摘　要

随着计算机网络和应用的迅速发展，网络安全问题也日渐突出和复杂化。路由器作为网络互联的关键设备和网络通向外界的大门，构成了互联网络的主要框架，所以路由器的安全变得愈加重要。

本文首先阐述了当前的安全技术，如：防火墙技术、入侵检测技术。介绍了防火墙技术和入侵检测检测技术的基本概念和技术特点；同时，分析了入侵检测技术的分类和体系结构。

其次，本文对路由器原理进行了详细的介绍，在此基础上对主流路由器的安全性进行了分析，同时，说明了安全路由器与防火墙之间的差异。

然后，本文通过对现有路由器的攻击方法和攻击行为进行研究分析，提出应采取“主动防御”的策略来提高路由器的抗攻击能力和鲁棒性。并设计了系统的体系结构，分析了构成基本框架的各个模块在整个系统中作用和相互关系，并给出了各个模块的具体设计与实现。

最后，本文对所做的工作进行了总结，并提出了下一步的研究方向。

关键词：安全路由器，主动防御，入侵检测，防火墙

Abstract

With the rapid development of computer network, network security problem is becoming more and more important. As the router is essential equipment in the network,and constitutes main frame of the internet, the router security is also becoming more and more important.

Firstly, main security technologies are introduced,such as firewall and IDS.We specify basic conception and characteristic of firewall and IDS, and study classification and the system structure of IDS.

Secondly, the router principle is introduced detailedly. The paper analyzes the mainstream router security, at the same time, explains the difference between the security router and the firewall.

Thirdly, after analyzing the attacking ways and modes of present routers, the paper adopts "the active defense" the strategy to enhance the anti- attack capability and robustness of the router. And the paper has designed the system structure, analyzed interactions between all modules of the system. The design and the implementation of each module are specific introduced.

Finally, the achievements made in the paper are summed up and the next step is pointed out.

Key words: Security Router, Active defense, IDS, Firewall

第一章　绪　论

1.1 选题的背景和意义

随着计算机技术和通信技术的发展，网络结构体系变得越来越庞大，网络协议变得越来越复杂，黑客对网络攻击和入侵手段也是形态各异，变化无常，网络安全问题也日渐突出和复杂化。路由器作为网络互联的关键设备和网络通向外界的大门，构成了互联网络的主要框架，也时常受到网络黑客的威胁，且逐渐成为网络攻击的关键点。在网络中，主机通常是放置于子网内部，而路由器是放置在子网的边缘，相当于子网的大门，连接沟通内外网络。当子网中的主机遭到攻击和入侵时，受影响的只是主机，但当路由器受到攻击和入侵时，灾难会殃及整个子网，使子网不能工作或异常工作，由此可见路由器在网络中的重要性。目前路由器对付攻击的防御手段大都采用了“被动防御”技术，即打补丁或关端口的方法来解决，是一种事后的行为。而黑客对网络的攻击往往会采用一些新的方法和手段，使得网络在未知攻击的情况下束手无策，因此新一代的防御技术应是“主动防御”，即事先发现自身的漏洞，并采取补救措施。因此为了增强路由器的抗攻击能力和抗入侵能力，研究路由器的“主动防御”技术是十分有意义的。

1.2 安全路由器系统的重要性

从1988年开始，位于美国卡内基梅隆大学的CERT CC（计算

机紧急响应小组协调中心）就开始调查入侵者的活动。从 CERT CC 给出一些关于最新入侵者攻击方式的趋势，我们就能看出安全路由器系统的重要性。

1.2.1 攻击过程的自动化与攻击工具的快速更新

攻击工具的自动化程度继续不断增强。自动化攻击涉及到的四个阶段都发生了变化。

扫描潜在的受害者。从 1997 年起开始出现大量的扫描活动。目前，新的扫描工具利用更先进的扫描技术，变得更加有威力，并且提高了速度。

入侵具有漏洞的系统。以前，对具有漏洞的系统的攻击是发生在大范围的扫描之后的。现在，攻击工具已经将对漏洞的入侵设计成为扫描活动的一部分，这样大大加快了入侵的速度。

攻击扩散。2000 年之前，攻击工具需要一个人来发起其余的攻击过程。现在，攻击工具能够自动发起新的攻击过程。例如红色代码和 Nimda 病毒这些工具就在 18 个小时之内传遍了全球。

攻击工具的协同管理。自从 1999 年起，随着分布式攻击工具的产生，攻击者能够对大量分布在 Internet 之上的攻击工具发起攻击。现在，攻击者能够更加有效地发起一个分布式拒绝服务攻击。协同功能利用了大量大众化的协议如 IRC（Internet Relay Chat）、IR（Instant Message）等的功能。

1.2.2 攻击工具的不断复杂化

攻击工具的编写者采用了比以前更加先进的技术。攻击工具的特征码越来越难以通过分析来发现，并且越来越难以通过基于

特征码的检测系统发现，例如防病毒软件和入侵检测系统。当今攻击工具的三个重要特点是反检测功能，动态行为特点以及攻击工具的模块化。

反检测。攻击者采用了能够隐藏攻击工具的技术。这使得安全专家想要通过各种分析方法来判断新的攻击的过程变得更加困难和耗时。

动态行为。以前的攻击工具按照预定的单一步骤发起进攻。现在的自动攻击工具能够按照不同的方法更改它们的特征，如随机选择、预定的决策路径或者通过入侵者直接的控制。

攻击工具的模块化。和以前攻击工具仅仅实现一种攻击相比，新的攻击工具能够通过升级或者对部分模块的替换完成快速更改。而且，攻击工具能够在越来越多的平台上运行。例如，许多攻击工具采用了标准的协议如 IRC 和 HTTP 进行数据和命令的传输，这样，想要从正常的网络流量中分析出攻击特征就更加困难了。

1.2.3 漏洞发现日益频繁

每一年报告给 CERT/CC 的漏洞数量都成倍增长。如图下所示：

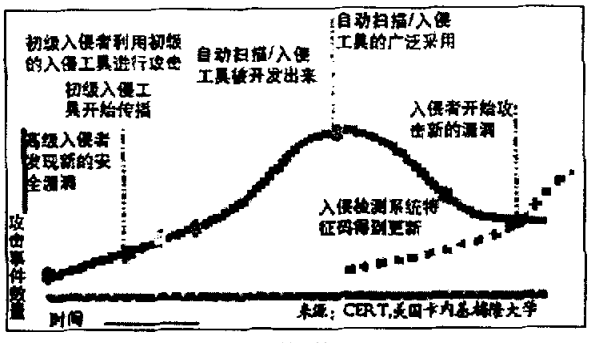

图 1.1 漏洞数量

CERT/CC 公布的漏洞数据 2000 年为 1090 个，2001 年为 2437 个，2002 年已经增加至 4129 个，就是说每天都有十几个新的漏洞被发现。可以想象，对于管理员来说想要跟上补丁的步伐是很困难的。而且，入侵者往往能够在软件厂商修补这些漏洞之前首先发现这些漏洞。随着发现漏洞的工具的自动化趋势，留给用户打补丁的时间越来越短。尤其是缓冲区溢出类型的漏洞，其危害性非常大而又无处不在，是计算机安全的最大的威胁。在 CERT 和其它国际性网络安全机构的调查中，这种类型的漏洞是对服务器造成后果最严重的。

1.3 国内外研究动态

我国信息网络安全研究历经了通信保密、数据保护两个阶段，正在进入网络信息安全研究阶段，现已开发研制出防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但因信息网络安全领域是一个综合、交叉的学科领域它综合了利用数学、物理、生化信息技术和计算机技术的诸多学科的长期积累和最新发展成果，提出系统的、完整的和协同的解决信息网络安全的方案，目前应从安全体系结构、安全协议、现代密码理论、信息分析和监控以及信息安全系统五个方面开展研究，各部分相互协同形成有机整体。

国际上信息安全研究起步较早，力度大，积累多，应用广，在 70 年代美国的网络安全技术基础理论研究成果“计算机保密模型”（bcu&lapadula 模型）的基础上，指定了“可信计算机系统安全评估准则”（tcsec），其后又制定了关于网络系统数据库方面和系列安全解释，形成了安全信息系统体系结构的准则。安全协议

作为信息安全的重要内容，其形式化方法分析始于80年代初，目前有基于状态机、模态逻辑和代数工具的三种分析方法，但仍有局限性和漏洞，处于发展的提高阶段。作为信息安全关键技术密码学，近年来空前活跃，美、欧、亚各洲举行的密码学和信息安全学术会议频繁。1976 年美国学者提出的公开密钥密码体制，克服了网络信息系统密钥管理的困难，同时解决了数字签名问题，它是当前研究的热点。而电子商务的安全性已是当前人们普遍关注的焦点，目前正处于研究和发展阶段，它带动了论证理论、密钥管理等研究，由于计算机运算速度的不断提高，各种密码算法面临着新的密码体制，如量子密码、dna 密码、混沌理论等密码新技术正处于探索之中。

对于安全路由器，目前国内外各大路由器生产厂商在其产品中都增加了一些安全保护策略和解决方案，对已知的攻击起到很好的预防作用。例如中兴、华为、Cisco 的路由器产品，这些产品都采用了加密、认证、包过滤、关闭协议和端口等方式，对以前的攻击行为进行防范，防止此类攻击再次发生。但是防御手段非常被动，在防御上缺乏主动性，因此对新生的攻击手段还是无能为力。

1.4 论文的主要内容和结构安排

本系统旨在架构具有主动防御能力的安全路由器系统体系，从而克服传统产品的缺陷，达到更安全地保护网络资源的目的。本文主要内容安排如下：

第一章 绪论。本章论述了选题的背景和意义，国内外的动态，以及安全路由器系统的重要性。

第二章 系统涉及的安全技术。本章对安全技术中的防火墙技术和入侵检测技术进行了细致的研究和分析。说明了防火墙技术中包过滤、状态检测和代理服务，同时，说明了入侵检测技术中的分类和体系结构。

第三章 路由器原理与安全性分析。本章对路由器原理进行了详细的介绍，在此基础上对主流路由器的安全性进行了分析，同时，说明了安全路由器与防火墙之间的差异。

第四章 具有主动防御能力安全路由器系统的设计。本章在分析对现有路由器攻击的基础上，提出了设计思想，分析了模块结构、功能和总体流程。

第五章 具有主动防御能力安全路由器系统的实现。本章在设计思想的基础上，分别对路由器控制模块、协处理器模块、远程控制平台、入侵检测模块和审计日志模块进行了设计和实现。

结论。对整个论文工作做了一个总结，提出了下一步的工作。

第二章 系统涉及的安全技术

2.1 防火墙技术

2.1.1 防火墙技术的定义

防火墙是目前最为流行也是使用最为广泛的一种网络安全技术，是指一种将内部网和公众访问网(Internet)分开的方法，实际上是一种隔离技术。在构建安全网络环境的过程中，防火墙作为第一道安全防线，正受到越来越多用户的关注。

防火墙是一个系统，主要用来执行两个网络之间的访问控制策略，可为各类企业网络提供必要的访问控制，但又不造成网络的瓶颈，通过安全策略控制进出系统的数据，保护企业的关键资源。

防火墙并不是一个单一的软件，而是一种概念，即如何在开放的网络环境中构造一个相对封闭的逻辑网络环境来满足人们对于网络安全的特殊要求。它形成阻止非授权的用户闯入内部网络的一道障碍。

防火墙通常由过滤器和网关组成，见图 2-1 所示。

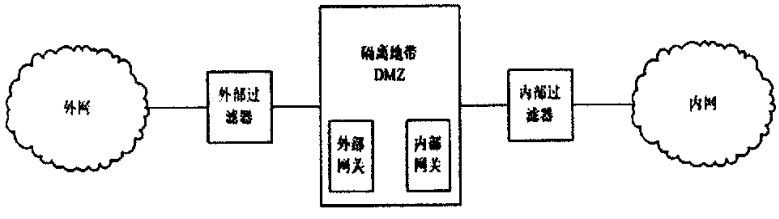

图 2-1 防火墙结构图

防火墙应具有以下属性:

- 所有的从外到内的信息及从内到外的信息都必须通过Firewall;
- 只有在受保护网络的安全策略中允许的通信才允许通过Firewall;
- 记录通过防火墙的信息内容和活动;
- 对网络攻击检测和告警:
- Firewall 本身对各种攻击免疫。

防火墙通常使用的安全控制手段主要有包过滤、状态检测、代理服务。

2.1.2 包过滤

包过滤是一种在路由器上实现的传统方法，是一种简单、有效的安全控制技术，它通过在网络间相互连接的设备上加载允许、禁止来自某些特定的源地址、目的地址、TCP 端口号等规则，对通过设备的数据包进行检查，限制数据包进出内部网络。包过滤的最大优点是对用户透明，传输性能高。但由于安全控制层次在网络层、传输层，安全控制的力度也只在于源地址、目的地址和端口号，因而只能进行较为初步的安全控制，对于恶意的拥塞攻击、内存覆盖攻击或病毒等高层次的攻击手段，则无能为力。

使用包过滤技术时，要特别注意一般的数据通信大多都是双向的，在设置过滤规则时必须予以考虑。

2.1.3 状态检测

与包过滤相类似的、更为有效的安全控制方法是状态检测。对新建的应用连接，状态检测检查预先设置的安全规则，允许符

对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。这种方式的好处在于:由于不需要对每个数据包进行规则检查，而是一个连接的后续数据包(通常是大量的数据包)通过散列算法，直接进行状态检查，从而使得性能得到了较大提高:而且，由于状态表是动态的，因而可以有选择地、动态地开通 1024 号以上的端口，使得安全性得到进一步地提高。

