

分类号：TP393.03

学校代码：10406
学号：G14085211008

南昌航空大学
硕 士 学 位 论 文
(专业学位研究生)

入侵检测与防御系统的研究与实现

硕士研究生： 占清华

导 师： 李其申

申请学位级别：硕 士

学 科、专 业： 计算机技术

所 在 单 位： 信息工程学院

答 辩 日 期： 2017 年 06 月

授予学位单位： 南昌航空大学

The research and implementation of intrusion detection and defense system

A Dissertation

Submitted for the Degree of Master

On Computer Application Technology

By **Zhan Qinghua**

Under the Supervision of

Prof. Li Qishen

Nanchang aviation university

Information Engineering College

June, 2017

摘要

当前, 伴随科学技术的不断发展, 计算机信息技术已经得到了显著的提高, 并被广泛的应用在社会生产和人民生活中的各个环节。与此同时, 网络安全领域也成为涉及影响国家安全发展和关系到百姓生活的重点领域。传统安全防御技术如防火墙、入侵检测 IDS 等技术已经普遍应用在网络安全的各个领域。然而这些技术中存在大概率的漏报和误报现象、检测效率低下、联动协作性差、智能性不高等不足问题, 因此缺乏对网络全面的保护能力, 为此, 提出了一个满足实际需求的网络安全防御技术多种技术优势相结合的防御体系是本文的主要任务。

本文首先陈述了防火墙在网络安全领域的应用情况和发展方向、介绍了被动式的网络安全入侵检测技术 IDS 分类及其存在的问题。接着介绍了入侵防御技术 IPS 相关技术的分类, 论述了各自的优缺点。分析了当前网络安全领域防御技术的类别及存在技术问题, 探讨这些分类的各自优缺点。最后, 对现有安全防御系统分别进行初步的总体设计和详细设计, 在此设计结束后进行系统的实现和测试过程, 同时举例开展仿真实验和测试。

本文研究的创新点及最终的成果包括:

(1) 在前期研究基础上设计了一套协同检测、联动防御的网络防御综合解决方案。

(2) 结合了入侵检测、防火墙技术、入侵防御技术等传统技术, 搭建了各自的数据通信和分组交换的桥接通道, 提升和实现系统的交互性和扩展性。

(3) 在现有网络安全模型的理论基础上设计了一个合作式的防御模型, 以此实现了一个协同作业、联动合作的入侵防御系统。经过仿真测试证明, 该系统具备较好的市场应用价值。

关键词: 防火墙, 网络安全, 协同防御, 分布式

Abstract

At present, along with the continuous development of social economy and science and technology, computer information technology has been improved significantly, and widely used in social industry, at the same time, network security is becoming more and more get the attention of people. The traditional firewall technology, intrusion detection and intrusion prevention techniques have been widely used in every field of network security, however, these techniques of misinterpretation and omission phenomenon exists in large probability, low efficiency, poor dynamic collaborative, intelligent detection of shortage problem, so lack of comprehensive protection to the network, therefore, design a meet the actual demand of network security technology integration defense system is the main task of this paper.

This paper stated the firewall, intrusion detection and intrusion prevention safety related technical background, discusses their respective advantages and disadvantages; Analyses the characteristics of intrusion detection and prevention system classification, problems, etc.

In this paper, the main innovation points and the final research results include:

(1) a dynamic defense system framework is proposed. The framework on the basis of providing static defense, emphasis on dynamic response and between various security components work together is a kind of active, active intrusion prevention system.

(2) is a blend of intrusion detection, firewall technology, intrusion prevention technology of the traditional technologies such as data communication interface and packet switching, make the system achieve better interactivity and extensibility.

(3) the final results of a question: designed a dynamic defense model, based on the implementation of a new type of defense system. Tests show that the system has good market application value.

KEY WORDS: Firewall, Network security, Distributed

目 录

摘 要.....	I
Abstract.....	II
目 录.....	III
第 1 章 绪论.....	1
1.1 研究背景与意义.....	1
1.2 国内外研究现状.....	2
1.3 研究的主要内容.....	3
1.4 论文章节安排.....	3
第 2 章 相关技术背景.....	4
2.1 防火墙.....	4
2.1.1 防火墙定义.....	4
2.1.2 防火墙分类及功能.....	7
2.1.3 防火墙存在问题.....	9
2.1.4 防火墙发展方向.....	10
2.2 入侵检测.....	11
2.2.1 入侵检测系统分类.....	13
2.2.2 入侵检测存在的问题.....	17
2.3 入侵防御.....	18
2.3.1 入侵防御系统的分类.....	18
2.3.2 入侵防御技术存在的问题.....	19
2.4 分布式技术.....	19
2.5 本章小结.....	20
第 3 章 系统总体设计.....	21
3.1 系统设计目标.....	21
3.1.1 现有网络安全模型介绍.....	21
3.1.2 动态防御模型.....	23
3.1.3 分布式防御模型.....	23
3.2 系统框架.....	25
3.2.1 数据处理流程.....	25
3.2.2 数据控制流程.....	27
3.3 系统体系结构.....	27
3.4 本章小结.....	29
第 4 章 系统详细设计.....	30
4.1 分布式网络探测器.....	30
4.1.1 网络探测器结构与功能介绍.....	31
4.1.2 规则匹配探测器.....	32
4.1.3 异常检测探测器.....	32
4.2 主机探测器.....	34

4.3 策略管理中心.....	35
4.3.1 策略管理中心的模块设计.....	35
4.3.2 探测器模块的设计.....	36
4.3.3 实时报警与数据库处理.....	37
4.3.4 联动处理模块的设计.....	37
4.4 系统控制台模块设计.....	37
4.5 联动响应模块.....	39
4.6 本章小节.....	40
第5章 系统实现和测试.....	41
5.1 开发环境.....	41
5.1.1 Java 开发环境.....	41
5.1.2 B/S 架构概述.....	41
5.1.3 Jsp+Tomcat+MySQL 环境配置.....	42
5.1.4 Tomcat 的安装及配置.....	44
5.1.5 安装 Mysql5.7.....	45
5.2 关键技术.....	46
5.2.1 策略管理中心.....	46
5.2.2 异常入侵检测.....	49
5.2.3 服务控制模块.....	50
5.3 运行界面.....	52
5.4 案例仿真实验.....	52
5.4.1 案例模型设计.....	52
5.4.2 模型结构.....	53
5.4.3 最优防御攻击节点的选取原则.....	54
5.4.4 防御模型机制.....	54
5.5 仿真实验.....	55
5.5.1 入侵事件数量对模型能耗的干扰.....	55
5.5.2 节点通信周期对模型能耗和丢包率的干扰.....	56
5.6 本章小节.....	57
第6章 总结与展望.....	58
参考文献.....	59
致 谢.....	61
硕士学位论文原创性声明.....	63

第1章 绪论

1.1 研究背景与意义

在“互联网+”背景环境下的今天，计算机技术以及网络技术越来越离不开人们的日常工作和工业生产，在社会生产和生活的各个领域都得到了广泛的应用。但随之而来的是不断暴露的安全问题。多元化和复杂化的网络入侵攻击等事件变得越来越频繁，严重扰乱正常的网络秩序，影响了社会经济发展。比如很多网络入侵与攻击直接导致电商行业的用户和商家利益受损。面对日益严峻的网络安全形势。近两年我国政府将“维护网络安全”写进了政府工作报告，将这一计划上升到国家战略。网络安全问题不仅关系到每个网民、更影响到社会稳定，可见，对我国互联网发展意义重大、影响深远。

近年来随着物联网和虚拟化设备的应用普及，网络攻击的规模量成指数上升，从PC端到移动端，入侵和攻击手段层出不穷，造成的严重数据泄露事件频频发生。在保卫网络信息安全的这个战场上，强大的敌人（入侵者）并不是最令人恐怖，恐怖的是未知的敌人。网络中的攻防战略亦是如此，被攻击者若是无法发现入侵，就无法及时的防护和响应。所以，传统网络安全领域的入侵检测系统或者是防病毒技术已出现技术瓶颈和显示明显的局限性。主要的问题有两点：一是新型入侵攻击无法被发现，另一个是大量误报漏报信息淹没了真实报警。因此，仅限某种单一的安全检测或防御技术已经无法达到人们对网络安全水平，更是无法满足当前时代下网络环境的发展需求。

因此，在网络威胁形势严峻的今天，协同联动是网络信息安全的制胜之道，也是网络安全所面临的矛盾与困境的必然产物。

如表 1-1 所示 360 网络安全公司提供的拦截漏洞攻击次数最多的 10 个漏洞类型。

表 1-1 漏洞攻击拦截 Top10 的漏洞及其拦截次数

TOP10	漏洞攻击类型	拦截次数（万）
1	SQL 注入	52234.3
2	扫描器	14663.8
3	备份文件探测	10432.5
4	Nginx 攻击	7569.7
5	XSS 攻击	6957.7
6	本地文件包含	4454.8
7	信息泄露	2863.9
8	命令注入	2702.9
9	UA 攻击	2428.9
10	代码注入	2105.0

1.2 国内外研究现状

随着计算机技术和网络技术的广泛应用，多元化和复杂化的网络入侵攻击等事件变得越来越频繁，严重扰乱正常的网络秩序，影响了社会经济发展。比如很多网络入侵与攻击直接导致电商行业的用户和商家利益受损。面对日益严峻的网络安全形势。近两年我国政府将“维护网络安全”写进了政府工作报告，将这一计划上升到国家战略。网络安全问题不仅关系到每个网民、更影响到社会稳定，可见，对我国互联网发展意义重大、影响深远。

根据“360”在 2016 年底作出的中国互联网政企安全报告显示：全球化的网络安全领域各项技术正在加速转型过程中，尤其在系统和网站的安全防御方面，其最大的特点就是从个人终端、单一技术的单点防御转型为多点联动的协同安全防御。

防火墙技术在网络安全技术和传统防护技术中应用比较多见。防火墙即简单原理就是隔离和防护。在内外网直接架设一道相应的控制模式和安全策略，实施内外网通信控制。它的主要任务是制定有效的访问策略，只有被授权的外网才可以访问内网 IP，保证内部网络的相对安全；

数字加密技术和身份识别相比防火墙技术而言，防御能力更加主动和灵活。

入侵检测系统（IDS）是防火墙在功能缺陷上的补充，可以防止网络基础设施即路由设备、交换机、服务器等受到拒绝服务攻击。由于网络安全问题的复杂性，IDS 分类两块：即一类是基于保障网络安全的入侵检测系统 NIDS，另一类为基于保护主机数据安全的 HIDS。

由于飞速发展的网络技术伴随着相应的攻击行层出不穷，一些以攻击为目的

的黑客的技术水平也在不断升级,因此导致了一个恶性循环的现象:即一方面网络被入侵和攻击次数的指数型增加和另一方面网络环境遭受破坏和被入侵攻击后所产生的应变能力越来越慢。本地多维网络安全技术的协同分析与处理能力不足、云端威胁情报技术的落后和缺位的主要原因。在此,网络安全领域迫切提出新的更高要求,尤其是针对高级威胁的发现,多维度检测技术、大数据分析技术和威胁响应技术。

1.3 研究的主要内容

本文从多个不同类型的的安全领域深入研究了适应我国当前网络入侵与防御技术的现状和发展趋势,分析了现有的安全技术设计了一个网络入侵检测防御模型。

深入分析了防火墙、IDS 和 IPS 技术的优缺点,在此基础之上研究并实现了一套网络入侵检测防御系统,最终详细设计并实现了一个协同合作的、动态防御的综合防御系统。

1.4 论文章节安排

本文从传统安全技术研究入手,逐步跟进网络发展前沿技术领域,采用现代防御技术的先进思想并实现了一个在传统防御技术上改进的协同防御系统。文章对系统详细设计过程和具体测试实现进行了深入论述,全文结构分为以下章节:

第一章 本文绪论。概述全文的研究背景与现实意义、介绍研究对象在国内外的现状。

第二章 相关技术背景。简述防火墙概念及分类,IDS、IPS 的功能及存在的问题,并较详细地总结了 IDS、IPS 中的优缺点。

第三章 系统总体设计。根据上一章背景知识进行引入现有网络安全模型,实现了系统框架的设计和防御模型的设计。

第四章 系统详细设计。在上一章的技术基础上进行了系统的详细功能结构划分,基本实现了协同合作的、动态防御的综合防御系统的设计。

第五章 系统实现和测试。系统实现过程演示介绍、举例测试网络入侵后最优防御攻击仿真实验。

第六章 总结与展望。分析本文不足和总结经验、展望未来继续研究的方向。

第2章 相关技术背景

在网络安全领域中较为传统的防火墙、病毒防御、入侵检测及防御技术等相关的技术概念和知识背景做了详细描述，根据以上各技术的自身特点进行了简要分析。

2.1 防火墙

2.1.1 防火墙定义

防火墙（FireWall），也称防护墙。是指提供相关安全策略和服务将不同网络设立一道安全防护系统。也是一种直接的防御系统。最初的防火墙是针对因特网中的安全威胁所采取的一系列相关保护内部网络的安全措施。

简单描述防火墙的工作任务即：“放行通过合法数据包”或“阻止拦截非法数据包”，防火墙如图 2-1 所示。

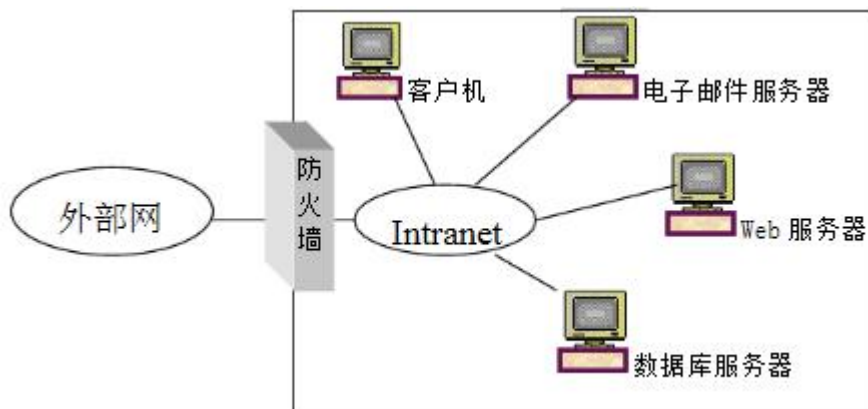


图 2-1 防火墙示意图

计算机安全技术的发展直接影响了用户对防火墙功能要求的提高，传统防火墙的代表即边界防火墙由于完全受制于网络拓扑结构的限制，暴露出很多局限性和弱点。其在网络中的漏洞和设计缺陷更多的成为黑客、木马病毒攻击威胁的对象。当然，边界防火墙依然是防御体系的第一扇门，安全处理能力较为简单，有着规则较少、效率高的特点。

用户为防止更大的损失和被破坏，将一种能够有效填补边界防火墙缺陷的新型防火墙安装处位于内外网络交界之处。这种新型的防火墙叫做：“分布式防火墙”（DFW： Distributed Firewalls）。

具有明显特征的分布式防火墙具有防堵内网中安全漏洞的特点。它又可分为有广义和狭义两类。它是完全不同于边界防火墙的一种全新结构和体系。它的体系结构如图 1-2 所示。

采用嵌入操作系统为特征的狭义分布式防火墙是一种安全软件。主要针对桌面应用。DFW 体系结构中的核心部分即中央策略服务器等五各功能模块。

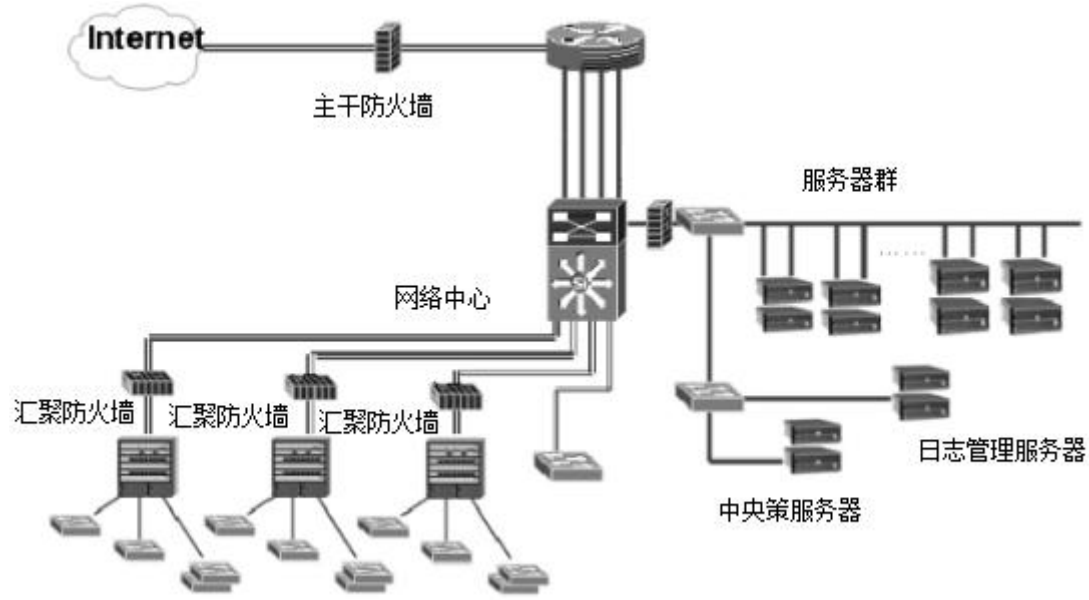


图 2-2 分布式防火墙结构

传统的边界防火墙与分布式防火墙对比有明显的不足：

- （1）传统防火墙无法完成内外兼顾、协同处理，无法确保更高的安全系数。
- （2）其次是配置灵活度不高，适用性较弱。
- （3）传统防火墙分散单点作业，管理较为分散。
- （4）分布式防火墙在防护结构完整，体系严谨。

分布式防火墙在当前市场应用领域中比较成熟，分别从阻止网络攻击方向对比和不同防护目标方面（如病毒、恶意插件、网络入侵、木马等）对比可见，防火墙主要功能分别见表 2-1、表 2-2 所示。

表 2-1 防火墙分类功能比较

防护功能	传统边界防火墙	传统软件防火墙	DFW 分布式防火墙	个人防火墙	病毒防火墙
病毒					✓
恶意网络插件		✓	✓	✓	✓
网络入侵	✓	✓	✓	✓	
木马			✓		
内网维护			✓		
个人计算机			✓	✓	✓
骚扰	✓	✓	✓	✓	
信息收集型攻击	✓	✓	✓	✓	

