View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Xiamen University Institutional Repository

学校编码：10384　　分类号_____密级_____
学号：X2010230648　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

网络异常流量监控系统的设计与实现

Design and Implementation of Network Abnormal Traffic Monitoring System

吴晓雷

指 导 教 师：姚 俊 峰 教 授
专 业 名 称：软 件 工 程

论文提交日期：2012 年 10 月
论文答辩日期：2012 年 11 月
学位授予日期：2012 年 月

答辩委员会主席：_____
评 阅 人：_____

2012 年 月

厦门大学博硕士论文摘要库

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　月　日

厦门大学博硕士论文摘要库

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

摘　要

在 Internet 飞速发展的今天，互联网成为人们快速获取、发布和传递信息的重要渠道，它在政治、经济、生活等各个方面发挥着重要的作用，改变了我们工作和生活的方式。但是互联网在为我们的生活带来了极大便利的同时，一些网络蠕虫、DDOS 等网络安全事件的频繁爆发也严重影响了互联网的可靠性和稳定性。为了达到对网络恶意行为的有效检测和控制，本文设计并实现了一个网络异常流量监控系统，该系统以 NetFlow 为数据源，集 TopN、应用协议统计分析、网络流量特征统计分析以及异常模式检测等方法为一体，实现了大规模网络异常流量的检测与控制。

网络流量是由网络用户行为所产生的，网络异常流量的检测与分析是网络行为分析的基本手段，因此首先需要获得适合于网络行为分析的可靠数据源。思科公司提出的基于统计信息的 NetFlow 协议，是目前通用的数据源，在此基础上可以描述多种网络数据特征。本文根据 NetFlow 协议的特征，采用层次化与模块化相结合的方法设计并实现了一个高速率环境下的网络异常流量监控系统。系统的 NetFlow 数据来自网络出口节点的路由器，系统监控端负责实现 NetFlow 数据的实时获取和统计分析。由于监控端不需要实现 NetFlow 数据的统计功能，在不影响网络服务性能的情况下大大降低了系统监控端的负荷，可以实现高速率环境下的网络异常流量监控。在系统开发过程中，综合运用 Java、JDBC、Jpcap、JFreeChart 等技术完成了各模块的设计与实现。

本文所设计的系统提供了包括历史流量显示、网络访问行为分布、流量特征分布、网络行为异常模式检测以及特定主机行为过滤与分析等功能，并且系统界面友好、通用性较强。在性能方面，由于系统底层所采用的算法简洁高效，降低了监控端的计算复杂度，使之能够适应高速率网络环境下的流量特征实时的监控与分析，测试结果也显示出系统在异常流量检测方面具有较高的准确性，达到了期望的检测率。

关键词：NetFlow；异常流量；监控系统；网络安全

厦门大学博硕士论文摘要库

ABSTRACT

Nowadays, Internet develops fast and it becomes one of the most important ways for people to obtain, release and spread the information as quickly as they can. It also plays an important role in every part of Politics, Economy and life. And it changes the way of life and work. The Internet brings great convenience to our life; meanwhile, some internet worms and DDOS security issues severely affect its stability and its reliability. In order to achieve the effective detection and control of network malicious behavior, the paper designs and implements a network the abnormal flow monitoring system.This system will take NetFlow as data source together with TopN, statistic analysis of application protocol, statistic analysis of network traffic characteristic and abnormal pattern detection. In this way, it fullfills the testing and control of large-scale network abnormal flow.

Network traffic is produced by the activity of Net users. So it is the basic method to analyze the Internet activity through testing and analyzing data sources. First, the reliable data source is needed to analyzing the Net activities. The NetFlow Protocol based on statistic information, which is brought up by SISCO Company, is nowadays' universal data source. And much net data characteristic can be described. According to the characteristic of NetFlow Protocol, this paper will design and fullfill the supervising system of abnormal flow under high-speed rate environment by using the method of uniting layering and modularization . The NetFlow data of the system is from router at Net entrance interface. The controlling interface of the system is responsible for instantaneous obtain and statistic analyzing of NetFlow data in the system. The control interface doesn't have to fullfill the statistic analyzing of NetFlow data, so it fullfills the control of abnormal flow under high speed environment by ways of reducing the load at supervising and controlling end of the system on condition that it won't affect the service performance of Internet. In the exploration of the system, the design and fulfillment of every block are done by using Java, JDBC, Jpcap, JFreeChart Techniques.

The system designed in this paper includes functions of historical flow display, net visiting activity contribution, net characteristic contribution, abnormal model testing of net activity

厦门大学博硕士论文摘要库

and activity filtering and analyzing of specific host computer. It has friendly interface and strong universal function. On performance, it reduces the calculation difficulty of controlling end due to the simple efficient calculation. It also fullfills the instantaneous supervising and analyzing of the flow characteristic under the high speed net environment. The result displays its highly accuracy on abnormal flow testing of the system. It achieves the testing efficiency of expectation.