此外，部分状态检测型防火墙还支持多种用户认证方式，提供了应用级的安全认证手段，增加了某些应用的代理功能，使得安全控制力度更为细致。

2.1.4 代理服务

代理服务是运行于内部网络与外部网络之间的主机(堡垒主机)之上的一种应用。当用户需要访问代理服务器另一侧主机时，对符合安全规则的连接，代理服务器会代替主机响应，并重新向主机发出一个相同的请求。当此连接请求得到回应并建立起连接之后，内部主机同外部主机之间的通信将通过代理程序将相应连接映射来实现.对于用户而言，似乎是直接与外部网络相连的，代理服务器对用户透明。代理机制完全阻断了内部网络与外部网络的直接联系，保证了内部网络拓扑结构等重要信息被限制在代理网关内侧，不会外泄，从而减少了黑客攻击时所需的必要信息。

代理服务器的应用也受到诸多限制。首先是当一项新的应用加入时，如果代理服务程序不予支持，则此应用不能使用。解决的方法之一是自行编制特定服务的代理服务程序，但工作量大，

而且技术水平要求很高，一般的应用单位无法完成。其次是处理性能远不及状态检测高。

2.2 入侵检测技术

2.2.1 入侵检测技术的定义

入侵检测的研究最早可以追溯到 1980 年 4 月，James P. Anderson 为美国空军做了一份题为《Computer Security Threat Monitoring and Surveillance》（计算机安全威胁监控与监视）的技术报告，第一次详细阐述了入侵检测的概念。其定义是：对潜在的、有预谋的、未经授权的访问信息、操作信息、致使系统不可靠、不稳定或无法使用的企图的检测和监视。他提出了一种对计算机系统风险和威胁的分类方法，并将威胁分为外部渗透、内部渗透和不法行为三种，还提出了利用审计跟踪数据监视入侵活动的思想。这份报告被公认为是入侵检测的开山之作。

入侵检测对安全保护采取的是一种积极、主动的防御策略，而传统的安全技术都是一些消极、被动的保护措施。因为，如果入侵者一旦攻破了由传统安全技术所设置的保护屏障，这些技术将完全失去作用，对系统不再提供保护，而入侵者则对系统可以进行肆无忌惮的操作，当然包括一些很具有破坏性的操作。对于这些，传统的安全技术是无能为力的。但是入侵检测技术则不同，它对进入系统的访问者（包括入侵者）能进行实时的监视和检测，一旦发现访问者对系统进行非法的操作（这时候访问者成为了入侵者），就会向系统管理员发出警报或者自动截断与入侵者的连接，这样就会大大提高系统的安全性。所以对入侵检测技术研究

是非常有必要的，并且它也是一种全新理念的网络（系统）防护技术。

2.2.2 入侵检测技术的分类

入侵是指有关试图破坏资源的完整性、机密性及可用性的活动集合，入侵主要包括尝试性闯入、伪装攻击、安全控制系统渗透、泄漏、拒绝服务、恶意使用等类型。

根据着眼点不同，对入侵检测技术的分类方法又很多。

1、数据来源

根据数据来源的不同，可以将入侵检测分为3类：

基于主机（Host-Based）：系统获取数据的依据是系统运行所在主机，保护的目标也是系统运行所在主机。

基于网络（Network-Based）：系统获取数据来源是网络传输的数据包，保护的目标是网络的运行。

混合型：勿庸置疑，混合型就是既基于主机又基于网络，因此混合型一般也是分布式的。

2、分析方法

根据数据分析方法（也就是检测方法）的不同，可以将入侵检测分为2类：

异常检测模型（Abnormally Detection Model）：也称为基于行为的入侵检测系统（Behavior Based IDS），这种模型的特点是首先总结正常操作应该具有的特征，例如特定用户的操作习惯与某些操作的频率等；在得出正常操作的模型后，对后续的操作进行监视，一旦发现偏离正常统计学意义上的操作模式即进行报警。

误用检测模型（Misuse Detection Model）：也称为基于知识

的入侵检测系统（Knowledge-Based IDS）这种模型的特点是收集非正常操作也就是入侵行为的特征，建立相关的特征库；在后续的检测过程中，将收集到的数据与特征库中的特征代码进行比较，得出是否入侵的结论。

3、实效性

按照根据分析发生的时间的不同，可以分为：

脱机分析：就是在行为发生后，对产生的数据进行分析，而不是在行为发生的同时进行分析。如对日志的审核、对系统文件的完整性检查等都属于这种。一般而言，脱机分析也不会间隔很长时间，所谓的脱机只是与联机相对而言。

联机分析：就是在数据产生或者发生改变的同时对其进行检查，以发现攻击行为。这种方式一般用于对网络数据的实时分析，对系统资源要求比较高。

4、分布性

按照系统各个模块运行的分布方式不同，可以分为：

集中式：系统的各个模块包括数据的收集与分析以及响应模块都集中在一台主机上运行，这种方式适用于网络环境比较简单的情况。：

分布式：系统的各个模块分布在网络中不同的计算机、设备上，一般来说分布性主要体现在数据收集模块上，例如有些系统引入的传感器（Sensor），如果网络环境比较复杂、数据量比较大，那么数据分析模块也会分布，一般是按照层次性的原则进行组织，例如 AAFID。

5、响应方式

根据入侵检测系统对入侵攻击的响应方式可以分为：

主动式：对被攻击系统实施控制，它通过调整被攻击系统的状态，阻止或减轻攻击影响，例如断开网络连接、增加安全日志、关闭相应的服务等。

被动式：在检测出对系统的入侵攻击后，只会发出告警通知，将发生的不正常情况报告给管理员，本身并不试图降低所造成的破坏，更不会主动地对攻击者采取反击行动。

2.2.3 入侵检测系统的体系结构

入侵检测系统的体系结构可以分为基于主机（host-based）,基于网络（network-based）和混合型。

1、基于主机的入侵检测系统

基于主机的入侵检测系统将检测模块驻留在被保护系统上，通过提取被保护系统的运行数据并进行入侵分析来实现入侵检测的功能。

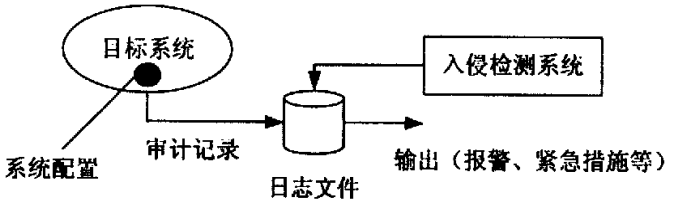

图 2.2 基于主机的入侵检测系统

目前基于主机的入侵检测系统很多是基于主机日志分析。

基于主机日志的安全审计，通过分析主机日志来发现入侵行为。基于主机的入侵检测系统具有检测效率高，分析代价小，分析速度快的特点，能够迅速并准确地定位入侵者，并可以结合操作系统和应用程序的行为特征对入侵进行进一步分析。基于主机

的入侵检测系统存在的问题是:首先它在一定程度上依赖于系统的可靠性，它要求系统本身应该具备基本的安全功能并具有合理的设置，然后才能提取入侵信息:即使进行了正确的设置，对操作系统熟悉的攻击者仍然有可能在入侵行为完成后及时地将系统日志抹去，从而不被发觉;并且主机的日志能够提供的信息有限，有的入侵手段和途径不会在日志中有所反映，日志系统对有的入侵行为不能做出正确的响应，例如利用网络协议栈的漏洞进行的攻击，通过 ping 命令发送大量数据包，造成系统协议栈溢出而死机，或是利用 ARP 欺骗来伪装成其他主机进行通信，这些手段都不会被高层的日志记录下来。在数据提取的实时性、充分性、可靠性方面基于主机日志的入侵检测系统不如基于网络的入侵检测系统。

2、基于网络的入侵检测系统

基于网络的入侵检测系统通过网络监视来实现数据提取。在 Internet 中，局域网普遍采用以太网协议。该协议定义主机进行数据传输时采用子网广播的方式，任何一台主机发送的数据包，都会在所经过的子网中进行广播，也就是说，任何一台主机接收和发送的数据都可以被同一子网内的其他主机接收。

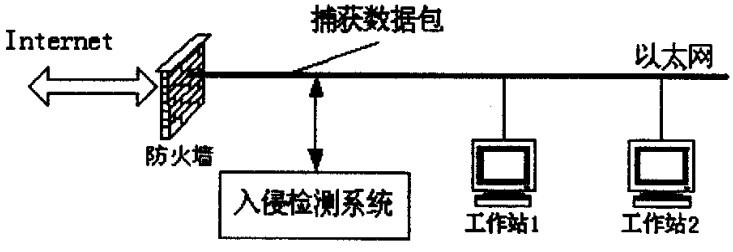

图 2.3 基于网络的入侵检测系统

在正常设置下，主机的网卡对每一个到达的数据包进行过滤，只将目的地址是本机的或广播地址的数据包放入接收缓冲区，而

将其他数据包丢弃，因此，在正常情况下，网络上的主机表现为只关心与本机有关的数据包，但是将网卡的接收模式进行适当的设置后就可以改变网卡的过滤策略，使网卡能够接收经过本网段的所有数据包，无论这些数据包的目的地是否是该主机。网卡的这种接收模式被称为混杂模式，目前绝大部分网卡都提供这种设置，因此，在需要的时候，对网卡进行合理的设置就能获得经过本网段的所有通信信息，从而实现网络监视的功能。在某他网络环境下，虽然可能不采用广播的方传送报文，但目前很多路由设备或交换机都提供数据报文监视功能。

网络监视具有良好的特性：理论上，网络监视可以获得所有的网络信息数据，只要时间允许，可以在庞大的数据堆中提取和分析需要的数据;可以对一个子网进行检测，一个监视模块可以监视同一网段的多台主机的网络行为，不改变系统和网络的工作模式，也不影响主机性能和网络性能:处于被动接收方式，很难被入侵者发现；可以从低层开始分析，对基于协议攻击的入侵手段有较强的分析能力。网络监视的主要问题是监视数据量过于庞大并且它不能结合操作系统特征来对网络行为进行准确的判断。由于基于网络的入侵检测方式具有较强的数据提取能力，因此目前很多入侵检测系统倾向于采用基于网络的检测手段来实现。

具体实现时往往基于主机和基于网络的入侵检测系统可构成统一集中的系统。而且随着网络系统结构的复杂化和大型化，系统的弱点和漏洞趋向分布式，入侵行为也不再表现为单一的行为，而是相互协作入侵的特点。随之出现了基于主体的入侵检测系统和分布式的入侵检测系统。

第三章　路由器原理与安全性分析

3.1 路由器基本原理

近十年来，随着计算机网络规模的不断扩大，大型互联网络（如 Internet）的迅猛发展，路由技术在网络技术中已逐渐成为关键部分，路由器也随之成为最重要的网络设备。

3.1.1 网络互连

把自己的网络同其它的网络互连起来，从网络中获取更多的信息和向网络发布自己的消息，是网络互连的最主要的动力。网络的互连有多种方式，其中使用最多的是网桥互连和路由器互连。

1 网桥互连的网络

网桥工作在 OSI 模型中的第二层，即链路层。完成数据帧（frame）的转发，主要目的是在连接的网络间提供透明的通信。网桥的转发是依据数据帧中的源地址和目的地址来判断一个帧是否应转发和转发到哪个端口。帧中的地址称为“MAC”地址或“硬件”地址，一般就是网卡所带的地址。

网桥的作用是把两个或多个网络互连起来，提供透明的通信。由于网桥是在数据帧上进行转发的，因此只能连接相同或相似的网络（相同或相似结构的数据帧），如以太网之间、以太网与令牌环（token　ring）之间的互连。

网桥扩大了网络的规模，提高了网络的性能，给网络应用带来了方便，在以前的网络中，网桥的应用较为广泛。但网桥互连也带来了不少问题：一个是广播风暴，第二个问题是，当与外部

网络互连时，网桥会把内部和外部网络合二为一，成为一个网，双方都自动向对方完全开放自己的网络资源。

2 路由器互连网络

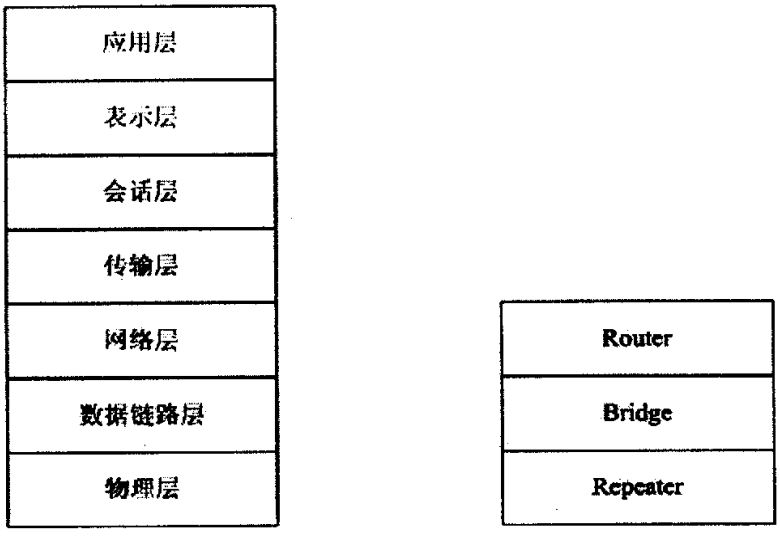

图 3.1　网络分层

路由器工作在 OSI 模型中的第三层，即网络层。路由器利用网络层定义的"逻辑"上的网络地址（即 IP 地址）来区别不同的网络，实现网络的互连和隔离，保持各个网络的独立性。路由器不转发广播消息，而把广播消息限制在各自的网络内部。发送到其他网络的数据首先被送到路由器，再由路由器转发出去。

IP 路由器只转发 IP 分组，把其余的部分挡在网内（包括广播），从而保持各个网络具有相对的独立性，这样可以组成具有许多网络（子网）互连的大型的网络。由于是在网络层的互连，路由器可方便地连接不同类型的网络，只要网络层运行的是 IP 协议，通过路由器就可互连起来。

