北京邮电大学

硕士学位论文

网络安全管理平台的设计与实现

姓名：裴娜

申请学位级别：硕士

专业：密码学

指导教师：杨义先

20060304

网络安全管理平台的设计与实现

摘　要

随着信息网络的飞速发展，越来越多的涉密信息都从传统的媒介转移到网络上存储和传输，使网络安全成为目前最迫切的需要人们去关注的问题，大量的关于网络安全的新技术不断地产生，网络安全设备也越来越多样化。人们对于网络安全的要求越来越高。

因此，网络安全管理这个概念应运而生，网络安全管理包括安全策略的集中分发和管理、安全事件的集中监控和处理、针对安全设备的特殊性质的特殊处理、防御体系的整体安全等，这些性质传统的通用网管软件是无法满足的。网络安全管理作为一种特殊的网络管理手段，提高了安全设备的协作性能，提高了整个防御体系的安全性，弥补了传统网络管理软件的不足。

本论文在开头介绍了网络安全管理技术较于通用网络管理技术的特点和优势，并设计了一个分布式多层架构的网络安全管理系统原型。该系统在结构设计上，采取了分散处理、分散存储、统一管理、统一审计的分布式结构，以适应网络安全管理的需要。系统设计的特点是采用了级联结构，可以无限级联，这种设计使系统结合了负载均衡和分布式技术的优点，具有很大的灵活性和扩张性。可以适应从简单到复杂的网络结构。

该安全平台通过集中的网络安全管理来实现对网络中多个安全设备的总体配置、调控整个网络多层面、分布式的安全系统，实现对各种网络安全资源的集中监控、统一策略管理、智能审计及多种安全功能模块之间的互动，使得网络安全管理工作由繁变简，更为有效。

本文主要介绍了系统的设计思想，原型系统的系统框架结构，最后总结了在系统设计中存在的不足和未来工作思路。

关键词：网络安全、安全管理、策略、SNMP

DESIGN AND REALIZATION OF NETWORK SECURITY MANAGEMENT PLATFORM

Abstract

In the large-scale computer network that provides sensitive service to the military, financial etc. the security is one of its main index. Current network inside service and new technical adoptions play increment, satisfied the applied need on the one hand, on the other hand increased the opportunity of safe loophole and network attack, forcing to increase and update security devices continuously. The safety of nearly whole system is determined by the weakest part in the system. There, to decline security risk to the lowest degree, the only way is to gather every kind of devices for security, unify the management, integrate them, setting up successive lines of defense. Moreover the increment of the provisions for security causes management of them becomes an important part of network security.

To manage and control the security devices and security applications and security events in the large-scope network, this paper designed a NSM (network security management), and realize a prototype system. The system attains unified and integrated management.

The target of system design is to manage every kind of network devices for security in sophisticated network circumstance. Using united software interface control and manage various devices from different vendors. The network security management system hopes to be scalable, dynamic etc.

It introduces the design of the whole system primarily, the system framework of the prototype system, tallied up the shortage exist in system design and the future work.

Key words: network security, security management, policy, SNMP

独创性（或创新性）声明

本人声明所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京邮电大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：裴娜 日期：2006.3.27

学位论文使用授权说明

学位论文作者完全了解北京邮电大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属北京邮电大学。学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存、汇编学位论文。（保密的学位论文在解密后遵守此规定）

非保密论文注释：本学位论文不属于保密范围，适用本授权书。

本人签名：裴娜 日期：2006.3.27

导师签名： 日期：2006.3.27

第1章 绪论

1.1 研究背景

近年来，网络逐渐渗透到社会生活的各个方面。人们在网上查询信息，企业在网上发布信息，而政府则在网上公开信息。

目前，在网络应用的深入和技术频繁升级的同时，非法访问、恶意攻击等安全威胁也在不断推陈出新，愈演愈烈。防火墙、VPN、IDS、防病毒、身份认证、数据加密、安全审计等安全防护和管理系统在网络中得到了广泛应用。

虽然这些安全产品能够在特定方面发挥一定的作用，但是这些产品大部分功能分散，各自为战，形成了相互没有关联的"安全孤岛"；各种安全产品彼此之间没有有效的统一管理调度机制，不能互相支撑、协同工作，从而使安全产品的应用效能无法得到充分的发挥。

从网络安全管理员的角度来说，最直接的需求就是在一个统一的界面中监视网络中各种安全设备的运行状态，对产生的大量日志信息和报警信息进行统一汇总、分析和审计；但是一方面，由于现今网络中的设备、操作系统、应用系统数量众多，构成复杂，异构性、差异性非常大，而且各自都具有自己的控制管理平台，网络管理员需要学习、了解不同平台的使用及管理方法，并应用这些管理控制平台去管理网络中的对象(设备、系统、用户等)，工作复杂度非常之大。

另外，对大型网络而言，管理与安全相关的事件变得越来越复杂。网络管理员必须将各个设备、系统产生的事件、信息关联起来进行分析，才能发现新的或更深层次的安全问题。

因此，人们越来越多的认识到单一的安全技术是不能防范攻击的，只有将防火墙、入侵检测、防病毒、认证和审计等各种技术结合起来，在统一的安全管理平台下协作，才能更好地保护网络。用户的网络管理需要建立一种新型的整体网络安全管理解决方案——统一安全管理平台，来总体配置、调控整个网络多层面、分布式的安全系统，实现对各种网络安全资源的集中监控、统一策略管理、智能审计及多种安全功能模块之间的互动，从而有效简化网络安全管理工作，提升网络的安全水平和可控制性、可管理性，降低用户的整体安全管理开销。

1.2 研究范围和主要内容

作者在参与网络安全管理平台的研究项目的过程中，研究了当今国内外安全管理平台的相关技术及解决方案，并结合在联想研究院信息安全实验室实习期间所作的工作，给出了一个网络安全管理系统的架构设计和部分主要模块（设备监控与策略管理）的实现。

本论文重点从以下几个方面入手进行了研究和实现：

1. 网络安全管理的定义，所需要解决的问题及范畴。
2. 探讨了网络安全管理技术与通用网络管理技术的区别，研究了网络安全管理的功能需求和体系结构。分析各项技术的优缺点和主要适用范围。
3. 网络安全管理平台的体系架构分析。提出了一个多层架构的网络安全管理平台。该系统采用无限级联模式，可以无限扩充，适用于从简单到复杂的网络环境。解决了以往的网络安全管理系统扩充性不够好的问题。
4. 系统设计与实现，探讨了网络安全管理平台的具体设计以及各模块的实现。将 XML 等标准组件技术应用于原型系统的设计，提出了该模型应该具有的一些性能和技术特性。

1.3 论文完成的工作和论文组织安排

论文分为以下几部分：

第一部分：综述。

第一部分由第一章和第二章组成，描述了论文的基本情况和技术背景。其中，第一章介绍了网络安全管理的研究背景以及论文的主要研究内容和组织结构，第二章描述了网络安全管理的各项技术。并着重讨论普通网络管理技术与网络安全管理技术的区别。

第二部分：网络安全管理平台的架构研究。

第二部分包括第三、四、五、六章，该部分是本论文的核心部分。第三章提出了一个分布网络安全管理平台的总体框架和系统部署，并介绍了系统的各个功能模块。第四、五章分别详细介绍了系统的核心模块：设备监控模块和安全策略模块的设计和实现。第六章介绍了系统接口，包括通信接口与系统接口。

第三部分即最后一章，该章节对论文作了总结，给出了本文所研究技术的实际应用价值，并对它的一些优缺点做了评论，提出了一些还未解决的问题，以及今后还需要作的进一步工作。

第2章 网络安全管理技术

随着信息网络的飞速发展，规模的越来越大，对现代网络管理的功能需求也就越来越复杂，目前这个时期，正是网络管理软件加速发展的黄金时期，原有的标准被不断的更新，目的就是为了满足日益增长的网络管理功能需求、提高网络管理的效率和降低网络管理的成本。

网络管理技术的发展和标准的制定是与现代网络管理的愿望和需求息息相关的，随着信息网络的发展，一些新的概念和新的技术不断地融入到现有的网络结构中，最近几年，人们对现有网络的安全越来越重视，大量网络安全设备不断涌现，如防火墙、入侵检测、安全审计等面向安全的网络设备，这些设备的出现改变了原有的网络管理观念，安全性渐渐成为首要的问题，这对现有的网络管理技术是一个严峻的挑战，今天的网络管理中，网络管理者的愿望和当今网络管理软件的实际实现之间还达不到一致。

下面，我们将针对一般的网络管理的功能需求和面向安全设备的网络管理的功能需求的异同进行探讨。

2.1 通用网络管理特点

2.1.1 通用网络管理系统的功能需求

在 OSI 参考模型中，将网络管理的功能需求划分为 5 大类，即故障管理、配置管理、帐务管理、性能管理和安全管理，这 5 个功能域在当今网络管理的设计和实现中通常都是要考虑的，常用的大中型网管软件如 HP OpenView、IBM Tivoli NetView、3Com Supervisor、Cisico Works、Sun NetManager 等都实现了故障管理、配置管理、性能管理及部分的帐务管理和安全管理。

从网络管理者的角度，一般的网络管理软件应该具有如下的功能特点：

1. 能够实现故障管理、配置管理、性能管理及部分的帐务管理和安全管理功能。
2. 应该具有一定的通用性，广泛支持各种网络设备，覆盖现在的和新的软硬件技术。
3. 可方便地实现集中或分布式管理（即提供可伸缩的二层或三层管理架

构）。

保护管理信息的安全和被管理设备的安全，确保重要信息和用户权限不被窃取。

5. 自动发现网络设备，自动构成网络拓扑图，并可支持主动发现网络设备作为补充。
6. 提供合理的表示方法，对管理信息进行分类或分层处理，使用户可以方便地使用和迅速地定位。
7. 保证管理信息的及时性，尤其是 TRAP 事件或 INform 事件，可对 TRAP 事件进行自动分类或过滤处理。
8. 对监控信息提供 BASELINE 控制，数值达到规定阈值则报警。对危险级别进行分类，达到一定级别就更换不同的颜色，给用户以直观的判断。
9. 提供必要的网络诊断工具，使用户可以不必借助其他工具就可以完成管理过程。

目前比较流行的网管软件基本可以实现以上的功能特点，但还有一些功能实现的不是很理想。

2.1.2 通用网络管理系统的体系结构

其实，目前国外比较流行的网管软件包括 HP OpenView 、IBM Tivoli NetView、3Com Transcend 、Network Supervisor、CA Unicenter、Sun NetManager、Fujitsu System Walker、Cabletron NetSight、Novell 网络管理方案 ManageWise、Cisco 网管方案等，国内的网管软件还处于刚刚起步的阶段，相关的产品如华为的 RMS 网管系统、大唐的 GHView 网管等电信网管系统及其他如北京游龙科技的 SiteView 和 TCL 的 TCL-View 等网管系统。

这些通用的网管软件一般都采用二层或三层管理架构。

在二层管理架构中，管理中心和管理控制台位于同一台设备中，从不同的被管网络实体中收集信息，其优点是结构简单，很容易部署，缺点是无法实现分布式管理。在三层管理架构中，由网络管理中心负责从各个被管理网络实体中收集信息，分散于网络中各个部位的管理控制台可通过用户登陆到管理中心，对各个管理设备进行管理，其特点是可实现分布式管理。

无论是二层还是三层管理架构，在网管接口通信协议方面，都是一致的，目前，已普遍接受的是基于 Q3 接口的 CMIP、基于 CORBA 接口的 IIOP 以及基于 Internet/SNMP 框架结构的 SNMP。每种类型的接口都有对应的信息模型，与

以上三种接口相对应，分别采用 GDMO/ASN.1、IDL/UML 和 MIBII 方式进行信息模型的描述。通用的网管软件通常都支持 SNMP 协议，一些大型的电信级网管软件如 HP OpenView 和 IBM Tivoli NetView 等还支持 CMIP 协议。

在安全方面，因为 SNMPV1/V2 协议对安全性方面考虑的比较少，而 SNMPV3 又是最近两年才趋向于成熟，大多数通用网管软件标准版本中都没有对 SNMPV3 的支持，即使实现也没有完全利用 SNMPV3 的优势，所以，通用网管软件在安全性方面实现的不是很理想，对管理信息和被管理设备来说，都存在着安全隐患，可能导致管理信息和用户信息被窃取。

HP OpenView 提供了 SNMP Security Pack 15.4 作为 HP Openview 支持 SNMPV3 的补丁包，IBM Tivoli NetView 也提供了 SNMPv3 Agents with NetView 作为补丁。虽然部分通用网管软件已经开始支持 SNMPV3，但无论是采用两层架构还是三层架构，它们的安全策略都是分散到各个管理设备上的，而不是由网管软件集中分发的，这种方式不利于集中的安全管理，所以留下了安全隐患。

总体来说，通用网管系统基本满足了 OSI 网络管理的功能需求，全部或部分实现了前面提到的网络管理系统应具有的九个功能特点。但它并不适应网络安全管理的要求。

2.2 网络安全管理特点

2.2.1 网络安全管理系统的功能需求

随着信息网络的飞速发展，越来越多的涉密信息都从传统的媒介转移到网络上存储和传输，使网络安全成为目前最迫切的需要人们去关注的问题，大量的关于网络安全的新技术不断地产生，网络安全设备也越来越多样化，鉴于网络安全设备同其他网络设备的不同和人们对网络安全越来越高的需求，对网络安全设备的管理有着特殊的功能需求。因为网络安全是最近几年人们才开始重视的问题，所以，在技术方面，还在不断地更新，这一点，传统的通用网管软件因为其通用性和庞大的规模而无法跟上发展的脚步，所以，无法更好地满足网络安全的网络管理需求特别是对安全设备的管理需求。

