学校编码：10384　　分类号_____密级_____
学号：X2011231058　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

税务信息系统中防火墙与入侵检测联动的设计与实现

Design and Implementation of Firewall and Intrusion Linkage for Tax Information System

金鑫

指 导 教 师： 龙 飞 副 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2013 年 10 月

论文答辩日期： 2013 年 11 月

学位授予日期： 2013 年 月

指 导 教 师：_____

答辩委员会主席：_____

2013 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

税收是国家财政收入的主要来源，是我国经济的重要组成部分，取之于民，用之于民，但传统的税收手段已不能满足社会发展的要求，税收信息化成为了社会发展和进步的必然选择，建设税务专网也成为各省地税系统的重要工作。

我省税务专网自建设之日起，一直是信息化工作的核心部份，其中安全建设更是成为其中的关键部份，经过几年来在网络与信息安全防护体系方面的建设，我省税务信息系统整体安全防护能力得到很大加强，但随着网络系统规模的扩大、各种应用系统不断完善和科学技术的快速发展，又对税务信息系统的安全提出了新的要求。

本论文以防火墙和入侵检测系统的联动为研究方向，分析了现有防火墙和入侵检测系统存在的问题，以及如何通过防火墙和入侵检测系统的联动来有效提高网络的安全性，最后进行实际测试以证明该系统能为专网带来的实际效果。

论文从项目背景出发，首先介绍了互联网的安全现状，然后详细介绍了防火墙、入侵检测及联动的相关内容，并设计了税务专网的安全防护结构，再次，以具体的环境进行了测试，对结果进行分析，最后针对防火墙和入侵检测的联动系统进行了分析和评价，并指明了下一步的改进计划。

关键词：防火墙；入侵检测；联动

Abstract

Tax is both a major source of sate revenue and an important part of our economy. It is taken from people and given back to people. Because the traditional tax measures can't meet the need of social development any more, the tax informatization becomes the inevitable selection of social development and improvement, and it also becomes the important work of provincial land tax system to construct tax private network.

Since the date of construction of our tax private network, it has become the core part of tax informatization, of which security building has been a key part. According to years of construction of network and information security protection system, the tax information system security capabilities have been extremely strengthened. With the expansion of the network system and the improvement of various application systems and the rapid development of science and technology, new demands have been put forward to the tax information system security.

In this Dissertation with the linkage of the firewall and intrusion detection system as the research direction, it analyses the existing problems of firewall and intrusion detection system, and how to improve the security of network through the linkage of the firewall and intrusion detection system, and the actual test at the end to prove that the system for private network actual effects.

This Dissertation embarks from the project background, firstly introduced the safety status of the internet, and then introduced the firewall, intrusion detection and the linkage of the related content, and designs the tax private network security protection structure. It was tested in a specific environment once again, after that the results were analyzed. Finally, the linkage of the firewall and intrusion detection system have been analyzed and evaluated. Meanwhile, the improvement plan of the next step was pointed out.

Key words: Firewall; Intrusion Detection; Linkage

目 录

Contents

第一章 绪 论

1.1 研究背景及选题意义

税收是国家为满足社会公共需要，凭借公共权力，按照法律所规定的标准和程序，参与国民收入*分配*，强制地、无偿地取得财政收入的一种方式。税收是国家财政收入最主要的来源，也是我国政府进行宏观调控的重要经济杠杆，它对于保证国家财政收入，加强宏观调控，深化改革，扩大开放，促进国民经济和社会的持续、健康、快速、稳定发展，起到了重要的作用。马克思指出：“赋税是政府机器的经济基础，而不是其他任何东西。”“国家存在的经济体现就是捐税。”恩格斯指出：“为了维持这种公共权力，就需要公民缴纳费用——捐税。”19 世纪美国大法官霍尔姆斯说：“税收是我们为文明社会付出的代价。”[1]这些都说明了税收对于国家经济生活和社会文明的重要作用。

当前，信息技术已经深入全球各个角落，各行各业都有信息化的参与，它已经对我们的社会、经济、文化和生活产生了巨大的影响，也成为我省的经济发展、产业优化升级的重要推动力量。

