学校编码：10384　　分类号_____密级_____

学号：X2011231018　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

基于安全域的南平市烟草公司信息网络的设计与实现

Design and Implementation of The Information Network of Nanping Tobacco Company Based on Security Domain

郭翔飞

指导教师姓名：史亮　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　　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

本论文以安全域的划分为网络架构设计思想，以南平烟草网络改造规划设计和实施过程为背景，依据烟草行业相关规范，结合南平市烟草公司业务系统的要求，将各信息网络划分为不同的安全域进行防护管理。对每个安全域进行层次化地有重点的保护，把一个复杂的大型网络转化为各个较小安全区域进行网络设计。

论文通过分析南平市烟草公司信息网络现状和应用系统的数据流向，基于建设一个结构清晰、可靠安全、扩展灵活的信息网络的目标，解决现有网络问题。本着安全性、实用性、投资保护的原则。依据现有信息网络功能结构，将信息网络划分为核心域、业务服务器域、楼层接入域、IT管理域、广域网域和外联域六个安全域。

在安全域划分的基础上，针对各安全域的特点提出相应的安全防护要求和防护措施部署方式以促进各区域的安全管理。通过部署安全域边界部分的安全设备防护加强物理层面的防护；通过ACL访问控制策略、网络防火墙、入侵防御系统等措施进行访问互联安全防护；通过漏洞扫描、安全配置加固、防病毒系统、身份鉴别、安全审计等措施进行内部安全技术管理。

最后根据设计方案的设备需求进行了相关网络和安全产品的选择。经过项目的实际实施改造取得了良好的效果。

关键词：安全域；信息网络；安全策略

Abstract

In this thesis, the partition of security domain for the network architecture design ideas, taking Nanping tobacco network reconstruction planning and implementation process as the background, on the basis of the tobacco industry related standards, combined with the tobacco companies business system requirements, will be divided into information network into different security domains for protection and management. For the protection of hierarchical focused on each security domain, a large and complex networks into each small safe area network design.

The flow of data through analysis of Nanping city tobacco companies information network status and application system, the construction of a clear structure, safe and reliable, flexible extension information network based on the objectives, to solve the network problems. In line with safety, practicality, investment protection principle. Based on the existing information network structure, the information network is divided into core domain, business server domain, floor access domain, IT domain, wide domain and outreach domain, A total of six security domain.

On the basis of the partition of security domain, according to the characteristics of each security domain and puts forward the corresponding security requirements and protection measures to promote the security management of the deployment region. Strengthen the physical protection level through the safety protective equipment to deploy security domain boundary; through the ACl access control, firewall, intrusion prevention system and other measures to access internet security; vulnerability scanning, the security configuration of reinforcement, anti-virus system, personal identification, security audit, internal security technology management measures.

Finally, the network security products selection according to the designdemand of the equipment. Good results have been achieved through actual implementation project.

Key Words： Security domain;Information network;Security strategy

目 录

Contents

第1章 绪论

1.1 项目背景与意义

近年来，随着烟草行业信息化建设和网络技术的不断发展，信息网络建设和网络安全保障对业务的发展和现代化管理水平的提高起到了重要作用。但随着信息网络系统规模不断扩大，结构逐渐复杂，网络架构各区域划分日渐模糊，区域边界保护开始存在不足。同时，随着安全管理策略的不健全，使整体网络面临黑客入侵、病毒破坏、信息泄露等风险。为了保证信息网络互联互通、安全可靠、高效快捷[1]，结合南平市烟草公司信息网络现状，针对网络架构、网络安全、网络管理等方面的不足，进行南平市烟草公司信息网络建设规划，使南平市烟草公司信息网络安全与网络“同步规划、同步建设、同步维护”。

烟草行业计算机网络建设是实现《数字烟草发展纲要》规划目标的基础和保障。2006 年 7 月国家局印发的《烟草行业计算机网络建设技术与管理规范》（国烟办综〔2006〕312 号），对规范行业计算机网络建设和保障网络的互联互通起到了重要作用。随着行业信息化建设和网络技术的不断发展，现有的烟草信息网络建设逐渐暴露出结构复杂、安全性低、管理性差等方面的不足。

