学校编码：10384　　分类号_____密级__

学号：X2010230616　　UDC _____

厦门大学

工　程　硕　士　学　位　论　文

南昌地税网络安全边界防护设计与部署

Design and Implementation of Network Security Boundary Protection on Nanchang Local Taxation

吴庆毅

指导教师姓名：段　鸿　副教授

专　业　名　称：软件工程

论文提交日期：2012 年 10 月

论文答辩时间：2012 年 11 月

学位授予日期：　　年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2012 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

随着税务业务信息化的不断加深，对信息化安全的要求也日益提高，税务信息化网络建设要向国家信息系统安全保护建设要求看齐，建设可靠、安全的信息网络。本文依照税务系统安全等级保护的相关要求从应用的角度对市级税务网络安全的持续改进和优化进行分析。

本文由市级税务网络结构简单、内部业务流不够明晰、安全设备自身安全性较低、接入客户端安全状况不可控、业务分支扩展和网络质量的矛盾等问题入手分析市级税务网络的安全风险和安全需求。根据市级税务网络内所有业务都属于同一个安全级别的前提对市级税务网络区域进行分域保护，根据业务和管理的需要的数据流向和类型划分若干网络区域，并确定各区域间安全策略。并从网络安全的边界防护、区域间安全、区域内安全等几个方面，对防火墙系统、入侵检测系统、漏洞扫描系统、病毒防护系统等的防护目标、策略、要求、性能指标等做了说明。最后根据分析做出市级税务网络分域防护拓扑图，对区域边界进行整合，简化策略，便于管理实施。使市级税务网络的边界管理、数据流向、监控审计、等级保护要求等进一步得到明确和提升。

本文的意义在于针对市级税务网络提出了贴近等保要求又具有整体性、可实施性的方案。力图从自身需求入手落实等保要求，避免了基层等级保护完全依赖厂商、安全服务商，成为一个严格对照条文的 Checklist，造成项目的不可控或彻底失败。

关键词：税务；网络安全；区域划分；边界防护

Abstract

With the deepening of the tax practice of information technology, information technology security requirements are increasing. In order to build a reliable and secure information network, the information network construction of local taxation should conform to security requirements of the national information systems security standards. This article is focusing on the continuous in accordance with the relevant requirements of the tax system, the level of security protection from the point of view of the application of municipal tax of continuous improvement and optimization of the network security analysis.

Considering the facts that the municipal tax network structure is simple, not articulate enough internal business flow, safety equipment is less secure, access client security situation is not controllable, the business branch expansion and network quality contradictions and other issues, this dissertation starts the analysis with the municipal tax network security risk and safety needs. Sub-regional protection is based on the Nanchang tax network business belonging to the same level of security area. Security regional areas and policy is divided based on the needs of the business and management of data flows.Secondly, the dissertation describes the system protection goals, strategies, requirements, performance indicators in system firewall, intrusion detection systems, vulnerability scanning systems, virus protection system from aspects of network security, border protection, inter-regional security and regional security.Finally, a topology map of the network protection was drawn according to the analysis. The map consists of the integration of regional boundaries, simplifying the strategy, and it makes the management of the implementation is easy and convenient. The boundary of the tax network management, data flows, monitoring, audit, grade protection requirements get a further clear-cut standard and upgrade.

The significance of this paper is to provide a feasible plan of the tax network construction conforming to the government protection requirements. Trying to start from the actual needs of the implementation of the level of protection requirements, this paper avoids totally depend on manufacturers and security service providers, and

avoids the possibility of becoming a strict control provisions checklist which will surely lead to an uncontrollable project.

Keywords: Tax; Network Security; Security Domain; Boundary Protection

目 录

Contents

第一章 绪论

1.1 研究背景

随着信息技术及税务信息化的高速发展，各种应用和系统脆弱性成指数增长，针对漏洞攻击的目的性越来越强、攻击时间越来越短，单点防护技术已显得过于简单和被动。传统的网络和安全建设相分离的防护方式，在具有部署简单的优点的同时，也存在防护被动、性能衰减大、管理割裂等缺点。无论是从技术上和还是管理上，都无法确保信息在目前新的安全形势下的保密性、完整性和可用性。

为加强信息安全工作，国内外进行了大量研究，欧美等国相继出台了大量标准，1999 年，公安部主持制定了国家等级保护标准《计算机信息系统安全等级保护划分准则》（GB17859-1999）[1],税务总局根据相关要求制定了《信息安全等级保护工作的实施指南》。《指南》从整体描述了当前条件下安全建设的各个方面，如何依照相关要求做到网络的有效安全防护，开展管理制度建设、技术措施建设，落实等级保护制度的各项要求，提高税务系统信息安全管理水平、增强安全防护能力、减少安全隐患、降低安全事故发生率，有效保障税务系统信息化健康发展，维护国家安全、社会秩序和公共利益[2]。实现“面向安全的网络设计”，是当前税务信息安全的重要课题。

当前，南昌地税根据已出台税务系统信息安全等级保护等相关文件，结合等级保护基本要求，对本单位税务信息系统安全进行了新一轮改造。在对网络安全进行规划、设计、实施与维护的过程中，根据实际应用和安全需要制定统一的安全策略，设计合理的技术框架与管理框架，形成有效的信息安全管理体系，提升网络的安全属性，从根本上解决网络和安全管理问题。