税务部门作为税收的主要管理和执行部门，在信息化高速发展的今天，必须时刻关注全球经济的发展和变化情况，不断更新思想观念和管理方式，才能在快速发展的现代化税收体系建设中把握新的机遇和应对新的挑战。充分利用现代化信息技术对我省的税收工作进行全新改造，实现税收信息化，已经成为我省税收工作的中心工作之一，只有实现现代化和信息化，才能更好的实现税务部门对税收的管理和执行作用， 当前，整个税务系统已搭成共识：税收信息化是税收工作的必由之路，是税收工作发展的新方向，更是一场税务体制的革命，已经开始的金税三期工程正是对十八大精神、落实新的工作思路、转变当前政府职能的真正实现。

税收管理信息系统是电子政务工程的重要组成部分，是具有重要战略地位的国家级信息系统，2002 年，中共中央和国务院联合下发了〔2002〕17 号文件《国家信息化领导小组关于我国电子政务指导意见》，要求大力推进金税工程（三期）建设，并作为电子政务工程重点建设的“十二金”工程之一。金税工程建设也已

写入《征管法》中。最终建立税收信息化综合管理系统，并与其它部门的信息系统实现数据共享和综合协作，是今后税务工作的重点内容。

我省地税信息化建设起步于 94 年地税分设以后，随着税收征管工作的深化和规范化管理要求的提出，各级地税在税收工作中，不断深化了信息化建设对组织收入和加强征管的重要性的认识，在工作中积极筹集资金，组织人力，加大信息化建设力度。

目前，税收信息化建设正处于向建立全方位税收服务系统迈进的时期。随着电子政务建设的逐步发展，我省的税收信息化建设进一步加强，对现有的税收征管与税收制度产生了现实影响，成为税收管理各项工作的重要依托。

随着我省税收征管改革的不断深化、国家税务总局“一个平台、两级处理、三个覆盖、四个系统”的“金税三期”建设要求的提出，为地税信息化工作提出了更新、更高的要求。我省地税目前信息化情况与总局要求、征管工作要求，以及与其他省市税务系统信息化建设相比较，还有很大差距，这种差距的存在严重制约了我省地税信息化的发展，在新的形势下，我省地税必须加大信息化建设力度和资金投入，精心组织，求真务实，以十八大为契机，以信息化为突破口，不断提升我省地税信息化建设水平和建设成效，为我省地税税收业务工作提供有力的技术保障。

我省税务专网自建设之日起，一直是信息化工作的核心部份，其中安全建设更是成为其中的关键部份，经过几年来在网络与信息安全防护体系方面的建设，我省税务信息系统整体安全防护能力得到很大加强，但随着网络系统规模的扩大、各种应用系统不断完善和科学技术的快速发展，又对税务信息系统的安全提出了新的要求。

面对来自外部与内部的各种安全威胁，我省地税系统信息化安全建设必须要按照纵深防御的思想，按照工作的实际要求和实际情况，逐步构建成完整的信息安全体系。

经过税务系统几年来在网络与信息安全防护体系方面的建设，税务信息系统整体安全防护能力得到很大加强，但仍需要针对信息安全保障工作中存在的薄弱环节，加强安全防范工作，其中之一就是加强安全设备间的联合防御能力，税务系统安全防护建设的边界防护主要通过防火墙和入侵检测系统，通过部署防火墙

加强基本边界保护能力;通过部署入侵检测系统加强对网络安全环境的基本监测能力，但单独的使用某一安全设备，由于设备自身的局限性，其弱点将会给入侵者带来可乘之机，如果能实现不同安全设备之间的联动，将不同的安全设备进行联动使用，使它们之间相互进行补充和完善，将会取得 1+1>2 的良好效果。

本论文以防火墙和入侵检测系统的联动为研究方向，重点研究联动功能在地税专网中能起到什么样的作用，对于提高专网的安全性有什么样的帮助，以及如何实现两者的联动功能并进行实际测试，由于此类设备已经在税务系统中广为使用，如果能够充分发挥联动功能，将会大大增强网络的防护能力，进一步提高税务专网的安全建设水平。