表 2-2 防火墙主要功能比较

阻止网络攻击	包过滤 基于状态的过滤
木马过滤	屏蔽已知木马（冰河、Back Orifice 2000 等） 检测未知木马，加入屏蔽列表 能防止木马使用加密隧道（Tunnel）技术
脚本过滤	包括 Java Script 脚本、Visual Basic 脚本、ActiveX 脚本等
统一的安全策略管理服务	由系统管理员专人监管提高安全保障能力，可降低防火墙的使用成本。 可使用策略下载缓释技术将策略文本分成小片，逐片下载，不影响用户网络宽带，不影响用户使用网络的感觉。 下载安全策略时，总是同时与服务器上的策略校验，保证不下载缺损策略而破坏安全设置。 本地安全策略加密存储，保证不能随意修改。
入侵检测 IDS	发现并阻止常用的网络攻击方法，如端口扫描、源路由数据包攻击、泪滴攻击、NMAP 扫描、TCP Flood 等等
同时支持以太网和 Modem 连接	全面防护每个可能的通道
动态升级	最新策略自动更新，并动态加载到系统的内核中，系统无需从新启动
实时网络状态监控	可实时查看网络连接的状态消息
完善日志记录和报警功能	包括软件安装、升级记录、安全策略记录、网络访问记录和受攻击记录等
全线支持 Microsoft Windows 平台	包括 Windows7/NT /2000

2.1.2 防火墙分类及功能

根据实现技术的分类，分为三个阶段：

(1) 包过滤防火墙

包过滤是指完成分析、选择和过滤的工作，通常作用在网络层。它是工作在网络层同时内置与 Linux 内核路由功能上的一种类型。

该技术作为一种数据安全保护机制。主要功能是实现监测、限制和修改数据流，它通常由定义的各条数据安全规则所组成，对外部网络实施屏蔽内部网的信息和维护管理。包过滤防火墙控制工作的流程如图 2-3 所示。

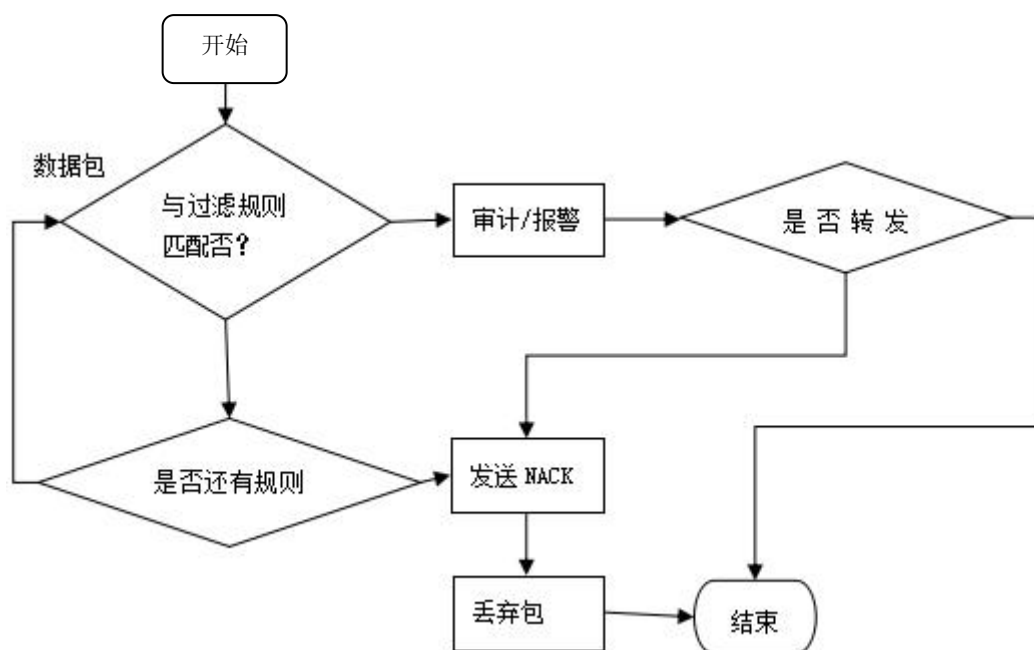


图 2-3 包过滤流程

(2) 应用代理防火墙

应用代理防火墙主要工作在教育层也是 OSI 的七层的最高层。它在通信链路主要功能是阻隔网络通信的数据流。完成对于不同类别的应用服务设置相应的代理程序，来实现网络数据流的监控作用。

针对指定的数据过滤协议和数据包进行分析并形成具体报告。应用层防火墙内部和外部之间的连接代理服务器的计算机系统之间的连接。是外部计算机网络链接只能达到代理服务器，具有隔离在防火墙内部和外部的影响计算机系统；缺点是执行速度慢，容易导致操作系统受到攻击。

由于其工作在最高层，因此他的大的优点就是安全。代理程序的实现分为了代理客户端和代理服务器两个部分。在数据流过程中实现客户机与服务器的桥接

作用，如图 2-4 所示。

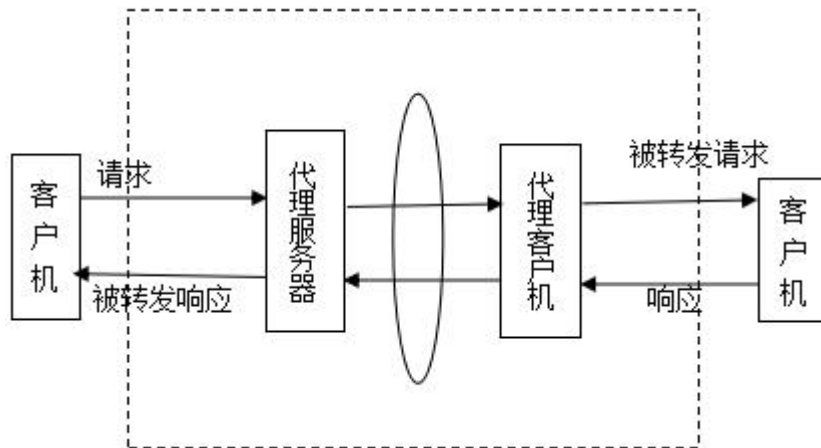


图 2-4 应用层网关模型

代理防火墙技术的特点是不仅仅实现包过滤防火墙的功能，还完全禁止内网外网的直接通信，使得内部系统真正的独立于外部系统。代理技术在实现过滤数据流的同时完成核对识别用户的身份认证。代理防火墙技术采用相应的安全策略方法，按照一定的策略规则或算法来保障安全体系，完成在高层实现过滤功能，代理技术相对包过滤技术较为安全，因此在实际应用中较普及。

（3）状态检测防火墙

状态检测技术工作在网络层。与上两类技术（包过滤和应用代理技术）不同，前面介绍的包过滤和应用代理防火墙是根据数据信息提取相应的行为规则为基础建立相应的安全模型，而状态检测防火墙则是预置安全模型，将新建的连接的全部分散的数据包作为连续对象通过散列算法进行检测。所有数据流的数据同时分析数据流的状态，因此状态检测是基于连接状态的检测和过滤。它在传统包过滤技术基础上进行了功能扩展和延伸。

状态检测技术是建立在网关上的安全检测模块，在不影响正常通信前提下抓取数据流信息进行审计和分析，通过随机监测分析其中部分状态信息，动态地保存起来建立策略规则表，分析识别表中的各个连接状态信息。由于在安全性能上有较大程度的提升，而且规范了网络层和传输层行为，所以状态防火墙又被称作第三代防火墙技术。

如图 2-5 所示。状态检测技术是在不影响正常通信前提下抽取数据流中的数据进行检测，解决了包过滤技术的不灵活性和代理技术的局限性。

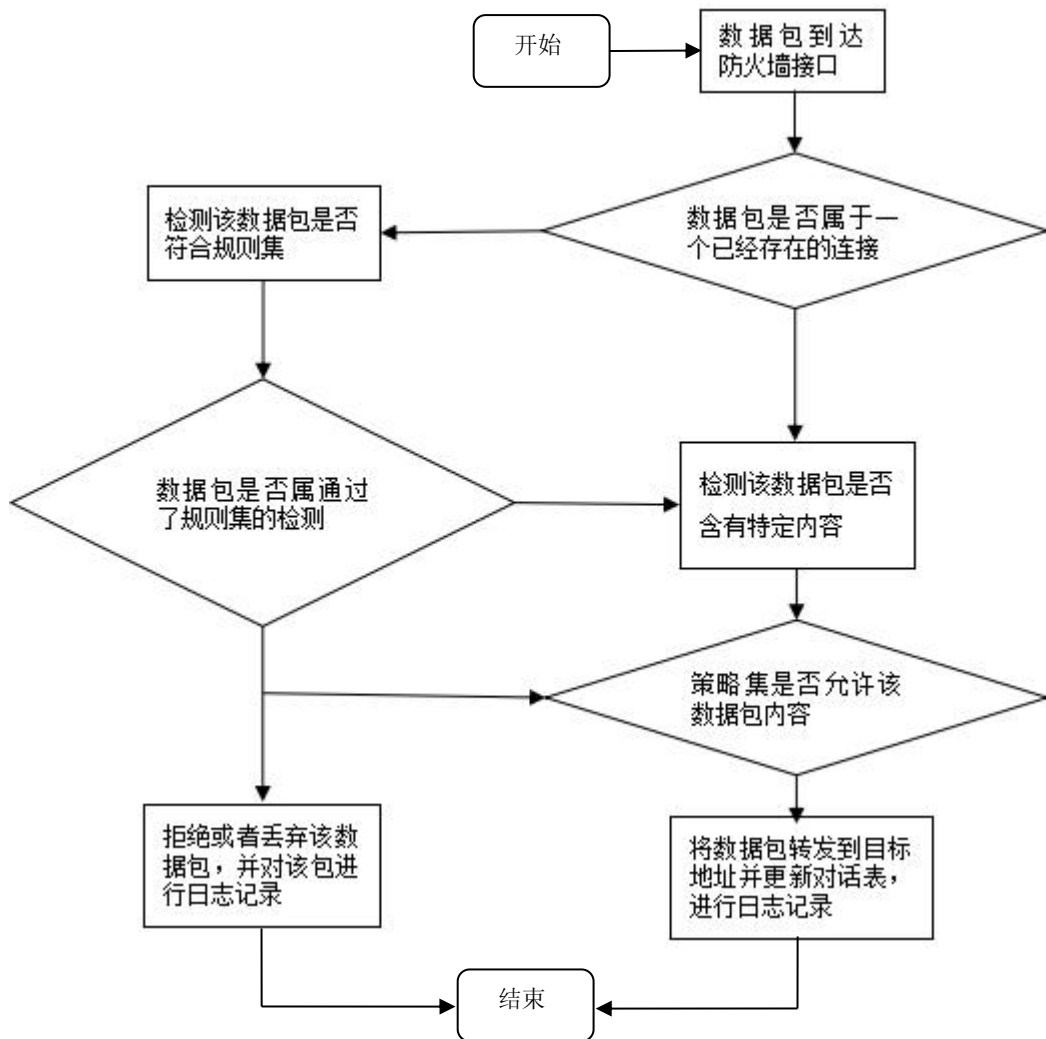


图 2-5 状态检测逻辑流程

根据防火墙分类总结以下功能：

(1) 强化安全策略的特点，有效有效地记录、监控、隔离器网络上的异常活动，同时具有审计和记录的功能。

(2) 划分与隔离不同范围和区域的网络安全边界的，实现定点监控每个主机服务器，一方面保护内网正常运行，隔离开网络中一个网段与另一个网段；另一方面防止外网的黑客等人为了的恶意攻击，是安全策略的检查站。

(3) 之所以需要防火墙架设在内外网之间的目的就是控制数据流的详细操作过程，针对数据流中的非法活动行为进行实时监控报警，作出全面的数据审计和日志记录。

2.1.3 防火墙存在问题

当前网络日趋严峻的安全形势下，防火墙并不能够解决全部的网络安全问

题，防火墙自身也存在很大的不足：

(1) 其固有的设计缺陷即“防外不防内”，如果内网中的用户恶意攻击或者通过后门、漏洞入侵破坏网络，将导致不堪设想的后果。

(2) 复杂分布式的网络黑客恶意入侵等带来繁杂不绝的攻击行为。防火墙虽然有一定的阻断外部攻击的能力，但是无法找到和阻击攻击源。

(3) 在判断和审查数据流的过程中，由于要分析判断、处理流经防火墙的每一个数据包，碰见某些流量大、并发请求多的特殊情况下，很容易导致拥塞，网络瘫痪。因此防火墙在一定程度上降低了数据流的处理速度同时也影响了网络性能。

(4) 防火墙无法处理如病毒、木马等，更是无法防止病毒的传染和扩散。

(5) 防火墙由软件或硬件独立实现，也有软硬件组合而成，无论是软件还是硬件其本身也会导致故障。

(6) 防火墙的功能实现中的各种规则和策略都是在收到攻击入侵之后由网络安全人员根据入侵特征而设计的系列防范策略措施，因此防火墙在未获取和收集入侵特征前提下不能够实现主动检测和防御功能。

2.1.4 防火墙发展方向

防火墙作为网络安全领域的第一道屏障，其市场占有率最大，技术也相对比较成熟。当前，在网络安全问题被各国高度重视和采取措施的同时，众多安全技术中，防火墙可谓是一棵经久不衰的常青树，在国家的 2009-2019 网络安全十年战略规划中，“下一代防火墙”的定义被首次提出，它应实现更多高级应用功能，并逐步走向普及。

(1) 智能云技术

在传统防火墙所具备的包过滤、路由、认证和加密、日志记录、支持网管、VPN、NAT 等功能以外。根据《中国下一代防火墙发展趋势研究》白皮书还明确提出：未来的下一代防火墙会趋向于更安全、更智能、更高速，同时功能完善和强大实现真正的云计算及大数据分析技术。

(2) 应用识别技术

应用识别技术三大核心即：深度包检测、深度流检测和会话关联检测是。深度包检测在技术实现上较为原始简单，主要实现单个报文中的明显应用特征进行匹配，但应用还是较多的。

(3) NGFW 与 UTM 对比

NGFW 与 UTM 在提供全面的安全防护保障。

(4) 云安全技术

随着近几年黑客变得越来越“企业化”和“规模化”。全数字化引领的技术环境的动态变化让依赖某单一防火墙技术完全无法达到现阶段的安全防御水平。云安全服务的发展给硬件防火墙提供了全新的发展机遇。云安全技术在提供更高的可视性、更高的机动性和更强的保护措施的同时为用户节省更多成本。

(5) 分布式防火墙

作为引领防火墙潮流的分布式防火墙 DFW，在新的安全体系结构下展示其自身优势。同时还弥补了传统防火墙结构上的不足和技术上的缺陷。用来设置网络保护障碍并放置在网络的任意网段的交界和接口位置，实现了一个多层次、多协议，内外皆防的综合立体的防御体系。

2.2 入侵检测

入侵检测系统（IDS: Intrusion Detection System），作为网络安全措施中的一种主动自我防护和避免被外界攻击的一种防御手段。它是在防火墙通常不能实现面对主动和实时的入侵检测功能方面进行技术填补。一般定义为识别为被授权使用的计算机系统和确定授权使用系统但却滥用的过程。IDS 作为预防黑客攻击的常用技术手段之一，它是通过收集并分析网络数据流中若干关键节点的信息活动特征来识别网络其它活动是否违反安全策略的行为。IDS 基本功能结构如图 2-6 所示。

对于 IDS 的核心问题是数据分析技术，包括建立数据库并完成原始数据的共享、归类、协调、识别及各种类型的深度分析，挖掘数据中具体共同行为的模型和算法，用于区分识别行为的合法性。

IDS 具体选择哪种数据分析技术，直接决定系统的检测能力和效果。

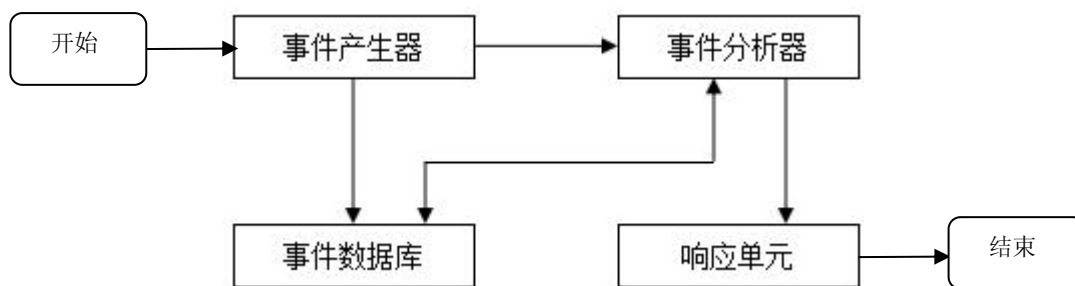


图 2-6 入侵检测系统基本流程

IDS 技术属于积极主动的入侵防御技术，IDS 具有防火墙相似的内部检测行

为活动、外部阻击和实时保护功能。所以，其特点之一是不影响网络性能。入侵检测系统 IDS 中最核心的问题技术就是对不同网段内的数据流进行有效的数据分析，包括对原始数据的同步、整理、组织、分类以及各种不同类型的精细分析，提取其中所包含的系统活动特征或规则，用来判断网络活动行为中的正常行为和非正常行为。

调用哪种数据分析技术即相应的策略规则，直接决定了 IDS 的检测能力和效果。据统计显示：IDS 按检测策略分类分为十二大类，其中又细化分类为 1500 种入侵行为规则，如常见行为规则：TCP、FTP、UDP、ICMP、IPX、HTTP、Telnet、SMTP、NFS、rsh、DNS、POP2、POP3、IMAP、TFTP、Finger、SSL、NETBIOS 等协议规则。因此，IDS 是防火墙技术的有益补充。

入侵检测通过以下功能来实现安全防护^[10]：

- (1) 设计数据模型和算法。
- (2) 监听和分析日常行为活动。
- (3) 识别已存在模型并主动应对。
- (4) 统计分析异常行为活动。
- (5) 分析系统中数据文件的整体特征。
- (6) 审计日志，判断安全策略。

