<<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

出版时间：清华大学出版社

作者：孙知信

页数：213

<<网络异常流量识别与监控技术研究>>

内容概要

本书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。
　本书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。
本书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

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。

<<网络异常流量识别与监控技术研究>>

书籍目录

章节摘录

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，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。

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。

版权说明