为适应行业的改革与发展，福建省烟草专卖局对现行的《烟草行业计算机网络建设技术与管理规范》进行修订，制定《福建省烟草商业系统计算机网络建设技术与管理规范》。 从烟草行业管理体制的特点和计算机网络技术要求出发，按照行业“统一标准、统一平台、统一数据库、统一网络”的信息化建设总体要求，为保证行业计算机网络互联互通、安全可靠、方便快捷，必须统一技术体系、管理体系和运维体系。

南平市烟草公司根据文《福建省烟草商业系统计算机网络建设技术与管理规范（试行）》（闽烟办[2011]23号）的通知要求，结合南平烟草计算机网络现状，和业务需求，找出在本单位网络架构、网络安全、网络管理等方面的不足，通过安全域划分的方法和原则制定了南平烟草公司安全域划分框架，并在此基础上制定了安全域对应的安全防护规范。

1.2 项目的目标和主要工作

本文对安全划分的方法和原则进行了简单的介绍，并结合南平市烟草公司信息网络的实际情况，提出了安全域划分网络的规划设计，同时针对安全域的划分，对各安全域的进行了安全域管理策略的制定。力求使改造后的南平市烟草公司信息网络具有如下特点：

1.模块化。该网络通过区域划分来进行模块化设计，在整个模块化架构中，对安全域作了明确的划分，并给出明确的定义。在此划分基础上，在不同安全域中发布相应的应用，模块化设计使得该网络易于扩展，具有较强的灵活性、实用性以及可靠性。

2.层次化。每一个安全域按照网络分层设计方法进行层次化、结构化设计，保障各区域网络在每个层次上的平滑扩展，实现各个区域在服务功能、网络规模上的扩展能力。整个网络架构以核心域为中心，其它安全域模块化处理。

3.灵活化。改造后的网络架构易于扩展，有较好的灵活性。使用者可以依照不同的需求新添相应安全域，而只要在该网络架构的基础上做稍微的改动。另外，还能在不影响部署在网络架构中另外一些应用的情况下对相关功能升级，问题和故障定位也更容易。

4.安全化。划分安全域后，每个安全域都可以根据自己业务的特点部署针对性的安全策略，可以有效提升区域安全度，从而根本上提升整个网络的网络安全等级。

本文主要工作如下：

1.分析了地市级烟草信息网络和应用系统的现状。

2.分析了安全域划分的必要性并提出了划分原则。

包含了安全域划分的必要性，制定了安全域划分的原则，结合网管网络的实际情况，对网络结构进行调整，对安全区域的划分进行细化。

3.明确了安全域保护管理的原则

包括安全域的安全防护要求和防护策略。

4.针对改造所需的新增网络和安全设备进行选型。

1.3 论文组织结构

本论文共分6章:

第1章项目概述。主要介绍南平市烟草公司信息网络的建设背景，改造目标和主要的改造内容

第2章网络现状及需求分析。通过分析南平市烟草公司信息网络现状和业务系统情况，发现存在信息网络的问题和风险，对网络改造建设提出原则和目标。

第3章基于安全域的信息网络设计。介绍了安全域划分信息网络的指导思想、基本原则和划分思路，结合南平市烟草公司信息网络现状和业务系统的特点进行安全域划分设计。

第4章网络安全域管理方案的设计。在安全域划分的基础上，根据安全域管理原则，制定了相应安全域的管理策略进行安全防护。

第5章设备选型方案。依照南平市烟草公司信息网络设计，对改造所需的新增网络和安全设备进行产品选型。

第6章总结和展望。主要是对本论文进行的总结和展望。

第2章 网络现状及需求分析

信息网络建设的最终目的是为各类烟草应用信息系统正确可靠运行提供安全保障。因此在进行网络设计时，必须首先了解南平市烟草公司烟草信息网络和应用系统的基本情况，并进行必要的分析和抽象处理，才能为最终形成符合南平市烟草公司实际需求的信息网络建设方案打下良好的基础。