IDS 在网络安全防御过程中不但可以辅助不同用的实时掌握系统的日志变化情况，还能够给网络安全策略的制订提供说明指导，IDS 部署方案如图 2-7 所示。

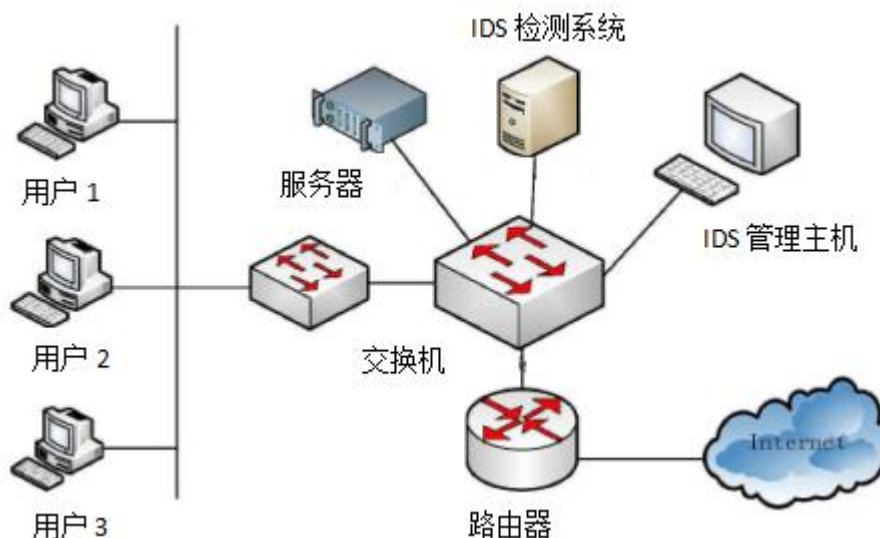


图 2-7 入侵检测部署结构

2.2.1 入侵检测系统分类

IDS 是一个对网络数据流中进行即时监控的一套软硬件设备。根据检测对象（数据信息检测来源）分类可分为：

（1）主机型入侵检测。

（2）网络型入侵检测。

按检测方式方法分类可分为：

（1）异常入侵检测。

（2）误用入侵检测。

IDS 不同系统分类如图 2-8 所示。

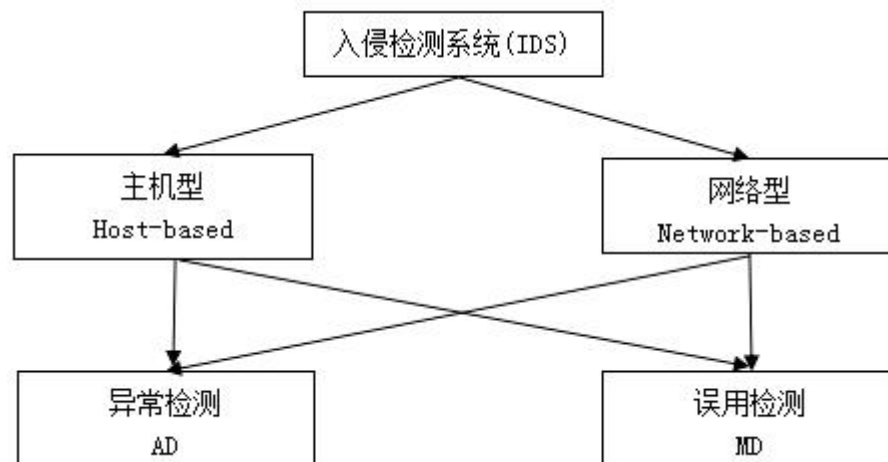


图 2-8 入侵检测系统分类

根据数据源的不同：HIDS 能够在某一个具体的单台主机上提取审计记录等数据源进行比较和分析。NIDS 则从网络环境中提取相关数据作为分析的数据源。

通常情况下 HIDS 只能侦听一台主机，而 NIDS 却能够同时完成侦听该网段内若干台主机。

（1）基于主机型(HIDS)

HIDS 运行在检测目标的主机上，通过策略智能分析和判断该主机的系统工作进程同时审计系统日志。如果判断该主机有非常规活动行为（常规特征或违反统计日志规则），HIDS 就会执行切断网络或者报警响应等措施。

HIDS 的优点：

- a.实施范围可控制性，硬件设备缺乏的条件下，入侵检测节省了人力物力；
- b.复杂度和误报率较低；
- c.检测目标的针对性强。

HIDS 的缺点：

- a.主机分散广，安装的设备太多导致系统效率低下，同时升级也收到影响；

- b.检测的规则和日志更新速度慢,无法动态检测最新的入侵行为;
- c.监控的对象范围较小,除了检测单机自身,其他网络对象都无能为力。

HIDS 基本流程如图 2-9 所示。

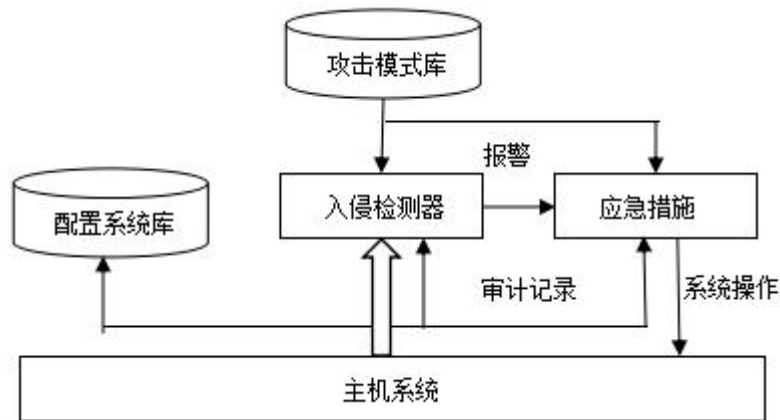


图 2-9 HIDS 流程图

(2) 基于网络型 (NIDS)

相对于 HIDS 数据源而言, NIDS 的数据源来自网络环境。该系统被设置在中央的网段上监测复杂的数据包,对数据包进行分析判断, NIDS 通过网络监视和抓取网络数据流中的数据和信息完成特征分析来实现防御网络入侵的。

具有较强的数据抓取和分析能力是 NIDS 的典型特征。在抓取网络数据包进行日志规则分析匹配,若是和系统预设的内部日志规则吻合, HIDS 则判断是合法,否则 HIDS 报警响应为非法入侵,严重情况下 NIDS 甚至切断网络连接。

NIDS 部署如图 2-10 所示。

NIDS 的优点:

- a.检测范围广,入侵攻击响应及时准确;
- b.不受限制,超越单台主机的配置和硬件环境;
- c.相对其它安全设备来说发生故障后业务方面影响小;
- d.由于网络环境的优势, NIDS 在安装上和更新上效率高。

NIDS 的缺点:

- a.检测网段范围不广,只能检测本网段的数据通信链路;
- b.检测目标范围小,检测方法和特征分析较为陈旧和固定;
- c.检测的网络数据源的内容多面积太大,导致监听和分析效率低,响应滞后;

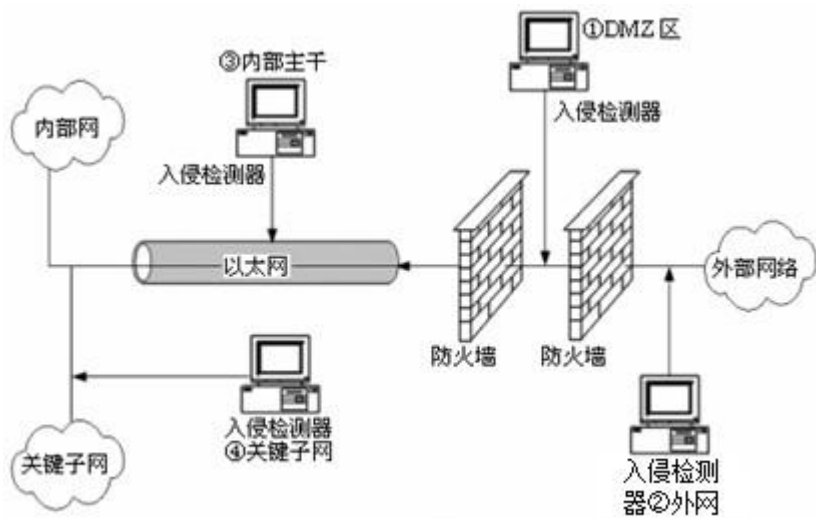


图 2-10 NIDS 部署模型

IDS 按不同检测方法分类主要可分为：异常检测（AD）和特征检测（SD）两类。通过下表介绍常用的特征检测和异常检测，AD 和 SD 常用方法如表 2-1 所示。

表 2-1 AD 和 SD 常用方法

类别	方法	描述
特征检测	模式匹配法	通过把收集到的信息与网络入侵和系统误用模式数据库中的已知信息进行比较，从而对违背安全策略的行为进行发现。
	专家系统法	把安全专家的知识描述为相应的规则，并存入知识库，然后使用推理算法实现检测。
	基于状态转移分析的检测法	将攻击看成一个连续的、分步骤的并且各个步骤之间有一定的关联的过程。在网络中发生入侵时及时阻断入侵行为，防止可能还会进一步发生的类似攻击行为。
异常检测	基于贝叶斯推理检测法	在任何给定的时刻，测量变量值，推理判断系统是否发生入侵事件。
	基于特征选择检测法	从一组度量中挑选出能检测入侵的度量，用它来对入侵行为进行预测或分类。
	基于贝叶斯网络检测法	用图形方式表示随机变量之间的关系。通过指定的与邻接节点相关一个小的概率集来计算随机变量的联接概率分布。

基于模式预测的检测法	事件序列不是随机发生的而是遵循某种可辨别的模式是基于模式预测的异常检测法的假设条件，其特点是事件序列及相互联系被考虑到了，只关心少数相关安全事件是该检测法的最大优点。
基于机器学习检测法	是根据离散数据临时序列学习获得网络、系统和个体的行为特征，并提出了一个实例学习法 IBL，应用 IBL 学习技术和一种新的基于序列的分类方法，发现异常类型事件，从而检测入侵行为。
数据挖掘检测法	将数据挖掘技术应用于入侵检测中，可以从审计数据中提取有用的知识，然后用这些知识检测异常入侵和已知的入侵。
基于应用模式的异常检测法	根据服务请求类型、服务请求长度、服务请求包大小分布计算网络服务的异常值。通过实时计算的异常值和所训练的阈值比较，从而发现异常行为。
基于文本分类的异常检测法	将系统产生的进程调用集合转换为“文档”。利用 K 邻聚类文本分类算法，计算文档的相似性。

(1) 异常检测 (AD:Anomaly Detection)

AD 是根据用户正常行为或活动状况规律建立的一个模型（活动简档）。AD 将其与当行为活动行为相比对，分析出该行为的模型规则，即可判断该活动是否存在攻击行为。

常用的 AD 统计模型为：马尔柯夫过程模型。

AD 优点：

- a.系统可以检测系统未知攻击；
- b.漏报率极低。

AD 缺点：

- a.模型一旦建立，后期更新较为困难；
- b.入侵者若分析得到模型算法和检测规律后，入侵攻击的隐蔽性大大增强。

AD 系统则无法应对带来入侵破坏；

- c.误报率却极高。

异常检测系统模型如图 2-11 所示：通过网络数据日志的检测分析，判断入侵行为的是否符合数据库中的正常行为描述，通过动态的更新行为描述的规则建立新的描述存储到描述库中。

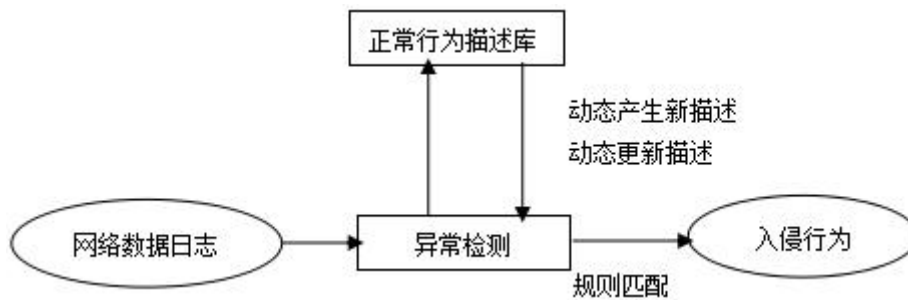


图 2-11 异常检测系统模型

（2）特征检测（SD:Signature-based Detection）

特征检测也叫误用检测（MD:Misuse Detection）。SD 检测入侵的行为活动是否匹配现有的安全策略模型。SD 能够成功检测到记录在册的策略模型或者行为规则，却不能够准确判断当前的入侵方法和行为，在响应报警上明显滞后。

相似于计算机病毒的检测方式，如何构建正确合适的规则模型既能够描述外来的非正常行为活动特征模型，同时不影响正在运行的合法行为活动，明确入侵行为和正常行为它们之间的特征区别。异常检测系统模型如图 2-12 所示。

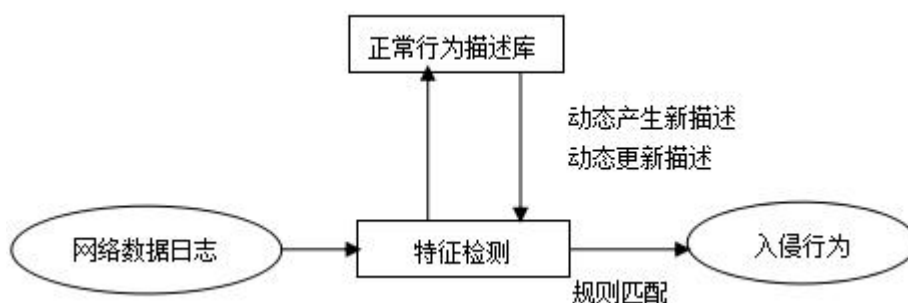


图 2-12 特征检测系统模型

SD 是质化的检测方式，那么 AD 则是量化的入侵检测方式。常用的检测技术为有模糊聚类、简单模式匹配（Pattern Matching）、基于聚类模型、专家系统、神经网络、免疫原理、遗传算法等。

2.2.2 入侵检测存在的问题

网络技术更新不断发展的具体。入侵技术的与时俱进应该是当前首要解决的问题：

（1）自适应能力差

网络环境的多变复杂形势下，由于网络防御技术的发展同时变得错综复杂。在传统的IDS在设计之初开发人员未曾估计到趋势化发展的网络方向，随着网络

应用的变化而网络上的数据也在发生日新月异的变化,黑客等各类入侵者进行网络安全破坏攻击过程中通常不会按常规的思维模式和单一的攻击方式方法达到入侵其目的,或在攻击初期掩盖其入侵的真实动机。这就说明了系统不能根据环境和数据源的变化自适应的智能修改检测模型。因此,实现一种更先进的、智能动态的、高效协同合作的IDS机理以适应不同对象环境的迫切需要。

(2) 缺乏准确定位处理机制

随着入侵技术的分布化发展,各种复杂的分布式入侵方式是网络攻击方式中较多用的威胁方式,单机入侵行为已经消退,DDOS在短暂时间内可攻击网络及系统导致全面系统崩溃。

(3) 误报和漏报

网络速度发展迅猛,而IDS的速度太慢,因此导致数据的错误分析和遗漏抓取。入侵主体对象的隐蔽性和间接化,入侵者使用相应的技术隐藏攻击主体相应信息,导致检测系统无法抓取有效数据信息进行模型比对。

(4) 攻击对象的转移。IDS技术通常使用的都是系统预设模型、特征模型的工作原理。黑客的攻击方式方法上在很大程度上优先于IDS模型,这样就直接导致相关的检测系统被动更新。

2.3 入侵防御

入侵者的攻击技术的升级和网络入侵案例数量的不断上升,网络安全的防御工作难点是缺乏预见性和可视性,导致用户对入侵行为毫无准备。可见当今的入侵技术基本超过了防御技术的响应能力。传统的安全技术弊端日渐凸显还有陈旧和淘汰的防御基础设施以及系统无法阻止入侵者的各种攻击能力。

为了改变这一现状,IPS发挥了有利的技术优势作用。

相对于传统的被动防御技术防火墙和IDS而言,IPS是集成了目前传统技术中的IDS和防火墙技术之长的系统。IPS不仅具备前面所述的侦测与预警的功能、响应与管理的功能,还具备了主动丢弃阻断网络攻击源等强大功能。可以说IPS在很大程度上是IDS和防火墙的综合升级技术和功能有效的补充。

2.3.1 入侵防御系统的分类

IPS同IDS系统类似,按数据源分为主机型和网络型。

(1) 基于主机的入侵防御系统^[1](HIPS)

HIPS实现针对主机上发生行为活动的具体控制, 不仅能检测入侵的行为活动, 还可以通过特定响应方式实施阻止攻击行为。HIPS是通过安装软件代理程序在主机或服务器上, 紧密结合操作系统以保护网络入侵操作系统和应用程序^[8]。

(2) 基于网络的入侵防御系统(NIPS)^[4]

通常是在线完成安装, 通过实时监测网络流量, 提供对网络系统的安全保护。通常NIPS设置在DMZ区的前面和边界防火墙的后面, 同时构建在内部服务器的前面以及端点的后面, 因此相应位置的流量必须完全流经NIPS, 由NIPS决定是否能够通过。

NIPS采用的是在线连接方式, 入侵行为如果被NIPS确定, 则立即复位会话。同时切断网络连接, 而不仅需要具备很高的性能, 以免成为网络的瓶颈^[12]。

NIPS在技术层面上加强和更新了目前NIDS所有的成熟技术, 特征检测具有准确率高、速度快的特点, 是目前广泛应用的技术, 如Snort和NFR。

2.3.2 入侵防御技术存在的问题

IPS具有动态实时监测和主动型防御特点。总结这一技术优势主要体现在如下几个方面:

(1) IPS实现了IDS技术和防火墙技术的优势融合。既拥有IDS实时检测的功能, 又保留了防火墙技术的在线安装功能。

(2) 先进的检测技术(ADT:Advanced Detection Technology)。可谓是IDS的升级版, 它采用了并行处理检测和协议重组分析技术大大提高入侵检测的质量和效率。

(3) 自我学习与自适应能力(SSA:Self-study & Self-adaptation Ability)。SSA即在网络数据流中抓取和匹配数据规则库, 挖掘有效数据信息建立新的安全策略模型。

然而, 任何一种安全技术都不是完美的, IPS技术亦如此, 总结IPS存在以下不足:

(1) 单点故障率较高。

(2) 误报率(False Positive)、漏报率(False Negatives)较严重。

(3) 性能瓶颈问题有待解决。

2.4 分布式技术

通常是指在不同地理位置的若干台计算机支持下的协同工作系统(CSCW: Computer Supported Cooperative Work)称之为分布式系统。

在这个分布式系统中,能够实现跨地域及跨系统的访问处理数据的需求。该技术在不同的硬件和软件环境前提下,实现了有效的数据通信、发挥了其可扩展性。分布式系统的特点:

分布式系统是由分布在不同地理位置、独立的、通过分工协作、连接在一起的计算机组成的。

分布式系统环境下的资源从拓扑结构上看属于某个特定的主机,完全可以同步访问其它主机。

分布式系统优点如下:

- (1) 共享资源: 在网络环境下才能真正实现分布式的优势。
- (2) 多用户参与: 实现了分布式环境下的多用户协同处理。
- (3) 可扩展性: 分布式系统由一个个的子系统组成, 根据具体情况每个子系统又是一个独立的功能模块。

- (4) 跨平台性: 在不同的软硬件平台实现数据通信和资源共享功能。

分布式系统的缺点如下:

- (1) 安全性: 网络连接子模块多而且复杂, 导致管理方面的安全性较低。
- (2) 复杂性: 分布式系统本身就是由多种软硬件平台以及技术实现, 导致了开发以及测试维护的复杂性。
- (3) 易错性: 分布式系统由许多相对独立的子模块组成的, 和一个整体的应用程序相比, 稳定性较差。

2.5 本章小结

在目前的实际应用中, 防火墙、入侵检测系统 IDS、入侵防御系统 IPS 等安全系统被安装在不同的硬件平台上。导致系统设备的多样性和复杂性, 既浪费了有限的资源又产生冲突。现有的 IPS 只是利用了防火墙的网络防护控制功能优势、同时结合了 IDS 的检测功能的部分技术。但它的出现又带来了新的缺陷如性能瓶颈, 误报与漏报率问题等。

本章阐述了传统领域的安全技术对比。分析探讨了 IPS 相关知识, 总结了 IDS 和 IPS 的具体分类以及存在的问题进一步设想了一代安全技术的发展趋势。做到完整部署安全防御工程中的“第一道”和“第二道”战略防线。