从安全的角度考虑，除一般网络管理的功能需求外，对安全设备的网络管理还有如下的功能需求：

1. 安全策略的集中分发和管理。从安全的角度考虑，所有安全策略都应该在管理中心集中分发，包括用户权限的分配、密钥的分发等，而不应该分散执行，否则就会因为过于分散而无法管理，导致安全问题。I

2. 安全事件的集中监控和处理。从网路管理者的角度考虑，从管理中心应该可以看到所有安全设备的当前运行状态和安全状态，反映整个防御体系的整体运行状态和安全状态。

3. 针对安全设备的特殊性质如动态连接、动态规则等进行专门的处理。管理中心应该可以根据网络安全设备的特殊性质，为用户提供针对性的表示方法，方便用户的管理。

4. 树立安全第一的观念，一切为了安全，强化安全防范措施。所有的管理环节都必须达到与安全设备相同的安全级别，否则，根据传统的木桶理论，任何一个环节没有安全防范措施，整体的安全性就会降低。

5. 根据最新的整体防御理念，网管软件管理的所有安全设备应该构成一个整体防御体系，具有整体的安全策略。

上面的这些针对网络安全设备的管理功能需求，通用网络管理软件是无法满足的，即使采用 SNMPV3 作为通信协议，但因为其架构和实现方法的不同，也无法满足这些安全管理需求。

2.2.2 网络安全管理系统的体系结构

为了满足前面提到的网络安全设备的管理功能需求，网络安全管理系统一般采用三层架构。

三级安全管理架构从逻辑上分为管理对象、管理域服务器和管理终端三个部分，这三个部分整体组成了一个安全管理域。

安全管理域代表了一个空间，这个空间包含管理对象、管理域服务器、管理终端三种类型的事物，管理员进入这个空间后，其管理行为都是通过这三种类型的事物的相互作用而发生，并且所有管理行为都不超出安全管理域所代表的空间。

一个安全管理域就是一个整体的安全防御体系，它具有有整体的安全防御策略。在安全管理域内，所有的管理内容都是以管理域服务器为中心，它是整个安全管理域的独裁者，它控制着整个安全管理域内所有的安全策略、权限分配和每一个交互的指令。

管理对象是需要管理的最终目标，它可以是某种物理设备如防火墙、入侵检测系统、VPN 网关等其他安全设备，它也可以是某种逻辑上的功能单元如访问控制单元、流量控制单元、负载均衡单元、用户认证单元等，甚至它也可以是运行在客户机的单点安全系统，不同的管理对象共同组成了管理对象域。对象的管理信息可以抽象为某种数据表达形式，相同的管理对象具有相同的管理信息结

构但结构中的属性不一样，它们可以看成管理信息结构的多个实例。

对管理对象的管理行为分两种：第一种，对目标对象的管理信息结构进行读写操作，这种情况下管理对象是被动的；第二种，管理对象主动的向管理域服务器报告某种事件的发生或状态的改变。

管理域服务器的是整个三级管理模型的中心，它是整个网络安全体系管理信息架构的集合，它统一的把可管理的信息资源表达给管理终端，并把来自于各个终端的对管理信息的访问，根据一定的策略重新定向到对应的管理对象。因此从管理终端的角度，管理域服务器集中了所有它可以管理的信息，管理域服务器就是一个巨大的管理对象，其中也包括它自己本身的管理信息对象。

管理域服务器作为安全域中的事件响应中心，负责接受管理对象的事件，并可根据预先制定的策略对事件作出响应，响应应该包括：记录、报警或者回应，同时管理域服务器会根据策略和权限通知相应的管理员或者在线的管理终端，或者对其他的管理对象进行相应的调整，即联动。

管理员可以制定策略，让管理域服务器定时采集管理对象的某些具有统计价值的管理信息，形成历史记录保存在本地数据库中，并提供相应的接口让管理终端提取历史记录。

管理域服务器可以作为内部安全子网用户的安全服务平台，为用户提供诸如：客户端安全软件的安装升级、客户端安全策略的分发、客户帐户的自助管理等服务。

为了提高系统的可靠性，管理域服务器应该是可以多机热备份的，同一安全体系中只存在一个主管理域服务器，但可以存在多个备份域服务器，各个服务器之间自动同步管理信息。

管理终端以某一管理员的名义对管理对象和和管理域服务器进行管理，管理终端直接面对管理员用户，需要提供易用的、图形化的界面，对管理信息进行格式化的输出，并按照一定的界面逻辑对管理员的输入进行处理。同时在线的管理终端可以接受管理域服务器转发的管理对象报告的 TRAP 和 INform 信息，以实时提示管理员用户当前所发生的事件。

通常用的管理终端有三种：通用 SNMP 终端、专用管理终端、Web 浏览器。

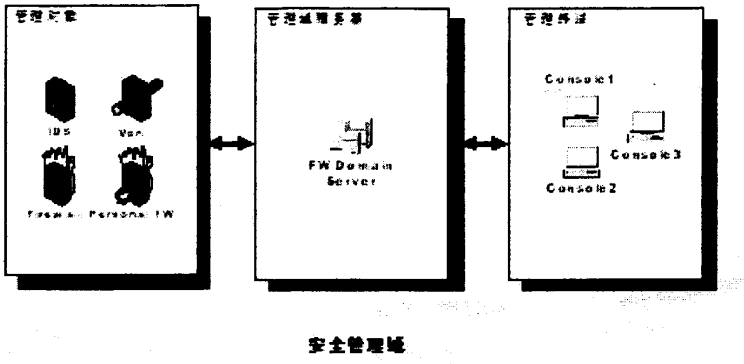

图 2-1 网络安全管理系统的三层架构

2.3 总结

通过前面对一般网络设备的管理功能需求和面向安全设备的网络管理功能需求的比较，我们可以清晰地看到，对安全设备的网络管理与一般的网络设备有着很大的不同，包括安全策略的集中分发和管理、安全事件的集中监控和处理、针对安全设备的特殊性质的特殊处理、防御体系的整体安全等，这些性质传统的通用网管软件是无法满足的，如果采用传统的通用网管软件，就会大大降低安全设备的效能，降低整个防御体系的安全性。所以，必须研究一种新的专门针对网络安全的网络安全管理系统。实际上，网络安全管理不是一个简单的系统，它包括的内容非常多，主要涵盖了安全风险控制、安全审计、设备监控、安全策略管理等几个方面。

设备监控管理

指对网络中所有的网络设备，如服务器、防火墙、VPN、防病毒、入侵检测(网络、主机)、漏洞扫描等产品实现统一管理、统一监控。

安全策略管理

指管理、保护及自动分发全局性的安全策略，包括对安全设备、操作系统及应用系统的安全策略的管理。

安全分析控制

确定、控制并消除或缩减系统资源的不定事件的总过程，包括风险分析、选择、实现与测试、安全评估及所有的安全检查(含系统补丁程序检查)。

网络安全设备审计

对网络中的设备、操作系统及应用系统的日志信息收集汇总，实现对这些

信息的查询和统计;并通过对这些集中的信息的进一步分析，可以得出更深层次的安全分析结果。

第3章 网络安全管理平台总体框架

3.1 设计思想

该网络安全管理平台的设计与实现特点如下：

1) 底层通信和数据交换协议采用 SNMPv3,这是一个被广泛接受和支持的网络管理协议;

2) 系统用分层架构实现，可实现 3 层乃至多层架构，易于扩展;

3) 能提供多种访问方式和开发接口;

4) 为确保体系自身安全，对体系间的信息交流进行加密传输(SSL)，并使用了访问控制措施。

3.2 设计原理和功能

网络安全管理平台中，用户需要一个完整的网络监控解决方案，通过采集网络信息、设备信息等，能够对网络设备、通信线路、网络状态、安全状况等进行监视和控制，并对这些网络设备和网络状态进行充分的管理，使它们能够达到本来的对网络安全稳定所起的作用。

设备监控系统将通过集中的管理平台来实现，集中式的管理平台能够总体监控整个网络多层面、分布式的系统，实现对各种网络安全资源的集中监控，使得网络安全管理工作由繁变简，更为有效。

对网络设备进行监控的时候，对于大多数普通网络设备，应以管理和监控设备的网络状态等基本内容为主，而针对于特定安全产品，除了对网络状态的监控外，重点在设备管理状态、安全状态、应用状态等的监控。

通过统一的监控管理系统，将分散在各地区、不同网络上面的各种设备有机的结成一个整体。监控管理系统是全局的网络状态为核心，实时地集中收集设备状态信息、并进行相关性分析，并为网络和设备提供真正有用控制，监控管理系统还提供多种预警和响应机制，及时控制和处理事件。

基于以上对功能和技术的需求，本文设计了一个灵活的可扩充的网络安全

管理平台。

该安全平台通过集中的网络安全管理来实现对网络中多个安全设备的总体配置、调控整个网络多层面、分布式的安全系统，实现对各种网络安全资源的集中监控、统一策略管理、智能审计及多种安全功能模块之间的互动，使得网络安全管理工作由繁变简，更为有效。

