服务质量作为保障,如果网络服务出现问题,快速修复机制在企业(特别是中小企业)网络管理中就是重中之重。本研究以某小企业为例,设计并实现如何利用低成本设备构建具有高可靠性的企业防火墙。本防火墙不仅可支持新的IPv6规格,还可以达到高效传输效能下的双备份机制,从而确保企业的信息安全。

【关键词】IPv6;防火墙;双备份;中小企业
【中图分类号】TP393.18 【文献标识码】A 【文章编号】1673-1891(2013)01-0068-02

1 前言

网络的快速发展,带给了使用者很大便利,当大家在享受这方便性的同时,渐渐的也注意到它的安全性,如何能在开放的网路平台上,既要享受便捷服务又能受到好的机制保护,这就是防火墙诞生的原因。在IPv4协议规格下,防火墙在技术或产品研发上已相当成熟。IPv6发展至今,网络的骨干基础建设都支持IPv6协议规格。通过本研究构建的防火墙,不仅支持下一代因特网通讯协议,也可减少网络地址转换时给应用程序带来的问题以及提升网络传输的效率。

2 相关研究

2.1 IPv6互联网协议

现有的互联网是在IPv4协议的基础上运行。IPv6是下一版本的互联网协议,也可以说是下一代互联网的协议,它的提出最初是因为随着互联网的迅速发展,IPv4定义的有限地址空间将被耗尽,地址空间的不足必将妨碍互联网的进一步发展。为了扩大地址空间,拟通过IPv6重新定义地址空间。IPv4采用32位地址长度,只有大约43亿个地址,估计在2005~2010年间将被分配完毕,而IPv6采用128位地址长度,几乎可以不受限制地提供地址。在IPv6的设计过程中除了一劳永逸地解决了地址短缺问题以外,还考虑了在IPv4中解决不好的其它问题,主要有端到端IP连接、服务质量(QoS)、安全性、多播、移动性、即插即用等。

2.2 双备份机制

备份机制一般指数据的异地备份,基于Windows的Acronis软件用来完成主机的高可用性(High Availability, HA),此机制备份方法主要是将主机上安装Acronis必要套件,网卡通过相互监听机制,并根据状态将两台主机上的特定数据同步处理,并每隔特定时间侦测主机是否异常,当监听的主机出现异常时,便将主导权转移至监听主机完成。通过Windows Acronis来完成高可用性具有相当好的效能,但在企业防火墙的需求下,数据同步并不具有迫切性,并且构建布署Acronis程序复杂,构建门坎相当高。本研究所提出的方法大幅简化设定程序,相对于复杂的Acronis,本研究提出的企业架构适用于所有中小企业信息资源管理者。

3 防火墙架构

3.1 架构规划

防火墙由安全策略管理服务器以及客户端防火墙组成。客户端防火墙工作在各个服务器、工作站、个人计算机上,根据安全策略文件的内容,依靠过滤、特洛伊木马过滤和脚本过滤的三层过滤检查,保护计算机在正常使用网络时不会受到恶意的攻击,提高了网络安全性。而安全策略管理服务器则负责安全策略、用户、日志、审计等的管理。该服务器是集中管理控制中心,统一制定和分发安全策略,负责管理系统日志、多主机的统一管理。另外本研究提出的架构还引入双实体备份线路机制。因此,本研究所规划的架构使用四台服务器,以及两台交换器,整体架构如图1所示。