1.2 存在的问题

2012 年，我国互联网快速扩面和发展，带宽得到有效提升，电子商务、云计算、新兴的网络媒体、移动办公业务等新技术新业务发展迅速，根据工信部 2012 年通信网络安全防护检查的情况，基础电信企业对网络安全防护工作的重视程度进一步提高，网络安全风险意识和防护水平显著提升，在政府部门、网络服务运营商、网络安全企业和人民群众的共同努力下，网络运行状况保持正常，网络用户的上网安全意识得到全面增强，从全国一年的网络运行情况来看，尚未发生严重的网络安全故障。

但从整体上看，网络安全事件仍然日趋频繁，网站挂马、网络钓鱼、手机终端恶意程序、DDOS 攻击事件呈现大量扩展的趋势，直接危害到广大网络用户和公司的权益,妨碍了互联网的正常发展;而新出现的针对特别选定用户的有组织、团体作战的 APT 攻击（简称：高级连续性攻击）日渐增多，整个国家的网络信息安全都将受到挑战。

从 2012 年的网络情况来看，我国互联网在安全方面面临的主要威胁有:

1、网站被黑客以技术段插入恶意代码等攻击事件呈增长态势，用户个人信息成为这些恶意代码偷取的重点内容，2012 年我国被恶意修改的网站数量为一万六千多个，其中政府网站有一万八千多个；被插入恶意代码的网站有五万二千多个，其中政府网站有三千多个[2]，情况如图 1-1 所示：

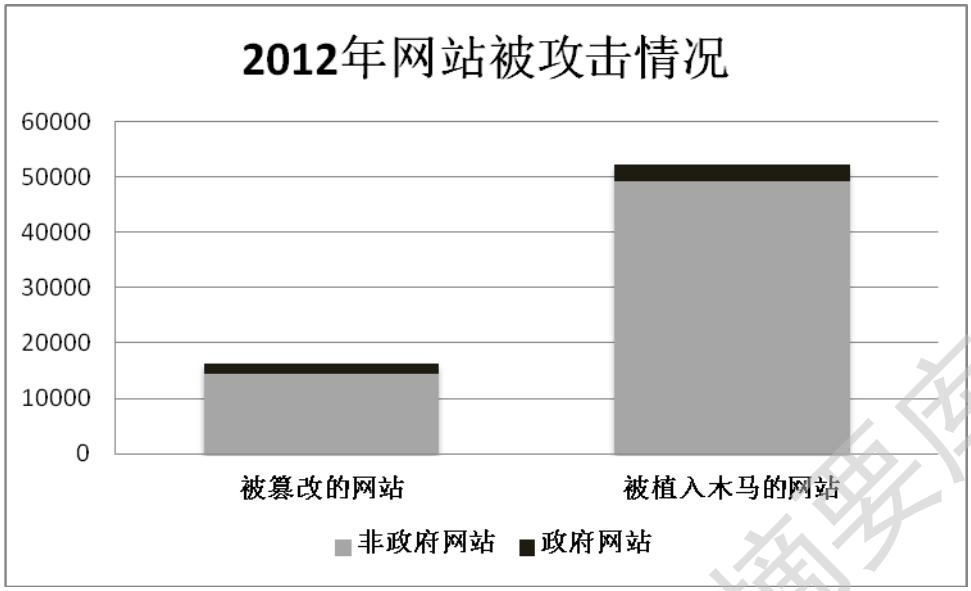

图 1-1 2012 年我国境内网站被攻击情况

2、日渐猖獗的钓鱼网站，已威胁到在线交易和电子商务的发展，威胁到社会安全，2012 年，国家互联网应急中心共统计监测到针对全国范围内的网站钓鱼页面二万二千多个，从钓鱼站点使用的域名来看，以商业应用的.com 最多，占 36.5%，排名第二位的是.tk 和.cc，仅国家互联网应急中心监测发现被黑客使用钓鱼手段得到的、很可能会给用户带来经济损失的用户银行交易相关数据就达 1.8 万条[2]。