第3章 系统总体设计

网络环境复杂而多变，单一的入侵防御技术无法全面的构建安全解决方案，一种协同检测、联动合作防御的安全模型应运而生。

3.1 系统设计目标

3.1.1 现有网络安全模型介绍

作为一个长期持续性研究对象，网络安全是一个与时间关联实时变化的动态。网络是否处于安全状态取决于某个特定的时间和特定的安全策略下；时代变迁，影响着网络环境的变化，相应的网络安全体系也发生变化。陈旧的安全体系和策略无法继续适应新网络环境。因此，复杂多样化的网络环境就需要智能动态、自适应的安全模型^[3]。

最早的安全模型 P2DR，它的组成模块分别是策略（Policy）、防护（Protection）、检测（Detection）和响应（Response）的首字母。模型的指导思想是构建一个具体操作系统访问控制、防火墙、数据加密，数字签名等功能的完整的安全体系。P2DR 模型进行有效分析和规范合理设计的安全策略，最终建立一套综合立体的安全体系。如图 3-1 所示。

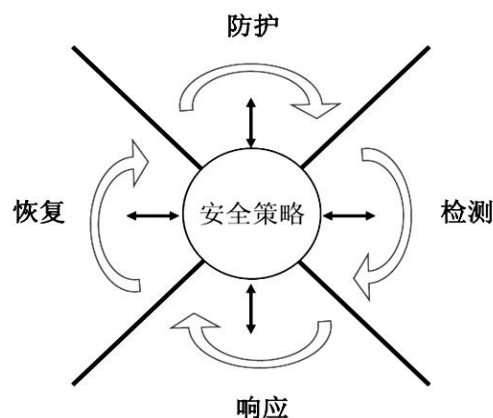


图 3-1 P2DR 安全模型

目前普遍采用的 PDRR 模型^[19]源自美国国际互联网安全系统公司 (ISS) 在 1995 年提出的自适应网络安全模型 (ANSM: Adaptive Network Security Model)。它是在 P2DR 模型的基础上发展而来。

由图 3-1 模型中可见模型的核心部分即安全策略,它为整个网络安全的依据。外围的保护、检测、响应都是围绕安全策略进行实施的^[12]。建立安全策略主要内容包括了策略模型的设计、评估和报警等。设计可行的策略模型取决于对安全策略的学习能力。

PDRR 模型也叫做“信息安全保障”。^[16]它主要包括:防护、检测、响应、恢复等四个部分。

PDRR 的英文全称分别是: Protection、Detection、Reaction、Restore。PDRR 安全模型如图 3-2 所示。

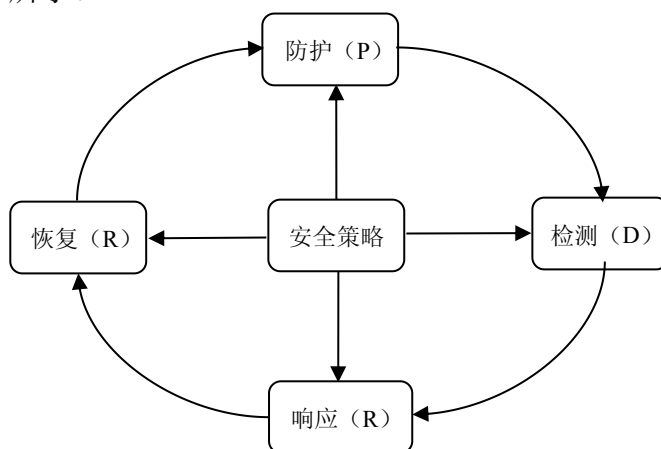


图 3-2 PDRR 安全模型

网络安全贯穿于整个 OSI 网络模型中,针对 TCP/IP 协议规则可见网络安全应贯穿于 OSI 的四个层。PDRR 模型中最重要的部分就是防护 (P),它是预先阻击入侵的先决条件。该模型是以动态形式运行与网络系统中,使用灵活多变的方法进行检测各种入侵,发现入侵时立即判断和修改安全策略模型来保护系统的安全。

PDRR 模型主要存在的问题是:

- (1) 控制的过程性相对简单。
- (2) 动态性检测功能相对较差。

3.1.2 动态防御模型

根据不同时期不同环境下的网络安全模型^[19]比较分析，早期以防护为主的静态防御技术逐渐淘汰。然而动态防御技术^[20]的需要地位得到了显著提高，分析在前两个动态安全模型 P2DR 和 PDRR 可以实现以下功能如表 3-1 所示：

表 3-1 动态综合防御各模块功能

类别	模型要素	功能描述
动态综合防御模型	策略	分析系统需求，制定主动防御的安全策略。该策略说明防护、检测、响应等的联动关系以及处理方法，是实施网络安全动态防御的指南
	防御	保障数据的保密性、完整性、用性等。将相关安全技术分类，建立防护技术体系
	检测	动态检测入侵及安全威胁，理解信息系统当前的安全状态。检查系统安全漏洞，实时检测入侵，评估入侵的威胁程度，及时响应
	响应	主动响应危及系统安全的入侵事件，防止危害蔓延和扩散；如果攻击造成了一定后果，及时恢复，保障系统提供正常服务
	反击	在必要的情况下，对攻击者进行跟踪追击或者入侵诱骗，获取攻击者详细的资料以备研究或取证

3.1.3 分布式防御模型

模型从整个拓扑结构分析如图 3-3 所示，分布在不同地域的子网根据防御安全系数的不同而采用不同的安全防御措施。分布式地保护各子网的安全，在物理结构上，划分不同的区域位置，然后分而治之^[27]。

分布式 IDS 技术除了包含传统的安全技术以外，还包括 IPS 的防御功能和 IDS 响应功能，可以总结分布式入侵防御模型具有如下特点：

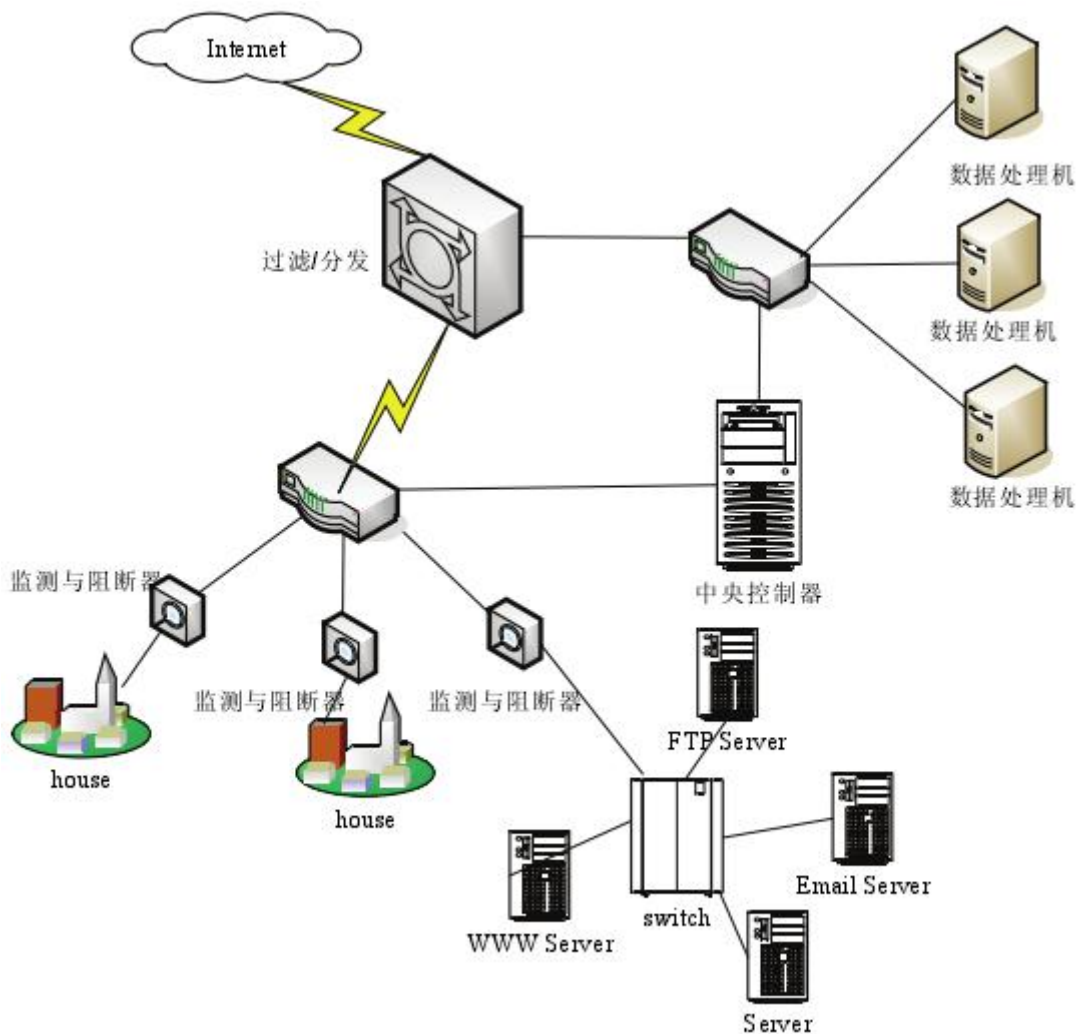


图 3.3 分布式入侵防御模型

（1）实时性

实时动态地监测和响应分布在不同地理位置上的网络通信。

（2）分布式

分布式拓扑结构的网络都部署了不同的子网和大量的交换机、路由器、服务器、工作站等网络设施。分布式动态防御体系可以实现共享数据资源。

（3）可信度

针对特定的行为活动设施相应的防御方案和检测算法，将入侵行为的误报与漏报控制很小的范围内。

（4）协同性

一方面实施多元化入侵防御系统融合技术，将所有安全模块（包括防火墙，IDS，IPS，路由器及交换机等）采用集中管理的同事使用分布式检测，动态策略管理中心统一指挥和协同各个独立的模块。模块之间是各自相对独立的子模块，在需要的情况下又能够实现统一调度和协同工作。

（5）化整为零

分布式防御系统采用了分而治之的思想。实现了集中式安全防御技术上的缺陷和瓶颈问题。各子防御模块采用来自于不同的安全防御体系和产品。为此大大提高了该系统的扩展性。

3.2 系统框架

根据整个系统的功能模块的组成可见如图 3-4 中所示。在协同合作模块的功能结构中，有各类探测器收集抓取网络数据流中的有效信息进分析建模，归类给策略管理中心。在联动响应模块里面，入侵检测系统可以动态对接策略管理中心，进行策略规则的修改和更新，响应系统负责报告用户安全事件。而用户根据需要进行动态修改防火墙策略规则，一般情况下用户只需要使用控制台去辅助管理各网络断的规则库即可。

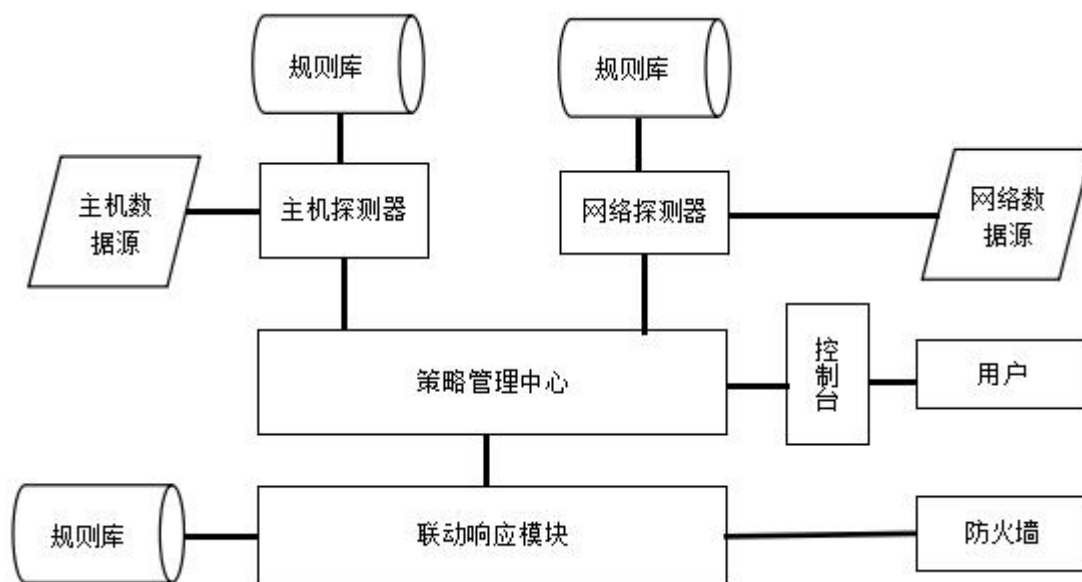


图 3-4 系统功能结构

3.2.1 数据处理流程

系统的结构信息流如图 3-5 所示。策略管理中心是整个系统技术的核心，每个单一的模块根本无法实现整个安全体系的保障，要做到立体的安全防护就需要每个模块发挥各自功能的基础上协同统一、互动合作的基础上开展防御工作。

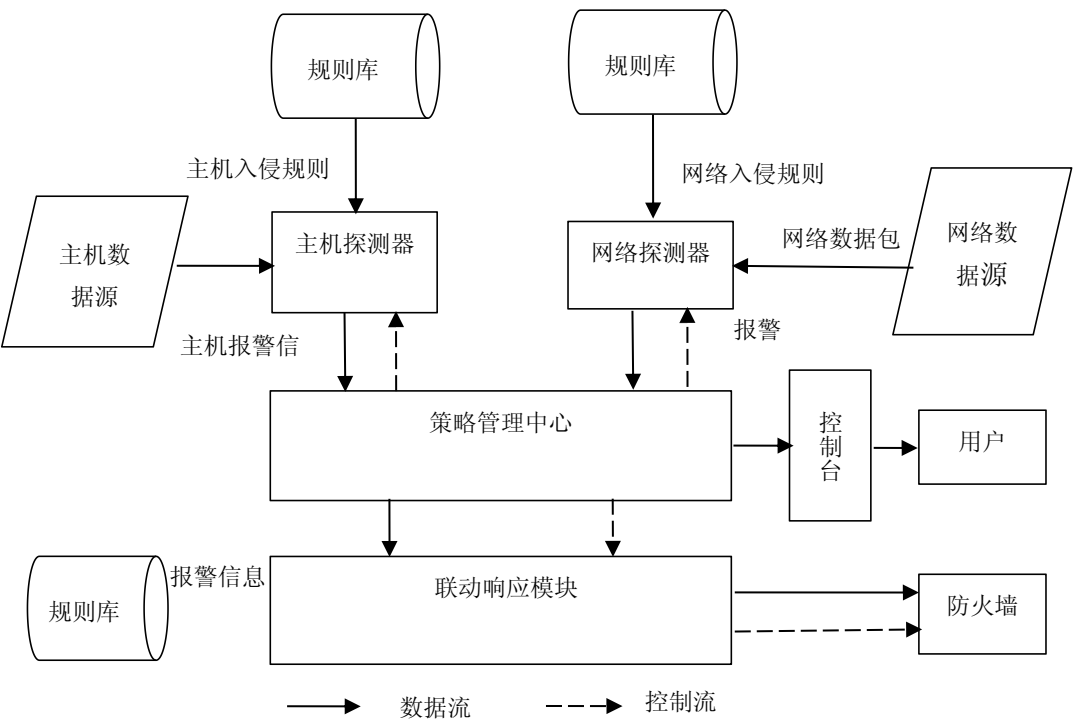


图 3-5 系统各模块间的信息流

表 3-2 描述了系统的数据处理流程如下：

表 3-2 系统数据处理流程表

系统对数据的处理	模块名称	数据处理流程表
	主机探测器	主机探测器接收主机数据源，获取主机日志信息后，从规则库中读取入侵规则，根据主机规则对主机日志进行分析，当检测到攻击后，按照统一的报警格式，向策略管理中心发送报警信息
	策略管理中心	网络探测器接收网络数据源，获取网络数据包后，从规则库中读取网络入侵规则，对数据包头及内容进行分析，对规则进行匹配。当检测到攻击后，按照统一的报警格式，产生网络报警信息并发送到策略管理中心
	控制台	策略管理中心接收到来自主机探测器和网络探测器的报警信息后，对各个探测器的报警信息进行关联分析，将报警信息传送给控制台，显示给终端用户，同时将报警信息保存到数据库，以供用户查询统计
	网络探测器	策略管理中心根据报警信息级别产生响应规则，发给动态响应模块
	联动响应模块	联动响应模块产生具体的防火墙规则，添加到其控制的具体防火墙中

3.2.2 数据控制流程

表 3-3 系统数据控制

系统对数据的控制	模块名称	数据控制功能描述
	控制台	用户通过控制台进行控制操作，向策略管理中心发送控制信息。
	策略管理中心	执行对控制信息进行分析，根据其控制对象转发给相对应模块。如果是主机探测器控制信息，则转发给对应的主机探测器；如果是网络探测器控制信息，则转发给对应的网络探测器；如果是防火墙控制信息，则转发给联动响应模块
	主机探测器	对于主机探测器，策略管理中心向主机探测器发送主机探测器控制信息，控制探测器开/关，执行规则更新以及相应的响应操作
	网络探测器	对于网络探测器，策略管理中心向网络探测器发送网络探测器控制信息，控制探测器开/关，执行规则更新以及配置文件等操作
	联动响应模块	对于联动响应模块，策略管理中心向联动响应模块发送联动控制指令，控制防火墙开/关，以及对防火墙规则进行添加、删除、更新等操作

3.3 系统体系结构

为了协同合作、动态防御功能的实现，就必须发挥系统整体功能结构的各个组成模块的充分协同合作的功能，使各种入侵风险降到最低程度。为此设计了如下图的级联式的系统原型体系结构，如图 3-6 所示。

