广西科学院学报
Journal of Guangxi Academy of Sciences
2006,22(4):287～288,297
Vol. 22,No. 4 November 2006

三层结构的证券公司计算机局域网络设计与实现
Establishment of a Three-layer LAN of a Stockjobber

崔保胜
CUI Bao-sheng

(宏源证券股份有限公司,广西桂林 541002)
(Hongyuan Securities Company,Guilin,Guangxi,541002,China)

摘要:在宏源证券股份有限公司桂林上海路证券营业部设计与实现了三层结构的证券计算机局域网络。该网络是在传统二层结构的证券局域网的数据管理层和用户界面层之间增加一个中间层,将局域网络划分为服务器端、中间件和客户端。这种三层结构的证券局域网络能够有效地防范黑客攻击,能够大大提高证券交易的工作效率,能够提高整个网络的安全性。

关键词:局域网 三层结构 交换机 拓扑结构 以太网
中图法分类号:TP303 **文献标识码**:A **文章编号**:1002-7378(2006)04-0287-02

Abstract: A three-layer LAN is developed by setting up a layer between the layer of data management and the layer of user interface in a normal two-layer LAN of stock market. This three-layer LAN consists of server, inter-part and client terminal. In this structure, the attacks from hackers would be blocked up more effectively, and the efficiency of transaction of stocks can be improved.

Key words: local area network (LAN), three-layer structure, switcher, topological structure, ethernet

证券行业是对计算机要求很高的行业,一般说来,每个证券营业部都有自己的计算机局域网。证券交易和证券行情业务数据都是以文字为主,仅带有少量图形信息,但数据量大,更新频繁,网络要求具有很高的可靠性、数据传输率和安全性。因此,证券公司营业部的计算机网络必须保证随时畅通无阻,确保客户交易的准确无误。计算机网络的任何拥挤和堵塞都会对客户产生巨大的经济损失和社会问题。作者经过多年的开发与研究,在宏源证券股份有限公司桂林上海路证券营业部设计了三层结构的证券计算机局域网络,对于提高证券行情和证券交易的效率,以及防范黑客攻击,提高整个网络的安全性起到了较好的效果。

1 三层结构证券局域网的产生背景

通常,传统的证券局域网一般是以交换机作为主干的二层星形网络结构。网络环境大多采用 100/1000M 交换以太网做主干,10/100M 交换以太网到桌面的连接方式。网络一般采用 C/S(Client/Server)模式,资金和交易数据主要保存在后台的 NT Server 上。无盘工作站可以直接访问前台的 Novell Server,但不能直接访问后台的 NT Server,而后台的 PC 工作站则可以在许可的权限范围内直接访问 NT Server。这种网络结构具有高效、易扩展等特点,但是,由于前台系统和后台系统存在物理上的连接,因而不能完全杜绝用户操作无盘工作站利用某种非法手段进入后台系统作案的可能性。而且这种作案一般不会留下可供追查的线索,使证券公司蒙受巨大的经济损失,同时也给犯罪分子以可乘之机。

随着近年来网络技术的飞速发展和 Internet 的普及,证券公司所面临的被恶意或非恶意入侵机会越来越多,特别是新技术和新思路的不断涌现,对证券网络的正常运行和日常维护提出了严峻的挑战,对信息系统的安全性、可靠性的要求越来越高。三层 C/S 结构的证券局域网络就是针对这些情况而提出来的。

2 三层结构证券局域网的结构

本证券局域网络是在传统二层结构的证券局域

收稿日期:2006-06-13
作者简介:崔保胜(1967-),男,工程师,主要从事电脑管理工作。

网的数据管理层和用户界面层之间增加 1 个中间层，将整个计算机网络的体系结构划分为服务器端、中间件（构成中间层的构件）和客户端。中间件将网络分隔为完全分离的内部网和外部网，使前端用户无法看到后台数据库服务器和文件服务器，有效地防止了黑客的攻击。中间件在系统处理能力上采用多线程技术，大大提高了工作效率，可靠性和扩展性也较二层结构强。三层结构证券局域网络符合中国证监会关于证券经营机构信息系统管理，数据与网络分离、技术与业务分离、前台与后台分离的“三分离”原则。该计算机网络属于硬三层结构的证券计算机局域网络，其网络拓扑见图 1。