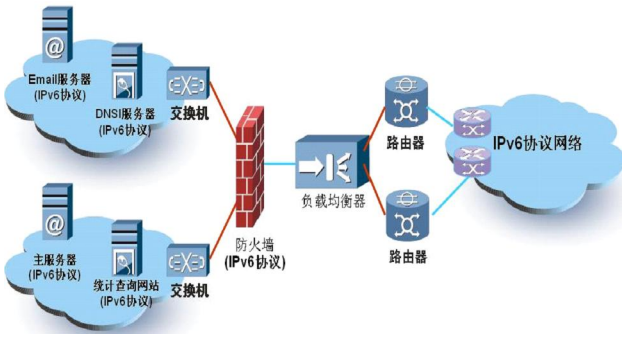

图1 防火墙架构示意图

从图中可以得知Internet接入的数据线分别接

收稿日期:2012-11-21
作者简介:张 媛(1984-),女,山西太原人,助教,研究方向:计算机应用。

至SERVER1、SERVER2以及SERVER3、SERVER4之后,再由每台防火墙分别接至两台交换器上,并且SERVER1与SERVER2以及SERVER3与SERVER4的之间以跳线相连接以便完成备份侦测机制。而后端服务器便通过交换器接取到因特网。

3.2 防火墙的设定方式

本研究中防火墙都以桥接模式将防火墙上的三个网络孔建立桥接。在试验环境中,将SERVER1、SERVER3两台防火墙分为主要防火墙,以及备份防火墙(SERVER2、SERVER4),本研究中清楚区分各防火墙的角色,其检测机制的流程图如图2所示,重要服务都会由担任主要防火墙的服务器进行,日后亦可修改脚本的内容让防火墙可以随机担任主要防火墙的角色。

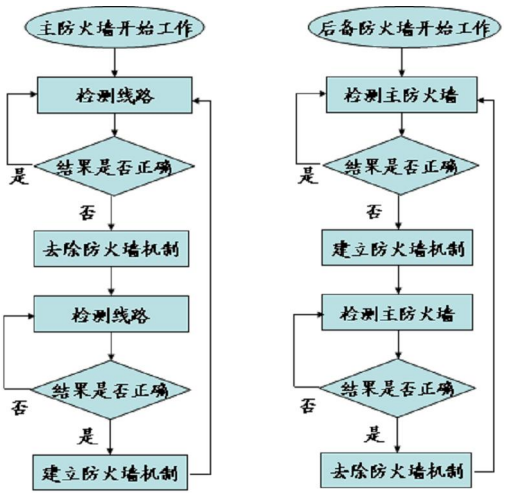

图2　防火墙检测机制流程图

4 效能测试

研究首先测试防火墙构建完成的时间。本研究使用最简便的Ping指令进行测试,通过防火墙内部对网站进行测试,此时便将主要防火墙重新启动,可以通过Ping指令的结果量测备份防火墙重新接替防火墙角色所需的时间。

本测试进行100次以便求得平均构建防火墙所需的时间,当主要防火墙已正常开机完成并且准备加载开机后构建防火墙时,备份防火墙已经可以通过对接的跳线侦测主要防火墙已经开机完成,因此立即停止已处于运作状态中的防火墙机制,以避免与主要防火墙发生同时构建防火墙的情况发生。可得知主要防火墙发生障碍时,备份防火墙仅需18秒将网路联机恢复正常。

第二部分对网络频宽进行效能量测,使用NetStress通过防火墙外的主机对防火墙内的主机进行大量的数据包传送,以测试防火墙最大传输量。测试的过程中将防火墙内部的主机启动Server模式,而防火墙外的主机将以多线程的方式传送大量数据包,一分钟内服务器端总共接收了2.86GB数据量,可得知本研究提出的防火墙机制在传输速率上具有良好的效能。

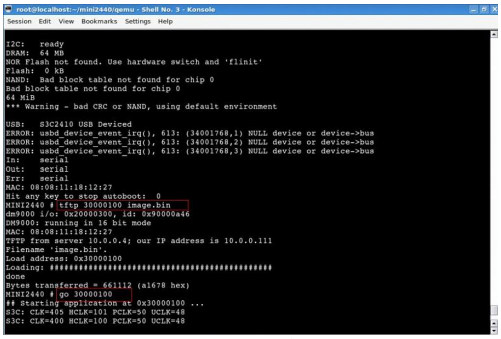

图3　联机状态测试

5 结论

本研究提出的中小企业防火墙具有双备份机制及负载高频宽的特点,由服务器搭配网卡的结构较大幅度的降低了构建成本。防火墙的构建方式也因为组装过程精简,不需耗费过多人力就可完成。实验表明,本研究所提出的支持IPv6、低成本、高可靠性企业防火墙可被广泛应用于各中小企业中。