网络中的设备用它们的网络地址（TCP / IP 网络中为 IP 地址）

互相通信。IP 地址是与硬件地址无关的“逻辑”地址。路由器只根据 IP 地址来转发数据。

一般网络通信只能在具有相同网络号的 IP 地址之间进行，要与其它 IP 子网的主机进行通信，则必须经过同一网络上的某个路由器或网关（gateway）出去。不同网络号的 IP 地址不能直接通信，即使它们接在一起，也不能通信。

3.1.2 路由原理

当 IP 子网中的一台主机发送 IP 分组给同一 IP 子网的另一台主机时，它将直接把 IP 分组送到网络上，对方就能收到。而要送给不同 IP 于网上的主机时，它要选择一个能到达目的子网上的路由器，把 IP 分组送给该路由器，由路由器负责把 IP 分组送到目的地。如果没有找到这样的路由器，主机就把 IP 分组送给一个称为“缺省网关（default gateway）”的路由器上。

路由器转发 IP 分组时，只根据 IP 分组目的 IP 地址的网络号部分，选择合适的端口，把 IP 分组送出去。同主机一样，路由器也要判定端口所接的是否是目的子网，如果是，就直接把分组通过端口送到网络上，否则，也要选择下一个路由器来传送分组。路由器也有它的缺省网关，用来传送不知道往哪儿送的 IP 分组。这样，通过路由器把知道如何传送的 IP 分组正确转发出去，不知道的 IP 分组送给“缺省网关”路由器，这样一级级地传送，IP 分组最终将送到目的地，送不到目的地的 IP 分组则被网络丢弃了。

路由动作包括两项基本内容：寻径和转发。寻径即判定到达目的地的最佳路径，由路由选择算法来实现；转发即沿寻径好的最佳路径传送信息分组。

路由转发协议和路由选择协议是相互配合又相互独立的概念，前者使用后者维护的路由表，同时后者要利用前者提供的功能来发布路由协议数据分组。下文中提到的路由协议，除非特别说明，都是指路由选择协议，这也是普遍的习惯。

3.1.3 路由协议

典型的路由选择方式有两种：静态路由和动态路由。

静态路由是在路由器中设置的固定的路由表。除非网络管理员干预，否则静态路由不会发生变化。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。

动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由器表的过程。它能实时地适应网络结构的变化。如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。

静态路由和动态路由有各自的特点和适用范围，因此在网络中动态路由通常作为静态路由的补充。当一个分组在路由器中进行寻径时，路由器首先查找静态路由，如果查到则根据相应的静态路由转发分组；否则再查找动态路由。

根据是否在一个自治域内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。这里的自治域是指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIP、IGRP、OSPF；外部网关协议主要用于多个自治域之间的路由选择，常用的是 BGP 和 BGP-4。

在一个路由器中，可同时配置静态路由和一种或多种动态路

由。它们各自维护的路由表都提供给转发程序，但这些路由表的表项之间可能会发生冲突。这种冲突可通过配置各路由表的优先级来解决。通常静态路由具有默认的最高优先级，当其它路由表表项与之矛盾时，均按静态路由转发。

路由算法在路由协议中起着至关重要的作用，采用何种算法往往决定了最终的寻径结果，因此选择路由算法一定要仔细。通常需要综合考虑以下几个设计目标：

1 最优化：指路由算法选择最佳路径的能力。

2 简洁性：算法设计简洁，利用最少的软件和开销，提供最有效的功能。

3 坚固性：路由算法处于非正常或不可预料的环境时，如硬件故障、负载过高或操作失误时，都能正确运行。由于路由器分布在网络联接点上，所以在它们出故障时会产生严重后果。最好的路由器算法通常能经受时间的考验，并在各种网络环境下被证实是可靠的。

4 快速收敛：收敛是在最佳路径的判断上所有路由器达到一致的过程。当某个网络事件引起路由可用或不可用时，路由器就发出更新信息。路由更新信息遍及整个网络，引发重新计算最佳路径，最终达到所有路由器一致公认的最佳路径。收敛慢的路由算法会造成路径循环或网络中断。

5 灵活性：路由算法可以快速、准确地适应各种网络环境。例如，某个网段发生故障，路由算法要能很快发现故障，并为使用该网段的所有路由选择另一条最佳路径。

3.2 路由器安全性现状分析

本小节以Cisco路由器为例，介绍路由器存在的一些问题和受到的常见攻击。

1 针对Cisco路由器的分布式拒绝服务（DDoS）攻击：

攻击原理：在DDOS攻击过程中，一些恶意的主机或者已经受恶意主机感染的主机向被攻击服务器发送大量的数据，由于一般靠近服务器的网络节点（其中包括Cisco路由器）通常在设计时只要求处理少量的数据（防止瓶颈的一种做法），当数据从通过边缘节点以服务器为核心聚集的时候，边缘节点将接受到大量的数据，从而导致网络资源枯竭。同时服务器也有可能因此而超载瘫痪。

防范措施：通常采用的方法是对路由器接收到的数据包进行过滤。常用而且较简单的防范措施有二。

1）通过访问控制表（access control list）来过滤所有的RFC1918地址空间；

下面是一个简单的使用ACL的例子：

```
interface xy
ip access-group 101 in
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 192.168.0.00.0.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 permit ip any any
```

2）使用"ip verify unicast reverse-path interface"命令；对该路由器所接受到的数据包的原地址路由进行检测，如果

发现原地址路由不存在该路由器的CEF（Cisco Express Forwarding）中，则丢弃该数据包。具体做法是先打开路由器的"CEF switching"或"CEF distributed switching"选项，然后使用该命令。

2 TFTPD守护进程目录遍历漏洞：

Cisco免费提供了TFTP服务，而Cisco培训的书籍总会介绍使用copy running-config tftp的命令来保存路由配置文件。由于该配置使得TFTPD守护进程存在目录遍历的漏洞，同过该漏洞，只要我们获得了TFTP的权限，就可以从远程系统中获取任意文件。

tftp〉 connect XXX.XXX.XXX.XXX

tftp〉 get cisco-conf.bin

Recieved 468 bytes in 0.7 seconds

tftpd〉 quit

该漏洞目前尚无任何补救措施。

3 HTTP帮助服务漏洞：

Cisco 安全建议小组在2000年10月30日公布了这个漏洞。IOS 11.0引入通过Web方式管理路由。”?”是HTML规范中定义的CGI参数的分界符。它也被IOS命令行接口解释成请求帮助。在IOS 12.0中，当问号邻接于“/”，URL解释器就不能正确解释其含义。当一个包括“?/”的URL对路由器HTTP服务器进行请求，并且提供一个有效的启用口令，则路由器进入死循环。因而引起路由崩溃并重起。 如果http起用，浏览http://route_ip_addr/anytest?/ 并且提供特权口令，则可以导致DoS攻击，导致路由停机或者重启。

防范措施就是关闭HTTP服务。#no localhost http server。

4 1999端口信息泄露漏洞：

Cisco产品存在IOSLOGON、HISTORY等BUG，这些BUG都是利用1999端口，所以，只要使用一般的端口扫描工具对某段IP进行扫描，观察返回信息，就能轻易发现哪些是Cisco产品，因为Cisco产品的1999端口返回信息都会包含有“Cisco”字样的。利用该漏洞并不能对直接对系统造成破坏，但是可以配合其他漏洞，使恶意黑客专门对Cisco产品进行攻击。

5 本地密码破解：

该方法常在密码丢失时，密码恢复的方法，但是也会被某些别有用心的人利用：

准备工作：一台微机运行终端仿真程序(可以在Windows 95/98下启动超级终端)，微机串口（COM1/COM2）通过Cisco公司随机配备的配置线与路由器Console口连接。

恢复步骤：

（1）开机，按Ctrl＋Break键，直到出现提示符。

（2）键入命令：“）o/r 0x142”。

（3）初始化路由器：“）i”。

（4）重新启动，屏幕显示系统配置对话："system configuration to get started?"，键入"no"，系统显示“Press RETURN to get started!"，按“Return"键，系统显示“Router〉

（5）键入命令："Router〉enable"进入超级用户状态(系统不再需要你输入超级口令了)；“Router＃show startup－config"显示配置参数，特别要注意记住所看到的密码（你也可以通过enable secret "changepassword"命令更改超级用户口令）。

（6）键入命令恢复原来的寄存器：

"Router(config)#config－reg 0x2102"；

"Router(config)#ctrl－z"；

"Router(config)#wr"存盘。

（7）重新启动："Router#reload"。

其实Cisco漏洞远不止这些，列举以上几个常见的漏洞只是为了说明路由器的安全漏洞随处可见，针对路由器的安全问题非常严重。

当然，路由器毕竟不是专门的网络安全设备，它所能做的也仅仅能够减少一些基于网络层上的攻击所带来的负面影响，但绝不能完全免疫。而且，在实现上述功能的同时，也是以牺牲部分CPU与内存资源为代价的。此外，它对于一些诸如登陆攻击、所有基于应用层上的攻击手段等则完全无能为力。如果发生这样的问题，还是必须要借助防火墙等专门的安全设备和在系统上进行严格设置等手段配合进行。

3.3 安全路由器与防火墙

一般来说，路由器跟防火墙是两个不同的概念，从字面就可以理解他们的区别。但是现在的路由器功能越来越多，其中很重要的一个功能就是具备了安全防护的功能，这个就是我们所说的安全路由器，它集成了防火墙和VPN等安全功能，这就很容易联想到防火墙与安全路由器之间到底有什么不同：

防火墙是专用的网络安全设备，它采用综合的网络技术，是设置在被保护网络和外部不可信任网络之间的一道关卡，用以分隔被保护网络与外部网络系统，防止发生不可预测的恶意入侵。

它是不同网络或网络安全域之间信息的唯一出入口，能根据相应的安全政策控制出入信息流，防止非法信息流入被保护的网络内。

安全路由器通常是集常规路由与网络安全功能于一身的网络安全设备，从主要功能来讲，它还是一个路由器，主要承担网络中的路由交换任务，只不过更多地具备了安全功能，包括可以内置防火墙模块。 一般来说,高性能安全路由器具有以下主要功能：

- 网络的互连
- 网络的隔离
- 流量的控制
- 网络和信息安全维护

安全路由器的主要技术指标：

1 互连协议：IP v4（网际互联协议）；

2 支持的网络端口：Ethernet；Fast Ethernet；千兆以太；串行口（V.35/RS232，可至E1/2.048M），SDH155M接口。

3 处理器类型： PowerPC 750@366MHZ

4 广域网支持：PPP协议

5 路由协议支持：静态路由；路由信息协议RIP v2；开放最短路径优先OSPF v2；边界网关协议BGP-4

6 操作与管理：Flash启动与存储配置；基于异步串口的操作与配置；简单网络管理协议SNMP agent；基于Telnet的操作与配置。

7 操作系统：自主版权的实时多任务操作系统HEROS（Highly Efficient Router Operating System）

8 安全特征：基于地址和端口的分组过滤（防火墙）功能；基于服务的分组过滤功能；抗源地址欺骗；抗源路由攻击；抗极

小数据段；抗重叠分片的分组过滤功能；利用合理的加密算法根据路由器安全需求实现 IP 数据报的智能加密；完善的密钥生成、分配、保存方案及实现；具有安全审计，追踪功能和告警的网络管理。

9 安全指标：对称密码的密钥长度不小于 128 比特；公开密钥密码的密钥长度不小于 512 比特；软件运算速度：对称密码大于 128Kbps、公开密钥大于 1Kbps。

我们可以这样说，防火墙工作在大型网络中，成为网络中的主要安全设备，主要布置在一个网络或子网与另一个网络的接口处，保障整个网络的安全。而安全路由器主要应用在中小型企业的网络中央，承担主要的路由功能，同时兼顾网络安全，但是整个设备不能因为安全功能而导致整体网络性能的下降。也就是说，安全是安全路由器的辅助功能。在中小型网络中，安全路由器的部署的确使防火墙成为一个配置在路由器之中的设备，因此就没有必要再部署防火墙了。但是在大型的网络中，两者是完全不同的安全设备。

虽然说从目前的情况看来,安全路由器取代防火墙还不太可能,但是安全路由器的发展势头相当强,很多路由器的厂家都愿意在路由器上大做文章,不断的完善路由器的各种技术,同时也加入新的技术。这些厂家想要做的是，突破传统的路由器的概念，路由器不是传统意义上的一台网络连接设备，而是一个将各种安全技术有机融为一体的高技术、高品质与人性化的安全产品。从实际的市场效果来看,安全路由器不但是受到中小型企业的喜爱,更多重要的是也有很多的家庭用户也采用了这种安全路由器。

第四章 具有主动防御能力安全路由器系统的设计

4.1 系统设计思想

4.1.1 路由器的攻击分析

根据网络协议的工作原理可知，路由器的所有辅助协议都是基于IP协议的，即工作在IP协议之上，而路由器是工作在IP层的。所以所有进入路由器的IP包根据其目的地址可分为两类：一类是目的地址指向其它主机的IP包，这里称之为“转发IP包”；一类是目的地址指向本路由器的IP包，这里称之为“终点IP包”。路由器对这两类IP包的处理，以及IP包对路由器的威胁如下：

1. 转发IP包：路由器对这类IP包的处理会根据策略进行转发或丢弃，不会耗费太大的资源。即使当这类的IP包太多，网络出现拥塞时，路由器也会根据排队的原则简单的丢弃一些IP包，路由器不会出现异常的举动。其潜在威胁就是一些类似于Smurf广播风暴的攻击，以路由器某个端口的IP地址作为虚假的IP地址形成虚假源地址IP包。这可以通过完善路由协议，在路由转发策略中根据路由器配置的子网地址来判断IP包源地址的虚假，以此来挫败此类攻击。