2.1 南平市烟草公司信息网络现状

南平市烟草公司信息网络架构基本上是在三层核心交换的基础上不断扩展网络规模，使得现有网络规模不断扩大、机构逐渐复杂。具体的拓扑如图2-1所示。

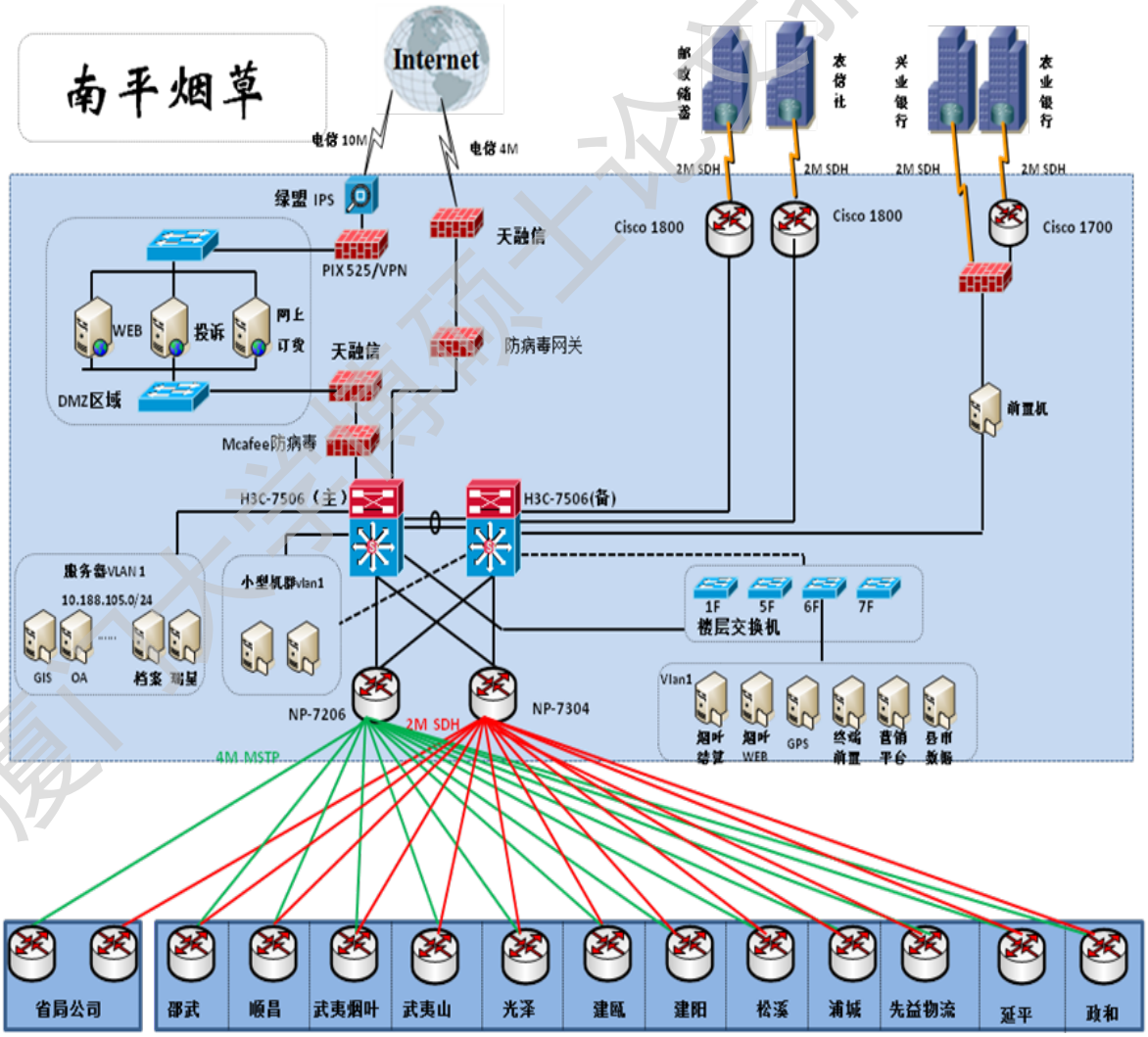

图 2-1 南平市烟草公司信息网络拓扑图

上述网络拓扑是伴随南平市烟草公司信息化发展而逐步形成的，公司网络

建设之初一台核心交换机就足够承载所有IT业务，从网络系统高可靠性出发部署双核心网络架构，后来业务系统增加，部分业务接其中一台交换机，出现部分子网双核心网络架构部分单核心网络架构（如银行接入）；最初DMZ区没有直连internet的链路，后来在上网人员越来越多，P2P等消耗出口带宽的应用越来越多的时候[2]，发现出口不畅的情况下增加DMZ区直连出口链路，实现内部工作人员的互联网上网业务与DMZ区对外服务业务的分流等。