注释及参考文献:

[1]戴蓉,黄成.防火墙的分类和作用[J].电脑编程技巧与维护,2011(4):43-47.
[2]何洪磊.IPv6防火墙研究[J].计算机安全,2009(7):69-78.
[3]刘忠,王俊卿.分析IPv6技术对网络安全的影响[J].微计算机信息,2009(9):31-41.
[4]张玉芳,熊忠阳,赖苏,等.IPv6下基于病毒过滤防火墙的设计与实现[J].计算机科学,2009(4):123-136.

Design and Implementation of Firewall based on IPv6 for Medium-sized and Small Enterprise Networks

ZHANG Yuan
(Foreign Language Normal College, Taiyuan University, Taiyuan, Shanxi 030012)

(下转73页)

逻辑结构、MVC模式结构,以及从业务角色、业务用例、数据库的设计等方面作了介绍。本系统的开发遵循J2EE规范,用由Web服务器、应用服务器和后台数据库形成的S/A/D三层结构,完全的Web应用方式,客户端需适应IE5.0以上版本或Netscape6.0以上版本的浏览器,全部客户端只需通过浏览器进行操作,不需安装任何其他软件;服务器层需适应主流的Web服务器、应用服务器及主流中间件,数据库层需用主流数据库技术。本网络服务系统能适应不同学科的实训室管理实训建设和管理,能对不同学科的教师学生提供服务,同时也可对外提供服务,提高了系统的性能、可用性和可扩展性。

注释及参考文献:

[1]赵强,乔新亮.J2EE应用开发[M].北京:电子工业出版社,2009:72-84.

[2]刘亚宾,杨红.精通Eclipse[M].北京:电子工业出版社,2004(5):330-331.

[3]王波,朱亚平,王经.基于Internet的自适应测试系统的设计和开发[J].计算机学报,2010,(5):34-36.

[4]RobertV Binder著,华庆一等译.面向对象系统的测试[M].北京:人民邮电出版社,2008,99-106.

[5]王国强,谢立.基于Web的仪器设备信息管理系统的开发应用[J].计算机研究与发展,2008(9):64-67.

The Research and Implementation of Practical Training Management System Based on the .NET Platform

LI Ying[1], RU Zheng-hua[2]

(1.Guangzhou railway vocational technical institute, Guangzhou, Guangdong 510430;
2.Railway construction investment group co., ltd. Guangdong; Guangzhou, Guangdong 510230)

Abstract: Nowadays, education is developing rapidly over China, and the current network teaching system can not meet the needs of development. In this paper, the design is discussed according to the needs of practical training, to implement a practical training network teaching service system, to implement reservation and billing when the practical training facilities are wanted, to implement the management to the practical training instrument under the premise of guaranteeing the accuracy and instantaneity of reservation, collecting, and billing, and to implement the resources sharing of the practical training instrument, the opening service of practical training teaching platform and improving the practical training teaching level.

Key words: Practical training; Facilities; Teaching; Platform

(上接69页)

Abstract: At present the network services have become more diversified. As the quatity of service is not a problem, we should be more concerned about the quality of service. If there is something wrong with the network service, rapid repair mechanism in an enterprise network management is very important. How to build enterprise firewall with high reliability using low cost is designed and implemented in this research. The design can not only support IPv6, but also can reach the dual backup mechanism with efficient transmission to ensure the security of corporate information.

Key words: IPv6; Firewall; Backup mechanism; Medium-sized and small enterprise