从上面可以看出，“中转IP包”对路由器的威胁相对比较小，且可以通过完善路由协议来克服，也不会对路由器形成太大的资源消耗。因此这里不是本文安全路由器考虑的重点。

2. 终点 IP 包：路由器对这类 IP 包的处理会根据策略丢弃或

2. 终点 IP 包：路由器对这类 IP 包的处理会根据策略丢弃或

传给高层协议处理。高层协议通常会根据这些 IP 包的请求，为其分配相应的内存，并阻塞某些端口，而且复杂的协议很可能会隐藏一些潜在的漏洞，且攻击形式呈多样化和复杂化。

这类 IP 包是直接针对路由器的，因此是潜在威胁最大的 IP 包，且攻击和入侵的 IP 包往往隐藏在这类路由器认为正确的 IP 包中。从目前路由器遭受的攻击来看，大都属于此类 IP 包，比如：SYN flooding 虚假连接攻击、ICMP 攻击、TELNET 远程攻击、HTTP 远程攻击，以及广播风暴等。这类攻击的判断对工作在 IP 层的路由器很难实现，特别是新的攻击方式，而且实现过程比较烦杂，影响路由器工作。

通过上面的对路由器攻击方式的分析，以及在IP层对IP数据包的分类，对路由器防攻击的研究应集中在对“终点IP包”的处理上。而且应采取“主动防御”的策略来提高路由器的抗攻击能力和鲁棒性，这样不会由于未知的攻击而出现不可预测的现象。

4.1.2 主动防御的思想

主动防御系统是相对于传统的被动式保护系统而言的。传统的保护措施比如防火墙，都是采用预先设定好的策略对网络安全性进行保护。防火墙的策略决定了它仅仅能够作为网络边界的屏障，而不能代替整个的安全系统的作用。那么主动的安全防御系统是什么呢？考察目前所有网络系统的关键资源，可以发现最关键的资源实际上就是驻留在主机和服务器上的数据。如果我们对这些数据进行了强制性、全面的防护，并且对其操作系统进行加固，对问题最多的超级用户的超级权力进行适当的限制，就可以

达到相当好的效果。这样，不管攻击者采用什么样的攻击方法，我们的防范方式总是能够主动识别攻击者的企图，对于不合适的访问予以拒绝。例如，如果一个入侵者利用一个新的漏洞获取了操作系统超级用户的口令，那么下一步他希望采用这个账户和密码对服务器上的数据进行删除和篡改。这时，如果我们利用主动防范的方式首先限制了超级用户的权限，而且又通过访问地点、访问时间以及访问采用的应用程序等几方面的因素予以了限制，入侵者的攻击企图就很难得逞。同时，这样的系统会将访问企图记录下来。这样，采用这种主动的安全保护系统就达到了对未知攻击方式的成功防范，为管理员处理这种新型的入侵方式争取到了宝贵的响应时间。

4.2 系统总体设计

本系统的架构中引入一个“协处理器”，协助路由器完成 IP 包的处理功能，并对路由器进行控制，实施“主动防御”，防止路由器遭受攻击。协处理器、路由器和网络的结构关系如图 1 所示。

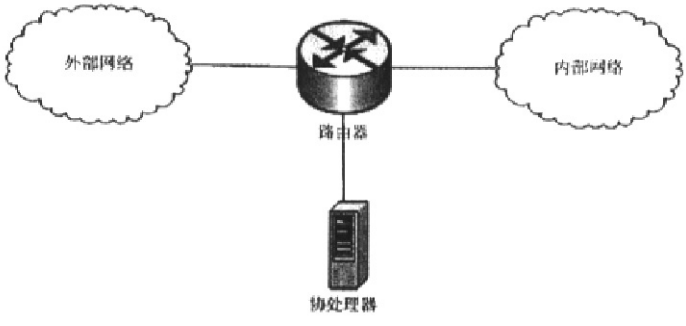

图 4.1 系统网络结构示意图

路由器和协处理器共同组成了“主动防御路由器”。当路由器收到来自外部网络或内部子网的 IP 包时，若是“转发 IP 包”则根据路由器的策略进行转发或丢弃；若是“终点 IP 包”时，则会根据策略丢弃或转交给“协处理器”进行处理。协处理器在处理这些 IP 包时会进行一定的分析和判断，然后做出适当的响应。

这样做有如下优点：

- 路由器免受来自“终点 IP 包”的攻击。当攻击发生时，遭受攻击的对象是“协处理器”，而非路由器，即使当“协处理器”出现 DoS 时，或其它状况时，路由器仍可以正常工作，具有很强的抗攻击鲁棒性。
- “协处理器”的处理程序可以不受路由器功能的干扰和限制而进行合理的设计，使其具有很强的分析、判断和学习的能力，对合理的 IP 包做出响应，对非法的 IP 包做出限制，协助路由器工作，使路由器更具智能性。
- “协处理器”与路由器分开，在增强路由器的抗攻击能力的同时，并不增加路由器的负担。
- “协处理器”与路由器分开，可以在不用过多改变现有路由器的基础上，实现原路由器到抗攻击路由器的升级。

在“协处理器”技术比较成熟和稳定后，“协处理器”和路由器可以集成为一体，这样在“协处理器”和路由器之间会具有更高的传输速度和更好的安全性。

4.2.1 系统体系结构

本系统分五大结构模块，分别是路由器控制模块、协处理器管理模块、审计日志模块、入侵检测模块、远程控制平台。

模块结构如下图所示。

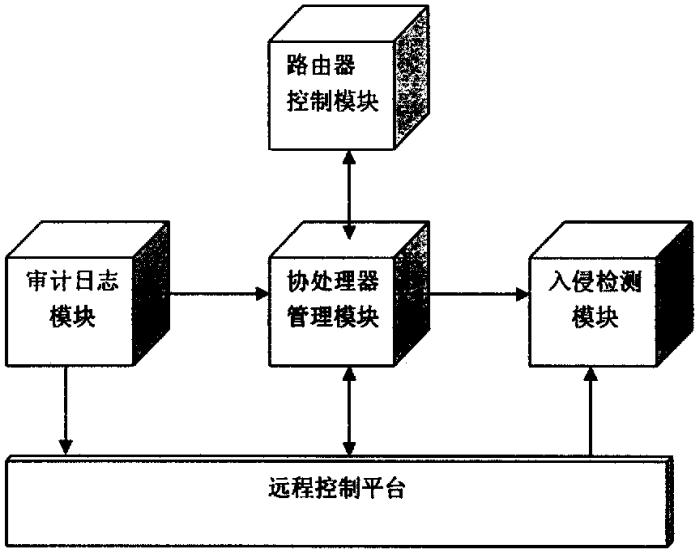

图4.2 系统结构模块

路由器控制模块：是系统和路由器的接口服务部分。到达路由器端口的终点数据包按照事先制定好的安全策略被转发到协处理器模块，并接收协处理器模块发送的解析后策略信息，根据信息丢弃有害数据包，让正常数据包通过。

协处理器管理模块：是整个系统的核心部分。是远程控制平台的后台服务器，响应来自远程控制平台的管理请求：基本配置、入侵规则管理、 审计日志的管理等，还负责路由器控制模块与路由器之间的通信。处理路由器控制模块转发过来的终点数据包，根据规则库解析此数据包是否为正常，如是攻击，立即做出反应，并将解析信息发送到路由器控制模块，丢弃此数据包。 确保路由器正常工作。

入侵检测模块：存储检测规则库。负责获取协处理器模块

的数据包，进行检测分析，对入侵进行告警，告警日志可以存入本机也可通过审计日志模块发送到远程控制平台。

审计日志模块：负责日志的存储和转发功能。发送到客户端或其他监控终端。对于正常的数据包在协处理器处理，结果经协处理器发送回路由器转发。

远程控制台客户端：是系统的用户接口。负责管理员配置、路由器地址配置、入侵检测配置、审计日志配置、转发策略配置和控制策略的配置。以及将系统反馈信息显示给用户。

4.2.2 系统功能参考模型

在本系统的具体设计中，又根据功能不同，提出参照图5的功能参考模型对主动防御型安全路由器系统进行分析。

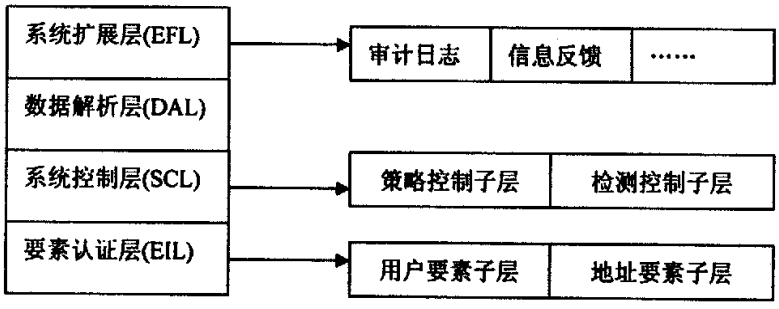

图 4.3 主动防御型安全路由器系统功能参考模型

该参考模型类似于 OSI（Open System Interconnection：开放系统互联）七层网络参考模型。它将本系统由低到高划分为四个大的功能层次，并根据所处理信息的不同，将其中几层分别细化为若干个并列的功能子层：

1 要素认证功能层(Element Identification Layer)：通常说来，启动一个系统必须要有关键性的用户审核、用于控制的本地和远程地址。参考模型将启动系统的用户，本地地址和远程地址等都抽象为一种认证要素(Element)。EIL 的作用就是对这些要素进行身份认证、地址信息等必要的检查，确定要素的合法性。功能上可以将此层细化为管理子层(Element Management)和认证子层(Element Identification)。软件功能当中的管理员配置、地址管理都属于此层功能。

2 系统控制层(System Control Layer)：该层应该是本系统模型的核心部分，它扮演着系统流程中控制核心的角色。本层的功能是，接收通过要素认证层认证的要素信息后，负责系统流程的控制。其处理内容包括竞标者是否策略转发、添加策略、删除策略、检测规则是否启动与成功等。

根据实际应用中的不同功能系统控制层又可以细化为策略控制(Policy Control)子层和检测控制(Detection Control)子层。检测控制子层专门负责系统中的检测信息，策略控制子层则根据实时情况来调整和控制策略信息。系统控制层将向底层（要素认证层）返回允许/拒绝用户登录、地址信息是否正确等信息；向其上层（数据解析层）传递策略信息和检测规则信息等。协处理器管理模块是此层的具体实现。

3 数据解析层(Data Analysis Layer)：负责处理系统控制层传来的策略信息（是否转发策略、添加控制策略、删除控制策略等），和分析入侵信息，根据规则库分析是否为正常数据包，依照启动的策略信息对数据包进行处理，丢弃有害数据包，让正常数据包通过。并将解析后处理的信息传递到高层，供高层做出相应处理。

4 系统扩展层(Extended Function Layer)：是本系统的高级应用层。对于一个孤立的主动防御型安全路由器系统，下三层实际上已经能够完成一个完整处理过程，但是对于系统整体功能的完善性来说，系统扩展层是一个非常有必要的功能层。根据不同的需求，系统扩展层可以扩展很多不同用途的功能子层。例如系统审计日志、信息反馈接口、系统用户管理和一些杂项功能。在本系统设计中，远程控制平台模块根据实际的需求实现了部分扩展层功能，协调系统运行和进行信息处理。

4.2.3 系统总体流程图

系统总体流程图如下所示。

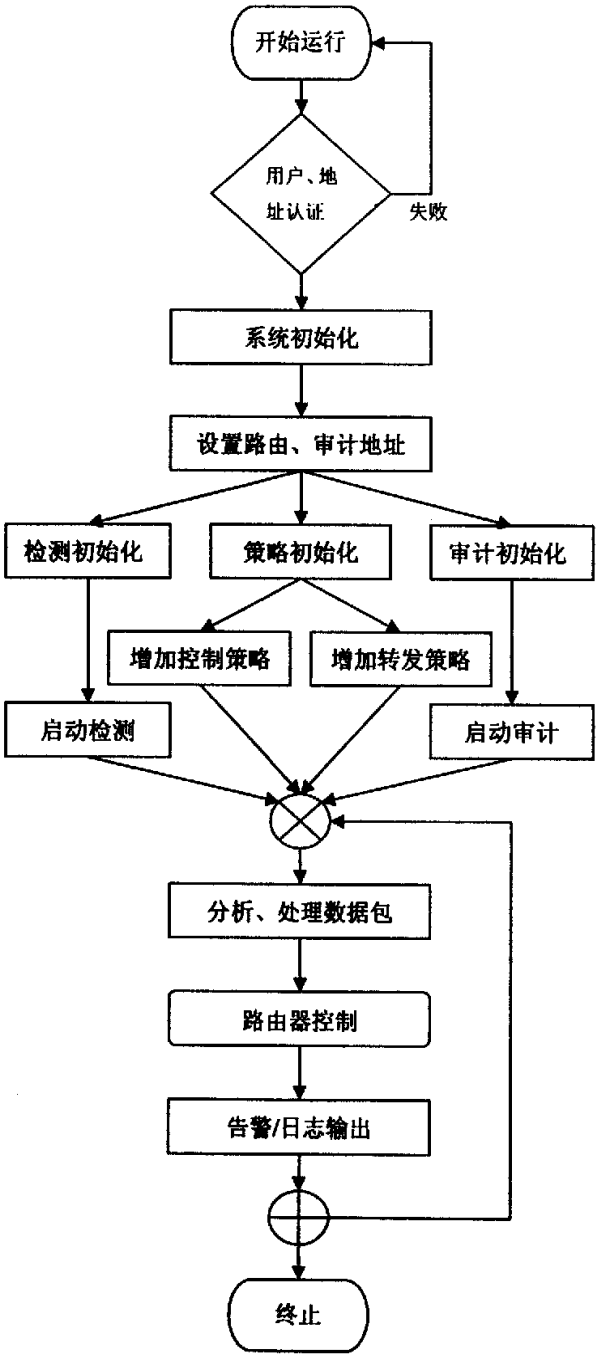
开始运行
用户、地址认证
失败
系统初始化
设置路由、审计地址
检测初始化
策略初始化
审计初始化
增加控制策略
增加转发策略
启动检测
启动审计
分析、处理数据包
路由器控制
告警/日志输出
终止