2012 年钓鱼站点域名按顶级域分布如图 1-2 所示：

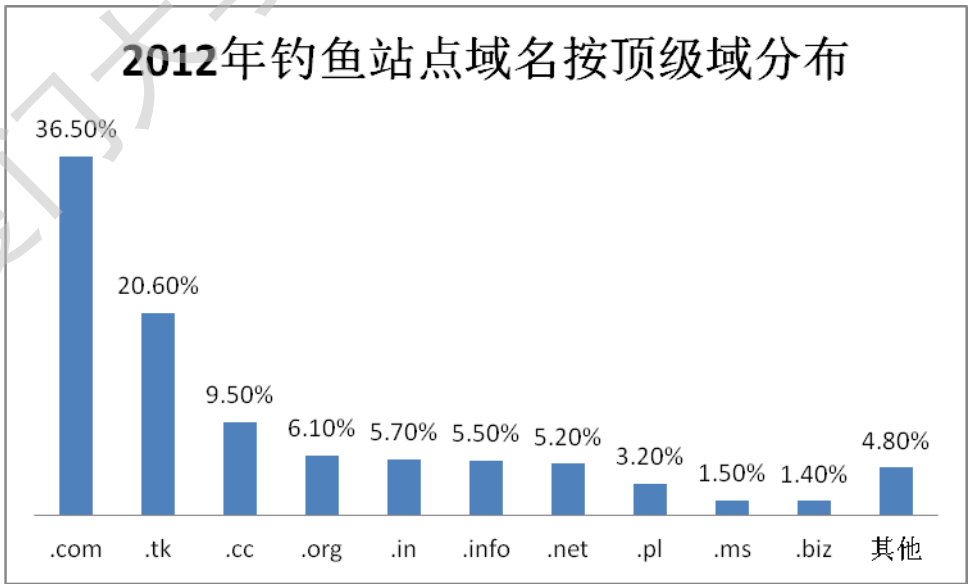

图 1-2 2012 年钓鱼站点域名按顶级域分布情况

3、移动互联网恶意程序数量和种类快速增长，移动上网设备成为重灾区，仅 2012 年一年，国家互联网应急中心监测和网络安全企业通报的移动设备使用网络进行传播和扩散的恶意程序就有十六万两千多个，比 2011 年增长 20 多倍。

4、拒绝服务式攻击对网络的危害依然在各种危害中排名第一，据国家互联网应急中心监测统计发现，2012 年我国每天平均发生的规模较大的拒绝服务式攻击就有一千多起，比 2011 年高出了三倍，在监测发现的拒绝服务式攻击事件中，约有近 90%的被攻击目标位于我国境内，从之前常用的攻击网站本身逐渐转为攻击这些网站域名所在的 DNS 服务器，而且黑客所采用的攻击手段日趋综合化和多样化，他们攻击 DNS 服务器可以使得这些服务器在短时间内由于访问量剧增而瘫痪，这样性质的攻击甚至可以对国内的网络整体运行造成严重干扰[2]。

