学校编码：10384　　分类号＿＿＿＿密级＿＿＿＿

学号：X2005230028　　UDC＿＿＿＿

工 程 硕 士 学 位 论 文

电子政务网络安全监控系统的分析与设计

Analysis and Design of E-government Network Security Monitoring System

龚伟斌

指 导 教 师：陈海山　教授

专 业 名 称：软 件 工 程

论文提交日期：2013 年 4 月

论文答辩日期：2013 年 5 月

学位授予日期：2013 年　月

指 导 教 师：＿＿＿＿＿＿

答辩委员会主席：＿＿＿＿＿＿

2013 年 6 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，本学位论文为(　　)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

电子政务是运用计算机、网络和通信等现代信息技术手段，实现政府组织结构和工作流程的优化重组，建成一个精简、高效、廉洁、公平的政府运作模式，以便全方位地向社会提供优质、透明、规范的管理与服务。在我国，随着电子政务的不断发展，对电子政务网络系统的安全性提出了更高的要求，因此研究建立有效的电子政务网络安全系统成为电子政务研究的重要内容。

本文主要围绕电子政务网络所面临的网络安全问题，分析了当前我国电子政务网络安全的主要挑战和安全要求，研究了电子政务网络安全主要安全技术手段，阐述了建立电子政务网络安全监控系统的重要意义，理论联系实际，分析了某市电子政务外网网络安全需求，结合网络安全技术，应用分层架构设计方法、关联规则分析等技术，设计实现了电子政务“网络安全监控系统”，并详细描述了系统设计和主要功能的实现 。

本文系统由数据采集、数据分析、数据展示等主要模块构成，实现了网络设备、网络安全设备、重要服务器的实时安全监控和管理、具有日志关联分析、故障自动定位、安全预警等功能，较好的满足了电子政务网络安全监控的要求。本文的设计思想和解决方案，对国内市级电子政务网络安全系统的设计与实现具有一定的参考意义。

关键词：电子政务；网络安全；监控系统

Abstract

E-government is the use of computer, network and communication of modern information technology, realize the optimization and reorganization of the government organization structure and the work flow, into a lean, efficient, honest, fair government operation mode, so that the full range of the community to provide quality, transparent ,standardized,management and service. In our country, with the continuous development of e-government, put forward higher request to the security of the e-government network system, so the research important content to build e-government network security system effectively has become the research of e-government.

The dissertation focuses on the network security problems faced by e-government network, analyzes the main challenges and safety of current our country E-government network security requirements, the means of e-government network security is the security technology, expounds the important significance of establishing e-government network security monitoring system. Linking theory with practice, analyze the demand of e-government extranet network security electronic city, combined with the network security technology, application of layered architecture design methods, association rules analysis, design and implementation of the electronic government "network security monitoring system", and a detailed description of the system design and implementation of the main function.

This system mainly consists of data acquisition, data analysis, data display module. The system implements real-time security monitoring and management of th network equipment, network security equipment, important server. It also implements log analysis, automatic fault localization, security early warning function, which satisfies the requirements of the e-government network security monitoring. Design ideas and solutions in this paper, has certain reference value for the Design and Implementation of the municipal e-government network security system.

Keywords: E-government; Network Security; Monitoring System

目录

Contents

第1章　绪论

1.1　研究背景及意义

自 20 世纪 90 年代电子政务产生以来，关于电子政务的定义有很多，并且随着实践的发展而不断更新。联合国经济社会理事会将电子政务定义为：政府通过信息通信技术手段的密集性和战略性应用组织公共管理的方式，旨在提高效率、增强政府的透明度、改善财政约束、改进公共政策的质量和决策的科学性，建立良好的政府之间、政府与社会、社区以及政府与公民之间的关系，提高公共服务的质量，赢得广泛的社会参与度。

在我国电子政务一般指：运用计算机、网络和通信等现代信息技术手段，实现政府组织结构和工作流程的优化重组，超越时间、空间和部门分隔的限制，建成一个精简、高效、廉洁、公平的政府运作模式，以便全方位地向社会提供优质、规范、透明的管理与服务。

电子政务的主要目的是推进政府部门办公自动化、网络化、电子化、全面信息共享等工作进程，从而营造运用信息及通信技术打破行政机关的组织界限的电子化虚拟机关，实现广义的政府机关间及政府与社会各界之间经由各种电子化渠道进行相互沟通，并依据人们的需求、使用的方式、要求的时间及地点，提供各种不同的针对个性的服务选择。电子政务对支持政府职能的转变，扩大对外交往的渠道，密切政府与人民群众的联系，提高政府工作效率的重要性不断提高。

随着电子政务的不断发展，其承载的政府管理和服务的信息系统日趋庞杂。一方面，电子政务在互联互通、信息共享的内在要求下，所依赖的电子政务网络系统日益复杂，包括政府网站、网上审批在内的各种应用资源越来越多面向 Internet 为广大公众提供快捷的便民服务，这些对电子政务网络信息系统的安全性提出了更高的要求。