图 4.4 系统总体流程图

主动防御型安全路由器系统总体执行顺序及调用关系如下：

1. 首先执行协处理器管理模块主函数main()，其中包括路由客户端，代理服务端。同时启动路由器控制模块，其中包括路由服务端。
2. 启动远程控制平台，验证用户资料的正确性，还有协处理器的IP地址信息。通过后，调用相关例程对系统配置、转发策略、控制策略、检测规则和信息输出进行初始化；调用关键的规则解析进程，构造规则库。
3. 在对数据包进行处理时，首先是调用各种网络协议解析例程，对当前数据包进行分层协议字段的分析，并将分析结果存入重要的数据结构 Packet 中。
4. 系统依次调用协处理器管理模块和入侵检测模块，根据设定的各种规则和添加的控制策略把当前所捕获数据包的协议分析结果，主动地做出相应的是否发生入侵有害行为的判断。
5. 如果当前数据包符合某条检测规则所指定的情况，或者符合新增策略对它进行得控制，系统则根据该条规则或者该策略信息所定义的响应方式以及输出模块的初始化定义情况，选择日志记录和告警方式。

第五章 具有主动防御能力安全路由器系统的实现

5.1 路由器控制模块的设计与实现

5.1.1 路由器控制模块的功能分析

路由器控制模块是系统和路由器的接口服务部分。到达路由器端口的终点数据包按照事先制定好的安全策略被转发到协处理器模块，并接收协处理器模块发送的解析后策略信息，根据信息丢弃有害数据包，让正常数据包通过。

路由器控制模块中，系统虚拟超级用户 root,对系统进行控制，包括初始化控制、转发策略，添加控制、转发策略，删除控制、转发策略。当启动路由器系统时，路由器控制模块对安全策略进行初始化，根据策略信息完成数据包与路由器系统之间的交互，并根据协处理器模块传来的命令对安全策略进行添加、删除。路由器控制模块功能用例图如下：

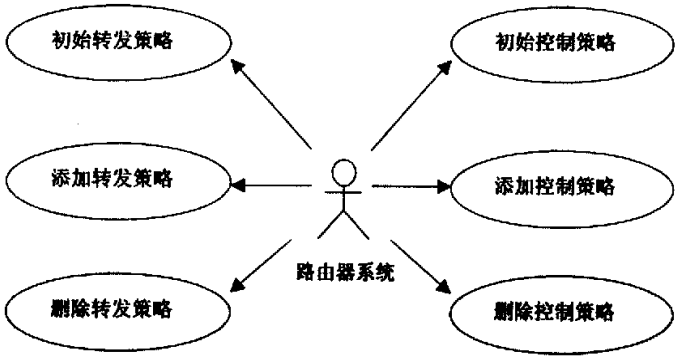

图 5.1 路由器控制模块功能用例图

5.1.2 路由器控制模块的类图实现

路由器控制模块可以配置多种策略。配置并启用这些策略，当发生事件时，模块依次调用这些策略，根据策略做出反应。本模块根据类图实现主要可以分为以下几个重要的类表：

1. ServerSocket

本模块的后台 Server 类，接受来自前台 Client 的响应，自动处理做出相应的发送，接收，类型识别，命令参数。包括 recvMsg()接收数据, recvMsgHeader()接收数据类型信息, sendMsg()发送数据等重要方法。

2. Modules

本模块的消息类型识别、处理部分的类表，以及后面的协处理器管理模块也要用到此类。此部分保存了多种消息类型模式，对每种模式进行相应的处理。

3. Router

本模块与路由器系统进行相应处理、操作的接口部分的类表。包括了一个重要链表 Rule(),存储了对通过路由器系统的数据包进行处理的规则，这些规则根据数据包目的地址，是否终点 ip 包，做出转发、接受、拒绝的处理。包括了 readRules()读取规则链, writerRules()写入规则链等重要方法。

4. RouteRule

本类功能即为根据 Router 类中的链表 Rule()中规则进行操作。根据源地址、目的地址、目的端口、协议、状态的不同对数据包的进行是否接受的动作、是否转发的处理。包括了 parseRuleLine()获取规则信息，toRuleLine()对规则信息进行处理，reverseRule()重

置规则信息等重要方法。

本模块类图实现关系如图所示：

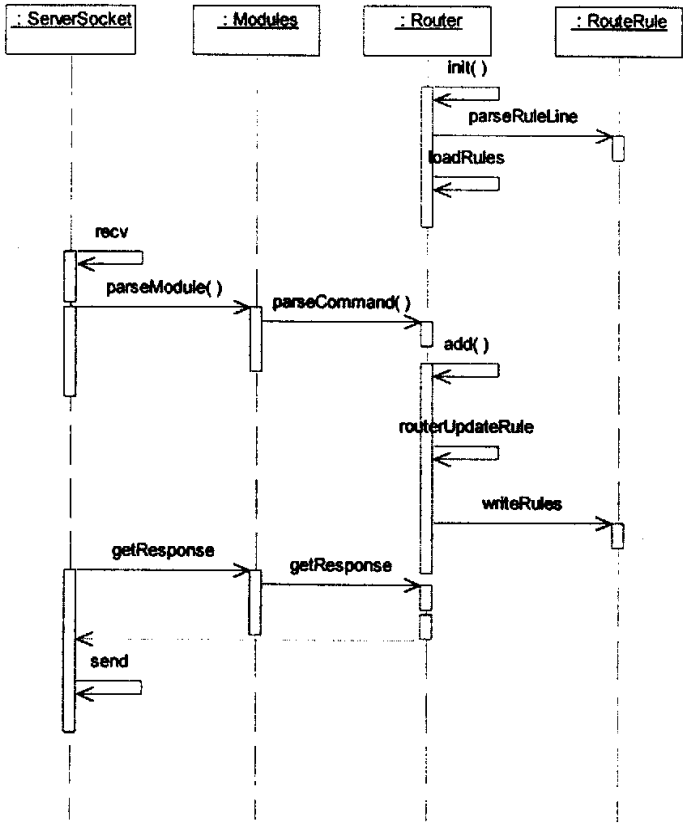

图 5.2 路由器控制模块类图实现

5.1.3 路由器控制模块的调用设计

RouteRule 保存了规则链中的各种状态，以及应该进行的操作信息。现将 RouteRule 分析如下：

public:

string m_status;　/* 规则链的状态分为 enable 或 disable*/

```
string m_src;       /* 规则链的源地址*/
string m_protocol; /* 规则链的采用的协议*/
string m_dst;       /* 规则链的目的地址*/
string m_dst_port; /* 规则链的目的地址的端口*/
string m_action;   /* 规则链的采用的动作*/
string m_to_dst;   /* 规则链的将要转发的目的地址*/
```

在后台 Server 启动，接受前台 Client 的相应，依次调用 Router 类和 RouterRule 类中的方法，实现整体路由器控制模块的调用。

1 初始化 bool Router:: init ()

该方法判断初始 Router 时是否加载了规则集，是则返回 true; 如果没有加载规则集，则调用 loadRule()方法，同时返回 false。

2 加载规则集 bool Router:: loadRules ()

在初始化 Router 后，遍历所用的规则，将用到的规则从初始到尾加载进 Router，并且返回 true。

3 规则读取 bool Router:: readRules ()

从本地的配置文件中 ROUTER_CONF_FILE，读取所用将要用到的规则，存到文件流中，以便 Router 操控，并且返回 true。

4 规则写入 bool Router:: writeRules ()

遍历文件流中的规则，将使用的规则存放到本地的配置文件中 ROUTER_CONF_FILE，并且返回 true。

5 命令分析 bool Router:: parseCommand(const Message &message)

传入一个 message 类的参数，通过传入的参数，本方法来分析该参数的命令，从而根据该命令，对 Router 进行操作。

6 规则操作 bool Router:: add (const Message &message), Router::

get (const Message &message), Router:: del (const Message &message), Router:: edit (const Message &message), Router:: clear (const Message &message)

传入一个 message 类的参数，根据参数内容的不同对规则进行控制，可以改变文件流中的规则，实现加、减、编辑、获取、清除这些操作，并且返回一个 bool 值。

7 规则升级 bool Router:: routerUpdateRule(const string ruleline)

传入一个 String 类的参数，该参数存放了对规则进行操作后的附加信息，文件流中的规则通过本方法将这些参数加载可以实现对 Router 中采用规则的控制，从而完成将路由控制模块装入协处理器控制模块处理的重要功能。

8 获取规则信息 bool RouteRule::parseRuleLine(const string ruleline)

传入一个 String 类的参数，该参数存放了文件流中的规则链的附加信息。通过本方法对规则链中的信息进行加工，以符合 RouteRule 类中定义的形式，并且返回 true。

9 规则处理 bool RouteRule:: toRuleLine ()

本方法对规则进行处理，成功则返回 true。

5.2 协处理器管理模块的设计与实现

5.2.1 协处理器管理模块的功能分析

协处理器管理模块：是整个系统的核心部分。是远程控制平台的后台服务器，响应来自远程控制平台的管理请求：基本配置、入侵规则管理、 审计日志的管理等，还负责路由器控制模块与路由器之间的通信。处理路由器控制模块转发过来的终

点数据包，根据规则库解析此数据包是否为正常，如是攻击，立即做出反应，并将解析信息发送到路由器控制模块，丢弃此数据包。 确保路由器正常工作。

协处理器管理模块中，系统虚拟超级用户 root,对系统进行控制，包括初始化控制，启动审计信息，停止审计信息、审计状态查看，启动入侵检测、停止入侵检测、检测状态查看。当启动路由器系统时，协处理器管理模块对检测信息、审计信息进行初始化，根据检测信息调用入侵检测模块对数据包进行处理，并调用审计模块来处理审计状态。协处理器管理模块功能用例图如下：

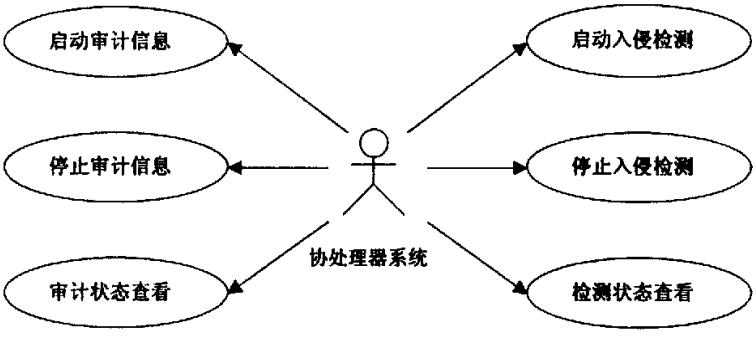

图 5.3 协处理器系统功能用例图

5.2.2 协处理器管理模块的类图实现

协处理器管理模块可以启动入侵检测模块，审计信息模块；当发生事件时，模块依次调用，并根据模块定义好的规则做出反应。本模块根据类图实现主要可以分为以下几个重要的类表：

1. ServerSocket

本模块的后台 Server 类，接受来自前台 Client 的响应，自动处理做出相应的发送，接收，类型识别，命令参数。包括 recvMsg()

接收数据, recvMsgHeader()接收数据类型信息, sendMsg()发送数据等重要方法。

2. Modules

本模块的消息类型识别、处理部分的类表，以及前面的路由器控制模块也要用到此类。此部分保存了多种消息类型模式，对每种模式进行相应的处理。

3. System

协处理器管理模块与系统执行操作的接口部分的类表。通过对 message 类中定义的命令 Command 进行分析,来判断它是何种类型，根据类型的不同，调用 SystemCfgFile 类和 SyslogdCfgFile 类中的方法进行操作，包括了 execute(),parseCommand()等重要方法。

4. SystemCfgFile

本类功能即为根据 System 类中的 parseCommand()中对 message 类中的命令进行分析而后的操作。根据接受来自远程控制平台的命令 Command 的不同，包括了设置、获取管理员密码，设置、获取协处理器地址，设置、获取协处理器端口，设置、获取路由器地址，设置、获取路由器端口等重要方法。

本模块类图实现关系如图所示：

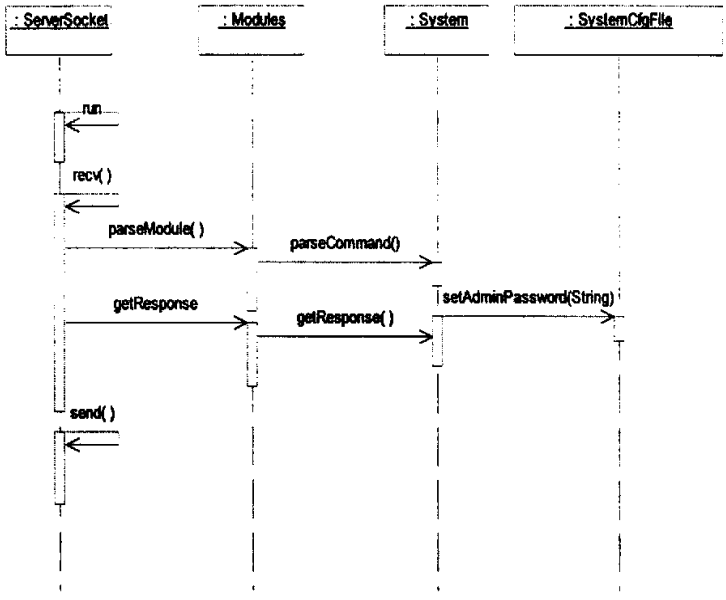

图 5.4 协处理器系统类图实现

5.2.3 协处理器管理模块的调用设计

MessageHeader 数据结构保存了发送过来的消息的类型命令，以及应该进行的操作信息状态，大小。现将 MessageHeader 分析如下：

```
typedef struct MessageHeader{
        int len;            /*消息信息的大小*/
        int module;         /*消息信息的模式*/
        int command;        /*消息信息的命令*/
        int status;         /*消息信息的状态*/
};
```