3.3 系统部署

由于安全设备管理处理本身的特点，在系统结构的设计上，采取了分散处理、分散存储、统一管理、统一审计的分布式结构，以适应安全管理的需要。

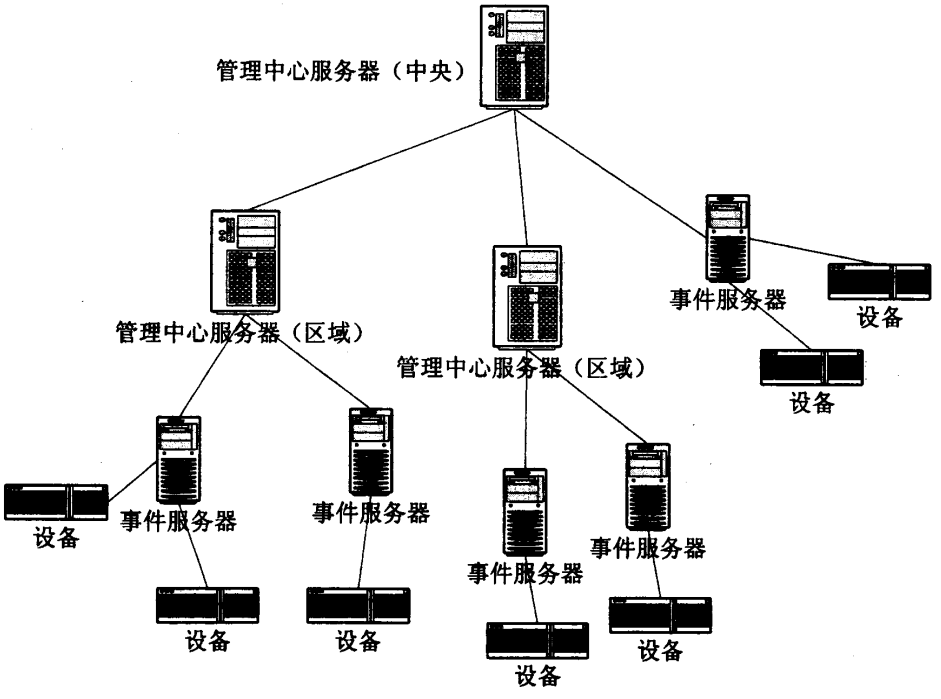

图 3-1 系统部署图

如上图所示：系统设计的特点之一是采用级联结构，可以无限级联，适应从简单到复杂的网络结构。

设备指包括被管理和监控的网络安全设备，以及路由器等普通网络设备。设备是最基础的管理节点。

事件服务器是网络安全管理平台的基础服务器，承担了系统结构中的“分散处理、分散存储”的功能。

作为基础服务器，事件服务器可以独立运行，拥有事件管理的全部基本功

能，可以作为一个小型节点（几台受控设备、比较小的网络范围）内的事件管理服务器。

每个事件服务器最多只能有一个上级的事件管理中心。

管理中心服务器是网络安全管理平台的中心管理服务器，承担系统结构中的统一管理、统一审计作用。

事件管理中心支持级联。每个管理中心最多只能有一个上级管理中心。

3.4 软件结构

下图是事件服务器和管理中心服务器的软件结构，反映了事件服务器和管理中心之间的级联关系：

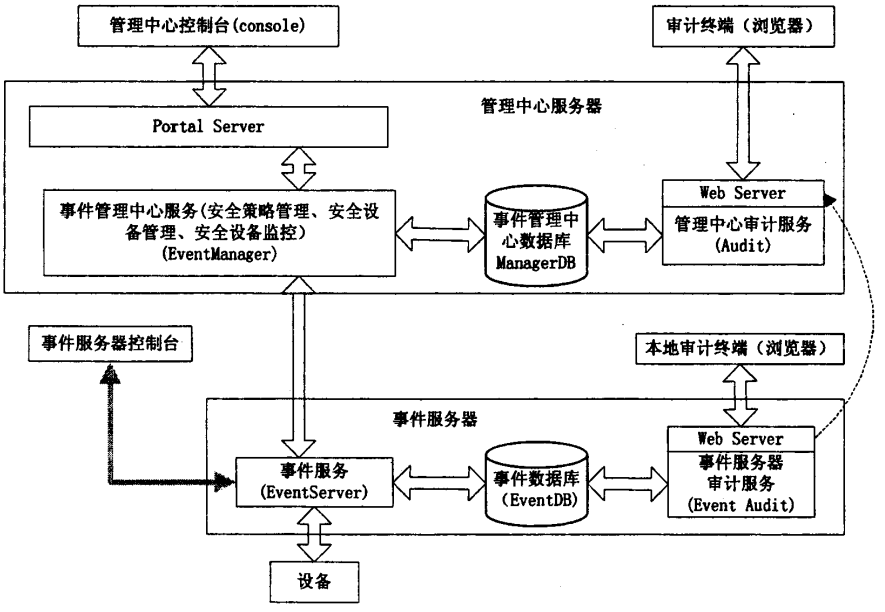

图 3-2 事件服务器与管理中心级联图

下图是管理中心之间级联的关系：

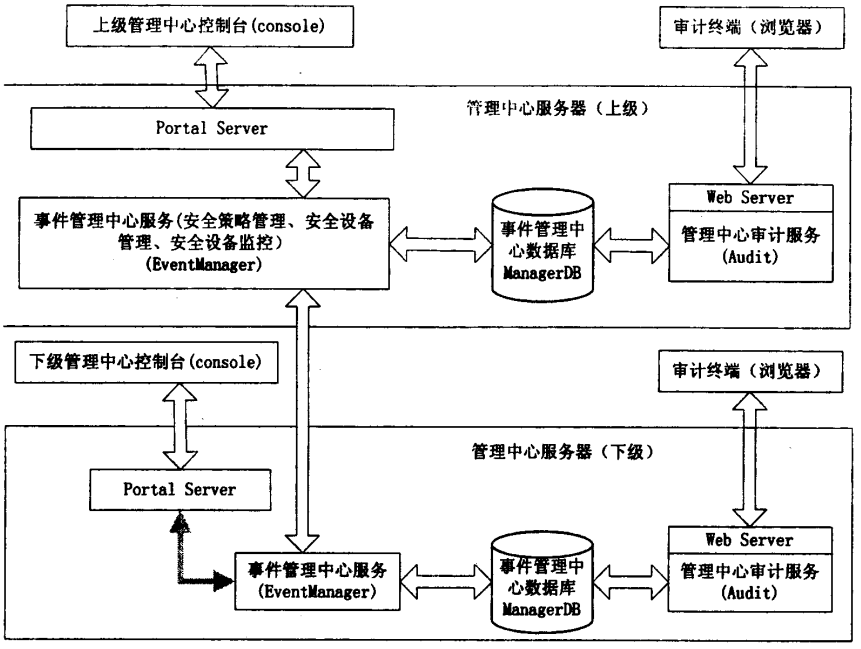

图 3-3 管理中心级联图

网络安全管理平台结构如上图。主要组件包括：

事件管理中心：中心控制台（ManagerConsole），管理中心（EventManager），数据库（ManagerDB），管理中心审计服务（ManagerAudit）。

事件服务器：事件服务器控制台（EventConsole），事件服务器（EventServer），事件适配器（EventAdapter），数据库（EventDB），事件服务器审计服务（EventAudit）。下面分别描述

3.4.1 事件管理中心

管理系统以事件管理中心（简称管理中心）为核心。事件管理中心通过事件服务器接收设备发出的事件，对事件进行实时分析，并写入管理系统数据库。同时，事件管理中心还接收并处理控制台的请求，管理设备组织结构，处理监控数据。此外，事件管理中心还处理系统自身的身份及权限等。

3.4.2 管理中心控制台

事件管理中心控制台（简称为管理控制台）是用户操作网络安全管理平台的界面，用户的操作通过控制台反映给管理中心，并将处理的结果返回给控制台

并显示出来。

控制台包括多个控制台模块。

系统管理控制台模块组提供对网络安全管理平台自身系统的管理与维护，包括用户与权限管理、事件服务器管理、系统日志管理等部分。

设备管理控制台模块组提供对设备组织结构的管理、设备地图等功能的界面，通过这个控制台，管理员可以设定整个管理系统运行的方式、范围等。

系统监控控制台模块组提供对所管理设备的运行状态、事件（日志）的实时监视界面。

一套网络安全管理平台系统可以有多个管理控制台。

3.4.3 审计服务器

审计服务器是一个单独的子系统，实现对存储在管理系统数据库中的设备事件的查询、统计分析，生成报表，并将结果通过 Web Server 发送给审计终端。审计终端就是一个浏览器（例如 IE）。

事件管理中心和所有事件服务器各带一个审计服务器。

3.4.4 事件服务器

事件服务器是管理系统的下级管理机构。事件服务器通过事件适配器接收设备发出的事件，对事件进行实时分析，并写入事件服务器数据库。同时，事件服务器还接收并处理控制台的请求，管理设备组织结构，处理监控数据。此外，事件服务器还可以接受事件管理中心的管理，将事件管理中心的控制命令通过事件适配器转发给控制台，并将设备的日志和属性参数等，传送给管理中心。

管理中心和事件服务器间通过专门的 TCP/SSL 通道连接。

一套网络安全管理平台至多有一个管理中心实例，可以有多个事件服务器实例。没有事件管理中心，事件服务器也可以自成体系，独立工作。

3.4.5 事件适配器

事件适配器直接与安全设备代理（控制台）连接，将事件服务器的控制命令转发给控制台，并将设备的日志和属性参数等，传送给事件服务器。

事件适配器必须与安全设备代理（控制台）安装在同一台计算机。

一套网络安全管理平台系统至少有一个事件服务器实例，可以有多个事件适配器实例。

3.4.6 事件服务器控制台

事件服务器控制台是管理中心控制台的简化，是事件服务器用户操作事件服务器的界面，用户的操作通过控制台反映给事件服务器，并将处理的结果返回给控制台并显示出来。

3.5 功能模块结构

3.5.1 安全设备管理

此类功能主要是以网络安全设备为管理对象。所管理的安全设备加入网络安全管理平台中或删除，在系统中的设备可以被配置和监控。并为用户提供多种表现这些设备在网络中的组织关系，位置信息的功能。以及用网络安全管理平台组建用户的安全管理组织网络的功能。此外还有为了安全信息审计的需要，提供的用户主机组织管理功能。具体的功能有：设备组织管理，设备配置，设备地图，主机管理。

3.5.2 安全设备监控

此类功能主要是以网络设备的安全信息为管理对象。网络安全管理平台对来自网络安全设备的安全信息分类进行处理：对设备实时状态信息（如 CPU，网口的状态参数）进行显示；对网络安全事件和设备工作日志进行识别、归一化、保存等数据管理工作；并同时对这些安全事件进行实时分析和统计，从中发现更多和更深入的安全信息；这些安全事件还可以实时显示在用户界面上。

3.5.3 安全策略

此类功能主要是提供集中的方式处理网络安全设备的策略配置问题，为用户提供统一的策略配置界面，用户可在该界面中进行策略个性化配置、策略模板应用和策略部署。

3.5.4 安全审计

此类功能主要是以存储在系统数据库中网络安全事件和安全设备日志为处理对象。可以对这些安全信息根据各种条件进行查询，找到每一条安全信息的详细记录。可以对这些安全信息根据各种策略和规则，进行综合分析和统计，产生各种报表，为用户提供各种网络安全统计信息，并以符合国内用户习惯的表格和图形的形式表现出来。

3.5.5 系统管理

作为安全管理平台，网络安全管理平台自身的安全也是很重要的问题。网络安全管理平台具有完善的自身用户管理，以及用户权限的管理。网络安全管理平台能够对系统本身的各种参数和安全性进行配置和控制。网络安全管理平台还可以记录并审计自身的工作日志。

第4章 设备监控模块的设计实现

在安全管理中心系统中，用户需要一个完整的网络监控解决方案，通过采集网络信息、设备信息等，能够对网络设备、通信线路、网络状态、安全状况等进行监视和控制，并对这些网络设备和网络状态进行充分的管理，使它们能够达到本来的对网络安全稳定所起的作用。

设备监控系统将通过集中的管理平台来实现，一个集中式的管理平台能够总体监控整个网络多层面、分布式的系统，实现对各种网络安全资源的集中监控，使得网络安全管理工作由繁变简，更为有效。

目前许多企业购置了大量不同的设备产品，功能的不同决定了它们有各自不同的着眼点。我们在对网络设备进行监控的时候，对于大多数普通网络设备，我们以管理和监控设备的网络状态等基本内容为主，而针对于安全设备产品，我们除了对网络状态的监控外，重点在设备管理状态、安全状态、应用状态等的监控。

通过统一的监控管理系统，将分散在各地区、不同网络上面的各种设备有机的结成一个整体。监控管理系统是全局的网络状态为核心，实时地集中收集设备状态信息、并进行相关性分析，并为网络和设备提供真正有用的控制，监控管理系统还提供多种预警和响应机制，及时控制和处理事件。

4.1 设计目标

设备监控功能允许用户能够监视整个计算环境中所有普通设备和安全设备的运行状态，控制和影响设备。主要提供：

设备监视：提供多个设备的信息同时监视和单个设备的详细信息监视；系统对于普通 snmp 设备监控标准 snmp 管理信息，对于安全设备提供更多设备相关的监控信息。

历史数据分析：对于某些重要监控数据提供一段时间内的数据图表分析，协助了解和诊断设备运行情况。系统提供对设备某一个事件段内的状态监控。

设备控制：提供设备的常用控制操作，包括关闭、重启、阻断网口等。

设备配置：集成安全设备 web 管理页面，允许用户直接配置设备。

日志数量监控与日志记录浏览：分类别统计被管设备的安全日志数量，并提供部分最新日志的浏览。

通过一个控制台，用户就能够监控整个计算环境中所有安全设备的运行状态，针对系统中管理的设备，重点监视设备的网络状态、运行状态，资源使用状态。通过监视设备网络状态来了解设备网络接口的网络负载，确定网络端口是否存在拥塞，判断网络接口是否正常工作。设备的运行状态主要是通过监视一些设备内的资源利用状况来分析确定，如设备的 CPU 利用率、内存利用率、磁盘利用率等。在本网络安全管理系统中，由用户指定对设备进行监控的项目，系统定期轮询设备相关数据，以动态曲线的方式在客户端界面上显示；当监控的某种参数值异常时，说明当前设备运行状态可能存在某些问题，系统给出告警提示，通知用户。

监视设备是否在线，普通设备以 ICMP PING 或 SNMP GET 方式；对于安全设备，以接收 HeartBeat、PING、SNMP GET 相结合的方式。

监控设备范围：设备监控对象包含两类：普通设备和安全设备（防火墙、IDS 等）。

4.2 处理流程

4.2.1 系统逻辑流程

服务器端：

- 启动网络设备状态论询服务 DeviceStatusPollingService；
- 启动设备监控调度服务 DeviceMonitorSchedulerService；
- 注册服务器端应用 DeviceMonitorMBean；
- 响应客户端请求
- 根据监听和论询服务，主动向客户端发送消息通知

客户端：

- 主程序加载
- 连接服务器，获取数据
- 显示设备状态等
- 接收服务器端消息并显示
- 接收用户操作

- 请求服务器
- 得到操作结果，显示

4.2.2 即时监控方式

当用户选中某设备，进行设备状态监控时，设备采用即时监控方式，由客户端发起设备监控请求，管理中心接收到客户端请求后，调用监控服务 Mbean，向设备或事件服务器查询设备监控数据，返回客户端显示。对于比较占用网络带宽、系统资源的操作，或对单一设备的中点监控，采用即时监控方式。

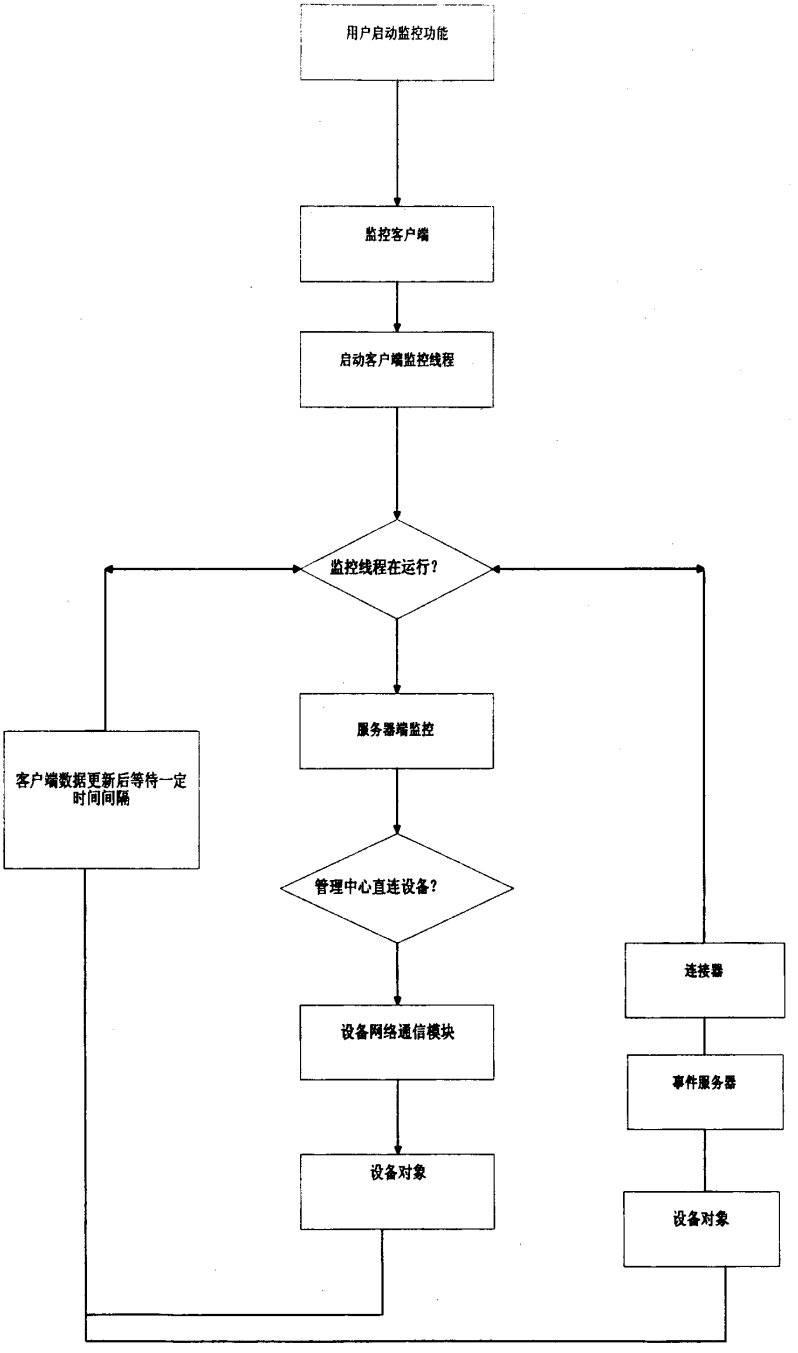

图 4-1 即时监控流程图

4.2.3 监控调度管理

系统可以对设备进行长时间的状态监控，首先由用户指定要进行自动监控的设备列表，然后安全管理中心后台从设备列表中读取设备，以一定的时间间隔

定期自动从设备或事件服务器上查询设备状态，并将设备状态数据以一定的格式记录到文件中。系统自动完成在一段时间内的设备状态的记录。当用户需要查看设备历史状态时，通过查看记录到文件的设备状态数据，形成设备状态呈现，并能够对设备状态历史数据进行分析，得到设备一段时间内的监控结果。

