

《网络异常流量识别与监控技术研究》

图书基本信息

书名：《网络异常流量识别与监控技术研究》

13位ISBN编号：9787302223573

10位ISBN编号：7302223572

出版时间：2010-9

出版社：清华大学出版社

作者：孙知信

页数：213

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《网络异常流量识别与监控技术研究》

内容概要

《网络异常流量识别与监控技术研究》系统地阐述了路由器端异常流量的检测与防范技术。首先介绍了DoS和DDoS的原理，综述了目前DDoS异常流量的检测技术现状和最新的研究成果；在此基础上介绍了作者创新性地设计并实现的5种DDoS检测算法以及对算法进行的局部仿真测试。在理论研究的基础上，作者结合一个具体的研究项目将上述算法应用到具体的开发中，阐述了开发的系统的总体设计、详细设计及安装测试。

《网络异常流量识别与监控技术研究》是作者多年从事科研项目研究的成果结晶，书中内容都来自具体的项目，有很好的工程基础，特色是学术与具体的工程应用相结合。《网络异常流量识别与监控技术研究》可作为计算机网络与信息安全相关专业研究生及高年级本科生的教材，也可作为科研人员的参考书，同时可作为研究生、博士生及老师论文写作的参考书。

《网络异常流量识别与监控技术研究》

作者简介

孙知信：博士、教授、博士生导师。1998年毕业于南京航空航天大学获博士学位。2001年至2002年在汉城国立大学做博士后研究，2002年11月博士后出站至今在南京邮电大学任教。主要从事计算机网络及安全、多媒体通信、计算机软件与理论等方面的教学和科研工作。

作为项目负责人已完成和正在从事纵横科研项目近20项，其中包括国家863项目、国家自然科学基金项目、科技部中小企业创新基金项目、江苏省科技攻关项目、江苏省自然科学基金项目、教育部和南京市回国人员资助项目等。在国内外学术期刊上发表论文30余篇，申请专利10余个。

书籍目录

第1章 DDoS攻击原理及特征	1.1 DDoS的原理及其发展	1.1.1 DoS / DDoS的概念	1.1.2 DDoS攻击原理	1.2 DDoS攻击的基本特征	1.3 DDoS分析方法研究	1.4 本章小结													
第2章 DDoS检测与防御相关研究综述	2.1 DDoS检测方法研究	2.1.1 基于流量自相似特性的流量检测	2.1.2 基于TCP攻击包中的SYN包和FIN包比例关系的检测	2.1.3 SYN Cache和SYN Cookie	2.1.4 Traceback	2.2 DDoS防范机制研究	2.2.1 基于认证机制的异常流量过滤	2.2.2 Ingress过滤	2.2.3 Pushback	2.2.4 自动化模型(控制器—代理模型)	2.3 路由器端防范DDoS攻击策略	2.3.1 基于拥塞控制的方法	2.3.2 基于异常的防范DDoS攻击策略	2.3.3 基于源的防范DDoS攻击策略	2.3.4 攻击响应	2.4 DDoS攻击的新发展及作者的研究成果	2.4.1 DDoS攻击的新发展	2.4.2 作者在DDoS攻击方面的研究成果	2.5 本章小结
第3章 基于路由器DDoS检测的改进CUSUM算法	3.1 DDoS流量统计特征分析	3.1.1 分析步骤	3.1.2 结果分析	3.2 CUSUM算法描述	3.3 基于路由器的改进CUSUM算法(M-CUSUM)	3.4 M-CUSUM算法检测路由器端网络异常流量	3.4.1 端口统计量分析	3.4.2 算法分析	3.5 本章小结										
第4章 异常流量特征聚类算法	4.1 算法描述	4.2 AFCAA算法提取网络异常流量特征	4.3 算法测试系统MCTCS	4.3.1 测试环境	4.3.2 测试内容	4.3.3 测试步骤	4.4 本章小结												
第5章 APA-ANTI-DDoS模型	5.1 模型定义	5.2 异常流量聚集	5.3 流量抽样	5.4 协议分析	5.4.1 协议分析反馈信息——Back调整	5.4.2 协议分析结构	5.4.3 过滤规则的产生	5.5 流量处理	5.6 配置	5.7 APA-ANTI—DDoS算法分析	5.7.1 Hash映射表分析	5.7.2 HashTable映射碰撞分析	5.7.3 Hash映射表下限动态逼近算法	5.7.4 Hash映射表间断性溢出问题	5.7.5 DDoS攻击行为分析	5.7.6 误判纠正行为分析	5.8 本章小结		
第6章 基于源目的IP地址数据库的防范DDoS攻击策略	6.1 基于源目的IP地址数据库的防范DDoS攻击策略介绍	6.2 SDIM系统体系结构	6.3 SDIM系统设计	6.3.1 SDIM采用的平台	6.3.2 SDIAD系统流程	6.4 源目的IP地址数据库	6.4.1 SDIAD的存储	6.4.2 SDIAD的更新	6.4.3 常用的合法源目的IP地址对集合的建立	6.5 攻击检测策略和攻击流量的过滤	6.5.1 滑动窗口无参数CUSUM算法	6.5.2 攻击响应的位置和策略	6.5.3 SDIM系统攻击响应策略	6.6 SDIM系统仿真	6.6.1 SDIM系统实验模型	6.6.2 SDIM系统实验结果	6.6.3 实验数据分析	6.7 本章小结	
第7章 防抖动的地址聚集及M-MULTOPS模式聚集设计	7.1 Bloom Filter算法	7.2 改进的Bloom Filter算法——Adapted-Bloom-Filter算法	7.3 防聚集抖动的CUSUM算法	7.4 MULTOPS结构与M-MULTOPS结构	7.4.1 MULTOPS结构	7.4.2 M-MULTOPS结构	7.5 模式聚集的研究	7.5.1 TCP、UDP和ICMP三种包的分类方式	7.5.2 TCP、UDP和ICMP三种聚集模式	7.6 基于M-MULTOPS结构的模式聚集数据管理	7.7 基于M-MULTOPS的检验系统的实现	7.8 系统仿真与测试	7.8.1 系统硬件配置及组网环境	7.8.2 系统参数配置	7.8.3 实验数据分析	7.9 本章小结			
第8章 AMAT系统总体设计	8.1 AMAT系统介绍	8.2 AMAT总体设计和子模块划分	8.3 异常流量识别模块	8.3.1 数据包采样子模块	8.3.2 地址聚集算法	8.3.3 地址聚集算法改进	8.3.4 基于Adapted-Bloom-Filter流量聚集子模块	8.3.5 防聚集抖动的累积算法	8.3.6 基于M-CUMSUM流量累积子模块	8.3.7 基于AFCAA的异常流量聚类子模块	8.4 异常流量分类子模块	8.4.1 异常流量分类子模块原型	8.4.2 异常流量分类子模块的设计	8.4.3 基于Adapted-MULTOPS的数据管理	8.5 异常流量匹配与拒绝子模块	8.5.1 异常流量反应流程框图及实现机理	8.5.2 多层模式聚集	8.5.3 “公平退火”算法	8.6 本章小结
第9章 AMAT系统详细设计	9.1 软件框架及配置简介	9.1.1 Netfilter在IPv4中的结构	9.1.2 软件结构	9.2 细化局部设计	9.2.1 内核空间系统	9.2.2 用户空间数据管理系统	9.3 模块详细设计	9.3.1 数据包采样设计说明	9.3.2 流量强度聚集设计说明	9.3.3 异常模式聚集设计说明	9.3.4 DoS / DDoS防御规则生成设计说明	9.3.5 目的地址识别设计说明	9.3.6 规则执行及反馈设计说明	9.3.7 系统信息输出设计说明	9.4 本章小结				
第10章 系统安装及测试	10.1 AMAT的软 / 硬件要求	10.2 Linux软件路由器的配置	10.3 AMAT的安装步骤	10.4 AMAT的配置方法	10.5 AMAT攻击端软件的安装和实现原理	10.6 AMAT攻击端工具使用方法和日志查看	10.6.1 攻击端工具使用方法	10.6.2 内核日志文件	10.6.3 用户层日志	10.7 AMAT具体测试	10.7.1 测试目标	10.7.2 测试用例及预期效果	10.7.3 TCP攻击部分	10.7.4					