在本模块 Server 启动，接受来自远程控制平台发送的消息，

对比消息中的信息，依次调用 System 类和 SystemCfgFile 类中的方法，实现协处理器管理模块的调用，并以此来控制路由器模块。

1 启动模块 void ServerSocket:: run ()

本方法初始化信息，绑定地址，监听端口，然后判断其是否可以成功的接受到远程控制平台发送过来的消息。

2 接收消息报头 bool ServerSocket:: recvMsgHeader ()

初始化协处理器管理模块后，调用本方法来接收发送过来的报头，即 MessageHeader 的数据结构，成功则返回 true。

2 接收消息 bool ServerSocket:: recvMsg ()

在调用 ServerSocket:: recvMsgHeader ()后，调用本方法，对接收到的报头信息进行判断，根据报头信息接收发送过来的消息。成功则返回 ture。

3 发送消息 bool ServerSocket:: sendMsg ()

系统接收到的消息处理后，调用本方法，将反馈的命令，信息封装好，发送到远程控制平台。成功则返回 true。

4 解析命令 bool System:: parseCommand (const Message &message)

传入一个 message 类的参数，通过传入的参数，本方法来分析该参数的命令，从而根据该命令，对协处理器模块进行操作。

5 反馈消息 Message System:: getResponse ()

启动后台成功后，接受到远程控制平台的消息命令，在执行命令后，调用本方法，反馈系统的现有的状态消息。

6 读取文件 bool SystemCfgFile:: readFile()

在系统初始化时，读取系统的上次运行的配置文件，该文件中包含系统配置的基本信息，如 ip,端口等信息。读取该信息分类放入系统定义的结构中，并返回 true。

7 写入文件 bool SystemCfgFile::writeFile()

系统运行后，通过远程控制平台发送过来的消息，系统进行配置，并将系统配置的信息写入到本地一个配置文件中。并且返回 true。

8 管理用户密码 string SystemCfgFile::getAdminPassword()，void SystemCfgFile::setAdminPassword(string password)

对远程控制平台发送的信息解析，获得密码信息，返回 string 类型的值。和对其管理，传入 string 类型密码信息，更改设置管理员密码。

9 配置路由器信息 string SystemCfgFile::getRouteAddr(),void SystemCfgFile::setRouteAddr(string route)，int SystemCfgFile::getRoutePort()，void SystemCfgFile::setRoutePort(int port)

对远程控制平台发送的信息解析，获得路由器地址信息，返回 string 类型的值；获得路由器端口信息，返回 int 类型的值。和对其进行管理，传入 string 类型路由器地址信息，更改设置路由器地址；传入 int 类型路由器端口信息，更改设置路由器端口。

10 配置协处理器信息 string SystemCfgFile::getProxyAddr()，void SystemCfgFile::setProxyAddr(string proxy)，int SystemCfgFile::getProxyPort()，void SystemCfgFile::setProxyPort(int port)

对远程控制平台发送的信息解析，获得协处理器地址信息，返回 string 类型的值；获得协处理器端口信息，返回 int 类型的值。和对其进行管理，传入 string 类型协处理器地址信息，更改设置协处理器地址；传入 int 类型协处理器端口信息，更改设置协处理器端口。

5.3 远程控制平台的设计与实现

5.3.1 远程控制平台的功能分析

远程控制台客户端是系统的用户接口。负责管理员配置、路由器地址配置、入侵检测配置、审计日志配置、转发策略配置和控制策略的配置。以及将系统反馈信息显示给用户。

系统管理员可以在任意一个与后台系统得pc终端上，搭建远程控制平台。在平台上，系统管理员可以对其进行全方位的管理。用户登录，用户配置，添加、删除路由控制策略，添加、删除路由转发策略，启动、停止入侵检测，启动、停止告警日志，查看告警日志，删除告警日志。当后台系统启动后，系统管理员即可以通过远程控制平台对其后台进行初始化配置，启动多种策略，完成检测、告警的功能。远程控制平台功能用例图如下：

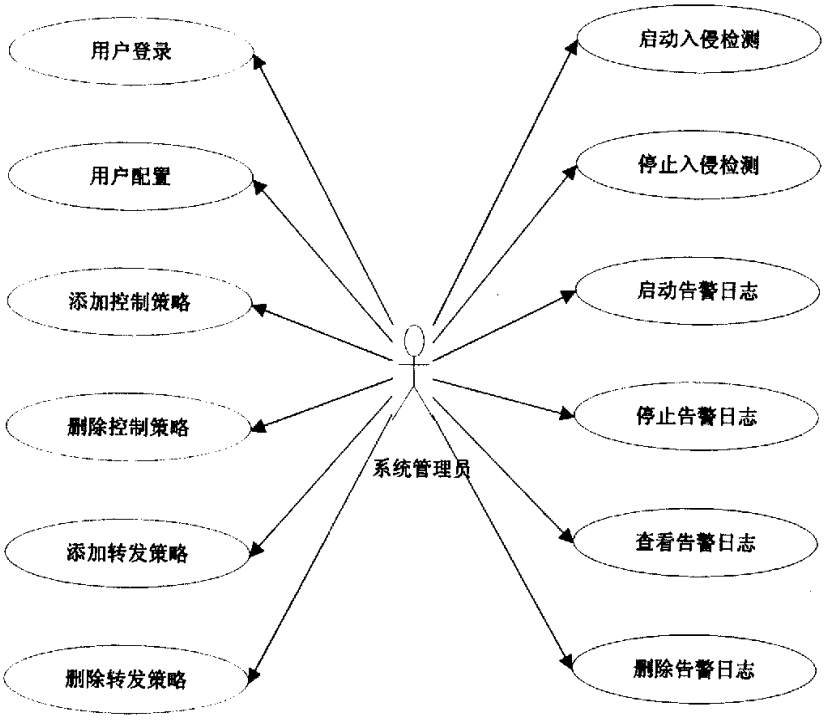

图 5.5 控制平台系统功能用例图

5.3.2 远程控制平台的体系实现

远程控制平台中 message 类包含了各种将要发送的消息状态、命令，将此发送到后台进行分析，监测。现将 message 类中消息分析如下：

```
class message
    {
        //模块的定义
        const int MODULES_SYSTEM_CFG = 1;
        const int MODULES_SNORT = 2;
```

```
const int MODULES_ROUTE_POLICY = 3;
const int MODULES_LOG = 4;

//管理员模块的命令
const int COMMANDS_ADMIN_LOGIN = 100;
const int COMMANDS_ADMIN_PASSWORD_SET = 101;
const int COMMANDS_ADMIN_ROUTE_ADDRES_SET = 102;
const int COMMANDS_ADMIN_ROUTE_ADDRESS_GET = 103;
const int COMMANDS_ADMIN_PROXY_ADDRESS_SET = 104;
const int COMMANDS_ADMIN_PROXY_ADDRESS_GET = 105;
const int COMMANDS_ADMIN_LOG_HOST_GET = 106;
const int COMMANDS_ADMIN_LOG_HOST_ADD = 107;
const int COMMANDS_ADMIN_LOG_HOST_DEL = 108;

//检测模块的命令
const int COMMANDS_SNORT_START = 200;
const int COMMANDS_SNORT_STOP  = 201;
const int COMMANDS_SNORT_STATUS_GET  = 202;

//路由模块的命令
const int COMMANDS_ROUTER_GET = 300;
const int COMMANDS_ROUTER_ADD = 301;
const int COMMANDS_ROUTER_DEL = 302;
const int COMMANDS_ROUTER_CLEAR = 303;
const int COMMANDS_ROUTER_EDIT = 304;
```

```
    //审计模块的命令
    const int COMMANDS_LOG_START = 400;
    const int COMMANDS_LOG_STOP = 401;
    const int COMMANDS_LOG_CLEAR = 402;
    const int COMMANDS_LOG_STATUS_GET = 403;

    //状态分类
    const int SUCCESS = 1;
    const int FAILURE = 0;
}
```

远程控制平台主要分为系统配置部分，入侵检测部分，路由策略部分，审计部分。详述如下：

系统配置部分（tabSystem）

本部分主要任务是相关系统初始的管理配置，分为实现用户登录、用户配置、地址配置，而地址配置又可以分为路由器地址配置、协处理器地址配置、审计地址配置。在 tabSystem 初始化时，系统会加载必要信息如下：

```
sys_load()              /*加载用户信息*/
ripAddress_load()       /*加载路由器地址信息*/
cipAddress_load()       /*加载协处理器地址信息*/
lstAddress_load()       /*加载审计地址信息*/
```

入侵检测部分（tabIDS）

本部分主要任务是对检测规则进行管理，分为启动入侵检测，停止入侵检测，配置入侵检测，对检测规则进行修改。在 tabIDS 初始化时，系统会加载必要信息如下：

IDS_load()　　/*加载 IDS 启动信息*/

IDSconf_load()　　/*加载 IDS 配置信息*/

路由策略部分（tabRoute）

本部分主要任务是配置路由控制策略和配置路由转发策略，路由控制策略分为添加、删除路由控制策略，启动、停止路由控制策略，路由转发策略分为添加、删除路由转发策略，启动、停止路由转发策略。在 tabRoute 初始化时，系统会加载必要信息如下：

routeCt_load()　　/*加载路由控制策略*/

routeSd_load()　　/*加载路由转发策略*/

审计部分（tabStat）

本部分主要任务是对告警日志进行控制，分为启动告警日志，停止告警日志，查看告警日志，删除告警日志。在 tabStat 初始化时，系统会加载必要信息如下：

start_Stat()　　/*开始监听审计服务*/

chStat_load()　　/*加载审计启动信息*/

本平台体系结构如图所示：

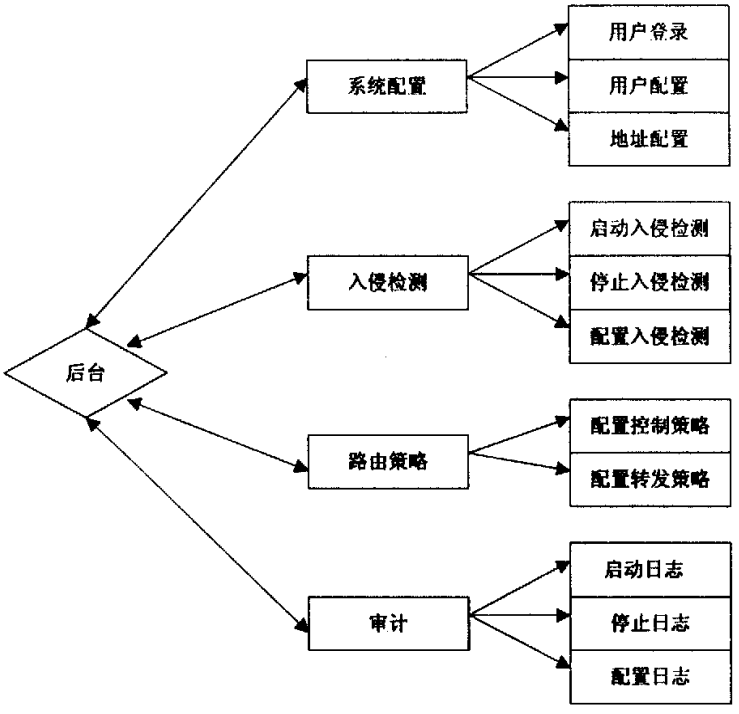

图 5.6 控制平台体系结构

5.3.3 CIIP 内部协议的设计

在远程控制平台启动后，要先接收后台的信息，然后将启动信息与配置情况发送到后台，并在接收反馈信息。为实现信息通信的流畅，设计开发了一套标准的控制信息交换协议(CIIP：Control Information Interactive Protocol)来完成此过程。该协议的握手及交换信息规程如图所示：

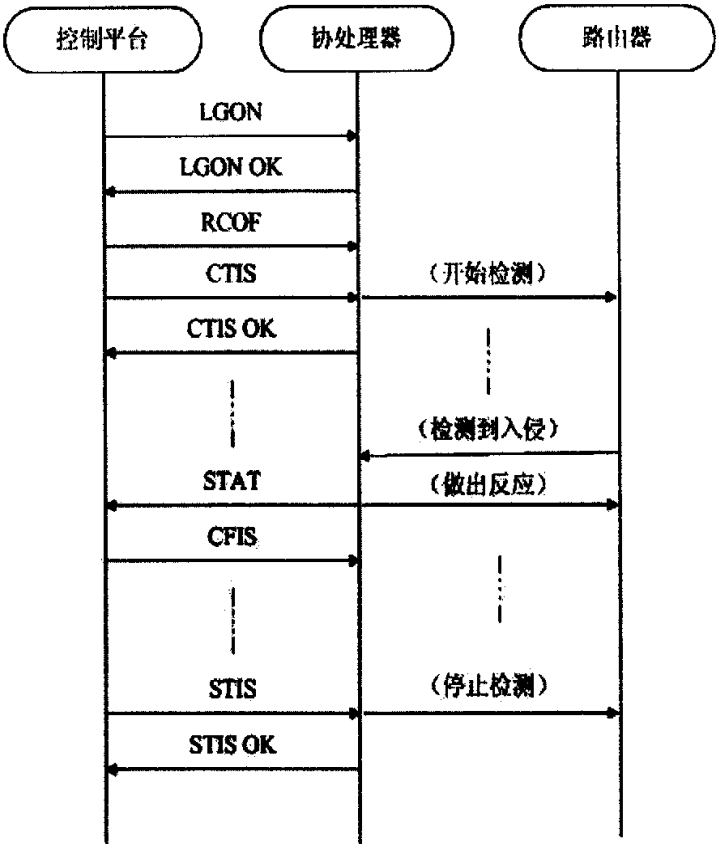

图 5.7 内部协议 CIIP

CIIP 内部协议规定了一系列具有特定含义的关键字来表示不同的操作意图，例如 LOGN 表示登录请求，CTIS 表示启动入侵检测请求等。

后台系统启动后，远程控制平台开始工作时，前端系统首先通过 SOCKET 向协处理器管理模块发送以 LOGN 为协议关键字的网络登录指令包；协处理器管理模块负责捕捉网络信息包，它收到 LOGN 后进行登录信息校验，校验成功后向控制平台返回含有 LOGN OK 关键字的校验成功信息；控制平台收到后接着发送以