系统对设备可自动监控的项目有：

- 普通设备：
  - 网络传输速率
  - 数据包传输速率
  - 网络利用率等；
- 防火墙等安全设备：
  - 网络传输速率
  - 数据包传输速率
  - 网络利用率
  - CPU 利用率
  - 内存利用率
  - 磁盘利用率
  - 防火墙会话连接数量
  - IPSec、PPTP /L2TP 隧道连接数量
  - 日志数量（事件服务器管理的设备）等。

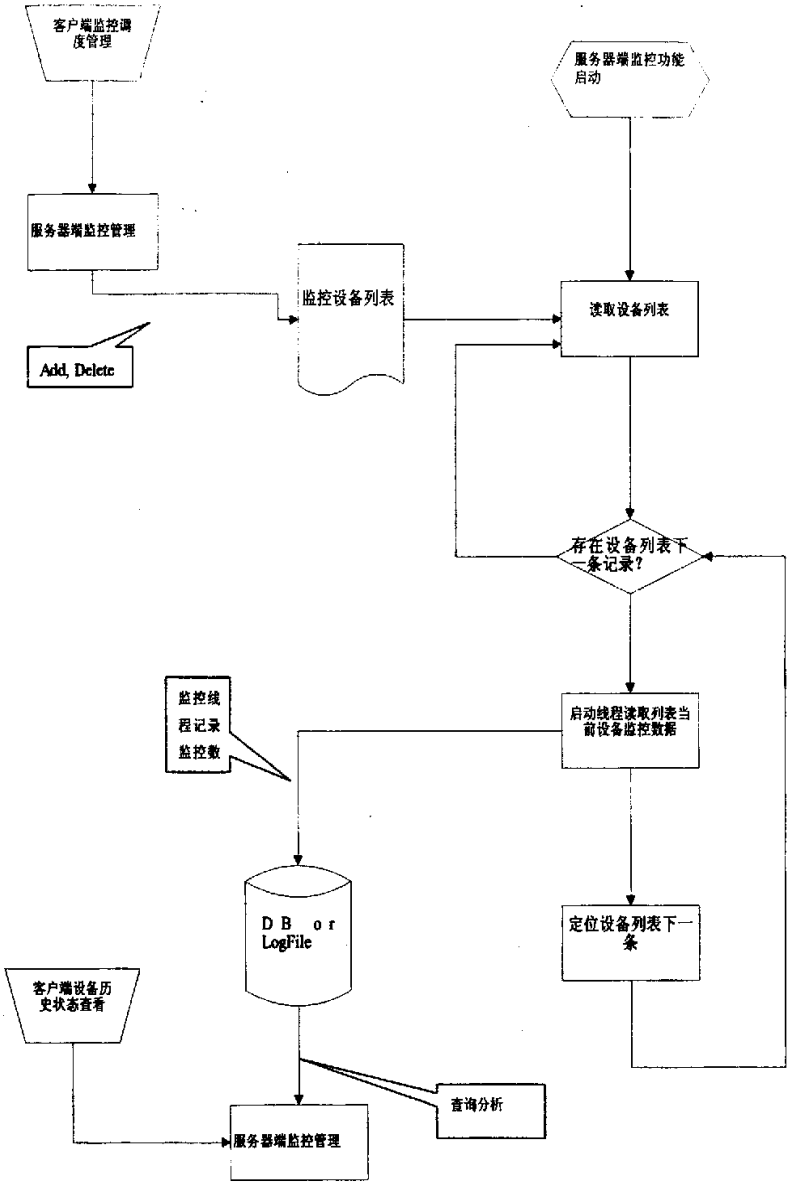

图 4-2 状态监控流程图

4.3 数据结构设计

设备监控数据单元的数据类的表示：

DevInfo：设备监控数据单元的数据类的表示
public interface DevInfo{

```
//操作单元名称
        public String getName();
        public void setName(String name);

        //操作设备对象
        public String getOperationHost();
        public void setOperationHost (String host);

//操作时间
        public long getOperationTime();
        public void setOperationTime(Date time);
 }
```

具体数据类的表示：

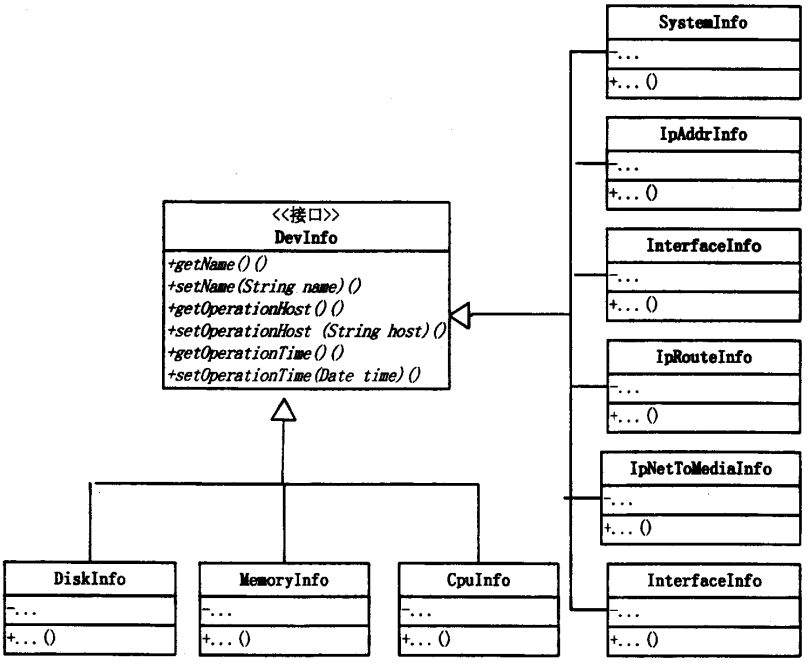

图 4-3 具体数据类的表示

类定义说明：

SystemInfo： system 组中的信息的类表示，具体包含系统名称、描述、联系方式、位置等属性的定义；

InterfaceInfo： interfaces 组中的信息的类表示，具体包含网络设备接口内容的定义，如接口类型、接口描述、接口速率、接口状态、接口收发包数、接口错误包数等属性；

IpAddrInfo： ipAddrTable 中的信息的类表示，具体包含网络设备接口 IP 设置的定义，如接口 IP 地址、接口子网掩码、接口广播地址等属性；

IpRouteInfo： ipRouteTable 中的信息的类表示，具体包含网络设备接口路由设置的定义，如接口路由地址、下一跳地址、路由类型、路由掩码、路由亮度等属性；

NetToMediaInfo： ipNetToMediaTable 中的信息的类表示，具体包含网络设备接口物理地址转换的定义，如接口物理地址、网络逻辑地址、转换类型等属性；

SystemInfo：设备系统信息的类表示，具体包含如设备类型、设备版本号、序列号等属性的定义；

DiskInfo：设备磁盘信息的类表示，具体包含如磁盘大小、已用磁盘大小、空闲磁盘大小、磁盘错误数据、磁盘路径等属性的定义；

MemoryInfo：设备内存信息的类表示，具体包含如内存总数、内存使用数、内存闲置数、共享内存大小、高速缓存大小等属性的定义；

CpuInfo：设备 CPU 信息的类表示，具体包含如设备 CPU 利用率等属性的定义；

以上定义类可根据表示的具体内容进行内容的补充。

4.3.1 网络设备访问接口定义

NetworkTransaction：网络设备访问类
public interface NetworkTransaction {

```
//读取设备系统组中的信息
public SystemInfo getSystemInfo(DeviceObject devObj);
//设置系统组中的信息
public void setSystemInfo(SystemInfo SystemInfo);

//读取设备接口组中的信息
public InterfaceInfo[] getInterfaceInfo (DeviceObject devObj);
//设置接口管理状态
public void setInterfaceAdminStatus (DeviceObject devObj, int ifIdx, int
status);

//读取设备 Ip 地址组中的信息
public IpAddrInfo[] getIpAddrInfo (DeviceObject devObj);

//读取设备 Ip 路由组中的信息
public IpRouteInfo[] getIpRouteInfo (DeviceObject devObj);

//读取设备 Ip 地址转换组中的信息
public IpNetToMediaInfo[] getIpNetToMediaInfo(DeviceObject devObj)
throws Exception;

//读取安全设备系统信息
public SystemInfo getSystemInfo(DeviceObject devObj);

//读取安全设备磁盘信息
public DiskInfo getDiskInfo (DeviceObject devObj);

//读取安全设备内存信息
```

```
        public MemoryInfo getMemoryInfo (DeviceObject devObj);

    //读取安全设备 CPU 信息
    public CpuInfo getCpuInfo (DeviceObject devObj);
    。。。。。。
     }
```

4.3.2 服务器端应用模块接口定义

```
DeviceMonitoringMBean：服务器端设备管理与监视
public interface DeviceMonitoringMBean {


}
```

其中接口中传入的参数待定

4.3.3 设备监控项 XML 配置与动态扩展

4.3.3.1 设备配置文件功能

系统通过 XML 配置文件，定义设备的监控项目，并实现动态对未知项目的监控扩展；配置文件中指定要监控项目的 OID、数据类型、范围、显示方式、读写属性等，系统启动时自动引导配置文件中的属性，运行过程中监控的内容可以以表格的形式显示和管理。

用户希望增加新的设备属性的监控时，以配置文件的方式，支持监控内容的扩展。系统支持配置文件扩展目前未知 oid 的管理信息，未知信息以列表形式提

供给用户。

设备配置文件包括如下部分：

- 设备基本特征

设备基本特征描述了设备的识别特征，以及基本的属性描述及获取方法，如设备的型号、SNMP System ObjectID，版本号，等。通过这些特征，事件服务器和管理员都可以很容易的识别出具体的设备。

- 设备监控配置

设备监控配置描述了设备的监控方式，包括设备的软硬件参数及获取方法、运行参数及获取方法。通过这些配置，事件服务器可以正确的获取设备的监控参数。

4.3.3.2 设备配置文件格式

下面是设备配置文件的格式描述，每个配置文件中可以定义一个或多个设备型号。每个配置文件是一个 XML 文件。

```
|-<devices>
|   |--<device NodeType="xxx" IconName="xxxf"
Description="xxxxxx" Category= "xx">
|   |   |--<properties>
|   |   |   |--
|   |   |--< INFOCONFIG >
|   |   |   |--
|   |   |--< MONCONIFG >
|   |   |   |--
|   |--<device NodeType="xxx" IconName="xxxf"
Description="xxxxxx" Category= "xx">
|   |   |--<properties>
|   |   |   |--
|   |   |--< INFOCONFIG >
```

| | | |--

| | |--< MONCONIFG >

| | | |--

< devices >是整个管理系统设备配置文件的根标签。

< properties >设备属性定义，可以定义设备 sysObjectID，如。

<properties>

<sysObjectID0>1.3.6.1.4.1.9833.1.1.200.1.1</sysObjectID0>

<sysObjectID1>1.3.6.1.4.1.9833.1.1.200.1.2</sysObjectID1>

</properties>

分别表示配置的 sysObjectID 相对应的设备均为该设备型号；

<DEVCONFIG>设备基本管理信息定义，可以定义设备的基本管理信息，如设备名称、序列号、配置方式、设备管理员联系方式等。

< MONCONFIG >设备监控信息定义，可以定义设备的监控对象内容、监控对象类型、监控方式等，如设备 CPU 利用率、内存利用率、磁盘利用率、网络利用率、设备连接状态等。

4.3.3.3 设备配置文件节点定义

4.3.3.3.1 COMPONENT

设备部件节点，指设备上的硬件或软件部件，如一个 CPU、一个网络接口、一个磁盘，等。设备部件节点有两种类型：

1. < COMPONENT NAME='XX' TYPE='XX'/>

简单设备部件节点，描述确定的设备部件。

- NAME 表示设备名称；
- TYPE 表示设备类型，设备类型是系统预定义的字符串，包括{"CPU","MEM","IF","DISK"}，分别表示处理器类型、内存类型、网络接口类型、磁盘类型。

2. < COMPCLASS NAME='XX' TYPE='XX' NUMOID='XX' NAMEOID='XX' FILETER='XX'/>

不确定数量的设备部件类型节点，描述一类设备部件，如网络接口。部件拥有相同的 SNMPOID，只在 OID 的最后一段不同。

- NAME 表示设备名称的前缀；
- TYPE 表示设备类型，意义和上一节相同；
- NUMOID 表示获取该类设备部件实际数量的 SNMPOID；
- NAMEOID 表示获取该类部件实际名称的 SNMPOID 前缀，获取时，需要在前缀后面加上“.序号”；序号是从 0 开始到实际数量的一个整数。
- FILTER 表示获取实际名称后的过滤条件，是一组用逗号隔开的字符串。字符串前面如果加上了'#'号，表示 NAMEOID 获取的名称中不包含该字符串，否则就是必须包含该字符串。多个字符串之间，不包含是并且关系，包含是或者关系。如果过滤规则被满足，该部件才需要被监控。如果过滤规则为空，所有部件都将被监控。