2.2 南平市烟草公司业务系统情况

南平市烟草公司主要的信息系统包括：国家局一号工程，卷烟营销管理系统，订货系统，烟叶生产经营管理系统，财务管理系统，OA办公自动化系统，专卖管理系统，门户网站等。网络承载业务多样，可靠性、安全性要求高。

1.国家局一号工程实现了计划分解与排产、件烟下线打码、件烟出厂扫描、件烟商业到货扫描、工商数据采集等功能，同时全面实现了专卖准运证与卷烟实物到货确认关联，形成了信息收集、交换、传输、集成以及服务的烟草行业信息平台与标准体系。数据由物流公司上报数据经市公司服务器收集后通过内部网络上报省局服务器并对数据进行加工存储，与其它业务系统的关联互通性强。具体数据流如图2-2所示。

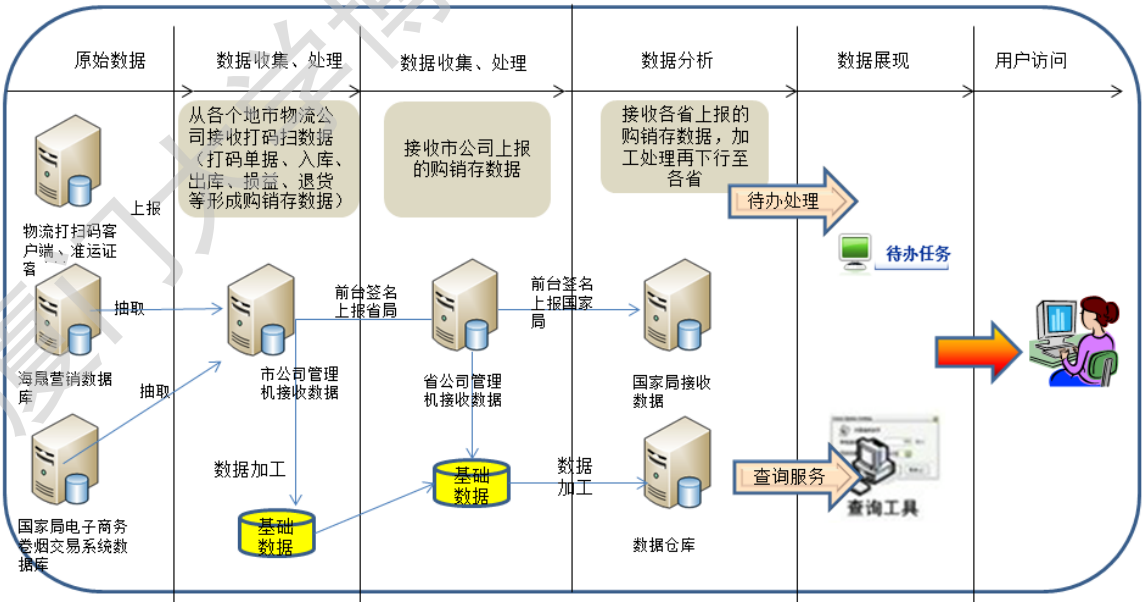

图 2-2 国家局一号工程数据流图