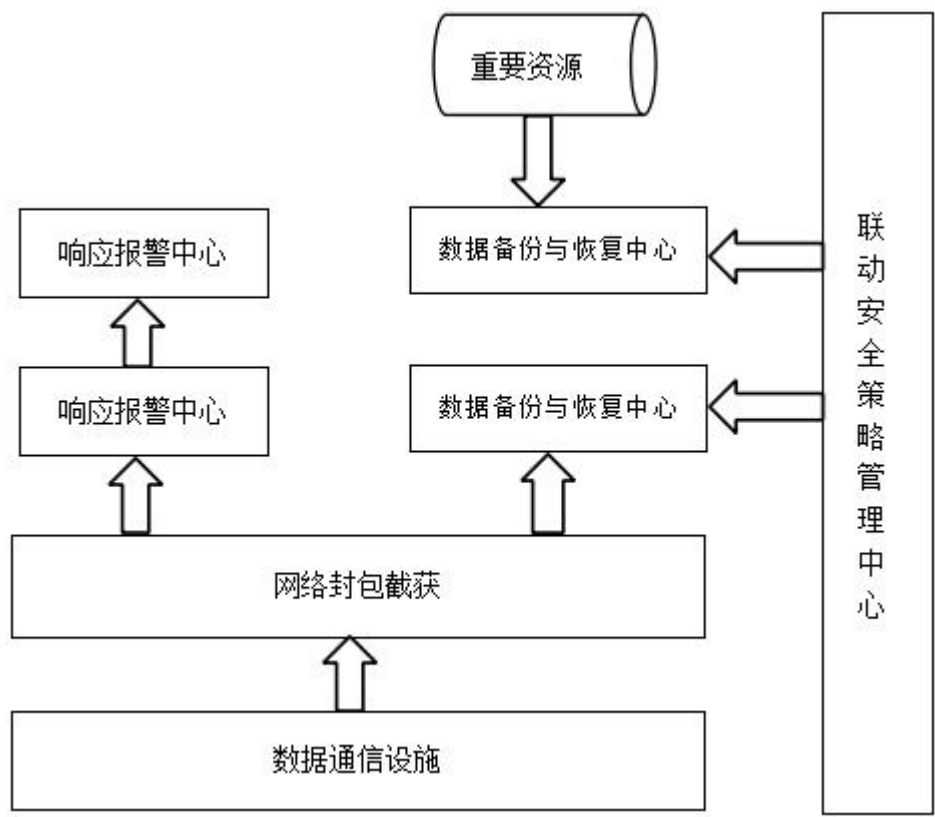


图 3-6 联动式体系结构

由图 3-6 模型的体系结构可见该具有如下表 3-4 功能特点：

表 3-4 系统组件功能描述

组件名称	功能描述
策略管理中心	负责协同、动态管理和防护、检测、分析和取证工作。
入侵防御中心	实时地保护信息系统不受实质性攻击的一种智能化的系统。
数据加密中心	使用了两种基于密钥的加密系统：对称的加密系统和不对称的加密系统实时地保护信息系统不受实质性攻击的一种智能化的系统。
响应与报警中心	针对入侵事件的响应可以分为被动响应和主动响应两种类型。在被动响应中，系统只报告和记录发生的事件；在主动响应中，系统阻断攻击过程或以其它方式影响攻击过程。
数据备份恢复中心	确保数据在任意情况下安全和（包括人工操作失误）具有完整的恢复能力。

3.4 本章小节

实施系统的总体设计的前提下首先概述现有的几种安全模型并分析其各自的优缺点。在此基础上提出了两种新的防御模型，即动态防御模型和分布式防御模型，根据其模型要求详细介绍了系统功能模块和数据处理流程等，最后设计了系统体系结构。

第 4 章 系统详细设计

本章继上一章后完成系统中的关键功能模块进行研究设计。

在网络环境下，控制台是实现整个系统详细部署的终端，每个模块在系统中的具体分工就作业如图 4.1 所示。防火墙就是控制台内网和 INTERNET 的一道隔离屏障。

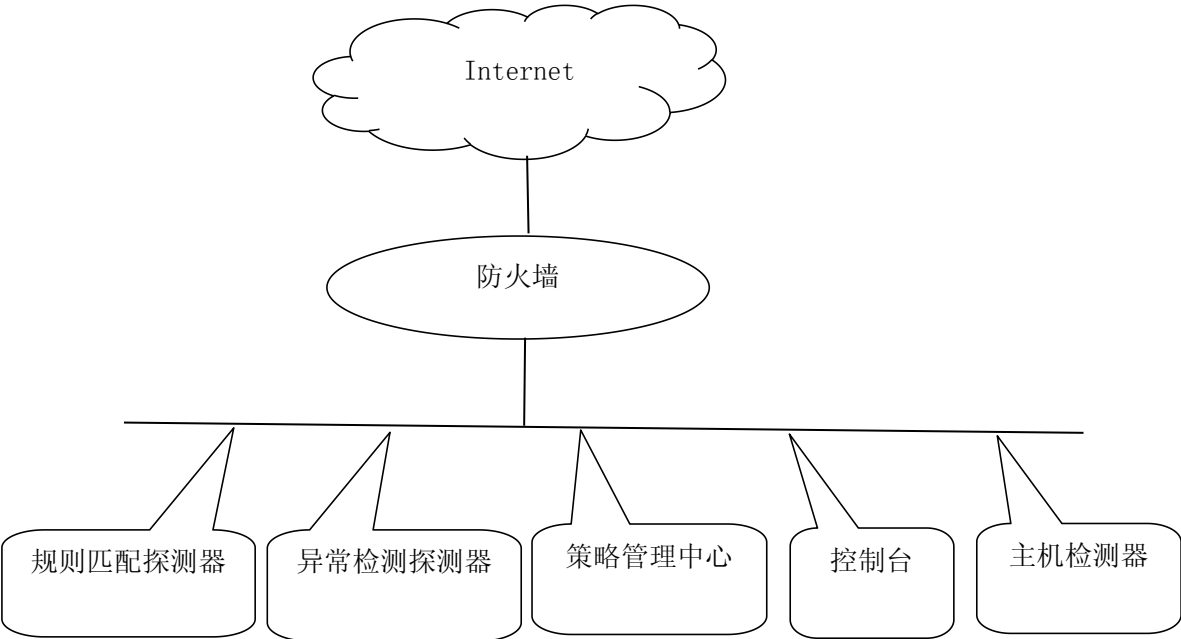


图 4-1 系统中各模块架构

4.1 分布式网络探测器

在上一章中已经初步介绍了系统各模块的功能作用。如网络探测器采用 IDS 中的 AD 和 MD 方法完成在网络中的数据包检测，发现异常及时报警并传递给系统中的策略管理中心作进一步处理。

4.1.1 网络探测器结构与功能介绍

分布式网络探测器^[12]组成及各部分信息交互如图 4-2 所示：

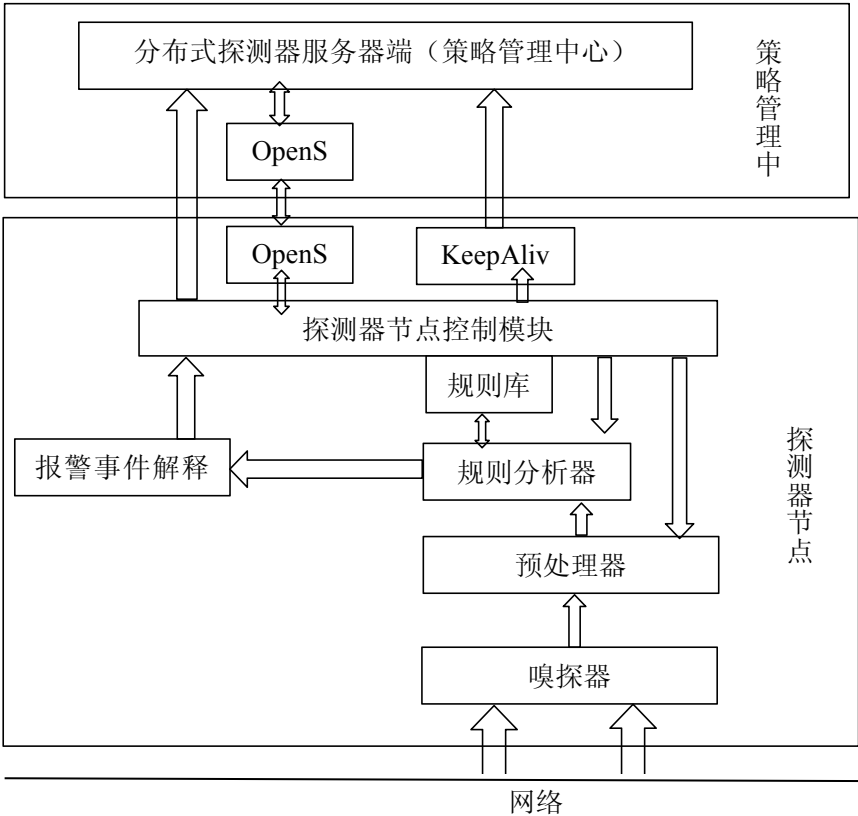


图 4-2 探测器的结构与信息交互

表 4-1 探测器组成模块功能介绍

模块名称	功能描述
数据收集模块	在网络中监听，捕获网络数据包，传递给数据分析模块。
数据分析模块	对获取的网络数据包进行过滤，统一数据格式并分析，然后传递给规则解析模块。
规则解析模块	根据匹配算法和规则库中的规则，对网络数据包及其其中的数据进行解析匹配，检测出其中的入侵信息，并转发给报警模块。
报警模块	按照既定的格式产生报警数据包，发送给策略管理中心。
探测器节点控制模块	接收策略管理中心发送的控制指令，对其进行解析，并执行相应控制动作。

4.1.2 规则匹配探测器

策略管理中心提取已设置检测模型和算法驱动规则匹配探测器实现 MD 的检测方法，比对算法库中的模型方法进行判断网络入侵。

如图 4-3 所示。

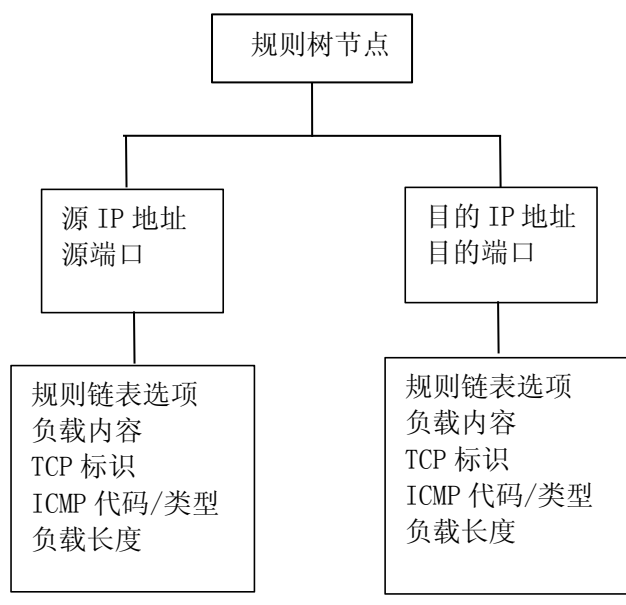


图 4-3 策略逻辑结构

4.1.3 异常检测探测器

异常检测（AD）一是基于模型的技术。异常是那些同模型不能完美匹配的对象。二是基于邻近度的技术；基于密度的技术；这些技术结合了自身的特点去探测网络异常行为，反馈给规则库建立异常模型。

在多达上百种的检测方法中，异常检测 AD 当前最流行的和实用性更强的基于模糊 C 均值聚类。

聚类在很大程度上可以有效的处理数据分类问题，在发展过程根据应用的方向的不同又提出了聚类划分算法。主要特点是他的应用领域广、设计思想灵活简单、结合数学模型基础较强等。

入侵检测 IDS 中的应用，目前在基于函数的算法中，FCM 应用较广和设计完善，一般情况算法可以分为两种：基于网格和基于模型。

模糊 C 均值聚类算法中关于虑属度的表示：

对象 x 隶属于集合 A 的程度的函数,一般记为 $\mu_A(x)$,其自变量范围是所有可能属于集合 A 的对象,取值范围是 $[0,1]$,即 $0 \leq \mu_A(x) \leq 1$ 。

其中的 $\mu_A(x)=1$ 表示 x 完全隶属于集合 A ,即传统集合概念中的 $x \in A$ 。一个定义在空间 $X=\{x\}$ 上的隶属度函数就定义了一个模糊集合 A ,或者叫定义在论域 $X=\{x\}$ 上的模糊子集 \tilde{A} 。对于有限个对象 x_1, x_2, \dots, x_n 模糊集合 \tilde{A} 可以表示为:

$$\tilde{A} = \{(\mu_A(x_i), x_i) | x_i \in X\} \quad (4-1)$$

和特征检测 (SD) 有了模糊集合的概念,一个元素隶属于模糊集合就不是硬性的了,在聚类的问题中,可以把聚类生成的簇看成模糊集合,因此,每个样本点隶属于簇的隶属度就是 $[0,1]$ 区间里面的值。

FCM 算法需要两个参数一个是聚类数目 c ,另一个是参数 m 。一般来讲 c 要远远小于聚类样本的总个数,同时要保证 $c > 1$ 。对于 m ,它是一个控制算法的柔性的参数,如果 m 过大,则聚类效果会很次,而如果 m 过小则算法会接近 HCM 聚类算法。

算法的输出是 c 个聚类中心点向量和 $C \times N$ 的一个模糊划分矩阵,这个矩阵表示的是每个样本点属于每个类的隶属度。根据这个划分矩阵按照模糊集合中的最大隶属原则就能够确定每个样本点归为哪个类。聚类中心表示的是每个类的平均特征,可以认为是这个类的代表点。

从算法的推导过程中我们不难看出,算法对于满足正态分布的数据聚类效果会很好,另外,算法对孤立点是敏感的。

聚类算法是一种比较新的技术,基于曾次的聚类算法文献中最早出现的 Single-Linkage 层次聚类算法是 1957 年在 Lloyd 的文章中最早出现的,之后 MacQueen 独立提出了经典的模糊 C 均值聚类算法,FCM 算法中模糊划分的概念最早起源于 Ruspini 的文章中,但关于 FCM 的算法的详细的分析与改进则是由 Dunn 和 Bezdek 完成的。

模糊 c 均值聚类算法因算法简单收敛速度快且能处理大数据集,解决问题范围广,易于应用计算机实现等特点受到了越来越多人的关注,并应用于各个领域。

算法描述,模糊 C 均值聚类算法的步骤还是比较简单的,模糊 C 均值聚类 (FCM),即众所周知的模糊 ISODATA,是用隶属度确定每个数据点属于某个聚类的程度的一种聚类算法。1973 年,Bezdek 提出了该算法,作为早期硬 C 均值聚类 (HCM) 方法的一种改进。

FCM 把 n 个向量 $x_i (i=1,2,\dots,n)$ 分为 c 个模糊组,并求每组的聚类中心,使得非相似性指标的价值函数达到最小。FCM 与 HCM 的主要区别在于 FCM 用模糊划分,使得每个给定数据点用值在 $0,1$ 间的隶属度来确定其属于各个组的程度。与引入模糊划分相适应,隶属矩阵 U 允许有取值在 $0,1$ 间的元素。不过,加上

归一化规定，一个数据集的隶属度的和总等于1：

$$\sum_{i=1}^c u_{ij} = 1, \forall j = 1, \dots, n \quad (4-2)$$

那么，FCM 的价值函数（或目标函数）就是式（6.2）的一般化形式：

$$J(U, c_1, \dots, c_c) = \sum_{i=1}^c J_i = \sum_{i=1}^c \sum_{j=1}^n u_{ij}^m d_{ij}^2, \quad (4-3)$$

这里 u_{ij} 介于 0, 1 间； c_i 为模糊组 I 的聚类中心， $d_{ij} = ||c_i - x_j||$ 为第 I 个聚类中心与第 j 个数据点间的欧几里德距离；且 $m \in [1, \infty)$ 是一个加权指数。

构造如下新的目标函数，可求得使（6.10）式达到最小值的必要条件：

$$\begin{aligned} \bar{J}(U, c_1, \dots, c_c, \lambda_1, \dots, \lambda_n) &= J(U, c_1, \dots, c_c) + \sum_{j=1}^n \lambda_j (\sum_{i=1}^c u_{ij} - 1) \\ &= \sum_{i=1}^c \sum_{j=1}^n u_{ij}^m d_{ij}^2 + \sum_{j=1}^n \lambda_j (\sum_{i=1}^c u_{ij} - 1) \end{aligned} \quad (4-4)$$

这里 λ_j , $j=1$ 到 n , 是（6.9）式的 n 个约束式的拉格朗日乘子。对所有输入参量求导，使式（6.10）达到最小的必要条件为：

$$c_i = \frac{\sum_{j=1}^n u_{ij}^m x_j}{\sum_{j=1}^n u_{ij}^m} \quad (4-5)$$

$$\text{和 } u_{ij} = \frac{1}{\sum_{k=1}^c \left(\frac{d_{ij}}{d_{kj}} \right)^{2/(m-1)}} \quad (4-6)$$

由上述两个必要条件，模糊 C 均值聚类算法是一个简单的迭代过程。在批处理方式运行时，FCM 用下列步骤确定聚类中心 c_i 和隶属矩阵 U [1]：

步骤 1：用值在 0, 1 间的随机数初始化隶属矩阵 U ，使其满足式（4-5）中的约束条件。

步骤 2：用式（4-1）计算 c 个聚类中心 c_i , $i=1, \dots, c$ 。

步骤 3：根据式（4-6）计算价值函数。如果它小于某个确定的阈值，或它相对上次价值函数值的改变量小于某个阈值，则算法停止。

步骤 4：用（4-4）计算新的 U 矩阵。返回步骤 2。

上述算法也可以先初始化聚类中心，然后再执行迭代过程。由于不能确保 FCM 收敛于一个最优解。算法的性能依赖于初始聚类中心。因此，要么用另外的快速算法确定初始聚类中心，要么每次用不同的初始聚类中心启动该算法多次运行 FCM。

4.2 主机探测器

本文设计的系统实现是将主机探测器安装在 server 上。因此，探测器功能是

基于 Linux 操作系统设计、对改主机完成侦听和分析异常入侵。其结构设计如图 4-4 所示。

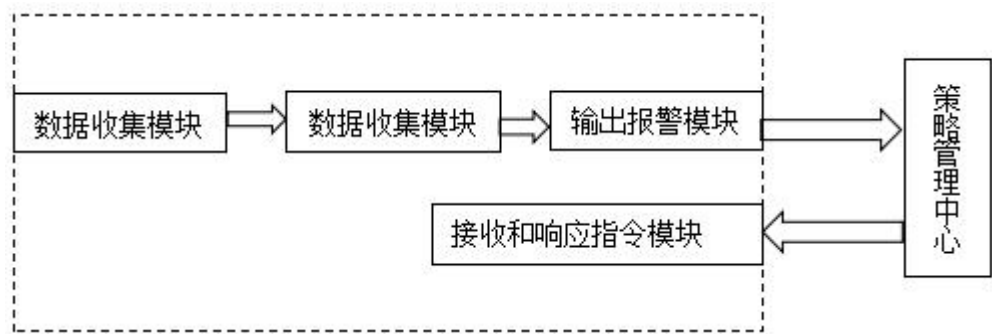


图 4-4 主机探测器的整体结构

4.3 策略管理中心

4.3.1 策略管理中心的模块设计

策略管理中心可以比喻为计算机中的中央处单元 CPU，功能也类似于 CPU，具备最高权限的管理和控制功能。具体模块包括了控制台功能模块及设计、主机探测器、网络探测器和防火墙的功能模块的设计。

各模块与策略管理中心协同交互的相关模块之间的对话如图 4-5 所示。

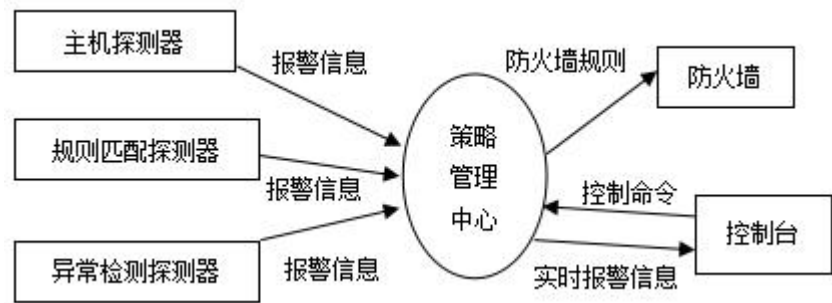


图 4-5 模块对话示意

在图 4-5 中进一步分析模块的核心部分即策略规则管理中心，它的作用如下。

- (1) 联动防火墙作业
- (2) 处理和存储异常信息
- (3) 收集探测器的报警信息

(4) 协同与控制台作业

策略管理中心的主要功能有：**a.**接收探测器的报警信息。**b.**将探测器报警进行处理（包括实时返回控制台报警，保存入数据库等）。**c.**与防火墙进行联动。**d.**接收控制台的控制指令控制以上功能。策略管理中心交互如图 4-6 所示。