另一方面，由 Internet 的发展而带来的网络系统的安全问题正变得日益突出，我国基础信息网络和重要信息系统安全面临的形势还比较严峻，主要表现在：一是针对基础信息网络和重要信息系统的违法行为不断上升，二是基础信息网络和重要信息系统安全隐患比较严重，三是信息安全保障工作基础还比较薄弱。

因此，研究电子政务网络安全技术，研究建立与电子政务网络信息安全要求相适应的安全策略、安全设施和构筑较为完善的网络安全系统，是一项很有现实意义的工作，也成为电子政务建设的一个重要内容。

本课题结合本人在某市电子政务中心的工作实践和实际需求，就电子政务网络信息安全技术进行研究和探讨，设计实现了电子政务“网络安全监控系统”。

1.2 研究目标

根据电子政务在网络信息安全的需求，按照信息安全等级保护的要求，应用软件工程系统分析方法和分层架构设计方法，结合主流的网络安全技术，设计并实现电子政务外网“网络安全监控系统”。

1.3 研究内容

1．电子政务网络信息安全分析，对我国电子政务网络所面临的主要公共安全挑战进行分析。

2．现阶段主流的网络安全技术的分析，分析了建立网络安全监控系统的重要意义。

3．电子政务外网网络安全需求分析，结合现阶段主流的网络安全技术，设计电子政务外网“网络安全监控系统”的总体架构，总体上系统分为三个层次：采集层、处理层、表示层。

4．根据总体架构设计，设计并实现电子政务外网“网络安全监控系统”。系统是按照分层架构设计的原则，以 SOA 架构设计方法为指导设计的，提供统一的管理门户，实现网络设备、网络安全设备、服务器的实时监控和管理，通过对各种网络设备、安全设备、服务器等设备事件的关联分析实现网络系统的安全告警。

1.4 本文结构安排

本文共分为五章。

第 1 章，电子政务网络安全系统的重要性进行分析，阐明课题的研究意义、研究目标和主要研究内容。

第 2 章，我国电子政务网络安全分析，分析常用的电子政务网络安全技术，分析建立网络安全监控系统的重要性，简要介绍网络安全监控系统采用的软件工

程分层架构设计体系。

第 3 章，理论联系实际，详细分析某市电子政务外网网络安全现状和安全需求，提出系统需求分析与总体设计。

第 4 章，详细描述电子政务网络安全监控系统的设计和实现过程。

第 5 章，总结和展望，对项目的主要工作和论文的主要内容进行总结，并对电子政务网络安全监控系统的进一步研究进行展望。

第2章　电子政务网络安全分析

根据课题研究的目标，本章简要分析了当前我国电子政务网络安全的主要挑战和安全要求，介绍当前主流的电子政务网络安全技术手段和措施，分析了建立网络安全监控系统的重要意义，并简要介绍了网络安全监控系统采用的分层架构设计体系。

2.1 电子政务网络安全问题分析

2.1.1 电子政务网络安全威胁

从技术层面上讲，当前国内电子政务网络面临的安全威胁主要表现在以下几个方面：

1、非法访问。指未经授权使用网络资源或以未授权的方式使用网络资源，主要包括非法用户进入网络或系统进行非法操作以及合法用户以未授权的方式进行访问操作。

2、来自网络外部的攻击。这是指来自网络外部的无意和有意的攻击，攻击者主要是利用网络层面 TCP/IP 协议的不安全因素进行黑客攻击，造成网络、服务器资源的大量无用消耗甚至系统瘫痪。攻击主要包括：拒绝服务攻击(Dos 攻击)、分布式拒绝服务攻击(DDos 攻击)、IP 欺骗攻击、ARP 攻击、密码暴力破解攻击、恶意扫描等形式。

3、来自网络内部的攻击。在内部网络（信任网络内部），也存在一些内部合法用户无意或有意的冒用其他合法用户身份登陆，查看非授权信息，修改信息内容，影响应用系统运行，以及信息非法外传等行为。

4、计算机病毒。表现在利用计算机病毒占用带宽，堵塞网络，瘫痪服务器，造成系统崩溃或让服务器充斥大量垃圾信息，导致系统性能降低。从“蠕虫”病毒开始到 CIH、爱虫病毒，病毒一直是计算机系统安全的威胁，网络更是为病毒提供了迅速传播的途径之一。

5、利用系统及应用软件的漏洞“后门”进行应用层面的攻击。该类攻击主

要是利用操作系统、应用软件平台本身隐藏的代码缺陷和漏洞进行应用层面的网络攻击，主要的形式有：缓冲区溢出攻击、CGI 攻击、SQL 注入攻击、跨站脚本攻击等。

2.1.2 电子政务网络安全要求

由于电子政务系统的特殊性，电子政务网络的安全要求也比较严格，主要是确保电子政务网络的可用性、完整性、可控性、机密性、与可审查性，具体表现在以下几个方面 ：

1、合理管理和分配网络资源，防止滥用网络资源导致网络瘫痪。

2、抵御病毒、恶意代码等对信息系统发起的恶意破坏和攻击，保障网络系统硬件、软件稳定运行。

3、保护重要数据的存储与传输安全，防止和防范数据被篡改，建立数据备份机制和提高容灾能力。

4、加强对重要敏感数据信息的保护，确保数据的机密性。

5、构建统一的安全管理与监控机制，统一配置、调控整个网络多层面、分布式的安全问题，提高安全预警能力，加强安全应急事件的处理能力，实现网络与信息安全的可控性。

6、建立认证体系保障网络行为的真实可信以及可审查性，并建立基于角色的访问控制机制。

2.2 常用电子政务网络安全技术

2.2.1 防火墙

防火墙技术是近年来电子政务常用的保护计算机网络安全的技术。它是一种隔离控制技术，在不同网络区域之间设置屏障，阻止对信息资源的非法访问，也可以防止重要信息从内部网络上被非法输出。