4.3.3.3.2 ITEM

部件的监控项目节点。每个硬件或软件部件都有一个或多个监控项目，每个监控项目是一个 4 个字节长度的整数。例如，CPU 部件包含了 CPU 系统利用率、CPU 用户利用率、综合利用率、温度、电压等。

4.3.3.3.2.1 ITEM 类型定义

ITEM 节点有两种类型：简单类型和计算类型

- 简单类型

简单类型指该监控项目的数值可以直接通过 SNMP GET 操作得到。格式如下：

```
<ITEM NAME='XX' MONITORID='XX' TYPE='XX' CURVE='XX' UNIT='XX' SNMPOID='XX'/>
```

属性定义如下：

- ◆ NAME 是该监控项目的名称，如 CPU 系统利用率；
- ◆ ID 是该监控项目的系统分配 ID。系统预定义了 5 个监控项目 ID，分别是 CPU 综合利用率、内存利用率、磁盘利用率、网络流量(pps)

和网络流量(bps)，对应的5个监控项目将被分配这5个监控项目ID，其余的监控项目则不分配该ID，该项目不存在；

- TYPE是监控项目类型，是系统预定义的字符串，包括{"USAGE","FLUX","STATUS", "SPEED", "TEMPERATURE", "DATA","FLOAT"}，分别表示监控数据中的"利用率"、"流量"、"状态"、"速度","温度"，"普通整数"，"普通浮点数"。
- CURVE说明该项目是否出现在监控曲线列表中。true表示显示监控曲线。
- UNIT是监控项目单位。
- SNMPOID是获取该监控项目数值的OID。特别的，如果该ITEM属于DEVCLASS父节点，在实际调用SNMP GET时，还需要加上部件序号（目前获取的是该类中第几个部件）。

- 计算类型

计算类型指该监控项目的数值不能直接通过SNMP GET操作得到，而是首先通过SNMP GET操作获得一个或多个数值，然后经过一定的计算得到一个结果。因此，计算类型中，SNMPOID属性不是一个OID字符串，而是指明了计算类型。

计算类型包括下面几种计算：

- 百分比

```
<ITEM NAME='XX' MONITORID='XX' TYPE='XX' CURVE='XX' UNIT='XX' SNMPOID='PERCENT'
VALUEOID = 'XX' TOTALOID = 'XX'/>
```

SNMP GET获取VALUEOID和TOTALOID两个数值，并计算VALUEOID/TOTALOID的百分比数值。

- 总和

指几个监控数值的总和。

```
<ITEM NAME='XX' MONITORID='XX' TYPE='XX' CURVE='XX' UNIT='XX'
SNMPOID='SUM'/>
    |--<OPITEM VALUEOID='XX'/>
```

|--<OPITEM VALUEOID='XX'/>

|--< .....

系统首先获取所有 OPITEM 子节点中 VALUEOID 指定的 SNMPOID 的监控数据，然后计算这些监控数据的总和。

◆ 平均数

指几个监控数值的平均数。

<ITEM NAME='XX' MONITORID='XX' TYPE='XX' CURVE='XX' UNIT='XX'

SNMPOID='AVG'/>

|--<OPITEM VALUEOID='XX'/>

|--<OPITEM VALUEOID='XX'/>

|--< .....

系统首先获取所有 OPITEM 子节点中 VALUEOID 指定的 SNMPOID 的监控数据，然后计算这些监控数据的平均数。

◆ 组（部件）监控项目总和

和前几种监控项目不同，该监控项目不直接和某个（组）部件及 SNMPOID 相关，而是其他多个监控项目的监控值的总和。

<ITEM NAME='XX' MONITORID='XX' TYPE='XX' CURVE='XX' UNIT='XX'

SNMPOID='GROUPSUM'/>

|--<OPITEM NAME='XX'/>

|--<OPITEM NAME='XX'/>

|--< .....

SNMPOID="GROUPSUM"时，表明该项目被用于计算 OPITEM 字节点中指定名称的监控项目的总和。注意，组（部件）监控项目总和类型监控项目和组（部件）监控项目平均数监控项目将不包括在内。

当某个部件(COMPONENT)有 GROUPSUM 类型的监控项目时，系统将在该部件的监控项目中查找名称出现在 OPITEM 子节点的监控项目，并计算它们的总和。这时候，该监控项目类似于上面的总和类型监控项目(SNMPOID="SUM")。

当某个分组(GROUP)有 GROUPSUM 类型的监控项目时，系统将在该分组，以及该分组的直接下级部件中，查找名称出现在 OPITEM 子节点中的监控项目，并计算它们的总和。特别的，如果分组中有 COMPCLASS 类型的部件，这个项目将会计算该类型的所有部件的某个（或几个）监控项目的总和，例如多个网络接口的流量总和。

◆ 组（部件）监控项目平均数

类似于组（部件）监控项目总和类型监控项目，这里计算的是多个监控项目(ITEM)的总和。

```
<ITEM NAME='XX' MONITORID='XX' TYPE='XX' CURVE='XX' UNIT='XX'
SNMPOID='GROUPAVG'/>
    |--<OPITEM NAME='XX'/>
    |--<OPITEM NAME='XX'/>
    |--< .....
```

SNMPOID="GROUPAVG"时，表明该项目被用于计算 OPITEM 字节点中指定名称的监控项目的总和。

4.3.3.3.2.2 ITEM 后续计算

后续计算是在获取了通过 SNMP 获取数据后，对获取的数据进行的后续计算。每个结果都可以有三个后续计算，计算的顺序是先执行第一个计算，再用结果执行第二个计算，最后再执行第三个计算。

- 增速（一阶导数）

增速指某个监控数值在单位时间内增加的数量。

```
<ITEM NAME='XX' MONITORID='XX' ..... >
|--<CALCULATE INDEX='X' OP='INCREMENT' OPERAND='XX'/>
```

计算在 OPERAND 秒的时间内某个监控数据的增长量。该计算是简单类型或者计算类型 1-5 的后续计算。INDEX 表示这是这个监控项目的第几个后续计算，从 1 开始计数。

- 加一个整数

在结果上增加一个整数。

```
<ITEM NAME='XX' ID='XX' ..... >
```

|--<CALCULATE INDEX='X' OP='ADD' OPERAND='XX'/>

该计算是简单类型或者计算类型 1-5 的后续计算。

- 乘一个整数

在结果上乘一个整数。

<ITEM NAME='XX' MONITORID='XX' ..... >

|--<CALCULATE INDEX='X' OP='MUL' OPERAND='XX'/>

该计算是简单类型或者计算类型 1-5 的后续计算。

4.3.3.3.2.3 ITEM 字典映射

对于状态类型或者某些其他类型的数据，可能的取值比较少，每种取值都表示某个特定的意义，如表示“正常”、“异常”、“连接”、“断开”等。监控项目的字典映射提供了一种机制，使系统可以将数值转换为对应的字符串显示给用户。

每个监控项目都可以有一个字典表。字典映射在后续计算完成之后执行，可以认为是第四个后续计算。

<ITEM NAME='XX' MONITORID='XX' ..... >

|--<DICTITEM ID='XX' VALUE='XX'/>

|--<DICTITEM ID='XX' VALUE='XX'/>

|--<DICTITEM .....

子节点 DICTITEM 给出了映射关系。

4.3.3.3.3 GROUP

设备部件组。对同类型设备部件进行的分组。

<GROUP NAME='XX' TYPE='XX'/>

NAME 是分组名称。

TYPE 是分组类型，系统预定义的字符串，等同于设备节点的类型。

4.4 模块划分及设计描述

4.4.1 结构图

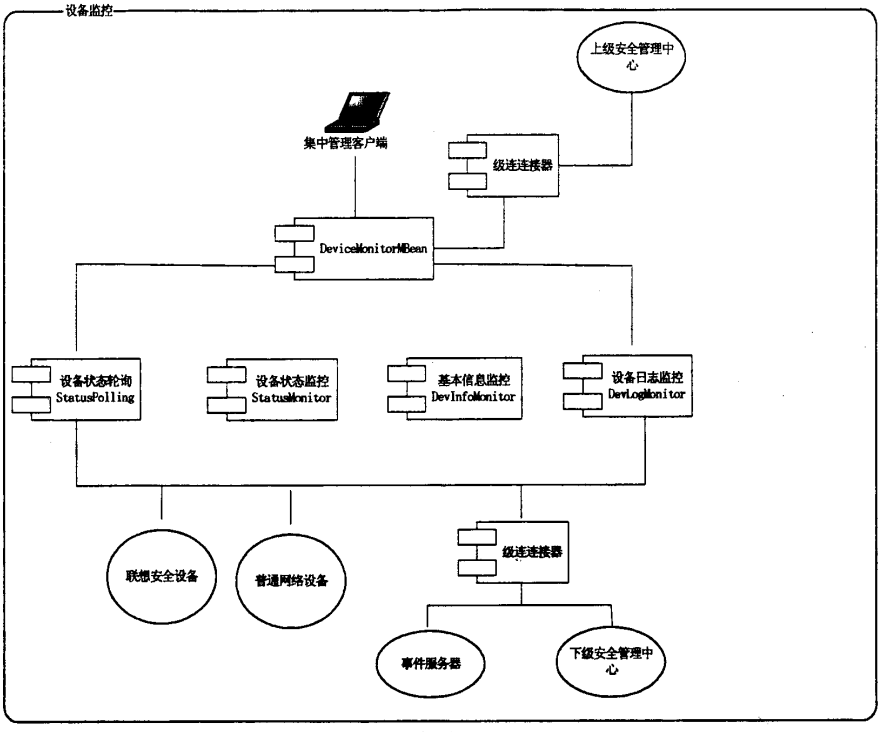

图 4-4 设备管理结构图

设备监控结构图：

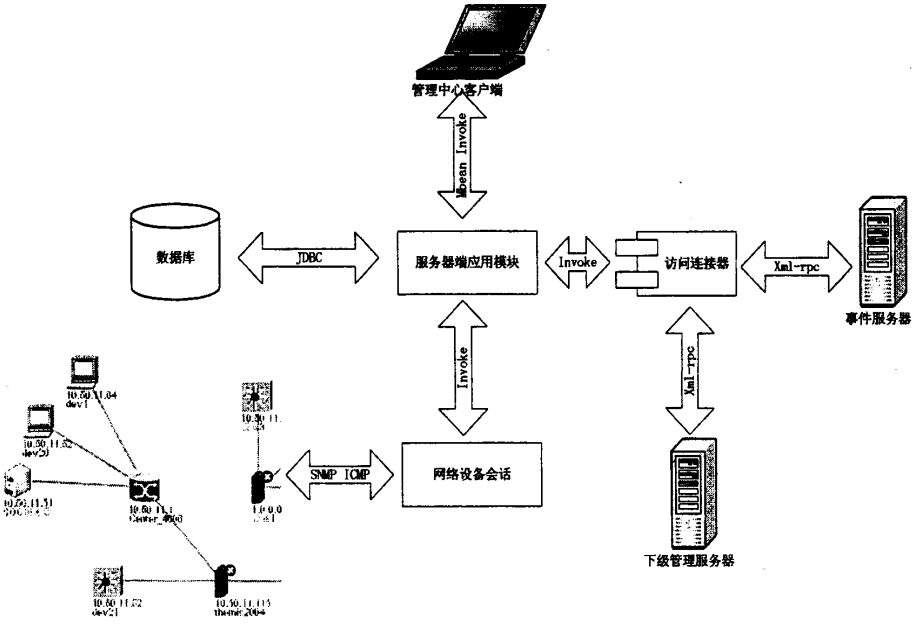

图 4-5 设备监控结构图

如上图所示，客户端应用模块实现客户端图形用户界面功能，接受用户的操作，显示操作结果；客户端通过 MBean 调用访问服务器应用模块。

服务器端应用模块是以 Mbean 的方式在服务器端注册，通过定义的接口，暴露公开的方法，接受客户端的调用请求，返回操作结果；通过调用网络设备会话模块可以对网络设备进行通信；通过 JDBC 可以对数据库服务器进行通信，实现数据存取的操作；通过连接器实现与事件管理器和下级安全管理中心通信，实现级联。

网络设备会话模块：以 SNMP 的方式，实现与网络设备的通信，通过 SNMP get 或 getNext 的方式读取设备配置、运行参数等信息，通过 SNMP set 的方式实现对设备配置参数的修改。以 ICMP 的方式，通过 ping 等方式，可以得到设备的运行状态，实现实现状态的监视。服务器应用模块可以直接调用网络设备会话层公开的方法或函数，得到相关操作结果。

模块功能简要说明

模块 1: 客户端应用模块

客户端应用模块实现客户端图形用户界面功能，接受用户的操作，显示操作结果；客户端通过 MBean 调用访问服务器应用模块；客户端实现监控结果的表现。

模块 2: 服务器端应用模块

服务器端应用模块是以 Mbean 的方式在服务器端注册，通过定义的接口，暴露公开的方法，接受客户端的调用请求，返回到客户端操作结果；通过 JDBC 可以对数据库服务器进行通信，实现数据存取的操作；通过调用网络设备会话模块可以对网络设备进行通信；通过连接器实现与事件管理器和下级安全管理中心通信，实现级联。

服务器端应用模块主要分为以下几个部分：

设备监视

设备控制

日志数量监控（通过事件服务器）

模块 3: 网络设备会话模块

网络设备会话模块：以 SNMP 的方式，实现与网络设备的通信，通过 SNMP get 或 getNext 的方式读取设备配置、运行参数等信息，通过 SNMP set 的方式实现对设备配置参数的修改。以 ICMP 的方式，通过 ping 等方式，可以得到设备