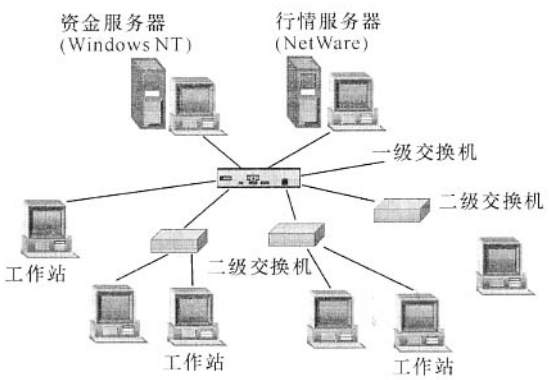

图 1 三层结构证券局域网拓扑

3 三层结构证券局域网的特性及应用效果

3.1 特性

三层结构证券局域网中外网主干交换机采用的是 Cisco Catalyst 4006，内网交换机为 Cisco3548。连接到桌面的网络设备采用 Cisco1924。中间件运行平台为 Windows NT4.0，中间件上安装两块网卡，分别连接内网和外网，在 NT 中安装 IPX/SPX 协议（不安装 TCP/IP 协议，这样可以有效防止 TCP/IP 数据包攻击）关闭这两块网卡的内部路由功能，这样外网的用户便无法利用中间件的软件路由功能直接访问内网数据，而客户的委托成交数据则利用中间件程序转发。为进一步增加安全性，还可将这两块网卡绑定不同的协议，如连接外网的网卡只绑定 IPX/SPX 协议，连接内网的网卡只绑定 TCP/IP 协议，由于两块网卡连接的协议不同，增加了系统的安全性。

在证券网络三层结构中，交易网络可以分为交易内网、交易外网和中间件系统。交易内网存放委托交易、客户资料等重要数据。交易外网提供股市行情数据，客户工作站均接在交易外网上，通过中间件访问内网数据。将原先存放在 Novell 服务器上的委托交易库和行情库分离，在外网的 Novell 服务器上提供行情数据和无盘站登录；在内网的 Novell 服务器上存放委托和交易数据；将原先的资金服务器（NT）也移至内网。内网数据是营业部的核心重要数据，所有需访问内网的数据包均需经过中间件检查，以此实现网络系统的安全性。中间件系统是内、外网之间的通信桥梁和过滤器，中间件系统由两台或两台以上运行中间件软件的服务器组成，主要是连接“客户”和“服务器”，并完成全部柜台及外围系统的交易及查询事务，包括多线程调度管理、客户请求队列及通讯管理，多数据库服务器连接及事务处理和结构集管理，事务描述分析处理，异地交易和转帐业务处理。所以，本系统是最安全、最可靠的三层网络结构，其主要特点表现为：(1)完全附合证监会提出的业务与技术分离、前台与后台分离、网络与数据分离三分离原则。(2)把整个局域网分为内、外网两个部分，内、外网的数据通信只通过中间件来实现。(3)三层结构可安全地防黑客的侵袭，因黑客无法看到实际的数据库服务器，中间件通讯采用加密算法，每个中间件有不同的密钥，黑客攻击无经验借鉴。

3.2 应用效果测试

用著名的 Sniffer 软件对本证券局域网络进行的检测结果见表 1、表 2 和表 3。从表 1 可以看出，主干交换机 4006 利用率为 25%，网络中错包和冲突包、CRC 错包数都是 0，网络工作状态良好。表 2 结果显示，数据流出现广播风暴。由于证券网中的乾隆等行情揭示系统往往采用广播方式传送行情，所以出现广播风暴是正常的。