防火墙（英文：Firewal）一般可如下定义：防火墙是位于两个或多个网络之间的安全阻隔，是包含软件部分和硬件部分的执行访问控制策略的一个或一组系统，是一类防范措施的总称，是最重要的网络防护设备之一。目前大多数主流的防火墙都是以专门的硬件形式出现，这种硬件设备也被称为防火墙。

防火墙通常放置在外部网络和内部网络（被保护网络）中间，如图 2.1 所示。

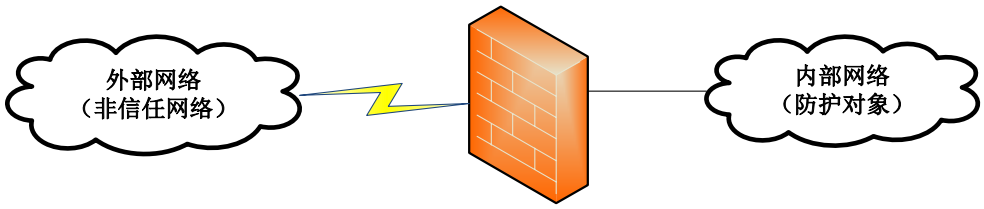

图 2.1　防火墙的部署位置

防火墙的主要功能包括：

1. 访问控制功能：这是防火墙最基本也是最重要的功能，通过安全策略禁止或允许特定用户访问特定的资源，保护网络的内部资源和数据，包括服务控制、方向控制、用户控制、行为控制等。

2. 全面的日志功能：防火墙能完整记录通过防火墙的网络访问情况，记录通过防火墙的信息内容和活动，可实现事后日志查询和审计。

3. 其他主要附加功能：

(1) 网络地址转换(NAT)：节省 IP 地址资源、隐蔽内部网络的功能。

(2) VPN 功能：作为一个公共网络接入内部网络的 VPN 接入控制点。

总的来说，防火墙技术是目前电子政务用来实现网络安全措施的一种主要手段，它主要是用来拒绝未经授权的用户访问，阻止未经授权的用户存取敏感数据，同时允许合法用户正常访问网络资源。

2.2.2　Web 应用防火墙(WAF)

Web 应用防火墙（英文：Web Application Firewall，简称 WAF）是通过执行一系列针对 HTTP/HTTPS 的安全策略，来专门为 Web 应用提供保护的一种网络安全产品。Web 应用防火墙是最近几年新兴的安全技术，从本质上说，Web 应用防火墙可以算是一种特殊的基于 Web 防护的应用层防火墙。

WAF 产生的背景：

1. Web 安全威胁日益严峻

随着机构的计算及业务资源逐渐向其数据中心高度集中，Web 成为一种普适平台，越来越多地承载了各类机构的核心业务，如电子政务、电子商务、运营商

的增值业务等。Web 服务器逐渐成为主要攻击目标，SQL 注入、网页篡改、网页挂马等 web 安全事件频繁发生。

2. 传统防火墙的局限性

传统的防火墙，不论是早期的包过滤型防火墙还是现在较为常用的状态检测防火墙主要是工作在 TCP/IP 协议的网络层，对外部网络层的非法访问和攻击（Dos，DDos 攻击等）具有较好的防御能力，但是在应用层防护方面比较弱，对于 web 应用防护更是不足。

与传统防火墙相比较，WAF 最显著的技术特点如下：

1．对 HTTP 有本质的理解：能完整地解析 HTTP 包括报文头部、参数及载荷，支持各种 HTTP 编码(如 chunked encoding)，提供严格的 HTTP 协议验证，提供 HTML 限制，支持各类字符集编码，具备 response 过滤能力。

2．提供应用层规则：Web 应用通常是定制化的，传统的针对已知漏洞的规则往往不够有效，WAF 提供专用的应用层规则，且具备检测变形攻击的能力，如检测 SSL 加密流量中混杂的攻击等。

3．提供正向安全模型（白名单模型）：仅允许已知有效的输入通过，为 Web 应用提供了一个外部的输入验证机制，提供更为可靠地安全性。

4．提供会话防护机制：HTTP 协议最大的弊端在于缺乏一个可靠的会话管理机制，WAF 为此进行有效补充，防护基于会话的攻击类型。

WAF 通常工作在防火墙 DMZ 区，透明部署在防火墙和 Web 服务器群之间，如图 2.2 所示。