KEY WORDS: NetFlow; Abnormal Flow; Monitoring System; Internet Security

厦门大学博硕士论文摘要库

目　录

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

CONTENTS

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

第 1 章 绪 论

1.1 研究背景及意义

1.1.1 计算机网络发展概况

计算机网络，是指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统，网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。对于用户来说，计算机网络是一个透明的数据传输机构，用户可以不必考虑网络的存在而访问网络中的任何资源。它把计算机技术与通信技术结合在了一起，能够为我们提供远程通信、远程信息处理和资源共享等很多功能。

计算机网络产生于 20 世纪 60 年代，经过了半个多世纪的迅猛发展，目前越来越多地被应用到经济、军事、生产、教育、科学技术及日常生活等各个领域。在现实的日常生活中，我们时刻都在与网络打交道。计算机网络的发展，缩短了人际交往的距离，给人们的日常生活带来了极大的便利。计算机网络的出现，使世界变得越来越小，生活节奏越来越快。

据不完全统计，Internet 现在遍及国家有 200 多个，容纳网络近 80 万个，提供了包括大型联网图书馆 1000 多个，800 多个联网的学术文献库，网上杂志 20000 多种，网上新闻报纸 9000 多种，5000 多万个 Web 网站在内的多种服务，总共近 1000 万个信息源。能够给遍及世界各地的用户提供大量的信息资源和交流共享的空间。

对于我国来说，截至 2012 年 6 月底，我国网民数量达到 5.38 亿，互联网普及率为 39.9%。IPv4 地址数量达到 3.30 亿，拥有 IPv6 地址 12499 块/32。域名总数为 873 万个，网站总数升至 250 万个。国际出口带宽达到 1,548,811Mbps，半年增长率为 11.5%。2012 年 3 月，国家发改委等七部门研究制定了《关于下一代互联网“十二五”发展建设的意见》，提出“十二五”期间，我国互联网普及率要达到 45%以上。在互联网应用方面，即时通信用户维持较高的增速，继续保持中国网民第一大应用的领先地位。此外，网络视频以及网络购物、网上支付等电子商务类应用的用户规模增幅明显，互联网的影响已经逐渐渗透到我国国民经济的各个领域和人民生活的各个方面。图 1-1 是截至 2012 年 6

厦门大学博硕士论文摘要库

月底的中国网民规模与普及率[1]。

图 1-1：中国网民规模与普及率

1.1.2 网络安全问题现状

互联网是一种开放和标准的面向所有用户的技术，其资源通过网络实现共享，但其随之而来的信息安全问题也日益突出，各种计算机病毒和网上黑客（Hackers）对 Internet 的攻击越来越激烈。尤其是国民经济信息化程度的不断提高，有很多敏感信息，甚至是国家机密都高度集中地存放在部分计算机中，所以难免会吸引来自世界各地的各种人为攻击。“信息泄漏”、“信息窃取”、“计算机病毒”、“数据篡改”等越来越威胁到网络的安全。黑客攻击的频度不断加大、网络病毒的传播速度和危害加重、攻击目标的受害程度和攻击的穿透深度都在加大。从拒绝服务攻击 DOS（Denial Of Service）到分布式拒绝服务攻击 DDOS (Distributed Denial Of Service)；从木马病毒到蠕虫病毒（Worm）；从僵尸网络（Botnet）到大量 P2P 的网络应用，互联网络不断面临着层出不穷的新问题。

根据国家计算机网络应急处理协调中心(CNCERT/CC)的统计[2]，2011 年共接收国内外报告网络安全事件 15366 起，较 2010 年增加了 47. 3% 。接收到的网络安全事件类型主要包括信息系统漏洞、网页仿冒、恶意程序、网页篡改、网页挂马等。在排名前三

厦门大学博硕士论文摘要库

位的安全事件类型中，恶意程序事件数量虽然排名下降了一位，排在了第三位，但事件数高于 2010 年，仍然是对互联网用户构成严重威胁的安全事件之一；网页仿冒事件数量随着互联网支付和应用的普及而出现显著增长，从 2010 年的第四位跃居到 2011 年的第二位；信息安全漏洞仍是接收的重点事件，排名第一位。据国家信息安全漏洞共享平台（CNVD）统计，自 2009 年成立以来，共收集整理漏洞信息 35032 个。其中，2011 年新增漏洞 5547 个，较 2010 年大幅增加 60. 9%。其中，高危漏洞 2164 个，较 2010 年增加约 2.3 倍。增长速度非常迅速。按漏洞影响对象类型统计，排名前三位的是应用程序漏洞，涉及网站相关的漏洞和操作系统漏洞。图 1-2 是从 2008 年一直到 2011 年以来，CNVD 统计的信息安全漏洞数量。.