2.卷烟营销管理系统实现了全市卷烟销售数据统计分析、销售进度跟踪、合同协议跟踪等数据分析功能。重各县市公司接受销售数据经市公司服务器处理加

工。具体数据流如图 2-3所示。

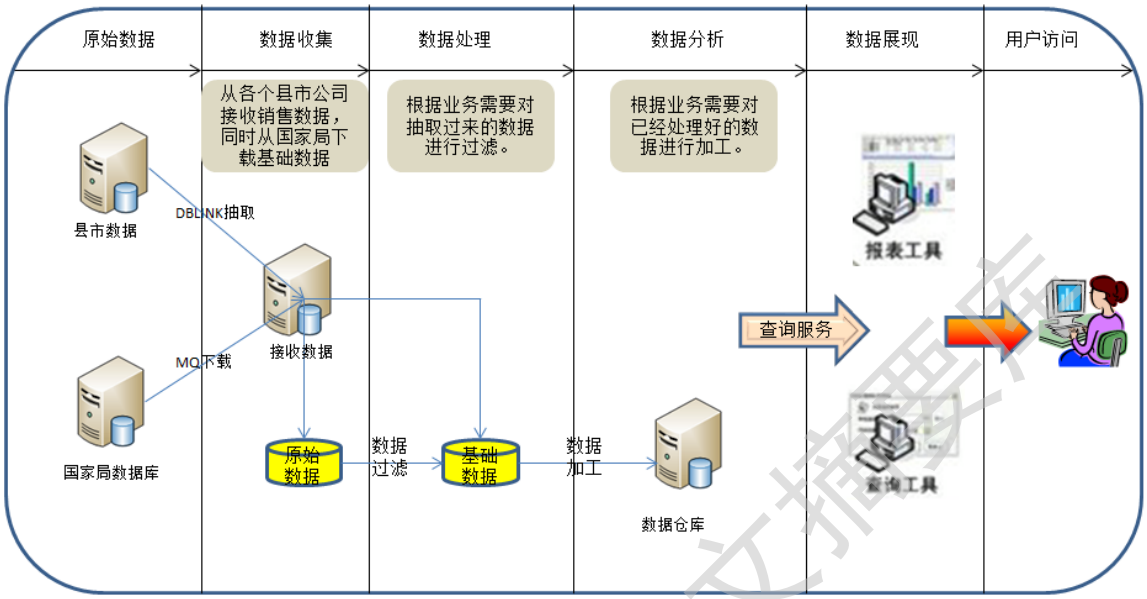

图 2-3 卷烟营销管理系统数据流图

3.订货系统实现了零售户连锁店面进销存、资金管理、网上订货，以及面向零售户的档案管理、积分兑换。订单数据经外网由零售户传输至市公司订货系统服务器，订货系统服务器同时从市局数据库获取数据反馈给零售户。对数据的安全性要求较高。具体数据流如图2-4所示。

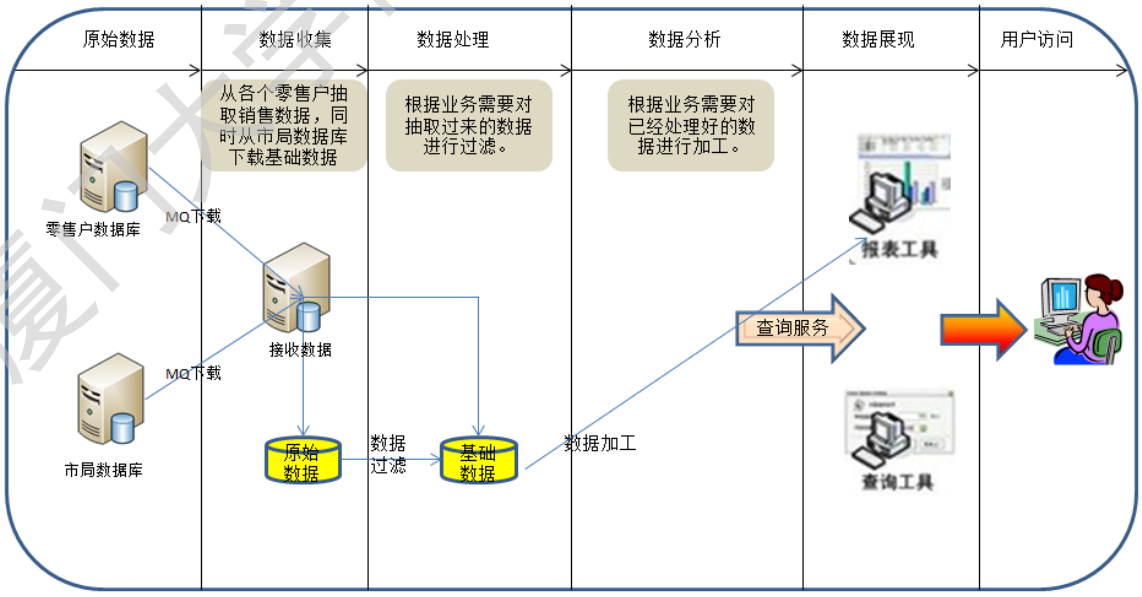

图 2-4 订货系统数据流图

4.烟叶生产经营管理系统实现了烟叶处日常文档管理、收购计划合同管