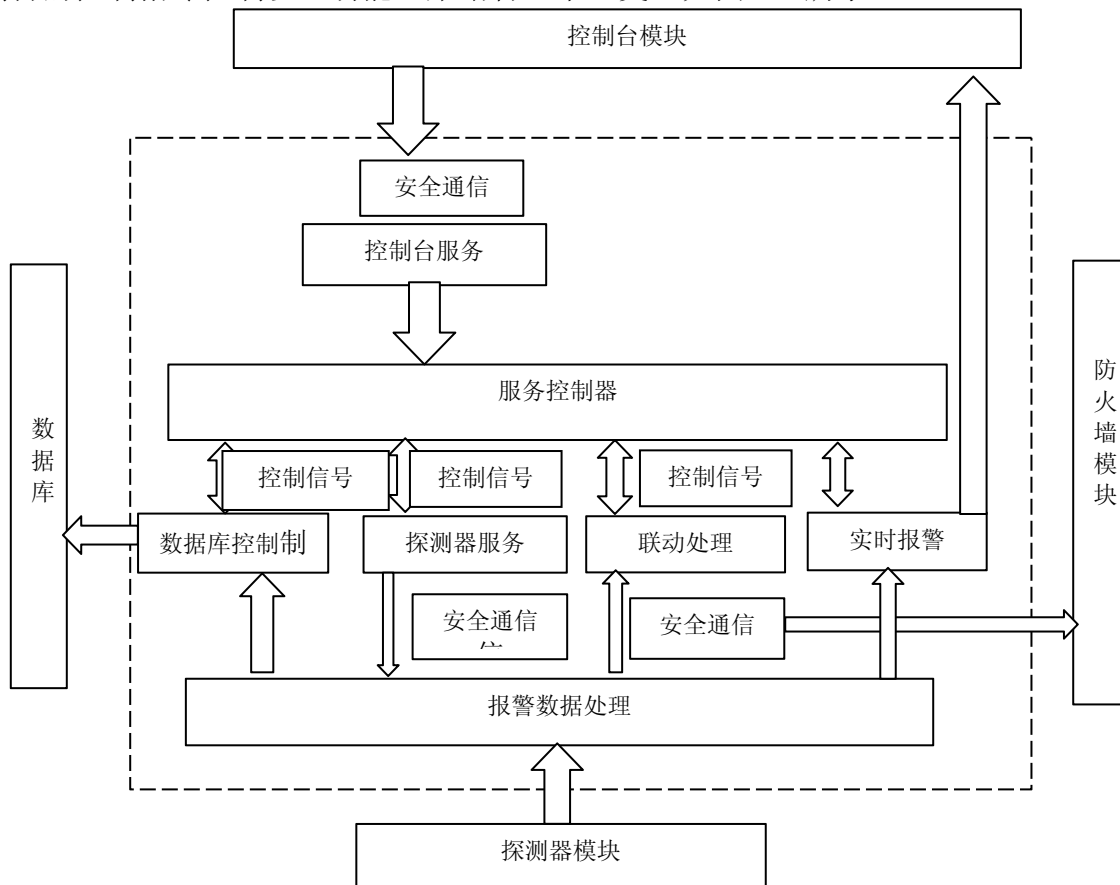


图 4-6 策略管理中心模块交互

4.3.2 探测器模块的设计

探测器服务模块在运行过程中主要是完成接收探测器响应的报警数据。该模块由两个部分组成，如图 4-7 所示。

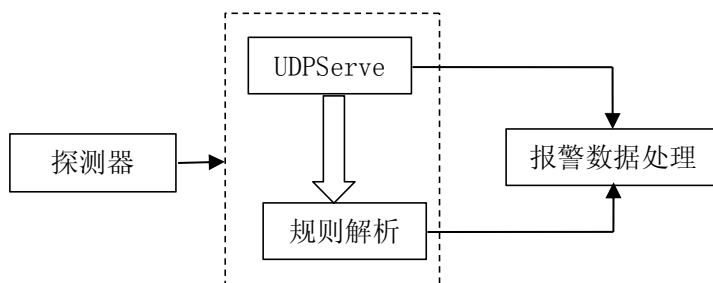


图 4-7 探测器服务模块

4.3.3 实时报警与数据库处理

这两个模块接收报警数据处理模块传递的信息进行操作。其中实时报警接收的是未经过解析的原始数报警信息，数据库处理模块接收经过解析的报警信息

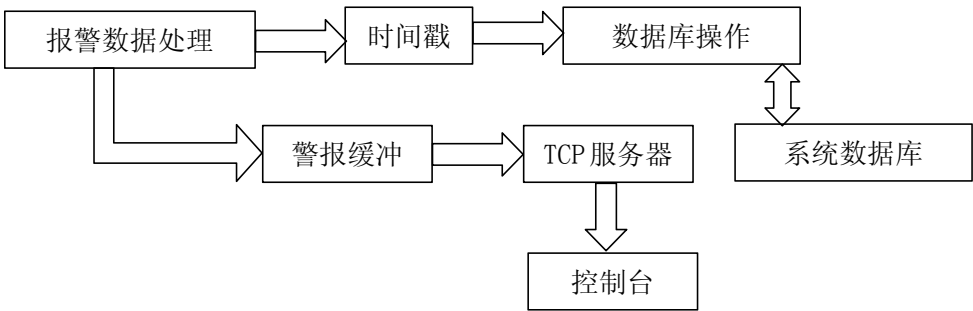


图 4-8 实时报警接收数据模块

4.3.4 联动处理模块的设计

在各模块互动的过程中，各节点与服务器端进行数据交换，最后由策略管理中心协同处理，以下是联动处理模块，如图 4-9 所示。

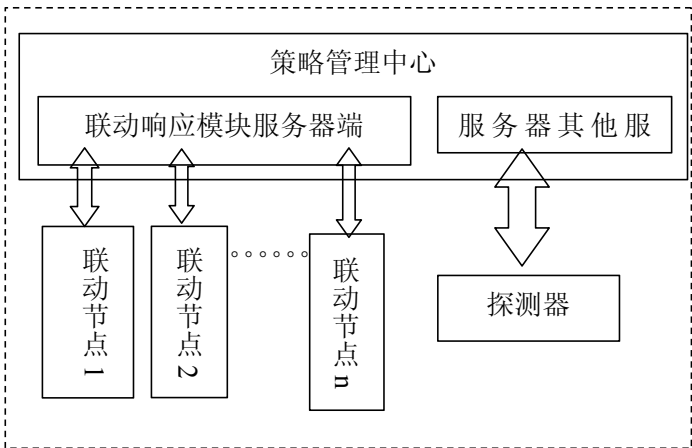


图 4-9 联动处理模块设计

4.4 系统控制台模块设计

该模块的主要功能有：

（1）提供管理员身份认证。

- (2) 策略管理中心的服务总开关。
- (3) 访问数据库并完成统计信息。
- (4) 访问并操作报警数据库。
- (5) 实时报警开关显示。

该结构中使用了瘦客户端的设计模式，下面给出控制台的模块设计如图 4-10 所示。

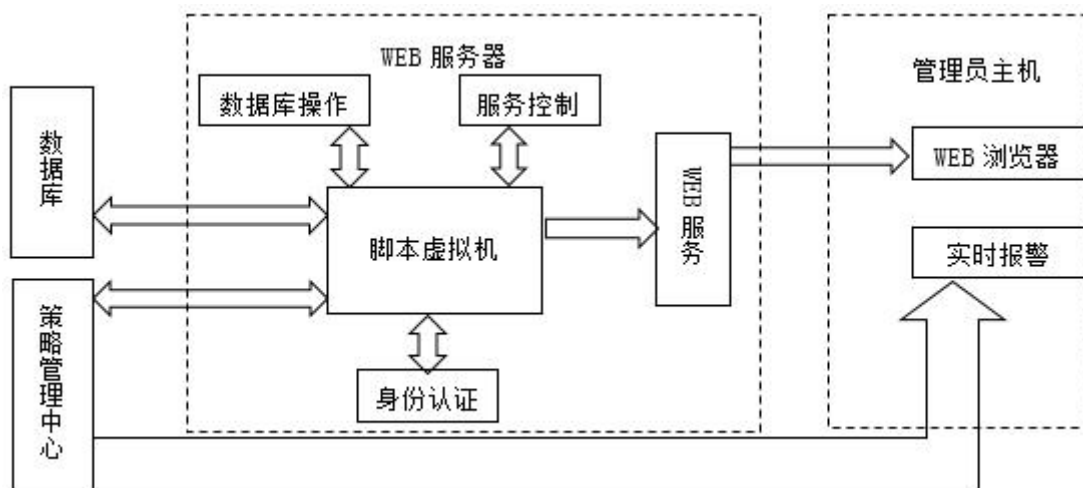


图 4-10 控制台模块

TCP/IP 协议三次握手，即建立相应的 TCP 连接。它是指建立一个 TCP 连接过程中需要客户端和服务端发送 3 个包以确认连接的建立。

下面是正式报警传输协议的叙述。

- (1) 报警开始过程。
- (2) 报警发送过程。
- (3) 报警停止过程

报警过程的如图 4-11 所示。

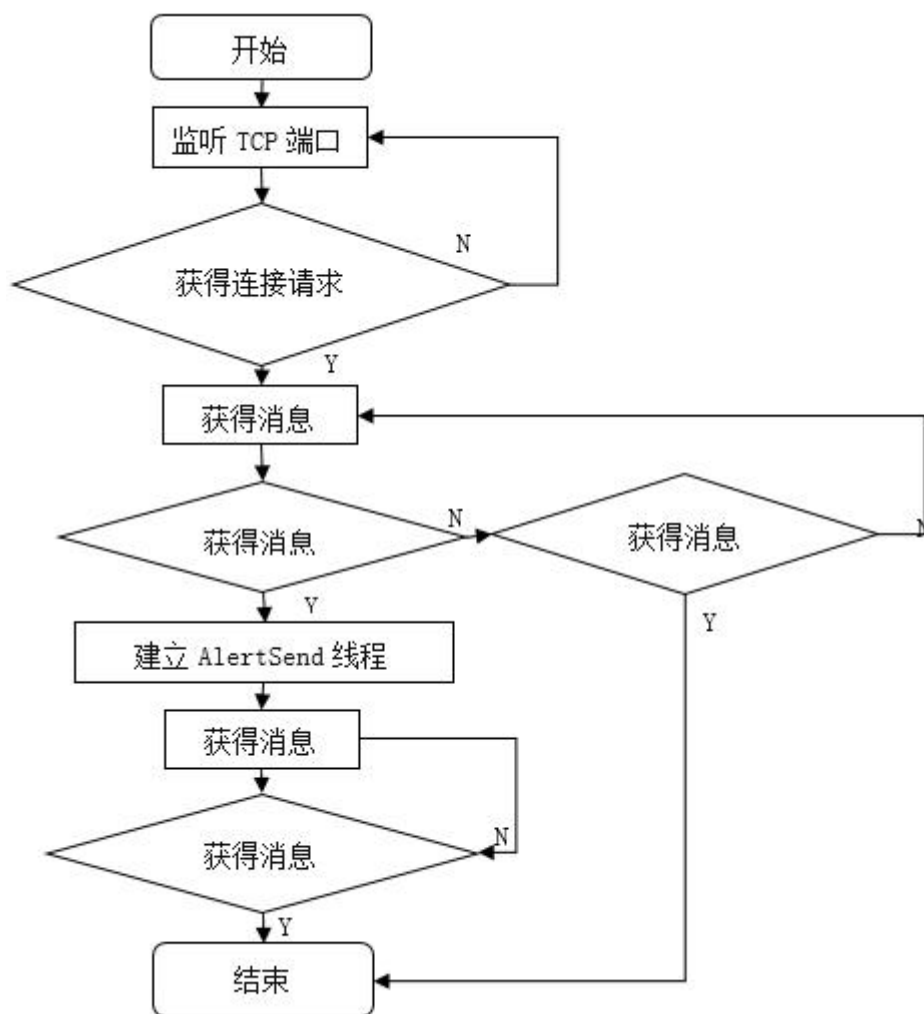


图 4-11 实时报警协议传输过程

4.5 联动响应模块

- (1) 联动响应模块采 B/S 模式。
- (2) 策略管理中心负责联动管理。
- (3) 策略管理中心和联动节点衔接。

联动控制主流程如图 4-12 所示。

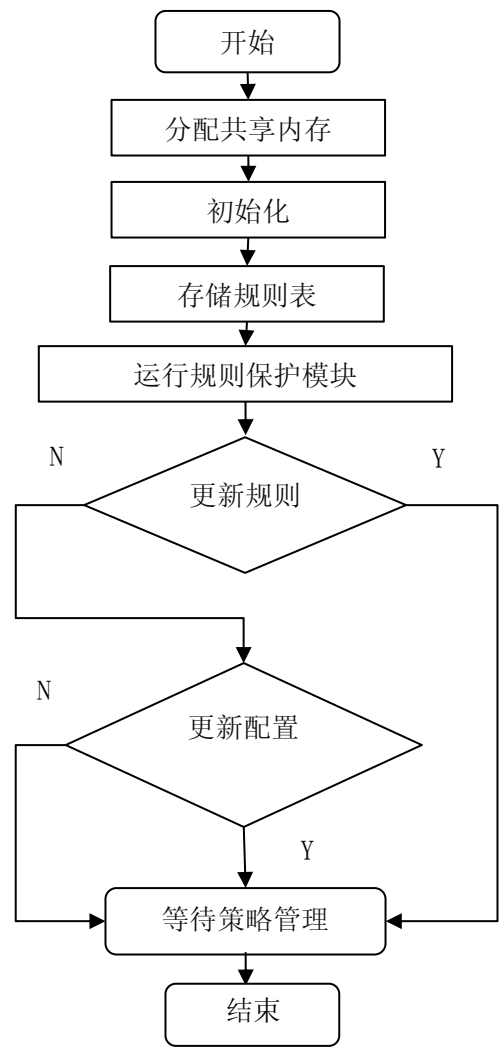


图 4-12 联动控制主流程

4.6 本章小节

本章内容进行了系统的具体设计，分析了子模块的功能构成。在此基础上，为下一章的仿真测试提供了相应的基础。

第 5 章 系统实现和测试

本章主要进行系统的实现，首先是对开发环境的介绍和关键技术的分析，接着在实际环境中举例介绍入侵案例的仿真测试，分析了入侵事件的防御用例，实验结果证明该系统的有效性和可行性。

5.1 开发环境

5.1.1 Java 开发环境

本文研究与设计的入侵防御系统测试实现主要是采用 Java 语言作为开发环境以保证系统具有广泛的通用性。于 1995 年，Sun 公司开发了 Java，后被 Oracle 公司正式收购。

Java 作为目前最流行的和使用广泛的面向对象开发语言。它分为三个体系：Java 标准级平台、Java 企业级平台、Java 微型级平台。Java 具有独立性、简洁性、多线程和多态性等多种特点于一体。本系统中采用了 JavaEE 作为开发平台。

5.1.2 B/S 架构概述

基于 B/S 架构（Browser/Server）。也是目前普遍使用的浏览器/服务器架构模式。B/S 架构主要是利用了现有的 Web 浏览器技术，只需一台能够上网的电脑就能使用和维护。系统的扩展非常容易，基于瘦客户端（Thin Client）的方式，以便集中管理、高部署效率以及不用专业 IT 员工就能够为企业节省巨大的成本开支。总结 B/S 架构的特点如下：

优点：

- a. 不需访问服务器，IE 浏览器即可。
- b. 可以放在广域网上，设定访问权限，交互性较强。
- c. 升级服务器简单方便。

缺点：

变量名: CLASSPATH=%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar;
系统变量名输入安装路径信息: C:\Program Files (x86)\Javajdk1.8.0_121;
配置完成后在 DOS 控制台中验证 JDK 是否配置成功,打开开始菜单的运行命令,
输入 CMD 后进去控制台界面后,输入: javac 后,窗口显示相应的验证提升代码
提示完成,然后输入 Java 命令测试,验证完成。若出如图 5-3 信息则表示安装成
功:

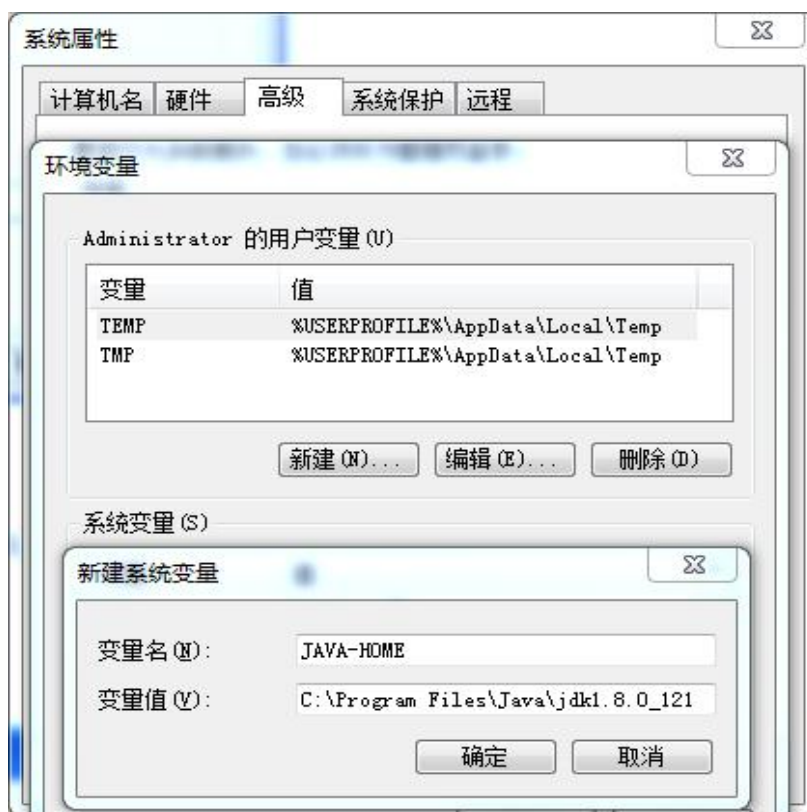
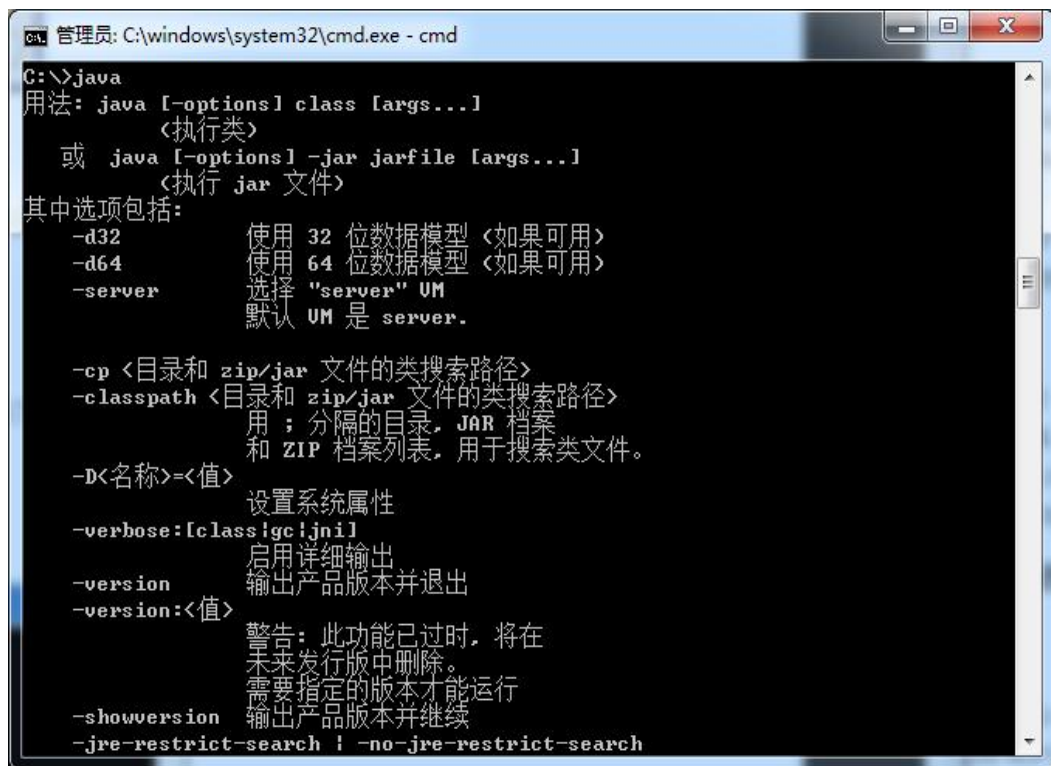