的运行状态，实现实现状态的监视。服务器应用模块可以直接调用网络设备会话层公开的方法或函数，得到相关操作结果。

模块 4: 级联访问连接模块

支持级联方式的分布式网络监控部署，即部署多层次的监控管理，下级服务器将所监控的信息上报到上级管理服务器，上级管理服务器通过连接器实现与事件管理器和下级安全管理中心通信，实现级联。每一个需要进行通讯都提供一个 XML-RPC 的连接器，其他需要与之通讯的系统采用连接器客户端访问连接器。对于 XML-RPC 连接器可以定义相互通讯专用的访问接口类。

第5章 安全策略模块的设计实现

随着网络规模与业务模式的不断增长变化，对 IT 基础设施的全局统一管理越来越成为企业 IT 部门的重要职责。策略的集中管理更有效的描述了全网设备的基本情况，便于设备间的协作、控制，能够提高问题诊断能力，提高运营的可靠性；另一方面，也极大的减轻了管理员的工作强度，使其工作效率大幅度提高。

本章描述了网络安全管理系统策略管理部分的基本思想和方法。从全局的观念讲述了策略的组织、审核、分类、分发等流程及其相互关系。

策略管理模块的特点：

策略自动生产：如果为具有层级关系的管理域创建策略后，加入到管理域中的设备，将自动拥有整个层级关系中的全部策略；

策略个性化配置：对于有特权的管理域或设备可以屏蔽上级策略，创建个性化的策略结构；

策略模版应用：可以建立安全设备的策略模版，模版可以直接应用到域或设备上；

策略自动部署：可以使用自动方式部署策略，只需要在管理中心的控制台编辑好策略后，策略就会自动分发到设备中。

策略管理的目标是可以通过集中的方式高效处理安全设备（防火墙、IDS）的策略配置问题。

5.1 设计目标

在本系统中，整个网络被划分为若干管理域，每个管理域中还有相应的下级组织部门。设备、设备所属的部门、部门所属的组织统统被认为是管理域中树状组织的的结点。

因此策略管理首先与节点信息相联系，这也就隐含了策略的层级配置管理。

另外，策略是由某个具有一定权限的管理员对某个管理域或设备制订的，因此策略是否能定制成功需要调用权限管理中的功能加以判定，因此隐含了策略的可行性管理。

全网策略被统一存储，结合节点管理，策略存储有它自身的结构特点，这些属于策略的存储管理。

策略按照一定的时间、顺序被部署到具体的设备上，无论策略是对管理域定制的，还是对设备制订的，所有相关的策略最终都要被下发到设备中去，下发的方式能够根据实际网络拓扑的变化而做适应性调整，这些属于策略的发布管理。

5.2 处理流程

下图描述了策略管理中的基本流程。

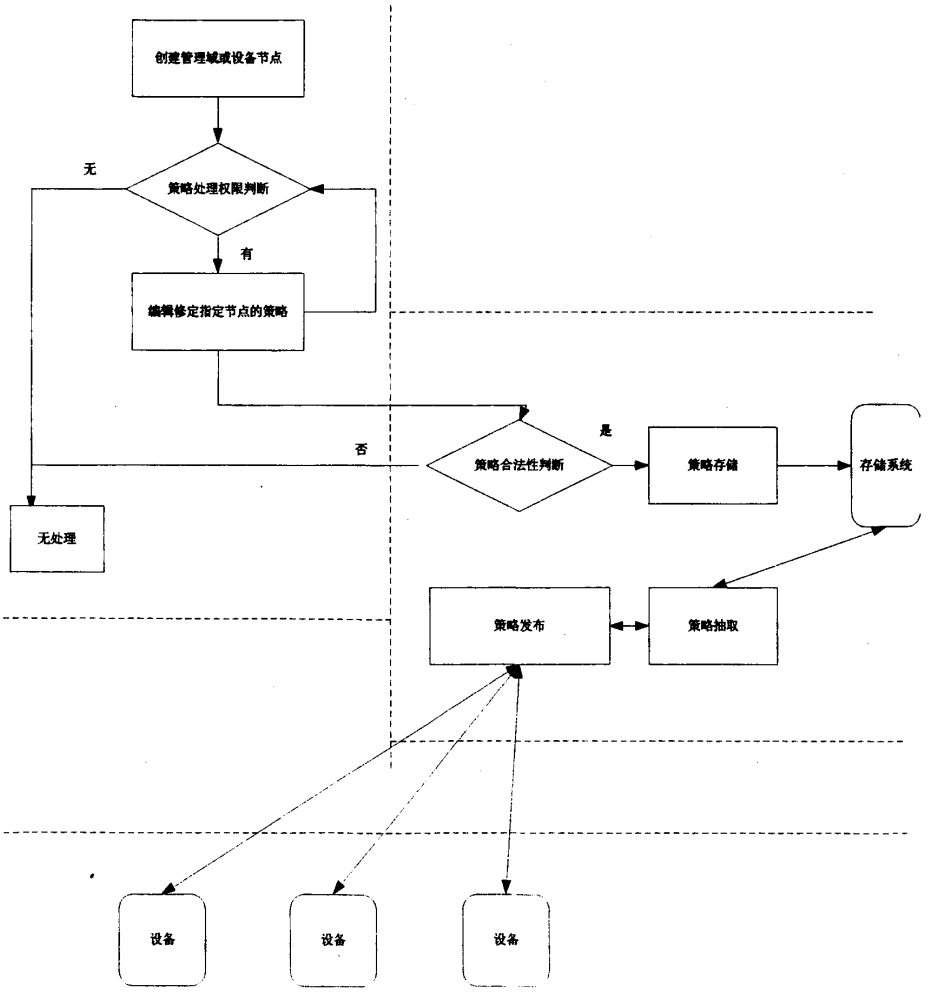

图 5-1 策略管理流程

策略管理分为两条主线：一是策略的维护，一般流程如下

1. 首先需要先创建管理域或设备节点;
2. 判断策略编辑权限，如果没有则不允许编辑策略;
3. 进行详细的策略编辑，见后文;
4. 策略存储前要进行合法性判断，如果不合法则结束;
5. 策略存储;

二是策略的发布，流程为：

1. Server 策略发布模块端接收到设备请求后，准备提取策略;
2. 策略抽取过程，采用增量或全部的提取方式将策略转为中间格式，并返回给策略发布模块;
3. 将策略发布到设备中;

5.3 数据结构设计

策略管理在集中管理器内保存了全网的策略数据结构。下面将从两方面加以描述。

5.3.1 策略基本分配结构

策略的分配与整个系统的管理层级结构密切相关。如下图

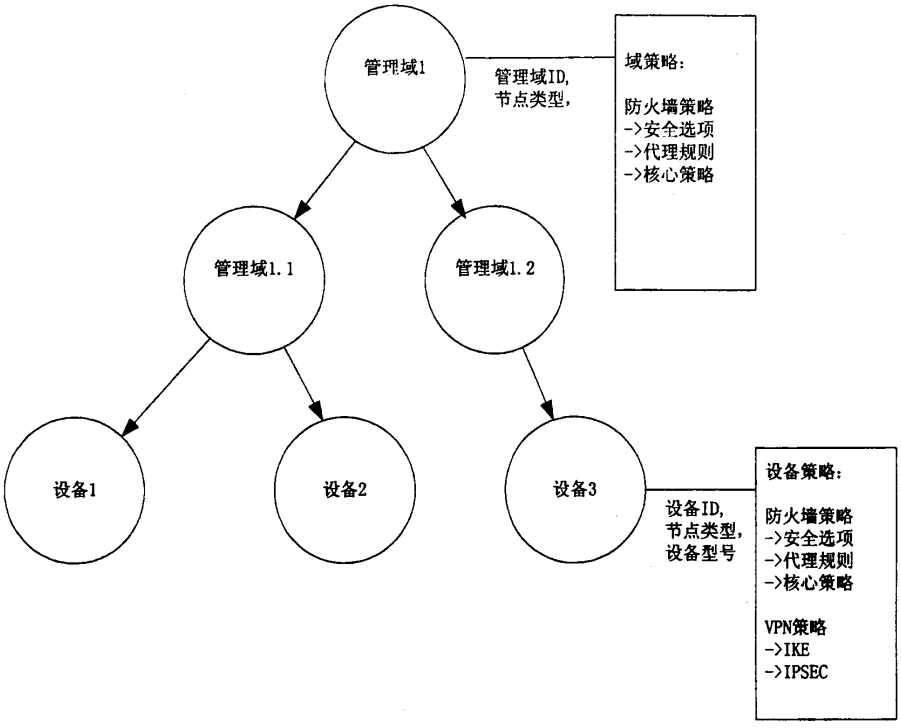

图 5-2 策略分配结构

需要说明的是每个节点[设备或管理域]都可能拥有策略，图中方框表示了该节点可能拥有的策略。方框中的内容只是该节点自己能够管理的策略，并且随着设备型号的不同，设备策略的内容会有所不同，可选的方案为对每一种相差甚远的设备类型单独设计它的策略表示结构，然后通过设备型号找到该设备对应的策略。

对于管理域策略而言，它的策略只是针对某一种特定设备类型下的域策略，由于每一种设备类型的策略是单独设计与存储的，所以很容易找到该管理域对不同设备类型描述的域策略。域策略将对该域内的设备与所有子域产生效力。

5.3.2 策略路径结构

5.3.1 节描述的是每个节点自己创建管理的策略信息，并且是策略的详细信息，但是它并没有描述某个节点所拥有的全部策略信息，即它的上级为它分配的策略等信息；另一方面，也需要描述一个节点所拥有的全部策略之间的关联信息，比如描述这些策略[包括上级制订策略与自身制订策略]之间的先后顺序等关系。因此还需要其他的结构来描述策略，即策略路径。

对系统中的任意节点[设备或管理域]都记录了它的策略路径。

如下面的示例：

	ObjID	RID	RSID	RType	Effective
1	100	10	1	1	1
2	100	15	2	1	1
3	100	8	3	0	1
4	100	9	4	0	1
5	101	10	2	1	1
6	101	15	3	1	0
7	101	8	1	1	1
8	101	9	4	1	1
9	101	17	5	0	1
10	101	18	6	0	1
11	101	30	7	0	1
12	101	32	8	0	1
13	101	50	9	0	1

表格 5-1 策略路径

说明：上面的表格中描述了两个节点的策略路径，这两个节点的编号分别是 100，101。

关于节点 100 一共有 4 条记录，说明与节点 100 相关的策略一共有 4 条，关于节点 101 一共有 9 条记录，说明与节点 100 相关的策略一共有 9 条。

每一条记录中包含节点的 ID 号即 OID,如表格中的 100，101；

策略编号 RID，是一条策略的唯一编号，此号在策略创建时分配；

策略的顺序号 RSID，该号表示此条策略在该节点所含全部策略中的位置顺序；

策略类型 RType，表明此条策略是节点自身创建的，还是它的上级创建的；

生效标记 Effective，此标记声明设备或管理域节点对策略的认可，比如：如果策略是上级创建的并被上级声明为有效，并且此节点的操作者有权限的话，它可以否认此条策略在此节点上生效，如第 6 条记录表示的那样。

从上面的表格中可以表示出一个简单的路径关系：

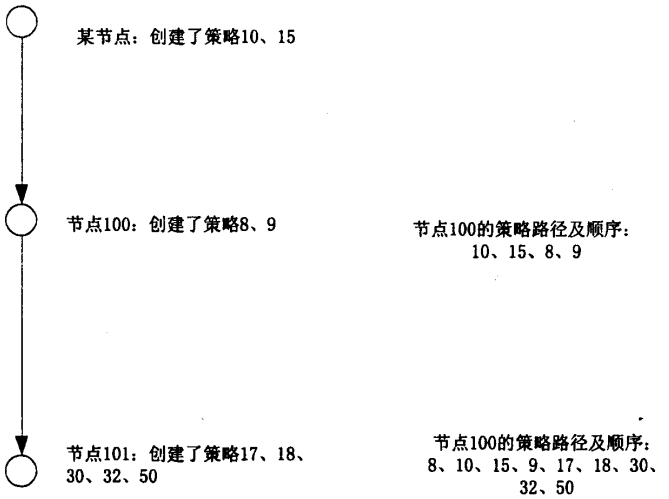

图 5-3 策略路径

5.4 模块划分及设计描述

此部分描述策略管理中策略维护的主要过程。

5.4.1 策略初始化

5.4.1.1 描述

策略的初始化总是伴随着的节点的创建而产生。即当添加了新的管理域或设备后，系统会为这些节点默认的初始化一些策略，以使得这些节点的策略能够有一个合理的初始化状态。这些被初始化的数据包括“资源”与“策略”。

5.4.1.2 流程

当添加设备[防火墙类型的设备]时，初始化的策略相关内容：

1）资源--普通地址列表：增加 1 条名字为 any 的记录；

2）资源--动态服务列表：增加 7 条记录；

3）如果为防火墙系列则：

3.1) 策略—防火墙通用安全选项：增加 1 条初始记录；

3.2) 策略—防火墙通用代理选项：增加 1 条初始记录；

3.3) 核心策略引用—防火墙核心规则对应表：建立该节点所拥有的全部上级策略的引用，操作是将此节点的上级节点在该表中的内容拷贝；

4）更新域或设备的 PmodifyTime 信息，以放映最新的策略修改情况；

5）需要统计 PnodeNumber，即路径节点数。

当添加域时，相应初始化的策略相关内容：

1）资源--普通地址列表：增加 1 条名字为 any 的记录；

2）资源--动态服务列表：增加 7 条记录。

3）对于防火墙系列则：

3.1) 策略-- 防火墙通用安全选项：增加 1 条初始记录；

3.2) 策略-- 防火墙通用代理选项：增加 1 条初始记录；

3.3) 核心策略引用-- 防火墙核心规则对应表：建立该节点所拥有的全部上级策略的引用，操作是将此节点的上级节点在该表中的内容拷贝；

4）更新域或设备的 PmodifyTime 信息，以放映最新的策略修改情况；

5） 需要统计 PnodeNumber，即路径节点数。

域和设备的主要区别在于域中可能存在各种类型设备，所以要初始化所有类型的策略，这些不同类型的策略会有不同的数据结构对应。策略初始化的一个最明显的作用，使得域或设备在加入到相应域内的时候，自动拥有了父域的策略。