表 1 网络运行状态记录

Network	Size Distribution	DetailErrors
Packets 472,573	64s 19,301	CRCs 0
Drops 0	65-127s 20,221	Runts 0
Broadcasts 21,275	128-255s 18,763	Oversizes 0
Multicasts 4,015	256-511s 12,418	Fragments 0
Bytes 618,700,250	512-1023s 3,177	Jabbers 0
Utilization 25	1024-1518s 398,693	Aligrments 0
Errors 0		Collisions 0

表 2 数据流量分析

Broadcase/Multicast Storm	
Threshold	40
Peak Broadcast Rate	143
Broadcast Frames	5,996
Locol Frames	11,874
Remote Frames	0
First Time	2001/7/3 10:00:24 266
Storm Duration	2m 23s 128ms
Stationl name	0036BE51000
Stationl name	002FDCC4029
Stationl name	0004271D3040

（下转第 297 页）

4 结束语

本文介绍的 NDIS 中间层驱动技术已经在内网安全监管系统的开发中得到应用。应用该技术开发的系统能应用于 Windows2000/XP/2003 系统中,且基本上能应用于各种以太网局域网中,能对 IP 数据包进行拦截和分析,得到其日志信息。以后还可以根据需要进行功能扩展,使其能对其它类型数据包进行拦截和分析。

参考文献:

[1] CHRIS CANT. Windows WDM 驱动程序开发指南[M]. 北京:机械出版社,2000.

[2] 谭思亮. 监听与隐藏—网络侦听揭密与数据保护技术[M]. 北京:人民邮电出版社,2002.

[3] 汪晓平,刘韬. 开发网络经典示例导航[M]. 北京:人民邮电出版社,2005.

(责任编辑:邓大玉 凌汉恩)

(上接第 288 页)

从表 3 可以看出,网络延时值较小,网络延时不到 1ms,说明网络延时很小,网络工作状态良好。表 4 结果显示,网络的日常运行正常,能够用于实际。

表 3 网络延时记录

Source Adderss	Dest Address	Summary	Len	Rel time	Delta Time
1E111.1	113.00400-565890	NCP:ROK	566	0:00:06 383	0.000.423
113.000021 D3E63	1E111.1	NCP: C Get current size of file F=DC4F0300	60	0:00:06 383	0.000.068
1E111.1	113.0050 BA72CD1	NCP:ROK	566	0:00:06 384	0.000.425

表 4 服务器运行状态记录结果

测试项目	结果
CPU 利用率	一般 10%~30%
CPU 利用率分布情况	IPX RTRNCP Work to do 0~15% Internupt 5%~15%
内存占用和空闲情况	
Current Srevice processes	<50
Dirty cache buffers	<500
Current disk requests	<51
Long term cache hits	100%
Long term cache dirty hits	100%
LRU sitting time	>1h
Cache buffers	>2000
工作站上网情况	
钱龙上网速度	正常
钱龙 81 速度	<2s
成交回报速度	<5s
与服务器、交换机相连端口错包率、冲突率	无

4 结束语

综上所述,证券公司计算机局域网络的三层结构对提高证券行情、交易的效率以及防范黑客攻击是非常好的。但是,中间件运行的操作系统 Windows NT Server 本身存在不少安全漏洞,加之针对 NT 的黑客工具较多,并不能百分之百地保证网络系统无坚不摧。所以,如何提高中间件自身乃至整个网络的安全性,仍然是我们证券行业计算机技术人员今后研究的重要课题。

参考文献:

[1] 常晓波,杨剑峰. 安全体系结构的设计部署与操作[M]. 北京:清华大学出版社,2003.

[2] 戴英侠,连一峰,王航. 系统安全与入侵检测[M]. 北京:清华大学出版社,2002.

[3] VITO AMATO. 思科网络技术学院教程:上册[M]. 北京:人民邮电出版社,2000.

[4] 方程. 操作系统—— Windows2000[M]. 北京:高等教育出版社,2003.

(责任编辑:邓大玉)