图 5-2 配置 JDK 环境变量



```
管理员: C:\windows\system32\cmd.exe - cmd
C:\>java
用法: java [-options] class [args...]
        <执行类>
    或 java [-options] -jar jarfile [args...]
        <执行 jar 文件>
其中选项包括:
    -d32          使用 32 位数据模型 <如果可用>
    -d64          使用 64 位数据模型 <如果可用>
    -server       选择 "server" VM
                  默认 VM 是 server.

    -cp <目录和 zip/jar 文件的类搜索路径>
    -classpath <目录和 zip/jar 文件的类搜索路径>
                  用 ; 分隔的目录, JAR 档案
                  和 ZIP 档案列表, 用于搜索类文件。

    -D<名称>=<值>  设置系统属性
    -verbose:[class!gc!jni]
                  启用详细输出
    -version        输出产品版本并退出
    -version:<值>   警告: 此功能已过时, 将在
                  未来发行版中删除。
                  需要指定的版本才能运行
    -showversion    输出产品版本并继续
    -jre-restrict-search | -no-jre-restrict-search
```

图 5-3 配置环境变量验证

5.1.4 Tomcat 的安装及配置

Tomcat 是一个开放源代码的 Web 应用服务器。优点是技术先进和性能稳定。深受广大用户和开发人员的欢迎。也被用作开发和调试 Jsp 程序的首选。运行下载的 Tomcat 安装程序, 如图 5-4 所示。



图 5-4 Tomcat 安装界面

添加系统环境变量，我的电脑->属性->高级系统设置->环境变量（操作同上）

变量名： CATALINA_BASE

变量值： C:\Program Files\apache-tomcat8.0（Tomcat 解压到的目录）

变量名： CATALINA_HOME

变量值： C:\Program Files\apache-tomcat8.0

变量名： CATALINA_TMPDIR

变量值： C:\Program Files\apache-tomcat8.0\temp

变量名： Path 变量值： D:\Program Files\apache-tomcat8.0\bin

5.1.5 安装 Mysql5.7

MySQL 是由 MySQL AB 公司开发的一个关系型数据库管理系统。将已经下载好的 MySQL 安装包，按向导提示流程完成运行和安装，然后选择配置方式，完成后进行启动服务并开发测试，安装过程如图 5-5 所示。



图 5-5 MySQL 安装界面

5.2 关键技术

5.2.1 策略管理中心

(1) 策略管理中心服务管理器

以下是如何实现服务管理器的功能。

首先 建立线程状态表，在 State_SyslogServer 类中有如下定义：

```
public class State_SyslogServer
{
    private boolean SyslogServerOn = false;
    private boolean SyslogServerIsRunning = false;
    private boolean available = true;
    public synchronized boolean get_SyslogServerOn()
    public synchronized void set_SyslogServerOn(boolean value)
    public synchronized boolean get_SyslogServerIsRunning()
    public synchronized void set_SyslogServerIsRunning(boolean value)
    public synchronized void wait_SyslogServerIs(boolean flag)
```

```

}

```

其中变量 SyslogServerOn、SyslogServerIsRunning 的作用同 Thread_Set 和 Thread_Running 作用相同。Boolean available 变量是一个读写锁。

set_SyslogServerOn 与 set_SyslogServerIsRunning 两个方法操作时先测试 available 的值, 如为 false 则阻塞, 如为 true 则设为 false 再进行操作。

available 变量实现表的完整性和有效性。

wait_SyslogServerIs 方法阻塞服务管理器线程直至 SyslogServerOn 改变。全部逻辑如图 5-6 所示。

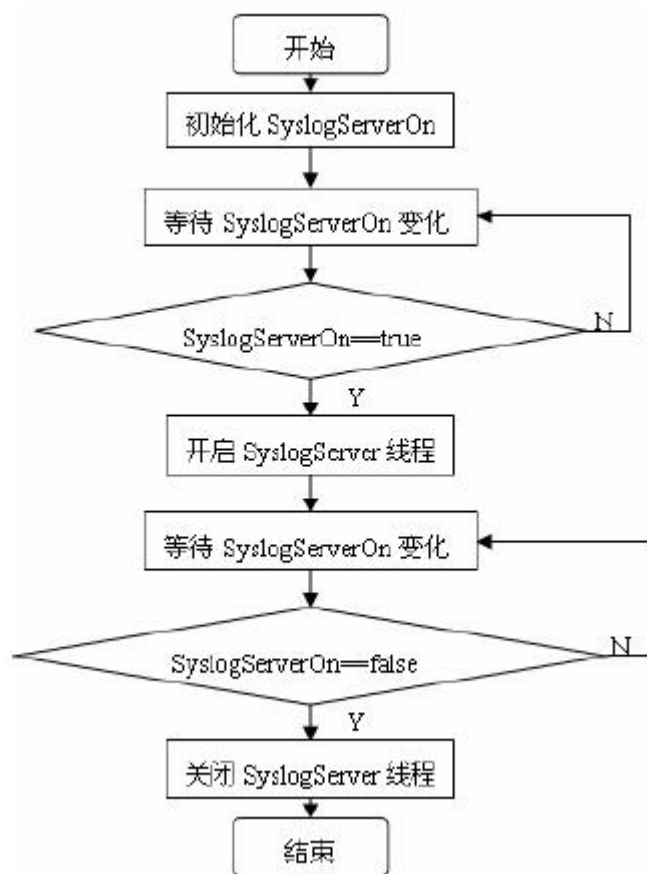


图 5-6 服务管理器流程图

(2) 报警响应处理, 用代码表示其算法如表 5-1 所示,

表 5-1 消费者生产者算法表

生产者:	消费者:
p(empty)	p(full)
p(mutex)	p(mutex)
add	take
v(full)	v(empty)
v(mutex)	v(mutex)

初始化的值分别为: empty=n, full=0, metex=1。

而 empty 与 full 提供了空/满阻塞的功能。

在设计程序项目过程中 java 进行了所需要的类名、成员变量和成员方法的定义声明过程,主程序段的代码如下:

```
public class Security{
    private int x;
    public Security(int i);
    public synchronized void p();
    public synchronized void v();
}
```

在 Java 项目中建立存储数据结构的队列类:

```
Public class QueryQueue extends java.util.Vector
{
    Private Security  available;
    Private Security empty;
    Private Security  full;
    Public QueryQueue(int size)
    Public void enq(Object x)
    Public Object deq()
}
```

可以看到以上代码中的特性。

available 初始值为 1 作为读写锁使用;

empty 初始值为队列大小,空阻塞信号量;

full 初始值为 0,是满阻塞信号量。

入队函数 enq()与出队函数 deq()的代码如下:

```
Public void enq(Object x)
{
    empty.p();
    available.p();
    super.addElement(x);
    full.v();
    available.v();
}
Public Object deq()
{
```

```
full.p();
available.p();
Objectx=super.elementAt(0);
super.removeElementAt(0);
empty.v();
available.v();
return x;
}
```

表 5-2 变量变化表

empty	full	说明
9	0	空阻塞状态，此时出队操作 deq()被阻塞
7	2	二个元素入队状态
...
0<empty<9	0<full<9	n(n<9)个元素在队中
0	9	满阻塞状态，此时入队操作 enq()被阻塞

5.2.2 异常入侵检测

(1) 异常检测(AD)

如图 5-7 显示了异常检测的模型。

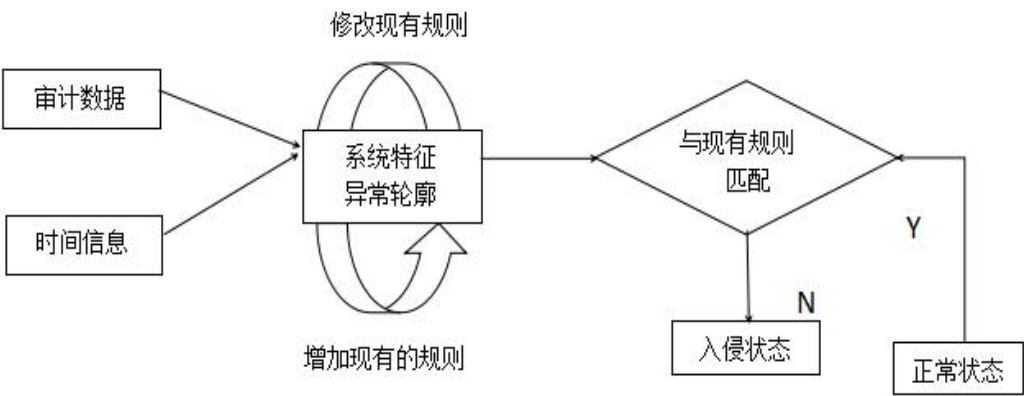


图 5-7 通用的异常检测模型

(2) 探测器节点控制

在 Connectione 类中，定义了如下变量：

```

private String host;//策略管理中心 IP
private int port;//与策略管理中心通信端口
private String s_ip;//受保护 IP 地址
private String mask;//掩码
private String flag;//标志字，用于判断执行哪项操作
private String line;//接收的字符串
private Socket client;//建立 Socket 连接
private String path;//更新文件的共享路径
private String ver;//规则库版本信息，发到策略管理中心判断是否需要更新*/
flag.equals("0")时：带参数启动探测器节点
flag.equals("1")时：更新探测器节点配置文件
flag.equals("2")时：更新规则库
flag.equals("3")时：关闭探测器节点
Control 类中 control(String source_ip, String netmask, String oc, String pathe)

```

变量访问了策略管理中心 IP，负责让变量 `runit()` 执行指令；`runitc()` 负责提取探测器节点进程号并将其终止。更新规则采用覆盖的方式，即将新规则完全覆盖原有规则。

5.2.3 服务控制模块

在策略管理中心功能模块里，设定响应报警并且连接策略管理中的线程，如流程图所示。

```

控制台运行 ControlServer 线程；
CmdCotainer 类进行命令解析同时定义常量；
状态表 ServiceState 来管理服务状态；
int cmd_SyslogServer_on= 1;
int cmd_SyslogServer_off= 2;
int cmd_SyslogServer_alive = 3;
int cmd_FirewallSend_on = 4;
int cmd_FirewallSend_off= 5;
int cmd_FirewallSend_alive = 6;
命令与这组常量比较获得变量名，执行结果。

```

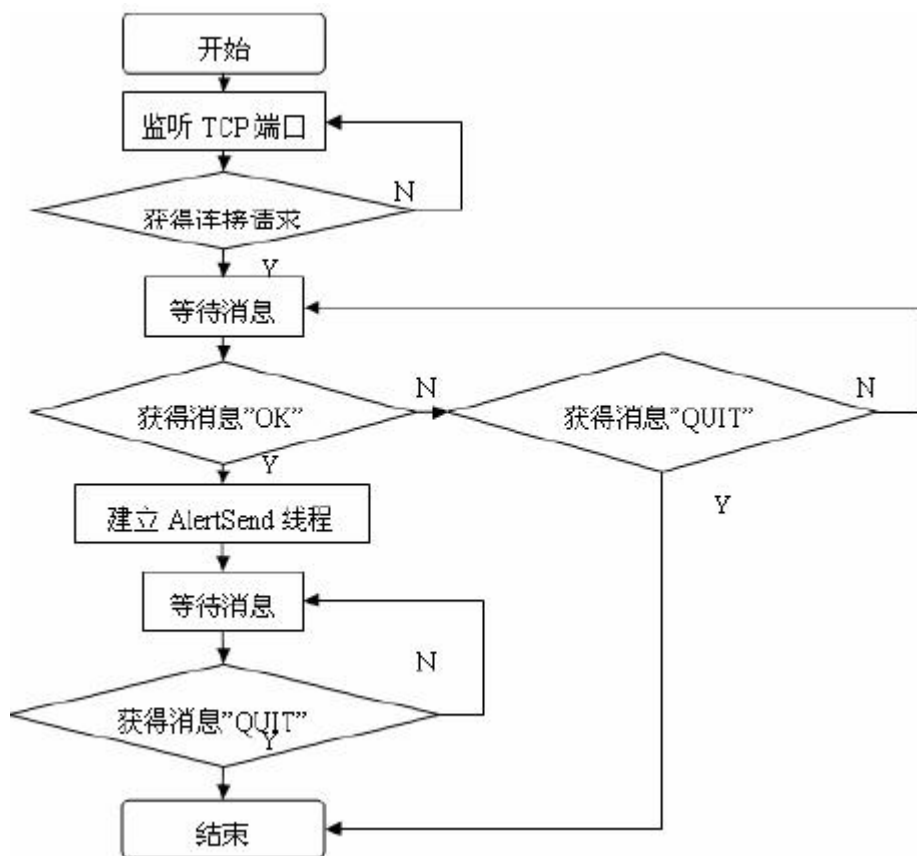



图 5-8 Alert Server 的流程图

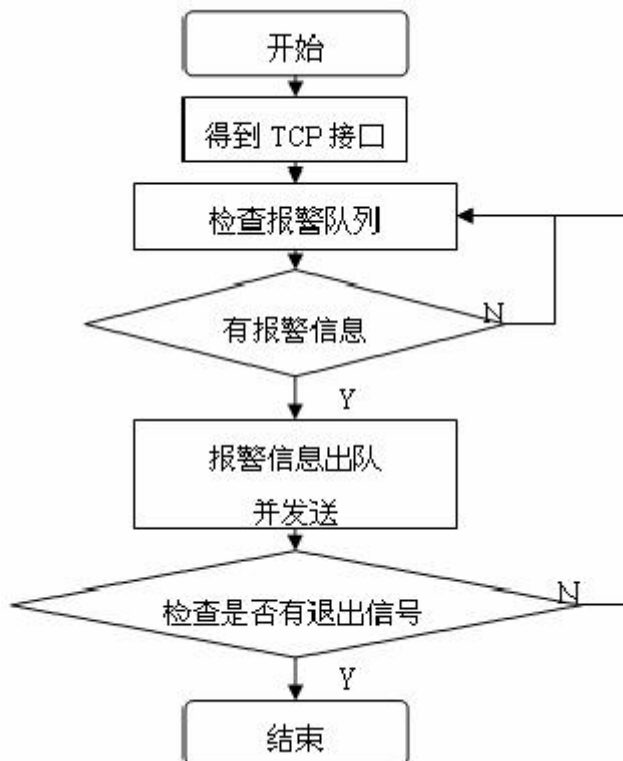


图 5-9 Alert Send 线程的流程图

5.3 运行界面

(1) 在已经配置完成 JAVA 虚拟机的系统上启动策略管理中心模块。在 DOS 控制界面中运行后显示结果如图 5-10 所示。

```
SyslogServer Waiting...  
FirewallSend Waiting...  
ControlServer started  
AlertServer Waiting...  
SQLSend Waiting...
```

图 5-10 运行策略管理中心模块

继续运行联动响应模块，显示结果如图 5-11 所示。

```
START  
RuleList is Empty  
RuleList is Empty  
RuleList is Empty  
RuleList is Empty  
RuleList is Empty  
RuleList is Empty
```

图 5-11 运行联动响应模块

5.4 仿真实验用例

以常见案例来测试分布式防御系统的功能，以下是对基于网络入侵后最优逃避攻击节点模型进行设计。

5.4.1 模型设计用例

一个网络的基本防御结构包含有源二端网络、中央网关和受害方法防御规则^[1]，这些结构都没能达到理想的防御能力，如果网络入侵源头隐蔽，防御将会失效。分布式防御能够将以上结构的单点式策略改成多点式策略，被入侵后使用网络内部节点遍历整个网络场景，选出最优防攻击节点进行网络数据传送或交换。设计基于分布式的网络入侵后最优防御攻击节点模型，模型需有灵敏的入侵响应机制和准确的攻击定位，且不会随意变更用户数据内容。如图 5-12 所示。

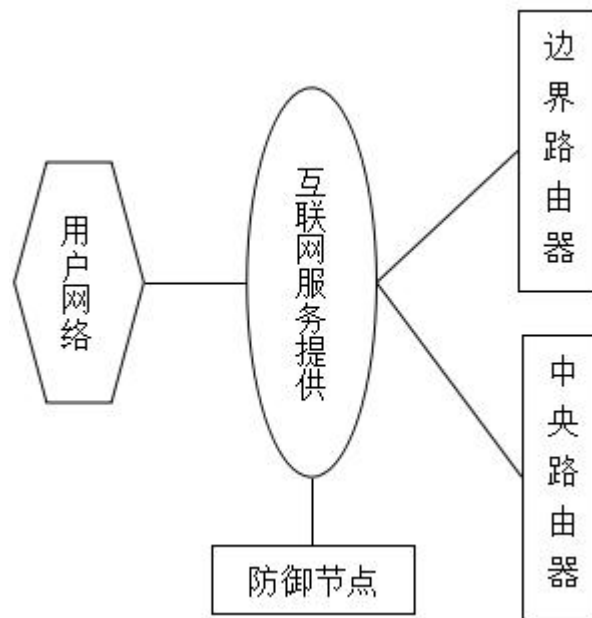


图 5-12 网络拓扑结构示意图

从图 5-12 所示的网络拓扑结构示意图中可以看到，用户网络由多个互联网服务提供商构成，互联网服务提供商可以随时获取用户网络中的路由消息，包括边界路由器和中央路由器中的消息^[3]。多个互联网服务提供商进行数据交互便形成了用户数据在网络中的流通。防御节点位于互联网服务提供商内部，基于分布式的网络入侵后最优逃避攻击节点模型便效仿互联网服务提供商内部防御节点的分布形式设计模型结构，但因为不同互联网服务提供商具有结构差别，同时为了快速响应网络入侵，模型只对能够逃避攻击的节点进行保护。