2012 年国家互联网应急中心监测发现的拒绝服务式攻击事件类型分布如图 1-3 所示：

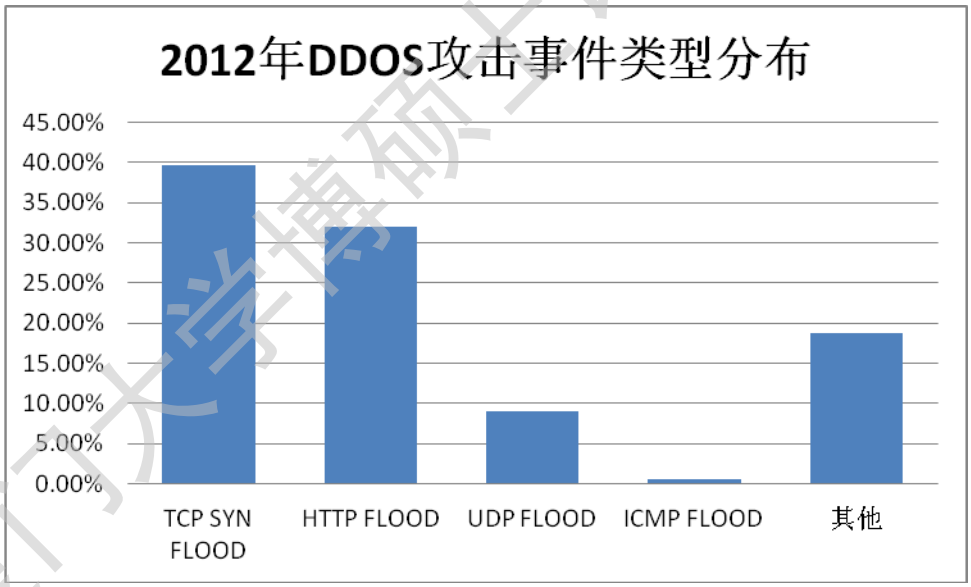

图 1-3 2012 年分布式拒绝服务式攻击事件类型分布情况

5、APT 攻击的恶意程序频频被披露，根据国家互联网应急中心的数据，2012 年我国境内至少有 4.1 万台主机[1]感染了具有 APT 特征的木马，这些木马的分布范围广，波及多个高新技术企事业单位、重要信息系统部门以及政府机构，由于上述受到 APT 木马感染的部门及企业网络中的信息以及自身系统的正常运行往往事关到民生、社会经济甚至国家安全等重大项目的正常运行，所以往往成为一

些带有特定目的组织或团体重点入侵的目标。

6、新漏洞迭出旧漏洞未补，根据国家信息安全漏洞共享平台在 2012 年共收集整理并公开发布的信息安全漏洞有 6800 多个，比 2011 年增长 23%，每月新增漏洞数量平均超过 500 个[2]，在大量新增的漏洞让网络维护人员应接不暇的同时，对一些在线运行系统的修复工作需要非常小心，一些补丁反而会造成系统的运行不正常，甚至会造成业务中断，从而带来更大影响，这些因素都导致网络维护人员对运行系统中存在问题修复的进程缓慢、周期较长。

7、国内网络受到境外攻击威胁的现象仍然严重，据国家互联网应急中心在 2012 年的抽样监测发现，我国境内 1400 多万台主机被境外约有 7 万多个木马或僵尸网络服务器进行了控制，比 2011 年大幅增长 56%和 59%，黑客远程操控这些被入侵的主机，首先可以从用户计算机上的窃取有用的信息，其次这些受控主机可能成为向他人发动新的攻击的跳板，同时达到足够数量的受控主机还可以组成僵尸网络，在黑客发动大规模攻击时成为他们的工具和平台。