1.2 研究目的及意义

南昌地税网络安全改造项目的提出主要针对以下问题：

（1）内外网络边界模糊

在内外网络隔离的环境中，如何确保内部网络边界的完整性，杜绝未授权终端联接以及防止内网终端违规联结外部网络是网络管理者面临的一大难题。传统的网络边界防护被理解为网络出口保护，而在现实情况中的边界早已超越了这一概念，无线技术的迅猛发展让随时随地接入互联网这一想法成为现实，无线技术在带来便利的同时，也对网络管理提出了更多的要求。从全网来看，边界防护更应该是所有网络边界的防护，并侧重于内网入口的防护。

（2）终端接入缺乏身份认证

内网身份认证机制包括访问服务器的身份验证或基于交换机端口的端口认证，以及配合以上方式的 CA、电子口令卡、radius 等。多种系统导致用户拥有多个帐号和口令，造成管理难度上升。而内部主机使用者缺乏特定的身份识别机制，使用有线或无线方式联入内部网络后，即可获取文件资料。受到忽视的终端之间非认证互访则成为了机密泄露和病毒传播的源头。

（3）内部网络访问控制不完整

南昌地税网络按照应用主体可划分为两大区域：是服务资源共享区域，第二是行政办公或业务区域，其中办公或生产区域又按行政区划分为不同县区分局等。两类逻辑区域共用一套物理网络，且尚未做明确的逻辑策略隔离。行政用户、业务用户甚至来宾用户在默认情况下，只要其接入内部网络并开通其网络访问权限往往可对服务器区域的资源进行访问。内网文件资源存在较大风险。

（4）终端及安全设备自身存在安全隐患

在采用安全设备对支撑系统进行安全加固的同时，安全设备自身的安全性不容忽视。当攻击发生时，如果安全设备自身不能抵挡，其保护的区域也岌岌可危。同样的，在“信息安全等级保护”中也建议对网络安全设备本身提供保护。

针对以上问题对现有业务、应用数据流加以整理、了解业务细节；划分安全区域、规范数据流路径；部署监控和分析设备、加强网络监管能力；应用防火墙技术、设定访问控制权限；部署管理平台、实现网络安全的集中管理；应用入侵检测保护主机资源、防止内部入侵；应用桌面终端、加强边界 防护；定期评估、加固和升级等。以此构建完整的网络安全防护系统。

1.3 研究现状与展望

江西省地税信息系统是以《江西省地税系统新一轮征管改革方案》中“加速信息化建设，推进地税信息一体化”的相关要求，按照国家税务总局金税工程（三期）建设的总体规划，根据一体化的原则，依托江西省政务信息网，建立的一个硬件环境统一、网络通讯环境统一、业务需求统一和应用软件统一，基于统一规范的应用系统平台，以江西省地税局为主、各设区市局为辅高度集中处理信息，功能覆盖各级地税机关税收业务、行政管理、决策支持、外部信息应用等的功能齐全、协调高效、信息共享、监控严密、安全稳定、保障有力的全省性地方税务管理信息系统。

江西省地税网络采用层次化设计原则，将网络系统划分层次，建立合理的网络结构，保证网络系统的稳定可靠、介入安全、便于扩充和管理、易于故障隔离和排除。全省地税广域网分省中心、地市、区县、征收分局四层，采用基于星形的分层结构组网，与地市局、区县局的连接采用政府信息网的 MPLS VPN 以太网电路与地市局、区县局的节点路由器连接，区县局与征收分局通过电信的 SDH 电路连接。

南昌地税网络是江西省地税信息系统的市级分支，由于兼有全省地税网络的备份中心，所以南昌地税网络在节点路由器的选择上选择了与省地税局同型号的 Cisco7609。

按照“一体化”和省级集中处理的原则，南昌地税依托江西省政务信息网建设了覆盖市县分局的三级星形网络。为保护内网的安全，根据南昌地税业务需求和网络安全的相关要求，南昌市地税以行政区划作为网络区域的边界，对各单位内网与外网物理隔离，采用统一的网关接入，在网关处架设防火墙、入侵检测等安全监控设备，在内网部署网络防病毒系统。

1.4 论文研究内容

本文研究的主要内容是在税务系统信息安全等级保护的相关要求下，市级税务系统的网络安全体系建设和边界防护的实现。从应用的角度对市级税务系统的区域划分和边界防护做了研究和设计。

通过对市级税务系统区域、边界的定义和划分，确定各区域的安全防护目标。以各区域间的数据流向整合区域边界，以实现数据流向、策略部署的简化和便捷管理的目标。

本文以业务需求为出发点，以安全设备部署和安全策略实施为重点，考虑各区域间的安全需求，建立较为完善的网络安全和边界防护设计。落实等级保护制度的各项要求，提高安全保护能力，减少安全隐患和安全事故。从物理安全、网络安全等方面落实安全保护技术措施。

1.5 论文组织结构

本文针对市级税务网络的安全及边界防护体系设计，论文组织结构如下

第一章 介绍税务网络的安全防护现状。

第二章 边界安全防护关键技术介绍。

第三章 介绍了南昌地税网络安全设计的相关原则、风险和需求。

第四章 介绍税务系统区域、边界的定义和划分，确定各区域的安全防护目标。

第五章 确定了市级税务网络区域拓扑，并分别对终端域、运维域、核心域的边界整合和边界安全策略做了说明。

第六章 通过对网络性能和常见威胁的功能测试说明网络的边界防护性能。

第七章 总结和展望。