RCOF 为关键字的指令要求协处理器管理模块初始化所有协处理器地址信息，路由器地址信息，审计地址信息，系统状态；然后以含有 CTIS 关键字的协议指令命令协处理器管理模块启动 IDS，开始检测；启动成功后协处理器管理模块向控制平台返回启动成功信息 CTIS OK。

如果没有入侵消息，系统正常运行下去。当出现入侵时，协处理器管理模块以 STAT 指令通知控制平台，平台收到后将信息告警，通知管理员查看。同时协处理器管理模块将启动响应措施做出反应。 当系统管理员根据情况配置入侵规则时 ，控制平台以含有 CFIS 关键字的协议指令命令协处理器管理模块配置 IDS 股则，然后重新开始检测，流程如上。

当准备停止系统时，控制平台以 STIS 指令通知协处理器管理模块停止检测；停止成功后协处理器管理模块向控制平台返回启动成功信息 STIS OK。

5.4 入侵检测模块的设计与实现

5.4.1 入侵检测模块的设计分析

入侵检测模块存储了检测规则库。负责获取协处理器模块的数据包，进行检测分析，对入侵进行告警，告警日志可以存入本机也可通过审计日志模块发送到远程控制平台。

入侵检测模块实现的原理如下图所示：

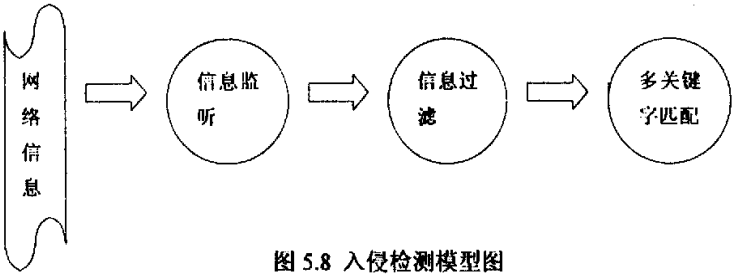

图 5.8 入侵检测模型图

在设计与实现入侵检测模块时，考虑选用了开放源代码的 Snort，主要基于如下几点考虑：

1 Snort 具有实时流量分析和记录 IP 数据包的能力，能够进行简单的协议分析，对内容进行搜索/匹配。还能够监测各种不同的攻击方式，对攻击实时报警。

2 Snort 具有很好的扩展性和可移植性。

3 Snort 遵循通用公共许可证 GPL，所以只要遵守 GPL 任何组织和个人都可以自由使用和改动。

Snort 有五个子模块组成，分别为主控程序、规则模块、数据包解码模块、数据分析模块和其他辅助模块，如下图所示：

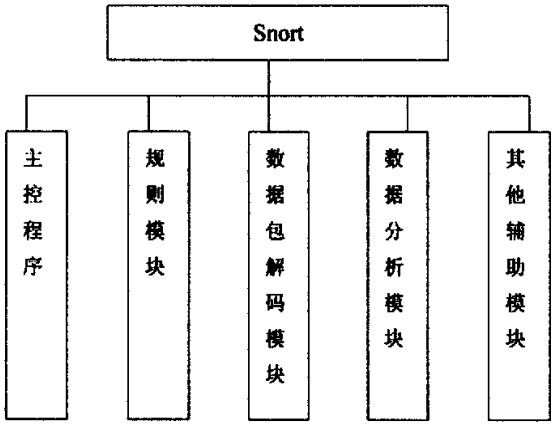

图 5.9 Snort 整体结构

Snort 的总体工作流程如下图所思，首先由主控程序做一系列

初始化以及命令行参数解析，然后初始化插件（建立插件索引表）、预处理器（建立预处理器索引表）和输出插件（建立输出插件索引表），如果在命令行中指定了外部规则，系统则需要加载由参数指定的规则文件，建立规则链表（预处理器链表、输出插件链表和插件链表），最后进入数据包采集、解码与数据分析过程。

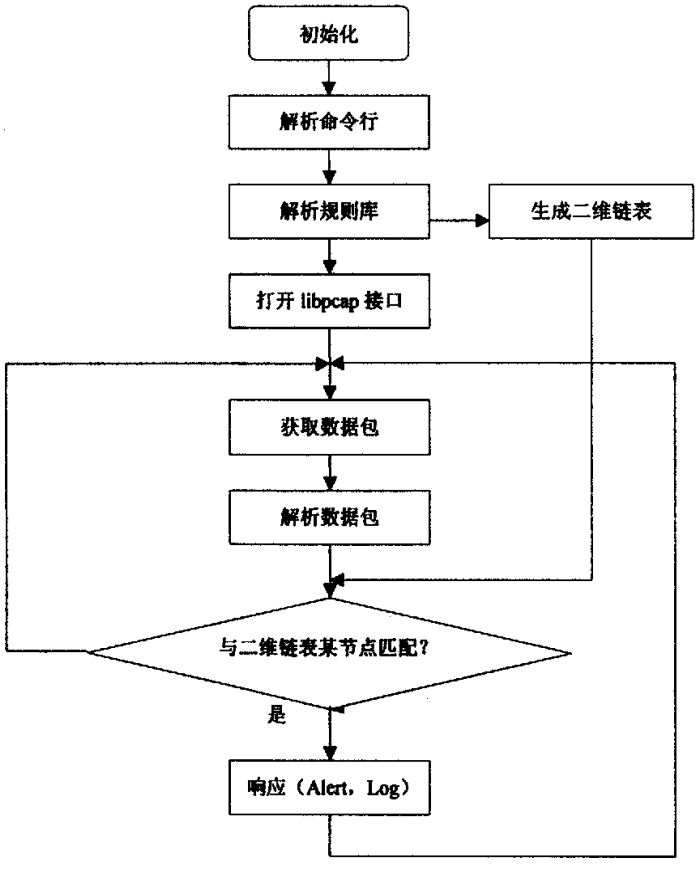

图 5.10　Snort 总体工作流程

5.4.2 入侵检测模块规则库的设计

在系统中，我们采用了规则库文件的方式来描述入侵行为，每条规则都可以分成逻辑上的两个部分：1)规则头；2)规则选项。规则头包括：规则行为、协议、源和目的 IP 地址、子网掩码以及源端口信息和目的端口信息。规则选项包含报警信息和异常包的信息(特征码)，使用这些特征码来决定是否采取规则规定的行动。

例如：alert tcp any any->202.112.146.51/24 135 (content:\ "|4500 005c 1a8d|"；msg: "mountd access")

其中 alert tcp any any->202.112.146.51/24 135 是规则头；

content: "|4500 005c 1a8d|"； msg: "mountd access" 是规则参数；content，msg 是参数关键字。

规则头

规则头包含一个报文关键的地址信息、协议信息以及当前报文符合此规则时各个元素应该采取的行动。它包括以下几个方面。

1. 规则行为

每条规则的第一项就是规则行为。规则行为告诉系统当发现匹配的数据包时应该如何处理。其中定义了五种的处理方式：alert、log、pass、activate 和 dynamic。

2. 协议字段

为了分析可疑的操作，目前包含了三种协议：TCP、UDP、IP 和 ICMP。将来，可能提供对 ARP、GRE、OSPF、RIP 等协议的支持。

3. IP 地址

这一个部分处理一个给定规则的 IP 地址和端口信息。关键词

"any"可以用来定义任意的 IP 地址。规则不支持对主机名的解析，所以地址只能使用数字/CIDR 的形式。/24 表示一个 C 类网络；/16 表示一个 B 类网络；而/32 表示一台特定的主机地址。例如：202.112.146.0/24 表示从 202.112.146.1 到 202.112.146.255 的地址。我们可以使用否定操作符"!"对 IP 地址进行操作。它告诉程序除了列出的 IP 地址外，匹配所有的 IP 地址。还可以使用 any 通配符来声明源、目的地址，any 代表所有的地址。

4. 端口信息

在规则中，可以有几种方式来指定端口号，包括："any"、静态端口号定义、端口范围，以及使用否定操作符。

"any" 表示任意合法的端口号。

静态端口号表示单个的端口号，例如：21(ftp)、23(telnet)、80(http)等。

范围操作符"："可以指定端口号范围。有几种方式来使用范围操作符，例如：

log udp any any -> 202.112.146.0/24 1:1024 记录来自任何端口，其目的端口号在 1 到 1024 之间的 UDP 数据包。

5. 方向操作符

方向操作符"->"表示数据包的流向。它左边是数据包的源地址和端口，右边是目的地址和端口。此外，还有一个双向操作符"<>"，它使程序能够对两个 IP 地址/端口之间双向的数据传输进行记录和分析，例如下面的规则用来记录以某个范围内的主机(202.112.146.0/24)作为服务器(telnet 服务的端口号 23)的所有 telnet 会话的双向数据流。

log ! 202.112.146.0/24 any <> 202.112.146.0/24 23

6. activate/dynamic 规则

activate/dynamic 规则对扩展了系统功能。使用 activate/dynamic 规则对，能够使用一条规则去激活另一条规则。动态规则和日志规则相似，不过它需要一个选项：activated_by。动态规则还需要另一个选项：count。当一个激活规则启动，它就打开由 activate/activated_by 选项之后的数字指示的动态规则，记录 count 个数据包。例如：

activate tcp any any -> any 23 (activates: 23;msg:" Potential Telnet Login Credentials Logged";)dynamic tcp any any ->any 23 (activated_by:23;count: 20;)

这个规则说明当发现 Telnet 默认使用的 23 端口有通信，activate 规则会被触发并启动 dynamic 规则，然后 dynamic 规则将遵循配置，记录后面的 20 个包。

规则选项

规则选项是实际特征和分配的优先级，构成了入侵检测引擎的核心。所有的规则参数以分号分隔开。下面列举了 24 个选项关键字，简述如下：

1) msg：给检测到的事件命名。
2) logto：把日志记录到一个用户指定的文件，而不是输出到标准的输出文件。
3) ttl：测试 IP 包头的 TTL 域的值。
4) tos：测试 IP 包头的 TOS 域的值。
5) id：测试 IP 分组标志符是否是一个特定的值。
6) ipoption：查看 IP 选项域。
7) fragbits：测试 IP 包头的分片位的值。

8) dsize：测试数据包的附带数据长度的值。

9) flags：测试 TCP 标志是否是某个值。

10) seq：测试 TCP 包的序列号是否是某个值。

11) ack：测试 TCP 包的确认域是否为某个值。

12) itype：测试 ICMP 数据包的类型域。

13) icode：测试 ICMP 数据包的编码域。

14) icmp_id：测试 ICMP 回送包的标志符是否为某个值。

15) icmp_seq：测试 ICMP ECHO 顺序号的值。

16) content：在数据包的数据段中搜索模式。

17) content-list：在数据包的数据段中搜索模式清单。

18) offset：设置开始搜索的偏移量。

19) depth：设置搜索最大深度。

20) nocase：大小写不敏感匹配内容字符串。

21) session：记录指定会话的应用层信息。

22) rpc：观察特定应用/进程调用的 RPC 服务。

23) resp：激活反应措施(断开连接等)。

24) react：激活反应措施(阻塞 WEB 站点)。

5.4.3 几种入侵行为的检测方法

本系统模块能够检测目前常见的大多数攻击行为，根据新的攻击，及时地添加自己定义的新规则。举例如下：

1. windows 系统漏洞

Remote Procedure Call(RPC)是 Windows 操作系统使用的一种远程过程调用协议，RPC 协议提供一种进程间的交互通信机制，它允许本地机器上的程序进程无缝的在远程系统中运行代码。

此漏洞可以通过 135(TCP/UDP)、139、445、593 等端口发起攻击。由于 Windows 的分布式组件对象模型技术(DCOM)实现在处理一个参数的时候没有检查长度。通过提交一个超长(数百字节)的文件名参数可以导致堆溢出，从而使 RpcSS 服务崩溃。精心构造提交的数据就可以在系统上以本地系统权限运行代码。攻击者可以在系统中采取任何行为，包括安装程序、窃取更改、删除数据、或以完全权限创建新账号。

W32.Blaster.Worm 是一种利用 DCOM RPC 漏洞进行传播的蠕虫，传播能力很强。它扫描端口号是 TCP/135，传播成功后它会利用 tcp/4444 和 UDP 69 端口下载并运行它的代码程序 Msblast.exe。这个蠕虫还将对 windowsupdate.com 进行拒绝服务攻击。

W32.Nachi.Worm 蠕虫如果发现被感染的机器上有“冲击波”蠕虫，则杀掉“冲击波”蠕虫，并为系统打上补丁程序，但由于程序运行上下文的限制，很多系统不能被打上补丁，并导致反复重新启动。ICMP 蠕虫感染机器后，会产生大量长度为 92 字节的 ICMP 报文，从而导致整个网络不可用。这些报文的特征如下：

xxx.xxx.xxx.xxx > xxx.xxx.xxx.xxx: icmp: echo request

4500 005c 1a8d 0000 7801 85be xxxx xxxx

xxxx xxxx 0800 26b1 0200 79f9 aaaa aaaa

aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa。

相应的 IDS 规则设计为：

1) alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"DCE RPC Interface Buffer Overflow Exploit"; content:"|00 5C 00 5C|"; content:!"|5C|"; within:32; flow:to_server, established;

reference:bugtraq，8205; rev: 1;)

2) alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"W32.Nachi.Worm infect ";content:"|aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa|";itype:8;depth:32; reference:cve , CAN-2003-0352; sid:11483; classtype:misc-activity; rev:2;)

3) alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC ISystemActivator bind attempt"; flow:to_server，established; content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1; within:1; byte_test:1，&，1，0，relative; content:"|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";distance:29; within:16; reference:cve , CAN-2003-0352; classtype:attempted-admin;sid:2192; rev:1;)

2. Dos 拒绝服务攻击

拒绝服务攻击是由人或非人为发起的行动，使你的主机硬件、软件或者两者同时失去工作能力，使你的系统不可访问并因此拒绝合法的用户服务要求。这种攻击往往是针对 TCP/IP 协议中的某个弱点，或者系统存在的某些漏洞，对目标系统发起的大规模进攻致使攻击目标无法向合法的用户提供正常的服务。常用的拒绝服务攻击如下：

1) ping 拒绝服务攻击(ping of death)

“ping”攻击是向目标端口发送大量的超大尺寸的 ICMP 包来实现的。由于在早期的阶段，路由器对所传输的文件包最大尺寸都有限制，许多操作系统对 TCP / IP 的实现在 ICMP 包上都是规定 64KB，并且在对包的标题头进行读取之后，要根据该标题头里

包含的信息来为有效载荷生成缓冲区，一旦产生畸形即声称自己的尺寸超过ICMP上限的包，也就是加载的尺寸超过64KB上限时，就会出现内存分配错误，导致TCP / IP堆栈崩溃，从而导致系统崩溃。这类攻击只要简单地使用命令：ping -l 65510 目标主机IP。

相应的IDS规则设计为：

alert udp $EXTERNAL_NET any -> $HOME_NET (msg:"DOS mstream handler ping to server" ; content: "ping"; classtype:attempted-dos; sid:245; rev:1;)

2) SYN flood攻击

SYN flood攻击也是一种常用的拒绝服务攻击。它的工作原理是，正常的一个TCP连接需要连接双方进行三个动作，即“三次握手”，其过程如下：请求连接的客户机首先将一个带SYN标志位的包发给服务器；服务器收到这个包后产生一个自己的SYN标志，并把收到包的SYN+1作为ACK标志返回给客户机；客户机收到该包后，再发一个ACK=SYN+1的包给服务器。经过这三次握手，连接才正式建立。在服务器向客户机发送返回包时，它会等待客户机的ACK确认包，这时这个连接被加到未完成连接队列中，直到收到ACK应答后或超时才从队列中删除。这个队列是有限的，一些TCP / IP堆栈的实现只能等待从有限数量的计算机发来的ACK消息，因为他们只有限度数量的内存缓冲区用于创建连接，如果这些缓冲区内充满了虚假连接的初始信息，该服务器就会对接下来的连接停止响应，直到缓冲区里的连接企图超时。如果客户机伪装大量SYN包进行连接请求并且不进行第三次握手，则服务器的未完成连接队列就会被塞满，正常的连接请求就会被拒绝，这样就造成了拒绝服务。

相应的 IDS 规则设计为：

alert tcp $HOME_NET any <> $EXTERNAL_NET any (msg:"DDOS shaft synflood"; flags: S; seq: 674711609; reference:arachnids,253; classtype:attempted-dos; sid:241; rev:2;)

3) UDP Flood 防范

以 trinoo 程序为例子，它使用了 UDP 协议。Trinoo master 程序的监听端口是31335，攻击者一般借助telnet通过TCP连接到master程序所在计算机。常用的抓包工具能够搜索到使用 TCP (类型 6) 并连接到端口 31335 的数据流。所有从 master 程序到代理程序的通讯都包含字符串"l44"，并且被引导到代理的 UDP 端口 31335。入侵检测软件检查到 UDP 端口 31335 的连接，如果有包含字符串 l44 的信息包被发送过去，那么接受这个信息包的计算机可能就是 DDoS 代理。

相应的 IDS 规则设计为：

1) alert udp $EXTERNAL_NET any -> $HOME_NET 31335 (msg:"DDOS Trin00\:DaemontoMaster(*HELLO*detected)"; content:"*HELLO*"; reference:arachnIDS，185; reference:url，www.sans.org/newlook/resources/IDFAQ/trinoo.htm; classtype:attempted-dos; sid:232; rev:2;)
2) alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"DDOS TFN Probe"; id: 678; itype: 8; content: " l44";reference:arachnIDS，443; classtype:attempted-recon; sid:221; rev:1;)

5.5 审计日志模块的设计与实现

5.5.1 审计日志模块的功能分析

记录重要的系统事件是系统安全的一个重要因素。日志就是操作系统或应用程序记录所发生的事件并保存这些记录用于以后分析的过程。操作系统一般都维护几个基本的日志文件来跟踪和记录系统中发生了什么事情，包括谁登录进入、谁退出登录、以及他们做了些什么。

日志文件对于维护系统安全很重要，它们为两个重要功能提供数据:审计和监测。它们通过提供一个历史记录（系统中关于活动的审计轨迹）允许用户或第三方回头来系统地评价安全程序的效率以及确定引起安全破坏或系统功能失效的原因。如果需要，它们还能作为呈现给权威机构的证据。它们还能用来“实时”地监测系统状态，检测和追踪侵入者，发现 hug 以及阻止问题的发生。虽然日志的存在不能提供完全的可记录性，但日志能使系统管理员和安全员做到:

- 发现试图攻击系统安全的重复举动。
- 跟踪那些想要越权的用户。
- 跟踪异常的使用模式。
- 实时跟踪侵入者。

日志能够帮助检测。当系统被攻击或有人侵入时，尽快知道很重要。虽然日志不能阻止侵入，但它能体现出基本账户安全的一个漏洞。甚至当账户安全失败，攻击者能够剥夺用户权利时，也希望这件事能记录下来。一旦知道发生了什么事，就可以采取相应的行动如切断用户、加强网络控制，监测侵入者以搜索证据

等等。记录日志、维护日志、日志监测和审计等策略都是完整安全策略的重要组成部分。

5.5.2 Syslog 设备的调用

Syslog 已被许多日志函数采纳，它用在许多保护措施中--任何程序都可以通过 Syslog 纪录事件。Syslog 可以纪录系统事件，可以写到一个文件或设备中，或给用户发送一个信息。它能纪录本地事件或通过网络纪录另一个主机上的事件。

Syslog 设备依据两个重要的文件：/etc/syslogd（守护进程）和/etc/syslog.conf 配置文件，习惯上，多数 Syslog 信息被写到/var/adm 或/var/log 目录下的信息文件中（messages.*）。一个典型的 Syslog 纪录包括生成程序的名字和一个文本信息。它还包括一个设备和一个优先级范围（但不在每个之中出现）。

每个 Syslog 消息被赋予下面的主要设备之一：

LOG_AUTH--认证系统：login、su、getty 等

LOG_AUTHPRIV--同 LOG_AUTH，但只登录到所选择的单个用户可读的文件中

LOG_CRON--cron 守护进程

LOG_DAEMON--其他系统守护进程，如 routed

LOG_FTP--文件传输协议：ftpd、tftpd

LOG_KERN--内核产生的消息

LOG_LPR--系统打印机缓冲池：lpr、lpd

LOG_MAIL--电子邮件系统

LOG_NEWS--网络新闻系统

LOG_SYSLOG--由 syslogd（8）产生的内部消息

LOG_USER--随机用户进程产生的消息

LOG_UUCP--UUCP 子系统

LOG_LOCAL0~LOG_LOCAL7--为本地使用保留

Syslog 为每个事件赋予几个不同的优先级：

LOG_EMERG--紧急情况

LOG_ALERT--应该被立即改正的问题，如系统数据库破坏

LOG_CRIT--重要情况，如硬盘错误

LOG_ERR--错误

LOG_WARNING--警告信息

LOG_NOTICE--不是错误情况，但是可能需要处理

LOG_INFO--情报信息

LOG_DEBUG--包含情报的信息，通常在调试一个程序时使用

syslog.conf 文件指明 syslogd 程序纪录日志的行为，该程序在启动时查询配置文件。该文件由不同程序或消息分类的单个条目组成，每个占一行。对每类消息提供一个选择域和一个动作域。这些域由 tab 隔开：选择域指明消息的类型和优先级；动作域指明 syslogd 接收到一个与选择标准相匹配的消息时所执行的动作。每个选项是由设备和优先级组成。当指明一个优先级时，syslogd 将纪录一个拥有相同或更高优先级的消息。所以如果指明\"crit\"，那所有标为 crit、alert 和 emerg 的消息将被纪录。每行的行动域指明当选择域选择了一个给定消息后应该把他发送到哪儿。例如，如果想把所有邮件消息纪录到一个文件中，如下：

```
#Log all the mail messages in one place
        mail.* /var/log/maillog
```

结　论

在现今网络飞速发展的时代中，路由器有着举足轻重的作用。因为路由器作为网络层中的中继系统，提供着一个在第三层网络数据的路由选择与转发功能。因此，路由器作为网络互连的关键设备，是网络与其它网络进行通信的一个“关口”，对其安全性有很高的要求。

本文完成的工作：

通过分析现有路由器面临威胁的基础上，开发出一种具有主动防御能力的安全路由器系统体系。在网络层对可能存在威胁的IP数据包进行分类，从而引入了协处理器的概念。协处理器把最具威胁性的终点IP包从路由器中引开，以保障正常的路由功能不受恶意IP包的影响。并通过入侵检测模块对可疑IP包的行为进行分析和学习，以便及时发现路由器自身存在的缺陷和漏洞，及早进行修补，使路由器具备了主动防御能力，且不增加路由器正常的工作负担。

进一步的工作：

在“协处理器”技术比较成熟和稳定后，“协处理器”和路由器可以集成为一体，这样在“协处理器”和路由器之间会具有更高的传输速度和更好的安全性。

致　谢

本次毕业论文的设计得到我的导师北京交通大学电子信息工程学院刘云教授的谆谆教诲，回首两年半的学习历程，与导师的每一次讨论和交流都使我深受启发、获益匪浅，我的每一次提高和进步都是与刘老师的批评和关心、鼓励分不开的。在此向刘老师致以最诚挚的感谢。

本论文的完成得到了深圳市科委计划项目（编号 05KJce019）的支持和深圳职业技术学院计算中心温晓军博士的大力协助，还受到了张长伦博士、宁红宙博士的指导，在他们的帮助下，本论文得以在结构性设计上取得突破。

感谢教研室孟司仪副教授、张振江老师、穆海冰老师、周春月老师的热心帮助和关怀，感谢所有在生活、学习中给予我无私帮助的同学们。

感谢我的父母，多年来他们一直给予我无微不至的关怀和巨大的鼓励，使我能够顺利地完成学业。

最后，向百忙中抽出时间来评审论文和参加答辩的老师表示深深的感谢！

参考文献

1. 谭浩强， c 程序设计（第二版），清华大学出版社，1999.
2. 严蔚敏，吴伟民著 数据结构（C 语言版）. 清华大学出版社，1997.
3. W. Richard Stevenss 著，尤晋元等译. UNIX 环境高级编程，机械工业出版社，2004.
4. Kurt Wall 等著，张辉译. GNU/Linux 编程指南，清华大学出版社，2002.
5. Neil Matthew，Richard Stones 著，杨晓云等译. Linux 程序设计，机械工业出版社，2002.
6. 谢希仁，计算机网络（第四版），大连理工大学出版社，2004.
7. 张宏科，IP 路由原理与技术，清华大学出版社，2000
8. 刘峰，李志勇，陶然，王越，网络对抗，国防工业出版社，2003
9. 唐正军，《黑客入侵防护体系系统源代码分析》，机械工业出版社，2002.3
10. 刘渊，乐红兵，宋志庆等， 因特网防火墙技术[M].，机械工业出版社，1998.5
11. Jack Koziol 著，吴溥峰等译，Snort 入侵检测实用解决方案，机械工业出版社，2005.1
12. 唐正军， 入侵检测技术导论，机械工业出版社，2004.
13. 何丰，保文星. Cisco 路由器安全技术研究[J]. 西北民族学院学报，2001，22(4).
14. W. Richard Stevens. TCP/IP Illustrate, Volume 1: The protocols. Addison Wesley Publishing Company, 1994.

15. Gray R. Wright W. Richard Stevens. TCP/IP IIlustrate, Volume 2: The implementation. Addison Wesley Publishing Company, 1994.

16. Information Science Institute University of Southern California. RFC791: Internet Protocol, 1981

17. Feng Zhang, Shijie Zhou, Zhiguang Qin, Jinde Liu. Honeypot: A Supplemented Active Defense System for Network Security[A]. Parallel and Distributed Computing, Applications and Technologies[C]. New York: IEEE, 2003. 231-235.

18. Weiler, N. Honeypots for Distributed Denial-of-Service Attacks[A]. Enabling Technologies: Infrastructure for Collaborative Enterprises[C]. New York: IEEE, 2002. 109-114.

部分网址：

Axent Technologies 公司网址: http://www.axent.com

Cisco Systems 公司网址:http://www.cisco.com

Internet Security Systems 公司网址:http://www.iss.net

Intrusion Detection 公司网址:http://www.intrusion.com

Network Associates 公司网址:http://www.nai.com

CyberSafe 公司网址:http://www.cybersafe.com/

中科网威公司网址:http://www.netpower.com.cn/