5.4.2 模型结构

最优逃避攻击节点模型由入侵筛检节点、分类节点、处理节点和安全节点构成，按照逻辑结构区分，入侵筛检节点、分类节点和处理节点属攻击检测层，安全节点分布在模型各个位置^[25]，用图 5-13 所示。

按照攻击层次区分，模型可分为上、下两层，上层包含安全节点和入侵筛检节点，下层包含分类节点和处理节点。安全节点统管下层所有节点数据，入侵筛检节点检查网络节点是否能够有效逃避攻击并下达防御指令给下层。下层负责在网络入侵后对攻击和防御指令做出响应，分类节点将路由消息的合法性进行分类并传给入侵筛检节点进行安全检查，获取最优逃避攻击节点。处理节点根据防御指令对用户数据进行过滤和传送，最后将用户数据交由最优逃避攻击节点。如图

5-11 所示。

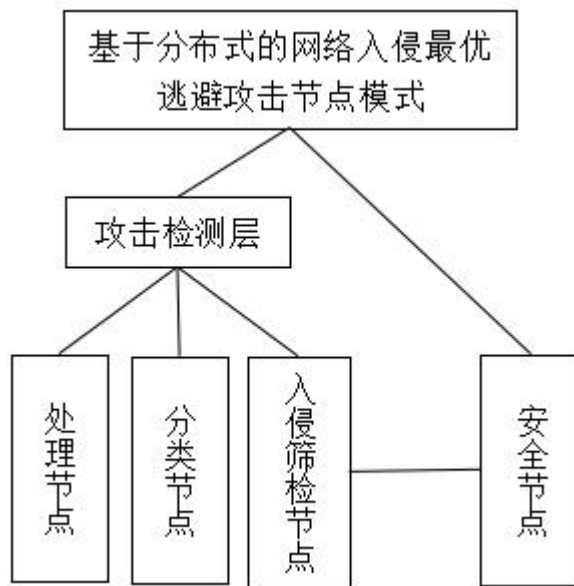


图 5-13 防御模型结构示意图

5.4.3 最优防御攻击节点的选取原则

入侵筛检节点所进行的最重要的工作就是在网络入侵后对最优防御攻击节点进行选取，总的选取原则是多点分布式遍历网络内部节点路由消息，以核心路由器为检测端，向各节点转发模型防御机制，发现入侵攻击情况立即发出警报^[25]。用安全节点的管理能力将逃避攻击节点构成一个网络通信通道进行用户数据安全通信。

模型对用户数据的传送速度有严格规定，超出额定传送速度，下层节点立即中止响应，表示网络入侵攻击方位已发生变化，需要重新进行最优逃避攻击节点选取工作。额定传送速度由边界路由器给定^[26]，在额定传送速度下，路由消息能在最优网络带宽附近进行传送，丢包率低，能确保网络通信顺畅，弱化网络入侵攻击强度。

5.4.4 防御模型机制

基于分布式的网络入侵后最优防御攻击节点模型的防御机制能够作用于网络内的所有互联网服务提供商，如图 5-14 所示，以两个互联网服务提供商 A、B 为例介绍模型防御机制。

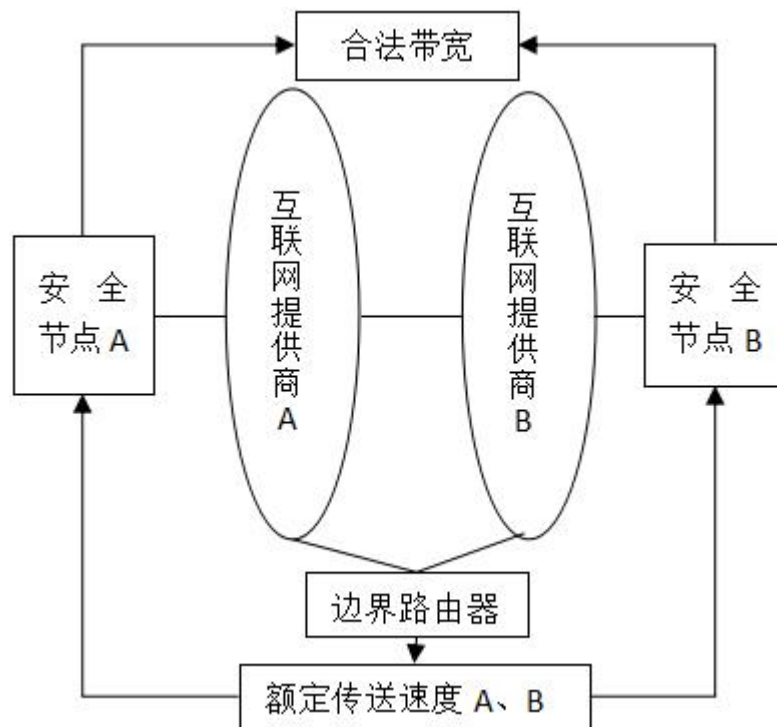


图 5-14 防御机制示意

防御模型机制表述是：有防御能力节点满足数据累积性、收益量化性^[27]，还显示网络主机状态。收益量化性指节点收益可用数字、矢量图等方式进行量化。数据累积性指节点量化与网络主机状态评估数据不断累积。

由图 5-14 可知，模型防御机制是以额定传送速度和网络带宽为依据建立的，互联网服务提供商 A、B 共用一个边界路由器同时给定额定传送速度。分属于两个互联网服务提供商的安全节点 A、B 接收各自额定传送速度 A、B，分布式遍历不同区域网络节点路由消息。网络带宽具有动态变化性，将满足额定传送速度、可逃避攻击且处于合法带宽中的网络节点看成最优防御攻击节点。

5.5 仿真实验

5.5.1 入侵事件数量对模型能耗的干扰

将虚拟网络场景中节点传送数据包的周期设为 1s，每个节点每次传送 80 个数据包，共有 90 个节点参与这项工作，它们与接收端点之间的跳数在 20 跳上下，浮动情况不超出 2 跳。在选取最优防御攻击节点并进行网络入侵防御的过程中，入侵事件数量对不同模型的干扰情况表示在图 5-15 中。

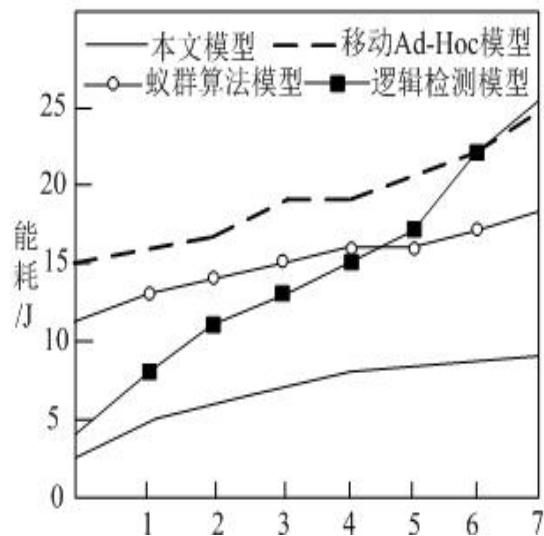


图 5-15 入侵事件数量对不同模型的干扰情况

图 5-15 中，随着入侵事件数量的不断变多，本文模型、移动 Ad-Hoc 模型、蚁群算法模型和逻辑检测模型的能耗产生不同程度的增长。逻辑检测模型虽然通过网络外添加监控节点指导网络内部节点进行攻击逃避，但显然这个监控节点没能统管所有内部节点，入侵事件数量达到一定数值后，逻辑检测模型能耗大幅度提升，意味着网络入侵成功，大部分节点失效，不能正常控制节点能耗。四种模型中，本文模型能耗受入侵事件数量的干扰不大，可选出最优逃避攻击节点，并维持节点功能。

5.5.2 节点通信周期对模型能耗和丢包率的干扰

设 100 个网络节点每次传送 80 个数据包，入侵事件数量为 3 个，更改节点通信周期对不同模型能耗和丢包率的影响表示在图 5-16 和图 5-17 中。网络丢包率是节点在传送数据包时的数据丢失量与所传数据总量的比值。

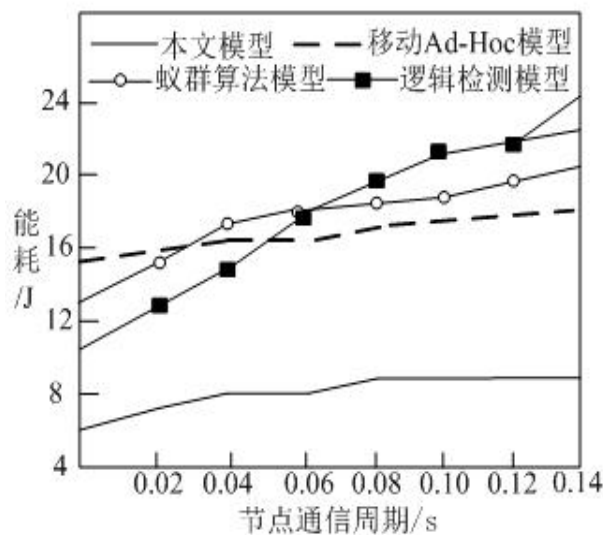


图 5-16 节点通信周期对不同模型能耗的干扰

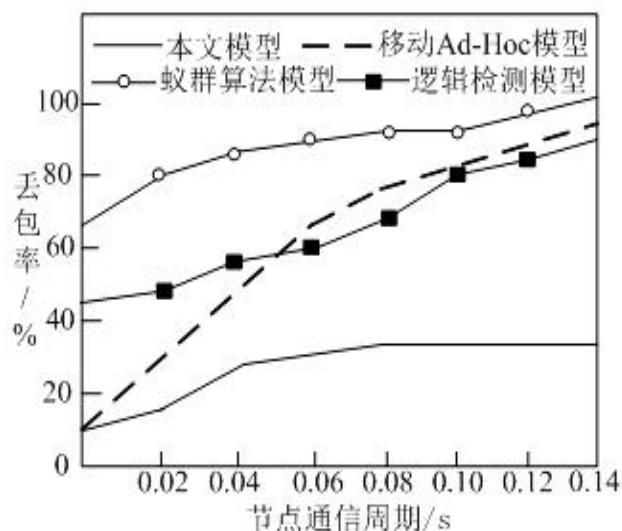


图 5-17 节点通信周期对不同模型丢包率的干扰

图 5-16、图 5-17 中，随着节点通信周期的上涨，此模型能耗明显低于移动 Ad-Hoc 模型、蚁群算法模型和逻辑检测模型，丢包率也逐渐平稳，最大丢包率为 32%，对应 0.08s 节点通信周期。

5.6 本章小节

本章介绍了系统的测试环境配置，完成了防御系统的测试过程、测试案例以及测试结果，并做出了具体测试说明。

第 6 章 总结与展望

计算机网络技术的发展号称人类历史的第四次工业革命。为人类社会带来了巨大的进步的同时网络攻击造成的重要资源的破坏和损失。在我国，网络安全法将于 2017 年 6 月正式施行。该部法律是互联网领域乃至整个经济社会领域至关重要的一部法律，堪称网络空间基本法。标志着网络空间安全已成国家意志并上升为国家战略。将在未来相当长时期内，对网络安全的政策监管、安全产业市场，乃至我国的各个领域、方方面面产生深刻影响。

本文研究了网络安全技术的基本思路，围绕着 IDS，防火墙技术，IPS 入侵等技术深入分析并扩展出两个模型，即分布式入侵防御模型和动态入侵防御模型。提出了基于分布式网络环境下的联动式的防御系统的体系结构，根据这些模型最终设计了一个协同检测，联动防御的安全防御系统。

论文主要创新点在于：

本文研究的创新点及最终的成果包括：

(1) 在前期研究基础上设计了一套协同检测、联动防御的网络防御综合解决方案。

(2) 结合了入侵检测、防火墙技术、入侵防御技术等传统技术，搭建了各自的数据通信和分组交换的桥接通道，提升和实现系统的交互性和扩展性。

(3) 在现有网络安全模型的理论基础上设计了一个合作式的防御模型，以此实现了一个协同联动型的入侵防御系统。经过仿真测试证明，该系统具备较好的市场应用价值。

本系统还不够完善，有待进一步完善和改进，这也使得本人后续要长期研究的工作方向。该系统未来研究内容主要包括：

- (1) 整个联动式防御系统其它功能的实现；
- (2) 防火墙和 IDS 的协同合作没有完全实现；
- (3) 设计该系统的过程中没有考虑到系统自身的稳定性和安全性；
- (4) 针对目前的物联网行业和移动端开发方面扩展性不够强。

参考文献

- [1] Robert Zalentski. Firewall technology. IEEE POTENTIALS, FEBRUARY/MARCH 2012. p24-30.
- [2] 王刚. 一种分布式网络入侵防御系统的设计与实现[D]. 天津大学 2007.
- [3] 沈萍. 动态防御系统的研究与实现[D], 成都:电子科技大学, 2006.
- [4] 张峰. 基于策略树的网络安全主动防御模型研究:[D], 成都: 电子科技大学, 2004: 1-8.
- [5] 车德军. 分布式入侵检测系统的研究与设计:[D], 北京交通大学, 2007.
- [6] 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, 2002.1~3.
- [7] 崔健双, 李铁克. 网络信息系统安全研究现状及热点分析, 计算机工程与应用, 2005. 35: 141-144.
- [8] 窦伟平. 联动式入侵防御系统的研究与设计: [D], 济南: 山东大学, 2006.10-12.
- [9] 陈海涛, 胡华平等.动态网络安全的框架模型. 国防科技大学学报,2003,VOL.25 NO.2, p60-63.
- [10] 穆成坡. 网络入侵分析与入侵响应: [M], 北京理工大学出版社,2011.
- [11] 刘萍萍. 分布式入侵检测系统模型的研究: [D], 长春: 吉林大学, 2004.11-12.
- [12] 张波. 分布式入侵检测与动态防御的技术研究及系统实现: [D], 河北: 河北工业大学, 2008.
- [13] R. N. Smith, Firewall Placement In a Large Network Topology, IEEE FTDCS 98, Portland, USA, USA: IEEE Press, 2013.
- [14] Jai Sundar Balasubramanian, Jose Omar Farcia-Fenrandez, An Architecture for ntrusion Detection using Autonomous Agents, Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks, New York, USA, May 2001, USA: IEEE Computer Society Press, 1999.17-31.
- [15] 杨德刚. 基于模糊 C 均值聚类的网络入侵检测算法: [J], 2005, 32(1): 86~91.
- [16] 冯剑红,谢汶. 电力信息安全体系结构研究及安全策略: [J], 《四川电力技术》2006.06.
- [17] 唐正军.入侵检测技术导论.北京: [M], 机械工业出版社,2004,20-24.
- [18] 熊小华. 网络入侵防御系统的研究与设计: [D], 山东: 山东科技大学, 2007.
- [19] 陈海涛, 胡华平等. 动态网络安全的框架模型: [J], 国防科技大学学报, 2003.
- [20] 李家春, 李之棠. 动态网络安全模型的研究: [J], 华中科技大学学报(自然科学版), 2003(3): 40~42.
- [21] 杨立友, 安全组件联动研究, [硕士学位论文], 西安: 西北工业大学, 2004.23-26.

- [22] 宋继军. 一种分布式入侵检测系统的实现, 计算机工程与科学, 2004. 5(5): 85-87.
- [23] 郭玲, 广域网入侵检测系统的实现研究: [D], 昆明: 昆明理工大学, 2004.
- [24] 张云鹏, 胡飞, 马春燕等. 基于 P2DR 模型的分布式入侵检测系统设计与实现, 计算机工程与应用, 2005. 35: 141-144.
- [25] W. R. Cheswick and S. M. Bellovin, Firewalls and Internet Security: Repelling the Willy Hacker, MA, USA: Addison Wesley Press, 2000.
- [26] 张野. 基于关联规则的入侵检测系统:[D], 沈阳: 东北大学, 2005.41~42.
- [27] 张丙凡. 入侵防御系统的研究与实现[D]. 江苏科技大学 2010.
- [28] S. Hofmeyr, Host intrusion prevention: Part of the operating system or on top of the operation system, Computers and Security, 2005(24): 440~442.
- [29] Muradiralan Gangadharan and Kai Hwang, Intranet Security with icro-Firewalls and Mobile Agents for Proactive Intrusion Response, Proceedings of IEEE international Conference on Computer Networks and Mobile Computing, Beijing, China, SA: IEEE Computer Society, 2002. 130~137.
- [30] Muradiralan Gangadharan and Kai Hwang, Intranet Security with Micro-Firewalls and Mobile Agents for Proactive Intrusion Response, Proceedings of IEEE international Conference on Computer Networks and Mobile computing, Beijing, China, USA: IEEE Computer Society, 2012. 130~137.

致 谢

白驹过隙，稍纵即逝，在即将完成学业的时候我更加体会到这段学习经历的可贵。我非常庆幸在这段岁月里遇上了这么多的良师益友，在我求学路上的指导和交流，让我在本专业领域上更上一层楼。

三年即将过去，本文的研究工作是在导师李其申教授的关怀和悉心指导下完成的。在求学的三年期间，学校的老师给了我在在学习上的很多指导和帮助。从论文的选题、撰写提纲、研究工作的进展以及到最后的成稿，都倾注了李老师大量的心血，让我在专业素养上得到提高，学术态度上学会更加严谨。在此，谨向李老师致以我深深的敬意和由衷的感谢，感谢他三年来在学习和工作上对我的关怀和帮助。

论文的顺利撰写除自身的努力和指导老师的帮助外，南昌航空大学信息工程学院的许燕老师和各任课老师对我的论文也提出的相关帮助和修改意见，他们不但帮助我熟悉业务，而且为我提供了不少资料和建议。并向所有支持、关心和帮助我的老师、同学和亲友表示由衷的谢意，感谢他们对我无私的支持、关怀和精神上的鼓励。

李老师渊博的学识、严谨的治学作风、求实的科学态度、孜孜不倦的工作精神给我留下了深刻的印象。师从于李老师门下，我不仅学习到了丰富专业知识，也学到了对待生活、对待工作的积极态度，这些都将是终身的宝贵财富。

最后，感谢我的家人，他们一直都在我最需要的时候给我莫大的支持和鼓励。亲人们的爱让我对未来的生活充满信心和勇气。感谢一切关心和帮助过我的亲人，老师，朋友和同学。

硕士学位论文原创性声明

本人郑重声明：所呈交的硕士学位论文，是我个人在导师指导下，在南昌航空大学攻读硕士学位期间独立进行研究工作所取得的成果。尽我所知，论文中除已注明部分外不包含他人已发表或撰写过的研究成果。对本文的研究工作做出重要贡献的个人和集体，均已在文中作了明确地说明并表示了谢意。本声明的法律结果将完全由本人承担。

签名：_____日期：_____