《网络异常流量识别与监控技术研究》

UDP攻击部分 10.7.5 ICMP攻击部分 10.7.6 MIX攻击部分 10.8 本章小结参考文献

传统的网络安全技术侧重于企业用户网络的系统入侵检测、防病毒软件或防火墙，这类安全措施通常并不能减少运营商网络中的非正常流量。为了降低网络中的异常流量，减少或消除用户所遭受的分布式拒绝服务攻击（Distribution Denial of Service Attacks, DDoS），运营商的网络与路由交换设备需要具备异常流量监控与拒绝服务能力。路由器中的异常流量监控与拒绝服务方法研究对于运营商向用户提供安全服务具有重要意义。运营商网络中的路由器应该能够对攻击用户的异常流量进行监控并做出反应，根据报文源地址、源端口信息和报文长度等信息的统计特征采用一定的干预规则，比如禁止某些端口的流量或者禁止来自某一端口地址的带宽，对这些非法流量进行抑制或者拒绝服务。路由器面临的威胁有：

- （1）将路由器作为攻击平台，入侵者利用不安全的路由器作为生成对其他站点的扫描或侦察的平台，并作为发动DoS攻击的一块跳板。
- （2）尽管路由器在设计上可以传送大量的传输流，但是它常常不能处理传送给它的同样数量的传输流，入侵者利用这种特性攻击连接到网络上的路由器，而不是直接攻击网络上的系统。相比较而言，前者的难度要大一些。因而DoS（拒绝服务）成为了对路由器发起攻击的主要手段，在大范围内带来服务器的可用性问题的，从而对整个因特网造成严重影响。目前应用于路由器安全的主要技术有防火墙技术、VPN技术、入侵检测和认证技术，这几种当前的主流安全技术在路由器中都得到了应用。此外，路由器特有的网络地址转换（NAT）技术也能进一步提高因特网的安全性。但是，多种安全技术也有相互制约的方面。防火墙根据IP报头中信宿地址、信源地址以及其他一些信息决定是否让该数据包通过，而NAT改变了信源或信宿地址。现阶段，端到端的IPSEC无法在NAT转换路由器中实现。

鉴于目前的这种状况，本书系统地阐述了路由器端异常流量的检测与防范技术。本书首先介绍了DoS和DDoS的原理，综述了目前DDoS异常流量的检测技术现状和最新的研究成果。在此基础上介绍了作者创新性地设计并实现的5种DDoS检测算法以及对算法进行的局部仿真测试。在理论研究的基础上，作者结合一个具体的研究项目将上述算法应用到具体的开发中，阐述了开发的系统总体设计和详细设计及安装测试。最后，作者对全文进行了总结。全书共分10章，主要内容介绍如下。

《网络异常流量识别与监控技术研究》

编辑推荐

《网络异常流量识别与监控技术研究》主要从6个方面对异常流量的检测进行了研究，创新性地提出了5种异常流量的检测方法并在具体的系统中得到了实现和验证。《网络异常流量识别与监控技术研究》的成果具有前沿性，同时又具备较高的应用价值。

《网络异常流量识别与监控技术研究》

精彩短评

- 1、中国人自己写的书，可以看一看

《网络异常流量识别与监控技术研究》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com