5.4.2 策略添加

5.4.2.1 描述

策略添加主要涉及为某一个域或设备增加新的策略。

5.4.2.2 流程

策略添加主要用于为一个域添加策略时的情况。

1）进行合法的策略添加；

2）如果第 1 步成功，则要更新该域以及子域及域内设备的策略路径，并一直递归到该域的每个子节点都完成一遍操作为止；[要区分添加的是哪种设备类型的域策略，从而仅更新相关的策略路径]

3）更新域或设备的 PmodifyTime 信息，以反映最新的策略修改情况。

5.4.3 策略修改

5.4.3.1 描述

策略修改主要涉及域或设备的策略修改；

5.4.3.2 流程

策略修改不涉及节点策略路径的变化；

1）对策略进行合法的修改；

2）更新域或设备的 PmodifyTime 信息，以反映最新的策略修改情况。

5.4.4 策略删除

5.4.4.1 描述

策略删除分为两种情况，一是删除某个域或设备上的策略；二是删除一个域或设备而引起的策略删除。

5.4.4.2 流程

删除域或设备上的策略时：

1）对策略进行合法删除；

2）如果删除的是域上的策略，则递归更新域、子域、设备的策略路径；

[要区别被删除策略的设备类型，仅更新相关设备类型的策略]

3）更新域或设备的 PmodifyTime 信息，以反映最新的策略修改情况。

删除域或设备时：如果删除的是域则将域下的子域、设备也一并删除，同时也要删掉记录的资源、策略信息；如果删除的是设备，则仅需要清除该设备相关的资源、策略信息。

5.4.5 策略约束

5.4.5.1 描述

在进行策略维护时还有一些通用的规则，在此说明。

1）依据策略自身的角度：策略有三种状态：编辑、发布、生效，策略的缺省状态是可发布与生效。

编辑状态：策略正在构思、编辑过程中，这时编写的策略不会发布到设备上去；换句话说，设备在向管理中心请求新策略时，如果发现该设备的设备路径[域-子域-设备]上有某个节点被标识为编辑时，则不会抽取相关策略，直至该状态被管理员重新标定为发布时。

发布状态：策略随时可以发布到设备上去的状态，如果编辑了一部分合法的策略，此时有设备请求策略时，这部分策略也会发布到设备上，而不管管理员是否已经修改、规划好全网策略。

编辑与发布状态的粒度是设备级的，它们在 Net_Device 网元结构中被标识为 PStatus。

生效状态：描述一条具体的策略是否应该在设备上起作用，它的粒度是核心策略级的。核心策略仅指包过滤、端口 IP 映射、NAT、代理而言[在超 5 中，代理规则已经和并到了包过滤中]。

它们在 PV_PolicyInfo 中被标识为 Effective；另外在策略路径中还有一个 Effective,它描述的与 PV_PolicyInfo 中的 Effective 是一回事，都是策略在设备上的生效状态，Effective 属于策略内容的一部分。不同的是策略路径中的 Effective 可以取替 PV_PolicyInfo 中 Effective 的作用，举个例子，域策略中有一条策略被

标识为 Effective，这个值记录在 PV_PolicyInfo 中，它的子域的策略路径中也有这条策略的引用，如果管理员有足够权限的话，它可以在该子域所属的策略路径中将此条策略的 Effective 失效，那么当策略在下发到该子域的设备上时，此策略将失效。

改变域的生效状态涉及对指定设备类型策略路径递归更新的过程。

2）依据操作者的特权角度：

在防火墙的策略中，有一种类型的策略，使得域或设备都可以对其进行设置[包括通用策略选项和代理规则]，这就会产生策略的冲突。系统缺省的做法是使用上级制订的策略覆盖下级制订的策略，但当下级有特殊权限时，可以屏蔽上级的此类策略。

这些是在系统中通过防火墙通用安全选项与防火墙通用代理选项中的 Effective 与 Privilege 两个标记实现的。

在某个节点[域或设备]上制订此类策略时，选中 Effective 表示希望自己制订的策略对本身及下级生效，如果自身的上级也选中了 Effective，则当前节点制订的策略内容不会生效；如果希望当前制订的此类策略生效，则需要选中 Privilege 标记[如果有权限的话]，那么它就屏蔽了上级对此类策略的制订。

第6章 系统接口

6.1 通信接口

6.1.1 网络协议

通信接口包括事件服务器与控制台、管理中心之间的接口。

控制台和事件服务器之间，管理中心和事件服务器之间都是通过 TCP/SSL 协议通信。通信协议使用通信接口类 CCmdSSLSock 和 CCmdSSLListenSock 封装，同时包括了数据的打包、解包。使接收、发送线程可以容易的传输接口对象数据包。

系统之间传输数据时，通信接口在每个数据包前添加一个 4 字节的网络格式无符号整数标示出该数据包的长度，当另一方的通信接口接收到后，首先取出这个整数，然后完整的读取这个长度的数据，这样，接收线程获得的就是一个和发送时一致的完整的数据包。

下图是数据报文格式。

length（4byte）	数据（长度为 length）

头部是 4 字节的网络字节序的无符号整数，数据部分采用位数据，传递请求和数据。

6.1.2 接口命令对象

在用户界面和管理中心之间采用对象化的方法传输请求和应答。所有的请求、应答和通知都被封装为对象，对象包括了请求、应答和通知的类型、名称以及参数表。这些对象可以自行序列化为预定义的格式传输到对方，然后自行反序列化为原有的对象，相当于在用户界面和管理中心之间直接传递请求、应答和通知的对象。这样的对象称为接口命令对象。

所有的接口对象都从 CCmdObject 类派生。

6.1.3 通信接口

通信接口包括两个接口类：侦听接口类 CCmdSSLListenSock 和通信接口类 CCmdSSLSock。

侦听接口类用于服务端，建立 TCP/SSL 侦听，有连接请求后建立连接，创建通信接口实例。

通信接口类用于客户端和服务端，封装了接口命令对象的传输。下图是 CCmdSSLSock 传输接口命令对象的过程说明：

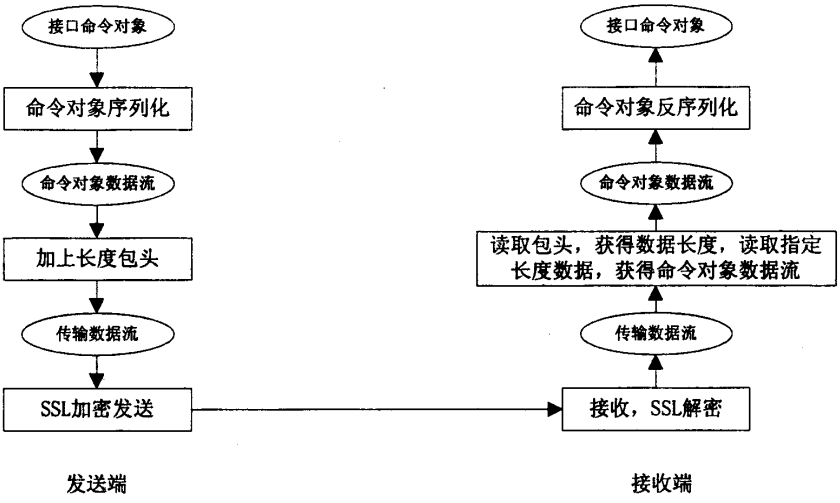

图 6-1 接口命令对象传输过程

6.2 访问接口

管理中心向其他模块（系统）提供的接口包括控制台接口、上级管理中心接口、集成接口。

事件服务器向其他模块（系统）提供的接口包括控制台接口和管理中心接口。

这些接口统称为访问接口。访问接口接收到的请求将被转换成为访问接口命令类，提交给访问服务处理。

6.2.1 访问接口方法

访问服务提供的接口方法，也就是访问服务可以处理的访问接口命令类。这些方法包括连接与登陆、设备管理、设备监控、策略管理、系统管理等。用于

提供给上级管理中心和本地控制台。

6.2.2 控制台接口

控制台接口是建立在前面描述的通信接口（侦听接口类CCmdSSLListenSock和通信接口类CCmdSSLSock）基础上的。

访问接口管理器首先处理控制台通过TCP/SSL的连接请求，建立通信连接。通信连接建立后，访问接口管理器将创建一个控制台接口。

控制台接口线程接收控制台通过TCP/SSL发送来的请求数据报文，将报文转换为某个访问服务请求类对象（CCRequestObject的派生类对象），发送给访问服务线程。

访问服务处理完成后，调用控制台接口的方法，将应答对象(CCResponseObjectd的派生类对象)转换为应答数据报文，发送给控制台。同时，通知对象（CCNotifyObject派生类对象）也会被控制台接口转换为数据报文，发送给控制台。

每个控制台接口是一个对象，包括一个线程（用于侦听并接收请求），以及一个用于发送应答与通知的接口。

6.2.2.1 管理中心接口

管理中心接口和控制台接口类似，也是建立在侦听接口类CCmdSSLListenSock和通信接口类CCmdSSLSock基础上的。

管理中心接口接收管理中心通过通信接口发送来的请求数据报文，将报文转换为某个访问服务请求类（CCRequestObject的派生类），发送给访问服务。

访问服务处理完成后，调用管理中心接口的方法，将应答对象(CCResponseObject)转换为应答数据报文，发送给管理中心。同时，通知对象也会被管理中心接口转换为数据报文，发送给管理中心。

系统中只有一个管理中心接口，在系统启动时创建。

管理中心接口是一个对象，包括一个线程（用于侦听并接收请求），以及一个用于发送应答与通知的接口。

6.3 上级管理中心接口

上级管理中心接口和管理中心接口类似。

6.4 配置界面接口

配置界面接口提供了本地配置界面进程的访问接口，只提供给本地的管理中心配置界面。

由于配置界面和管理中心在一个主机中，因此，和其他接口不同，配置界面接口不是通过 TCP/SSL 方式，而仅仅使用本地环路（127.0.0.1）的 UDP 接口进行通信，因此，也不采用命令对象方式，而是简单的采用 XML 字符串来传输配置请求。

配置界面提供的方法包括：

名称	参数	说明
ADDEVENTSERVER	事件服务器参数	添加一个事件服务器到管理中心
REMOVEEVENTSERVER	事件服务器 ID	删除一个事件服务器
SETEVENTSERVER	事件服务器参数	修改一个事件服务器的参数
GETCONSOLES		获取连接中的控制台状态
GETEVENTSERVERS		获取全部下级事件服务器状态
GETMANAGERSTATUS		获取上级管理中心连接状态
SETCONFIG		配置文件已更新，重新调入配置文件
KICKUSER		强制断开在线上的用户
SYSTEMTIMECHANGED		机器时间被修改

表格 6-1 配置界面方法列表

6.5 事件服务器设备插件接口

事件服务为某些类型的设备编写一个插件，用来处理这个设备特有的数据，

如解析特殊格式的日志字符串、监控特别类型的设备状态，获取（设置）该设备特有的参数，等等。

设备插件是一个按照约定接口编写的 DLL。事件服务器的设备插件接口包括 DLL 识别接口和对象接口。

DLL 识别接口是事件服务用来识别一个 DLL 是不是设备插件的接口，是 DLL 输出的接口方法。插件 DLL 必须具有这些接口。这些方法包括：

获取插件的版本号：bool GetPluginVersion(char * buf, int buflen)

获取插件的模块号：bool GetModule(char * buf, int buflen)

获取插件对应设备的 SystemObjectID：bool GetSystemObjectID(char * bufoid, int buflenoid, char * bufName, int buflenName)

创建一个插件接口对象实例：IDeviceInterface * CreateInterface()

插件接口对象(IDeviceInterface)是插件提供给事件服务的接口对象。通过这个对象，事件服务就可以访问设备插件的方法，实现对设备的管理。每个设备对象都将创建一个插件接口对象实例。插件 DLL 必须继承这个接口对象，并实现全部方法。

virtual bool Set(unsigned long nDevMgrIP)：设置设备接口实例的管理 IP 地址

virtual CDevEventObject * ParseLog(const char * strLog)：解析该设备发出的原始日志字符串

virtual CSecDeviceData* GetDeviceInfo()：获取设备的设备的硬件及软件信息

硬件及软件信息以 XML 串的形式提供(CSecDeviceData 的 m_xmlDevInfo 属性)：virtual unsigned short GetDevMonitorData(MONITORVALUE * arrayDataBuf, unsigned short size)

获取设备的运行参数：virtual int GetDevAlertState(sstring & strAlertMessage) 获取设备的报警状态

virtual sstring GetDevPolicy(int nType)：获取设备的管理规则（设备的管理规则指管理员为设备配置的运行分析规则，如 IDS 的分析规则，防火墙的过滤规则，路由器的路由表等等）

virtual bool SetDevPolicy(int nAction, int nType, const void * bufPolicy,

unsigned long nPolicySize)：设置设备的管理规则。

第7章 总结和下一步工作

7.1 总结

本文讨论了网络安全管理的范畴和技术。提出了一种新的分布式多层次的网络安全管理平台的设计，并给出了设备监控与安全策略这两个关键模块的详细设计。该平台从网络的整体安全出发，通过对网络中各个网络设备的集中监控，集中配置，以及通过集中收集、格式归一化和关联存储等功能来管理网络中来自于各个网络设备的安全信息（安全事件和各种日志），进而实现实时监测网络中的安全状态，动态调整网络安全策略，综合审计网络安全信息，有效提升了用户网络安全的可管理性和安全水平。