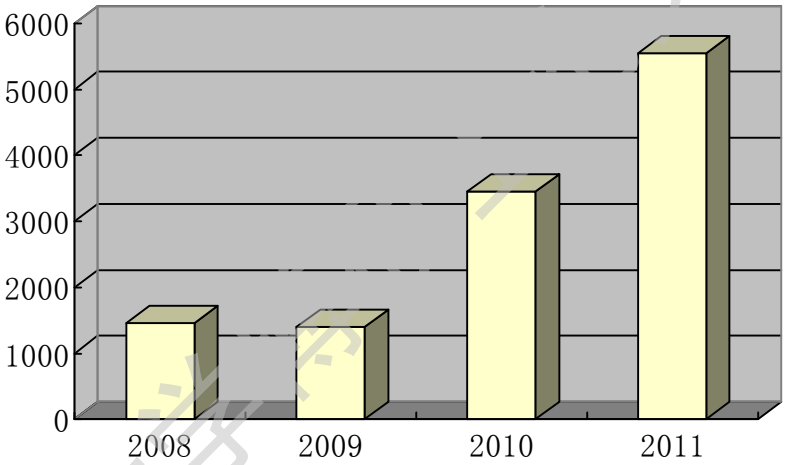

图 1-2： 信息安全漏洞数量统计

另据赛门铁克公司发布的 2011 年安全状况调查报告显示[3]，29%的公司定期遭受网络攻击，71%的企业在过去的 12 个月里遭受过网络攻击。92%的企业因为网络攻击而遭受过损失。此外，有 21%的受访者表示，网络攻击的频率仍在增加，49%的受访者表示，黑客仍然是企业最为关注的问题。该调查显示最主要的攻击方式是恶意代码、社会工程学以及外部恶意攻击。

虽然近年来信息网络使用单位对网络安全防护工作的重视程度有所提高，在网络安全方面也做出了越来越多的努力，安全防护技术水平不断提高，网络安全状况较以往有

所改善。但攻击者也会采取更加阴险、复杂和隐蔽的方法来窃取数据并制造破坏，而大部分的单位对信息安全事件处置方法和手段比较单一，防范措施不够完善，信息安全管理水平整体上仍然落后于信息化发展的要求。

1.2 网络异常流量检测概述

网络流量反映了网络的运行状态，为网络的运行和维护提供了重要的信息，是判别网络是否正常运行、网络服务是否变差的关键数据，这些数据对网络的资源分布、容量规划、服务质量分析、错误检测与隔离、安全管理都十分重要。因此对于网络流量特性的研究是网络安全领域一个非常重要的研究课题。同时网络流量作为网络行为信息的基本载体，对其特征的有效描述可以实现网络异常行为的检测，流量特征分析是网络异常行为检测的主要手段。

1.2.1 异常流量对网络的影响

近年来异常流量对互联网的影响越来越大，主要体现在两个方面：占用大量的带宽使互联网堵塞，从而导致网络丢包、时延增大等后果，严重时可造成网络的瘫痪；占用网络设备的 CPU、内存等系统资源，导致网络服务不正常。目前，能够对互联网造成重大影响的异常流量主要包括以下几种：

1. 拒绝服务攻击（DoS）：拒绝服务攻击的目的为了干扰目标机器的正常连接和正常服务，所攻击的机器通常是互联网服务器或连接到互联网上的主机。攻击能够导致服务器或其他主机的性能下降，也能够占用大量的带宽，影响用户之间的正常通信，使网络服务不能正常使用。例如拒绝服务攻击可以利用 TCP 协议的缺陷，通过 SYN 打开半开的 TCP 连接，占用大量系统资源，使正常的用户不能建立 TCP 连接。

2. 分布式拒绝服务攻击（DDoS）：分布式拒绝服务攻击是拒绝服务攻击的进一步发展，这种攻击的危害也更巨大。分布式拒绝服务攻击能够发起自动化的攻击行为，可以同时联系网络上的多台计算机发起攻击，这时就会有一股拒绝服务的洪流不断的冲击网络，导致被攻击的目标系统崩溃。

3. 网络蠕虫病毒流量：网络蠕虫病毒可以不依附于其他程序而独立存在于系统中，并能够主动在网络中传播。近几年相继爆发的红色代码、振荡波、求职信、尼姆亚等蠕虫病毒，对用户主机和网络的正常运行都造成了极大危害，其破坏力和传染性不容忽视。

厦门大学博硕士论文摘要库

Degree papers are in the “Xiamen University Electronic Theses and Dissertations Database”. Full texts are available in the following ways:
1. If your library is a CALIS member libraries, please log on http://etd.calis.edu.cn/ and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to etd@xmu.edu.cn for delivery details.

厦门大学博硕士论文摘要库