2012 年控制我国境内计算机的国外木马或僵尸程序控制服务器 IP 按国家和地区分布情况如图 1-4 所示：

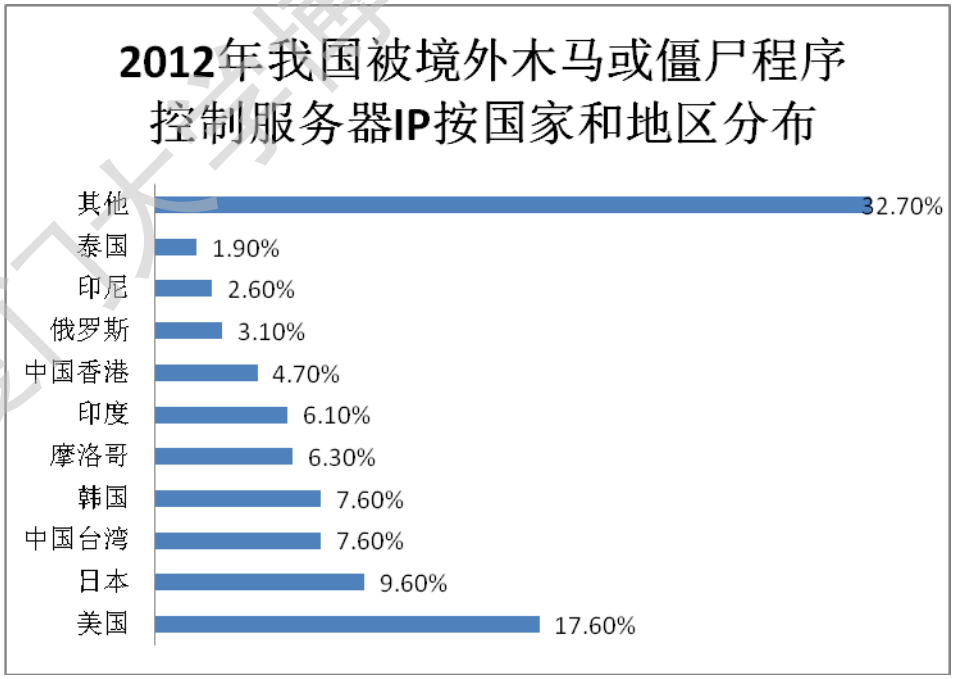

图 1-4　2012 年我国境内木马或僵尸程序控制服务器 IP 主要来源分布情况

2012 年控制我国境内计算机的国外木马或僵尸程序控制服务器 IP 按国家和地区分布情况如图 1-5 所示：

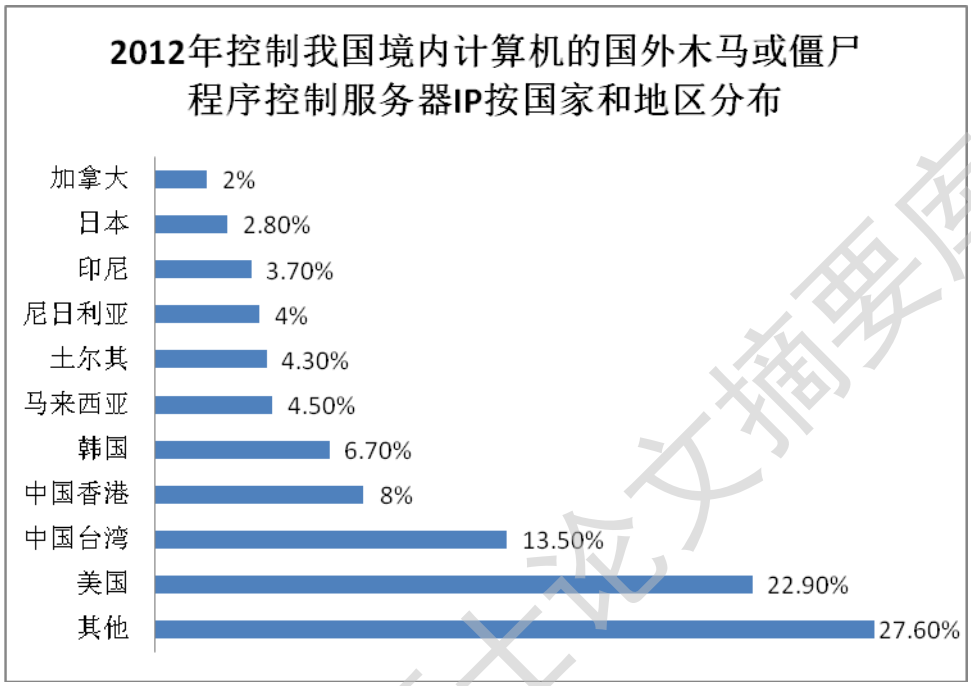

图 1-5　2012 年控制我国境内计算机的国外木马或僵尸程序控制服务器 IP 按国家和地区分布情况

随着网络信息技术的不断提高以及各种税收业务的不断扩展和改进，地税系统的系统防护任务已经得到了高度的重视和落实，但网络中的各种黑客行为仍然层出不穷，攻击技术使用门槛的降低，各种攻击工具的泛滥，黑客年龄的年轻化，攻击目的的复杂化，这些都对地税网络的安全提出了更高的要求，在考虑系统安全性的同时还需要考虑数据的保密性和系统的可扩展性，从目前的情况来看，我们首先要解决的网络安全问题有[3]：

一、　病毒：计算机程序中的一组特殊的指令或者程序代码，其具有传播性、隐蔽性、感染性和潜伏性，当病毒运行时能够破坏用户数据和计算机系统。

二、　木马：是黑客常用来盗取个人信息，或者远程控制对方的计算机而特别制作的一种特殊程序，该程序更具有隐蔽性，一般难以发觉的，运行时很难阻止它的行动。

三、　缓冲区溢出攻击：是一种向系统的数据缓冲区中写入长度超出了原始缓冲区定义大小的攻击手法，此类攻击可以让黑客利用它执行非授权指令，甚