系统的主要特点在于：该平台采用级联结构，可以无限级联，适应从简单到复杂的网络结构。结合了负载均衡和分布式技术的优点，具有很大的灵活性。解决了以往网络安全管理平台可扩充性不够的缺点。

在两级级联（事件服务器-设备）的情况下，该系统可以对 0-255 台设备进行安全管理。在多级级联（管理中心服务器-事件服务器-设备）的情况下，理论上可以对无限数量的设备进行安全管理。

根据该原型系统设计的商业软件已投入实际使用。

7.2 下一步工作方向

随着技术进一步发展，网络的复杂度增加，以 SNMP 技术为基础的网络管理技术已经逐渐不能满足网络安全管理的需求。为降低网络设备管理系统的开发成本及管理成本，并解决不同的服务器与周边设备因接口不同而无法沟通的问题，Intel、HP、NEC、Dell 共同领导制定了一项重要的共通规格 -- IPMI (Intelligent Platform Management Interface)。

将 IPMI 技术引入网络安全管理领域将是新的发展和挑战。

参考文献

[1] SourceForge(http://www.sourceforge.net/)，Net-SNMP Tools Install Document，2002

[2] SourceForge(http://www.sourceforge.net/)，Net-SNMP Tools Agent Document，2002

[3] Marshall T. Rose A Convention for Defining Traps for use with the SNMP[S1 RFC 1215 1991

[4] James M. Galvin，Keith McCloghrie，Administrative Model for version2 of the Simple Network Management Protocol (SNMPv2)[S]，RFC1445 1993

[5] William Stallings， SNMP 网络管理[M]，中国电力出版社 2001

[6] W. Richard Stevens ，TCP/IP 协议详解[M]，机械工业出版社 2000

[7] Case J，Fedor M，Schoffstall M. and J. Davin A Simple Network Management Protocol(SNMP)[S]， RFC 1157 1990

[8] 赵振平，宋琦等，SNMPv3 对网络安全性的提高[J] ，现代电信科技 2000．3

[9] 杨富国编，网络安全设备与防火墙，清华大学出版社，北京交通大学出版：2005。

[10] 夏海涛，詹志强 编著，新一代网络管理技术，北京邮电大学出版社：2005。

[11] Russell Lusignan，Oliver Steudler，Jacques Allison 著，王勇译，CISCO 网络安全管理，中国电力出版社，2002。

[12] Intelligent Platform Management Interface Specification V2.0，Intel Hewlett-Packard NEC Dell，2004。

[13] 郎国军，面向安全设备的网络管理方法，2005

[14] William Stallings，网络安全要素— 应用与标准「M]人民邮电出版社，2000

[15] H. Krawczyk， M. Bellare， R. Caneti HMAC，Keyed-Hashing for Message Authentication[S] ，RFC2104 1997

[16] D. Levi， P. Meyer， B. Stewart ，SNMP Applications[S] ，RFC2573

[17] U. Blumenthal， B. Wijnen， User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)，RFC2574 April 1999

[18] B. Wijnen， R. Presuhn， K. McCloghrie，View-based Access Control Model (VACM) for the

[19] Simple Network Management Protocol (SNMP) RFC2575 April 1999

[20] H.Erik Hia， Scott F.Midkiff， Securing SNMP Across Backbone Networks， 2001

[21] Robert L.Ziegler， Linux Firewalls， New Riders Publishing， 2000

[22] T.K.Apostolopolos， V.C.Daskalou， S.K.Katsikas， Enforcing Security Policies in Large Scale，Communication Networks， 2000

致谢

首先，我要特别地感谢我的导师杨义先教授。杨老师渊博的知识，深邃的洞察力，严谨的治学态度和对事业孜孜不倦的追求是我一生的楷模。同时也感谢徐国爱教授和钮心忻教授，在他们的悉心关怀和帮助下，我们能够在一个良好的环境下学习、研究和工作，我们能够参与到实际的工程项目中提高我们的科研和实践能力，我们能够顺利的完成论文工作。

同时也感谢还要感谢课题工作期间合作共事的同学们，和他们进行的讨论和交流使我获益非浅，和他们一起共事是很愉快的。他们是刘楠、刘松、张扬、张楠、何景根等等。

本论文受益于参考文献中所有作者的工作，向这些作者表示衷心的感谢！

最后，对百忙之中审阅我论文的老师，以及参加答辩会的各位老师和同学表示深深的谢意。

网络安全管理平台的设计与实现

作者： 裴娜
学位授予单位： 北京邮电大学

相似文献(10条)

1.期刊论文 李力.杨鹏.LI Li.YANG Peng 网络安全及医院信息系统安全管理的探讨 -中国医疗设备2009,24(5)

本文介绍了网络安全的概念和特征,指出了网络安全面临的主要威胁,着重给出了保障网络安全的系列措施,同时就网络安全问题在医院信息系统安全管理中的特殊性作了进一步阐述.

2.期刊论文 单智勇.石文昌.SHAN Zhi-yong.SHI Wen-chang 多级分布式网络安全管理系统的体系结构 -计算机工程与设计2007,28(14)

对多级分布式的大型网络进行集中安全管理,可以有效提高网络的安全防御能力和安全管理效率,成为网络安全研究的一个迫切问题.提出了多级分布式网络安全管理系统(hierarchical and distributed network security management system,HDNSMS)的体系结构,并描述其体系结构,然后讨论多级分布式架构下的会话模型问题,最后简述其实现以及测试结果.

3.学位论文 吴超 安全管理平台中通信中间件的研究与实现 2007

随着互联网络的普及，网络安全问题日益严重，单一的安全软件或安全设备已经不能满足对于安全状况的需求，因此，网络安全管理平台应运而生。一个完整的网络安全管理平台能够集成多种网络安全设备或软件，收集各种不同类型的安全信息，对当前的网络安全状况作出综合评估并给出相应的策略。同时临近网络中的网络安全管理平台还能互相联系，向临近网络发出预警等信息。由于各种安全软件或设备类型不同、厂家不同，采用的通信方式也各不相同，没有一个统一的标准，给安全信息的收集工作带来了很大的麻烦。同时，相邻网络之间也涉及到局域网-广域网通信等问题。因此，需要为网络安全管理平台设计一个专用的通信系统，来解决通信过程中遇到的各种问题。

本文针对网络安全管理平台中对通信的各项需求，在对现有通信中间件进行详尽分析的基础上，综合了多种现有通信中间件的优点，同时考虑了网络安全管理平台的通信特点，设计了一款专用的通信中间件。该通信中间件主要有以下特点：

多语言支持：为了适应多种编程语言的需要，为不同语言提供不同的用户接口。

多平台支持：通信中间件的主体服务部分使用Java语言编写，可以在多种操作平台上部署。

屏蔽口地址：各用户使用名称作为标识，不使用IP地址。在通信时，只需要知道对方名称，不必知道IP地址，双方即可通信。

自恢复功能：在通信过程中自动检测网络状态，一旦有异常情况发生，将自动重新建立通信连接。

第三方扩展：可以根据需要在广域网通信时使用第三方提供的通信程序，自身只作为局域网内部通信使用。

在本通信中间件的设计中，主要使用了多线程(异步传输)、socket(实现通信)、线程池(多用户支持)、JNI(第三方扩展)等技术。

本设计的实现，为用户提供了简单的接口，使网络安全管理平台的开发人员在进行设计的时候，不必再考虑复杂的通信问题，减轻了负担，提高了效率。

4.会议论文 陶秋刚 浅析电视台网络安全解决方案 2006

电视台每天都要采集、加工、发布许多信息,而对电视台自身来说,每天又有比发布的信息更大量的海量信息需要处理,包括为生产发布信息而需要的管理和运营信息.从某种角度来说,电视台自身处理信息能力的高低,决定了其电视节目在社会上的受关注和受欢迎程度.电视台进行数字化、网络化的优势是不言而喻的,也是全球媒体行业的大势所趋.从90开始,国内各级电视台就逐步开始电视台数字化、网络化的建设,我们当然不能退回到传统线性工作模式,我们需要在整个电视节目生产业务环节全面推进数字化、网络化,增强新数字AV设备的网络友好性,实现现有线性生产域中AV设备与新非线性生产域的IT网络设备间的双向联通,把节目生产域的网络和办公业务管理域的网络有机联系起来,形成一个层次分明、分工合理、互联互通的全台大网络.

数字化、网络化后也随之带来了许多新的问题,首当其冲的就是网络安全问题,数字化、网络化在给我们电视台带来许许多多便利的同时,使得电视台愈来愈离不开电脑及其网络,一旦电脑出现故障或者网络出现故障,轻则给工作带来不便,重则就会造成灾难性后果.

我们在开展数字化、网络化工作之前,必须高度重视计算机及其网络的安全管理事项,只有严格的、周全的安全管理措施,才会有一个良好的、有序的、可靠的数字化、网络化电视台. 本文就安全问题浅析本人对电视台网络安全方面的看法.包括，1从物理层上强化安全管理，2防火墙，3密码技术，4虚拟专有网络(VPN)，5安全检测和监控监测，6防毒软件，7综合防范。

5.会议论文 张晟.张辉 山西网通DCN网络安全解决方案 2007

网络安全是目前通信领域的热门话题，本文从山西网通DCN网络安全域划分入手，简要介绍了网络边界防护技术、主机安全防护技术、终端安全防护技术、身份认证技术和安全管理中心等网络安全技术，形成了一个较为完整的网络安全解决方案。

6.学位论文 杨青 安全管理中心（SOC）中的脆弱性管理 2005

进入二十一世纪以来，网络安全越来越受到社会各个领域重视。而作为我国当前经济生活所不可或缺的通信业务提供商，电信公司的网络和业务是我们整个国家关键基础设施的不可分割的一部分，其网络安全的重要性更是显得尤其突出。

安全管理中心（SOC）是专门针对中国的电信运营商提供的集中的安全管理支撑系统。它以资产为视角，通过统一的安全风险指标将事件、威胁、脆弱性统一起来，并支持接收全部设备、系统的事件，提供电信企业统一的安全状况分析和安全运营支撑。因此它解决了电信企业中大量安全设备无法管理，且管理中缺乏有效信息指导的问题，有效降低了电信企业的安全风险。

P2DR模型是动态的自适应网络安全理论的主要模型。基于P2DR模型的电信安全管理中心充分利用了系统安全管理的持续性和安全策略的动态性，做到了“安全是一个过程，而不是一个产品”。

本论文结合安氏互联网安全系统（中国）有限公司的中国电信集团SOC项目，对脆弱性管理的方法和技术进行了研究。论文首先介绍当前电信公司的网络现状及存在的问题，研究了以P2DR为主要模型的自适应网络安全理论，然后阐述了中国电信集团SOC的解决方案。最后，论文分析了SOC系统中脆弱性管理的作用；设计和实现了配置收集的关键功能；描述了漏洞扫描功能的实现。

7.期刊论文 田兰.汪君勇 贵州气象信息网络安全问题研究 -贵州气象2008,32(6)

主要针对气象信息网络存在的安全问题进行研究,在总结了贵州气象信息网络安全现状后,分析了威胁网络安全的来源,然后从如何进行安全管理和提高安全技术方面阐述了加强贵州气象信息网络安全的策略.

8.会议论文 贾永年 网络安全形势与对策 2001

本文综述了网络安全形势、网络安全三要素和实现网络安全的方案,重点阐述了怎样将网络安全技术与安全管理相结合来保证网络的系统安全和信息安全.

9.学位论文 丁浩 基于CIM的安全管理技术研究与实现 2008

网络技术的飞速发展使得网络安全问题日益严重，单一安全产品由于功能和性能的局限性，只能满足特定的安全需求。安全管理系统将各类安全产品进行有机的结合，实现统一的管理和控制，体现了网络安全的整体性和动态性，提高了网络的安全性、可用性、可靠性和运行效率。

本文对基于CIM的管理信息建模方法进行研究，并以该模型为基础，对安全设备的安全管理系统进行了设计与实现，主要工作有：

(1)设计一种基于CIM/WBEM的安全管理框架。在研究CIM模型的有关理论以及基于CIM的管理信息建模方法的基础上，深入研究了基于CIM模型的管理实现框架，设计了一种基于CIM/WBEM的安全管理框架。

(2)建立网络安全设备的CIM信息模型。在分析和归纳网络安全设备的基本功能的基础上，在CIM核心模型和公共模型之上建立了网络安全设备的扩展模式，并以安全隔离设备的建模过程对CIM信息建模的实效性进行验证。

(3)提出一种安全管理系统的体系结构。在安全管理框架的基础上，采用分层抽象的方法融合了安全管理系统的多样性，将安全管理系统从概念上分为资源层、数据层、应用层和用户层的四层结构。

(4)基于CIM的安全管理原型系统的设计与实现。设计并实现了管理系统的各个功能模块、多种设备代理和数据分发机制等。

研究成果应用于某军队科研项目，应用效果表明，本文的建模方法具有良好的通用性和工程指导价值，安全管理系统具备良好的可扩展性。

10.会议论文 袁飞 基于NDIS的内网安全管理技术探讨 2008

信息化建设的深入和互联网的迅速发展，使信息资源得到最大程度的共享。但随之带来的网络安全和管理问题也日渐凸出，成为企事业单位和部队信息化建设需要解决的重要问题。本文对利用NDIS中间层驱动实现网络数据包过滤相关技术展开研究，提出了基于NDIS的内网安全管理方案，实验验证该方案能有效解决内网的安全问题。