

文章编号:1005-0523(2005)02-0050-05

基于模拟真实环境的防火墙性能测试系统的实现

汤文亮,袁可风,丁振凡

(华东交通大学 信息工程学院,江西 南昌 330013)

摘要:防火墙产品的性能测试对于用户选购和正确配置防火墙有重要的指导意义.本文介绍的防火墙性能测试系统是一种基于模拟真实环境测试防火墙产品性能的测试工具,文章对该测试系统的具体实现作了较详细的论述.

关键词:网络安全;防火墙;性能测试;真实环境测试

中图分类号:TP309.2

文献标识码:A

1 引言

防火墙是目前网络安全领域广泛使用的设备.其主要目的就是保证对合法流量的保护和对非法流量的抵御.在网络带宽不断提速升级的趋势下,处于网络末端的防火墙的性能对最终用户所能得到的实际带宽具有决定性的影响.因此,防火墙的性能测试要求在模拟真实环境下进行,以便在测试时考察其在真实环境中的表现,这样测试出来的数据才有实际意义.

所谓真实环境测试(Real World Testing)是国外领先测试仪器和网络设备厂商及运营商提出来的一个概念.目前该测试理念在北美已经得到广泛推广,成为测试领域的又一大热点.相对于“基准测试”来说,真实环境测试有几个特点:首先测试中考虑到了更多的实际情况;其次测试的层次有所提高.从二层三层的测试延伸到了四层到七层服务质量的衡量.真实环境测试通常都会把测试的层次推到高层服务,因为在这里最能体现真实环境测试的优势.当我们测试网络服务的时候,流量环境就必须是真实的.比如,当一个重要的电子商务网站就要开始启动服务之前,如果经过严格的真实环境测

试,那么使用者就可以放心的开始服务了,否则就要在网络上面去做真实测试,但这样做将冒很大的风险.

真实环境测试实际上是一种绝对测试,即对测试个体在网络的真实运行状态的一个绝对的评价;“基准测试”则是一种稳定的相对测试,侧重点在于不同产品之间的比对.二者各有其优势^[1].模拟真实环境测试就是在测试实验室构建计算机网络支撑平台,并运行相关软件(或系统)来模拟真实网络以便尽可能地让测试的流量和测试的环境接近于真实情况.

为了公平地评价防火墙的性能,必须按照相关规范并使用统一的测试系统进行检测.本文就我们开发的一个基于模拟真实环境的防火墙性能测试系统的功能结构及实现技术进行介绍.

2 系统目标与结构设计

2.1 系统目标

对于网络设备来说,性能都是率先要考虑的问题.与其他网络设备相比,防火墙的性能一直被认为是影响网络性能的瓶颈.如何在启动各项功能的同时确保防火墙的高性能对防火墙来说是巨大的

收稿日期:2004-05-10

作者简介:汤文亮(1969-),男,讲师,主要研究方向为计算机网络通信、信息系统与信息安全.

中国知网 <https://www.cnki.net>

挑战^[2].性能测试主要依照 RFC2544、RFC 2647 以及中华人民共和国国家标准 GB/T 18019—1999《信息技术包过滤防火墙安全技术要求》、GB/T18020—1999《信息技术应用级防火墙安全技术要求》和 GB/T17900—1999《网络代理服务器的安全技术要求》.因此,防火墙性能测试系统的设计也必须参照以上标准,而不能与之相背.

根据以上所述标准的技术要求及测试要求,防火墙性能测试系统的设计目标是对防火墙产品(包过滤防火墙及应用代理防火墙)的性能起检测评价作用,统计性能测试指标,生成待测防火墙产品性能测试报告.在模拟真实环境的网络平台上可以配置系统基础数据和系统管理设置,可以自由调整网上流量模式.例如,可配置总提交服务申请次数,其中 FTP、WWW 服务的申请次数,总传输量;以及可

调整内部网、外部网、DMZ 三者之间的流量.配置该系统的模拟真实环境测试平台可对包过滤和应用代理型防火墙进行性能测试,测试项目(含基准测试)主要包括:双向性能、单向性能、启用 NAT 功能后的性能、每秒的处理连接速率和最大并发连接数.其中,双向性能测试项目为吞吐量、10%线速下的延迟、吞吐量下的延迟以及帧丢失率;单向性能测试项目包括吞吐量、10%线速下的延迟;启用 NAT 功能后的性能测试包括吞吐量、10%线速下的延迟.

2.2 概要设计

防火墙性能测试系统采用客户/服务器的应用模式.我们将系统的组织结构从功能角度分为三个组成部分,管理器、客户应用程序以及通信线程应用程序.各组成部分的功能和安装位置如表 1 所示:

表 1 系统结构及功能

组件	功能	安装位置
管理器(fwtest)	生成任务表、发送任务表、接收测试数据、分析测试数据和显示打印报告	模拟测试环境中内网(private)的一台服务器上.(参考图 2.1 设备环境,下同)
客户应用程序(fwmain)	接收任务表、填写协议参数、记录测试数据、发送测试数据和显示测试进度	模拟测试环境中内网(private)、非军事区(DMZ)、外网(public)的客户机上.
通信线程程序(fwtester)	创建测试线程、连接登录服务器、发送测试数据、数据格式转换和接收测试数据	与客户应用程序安装位置相同,并被其调用.

配置测试系统的支持环境是测试实施的一个重要阶段,测试环境的适合与否会严重影响测试结果的真实性和正确性.测试环境包括硬件环境和软件环境,硬件环境指测试必需的服务器、客户端、网

络连接设备以及网络扫描仪等辅助硬件设备所构成的环境;软件环境指被测软件运行时的操作系统、数据库及其他应用软件构成的环境.

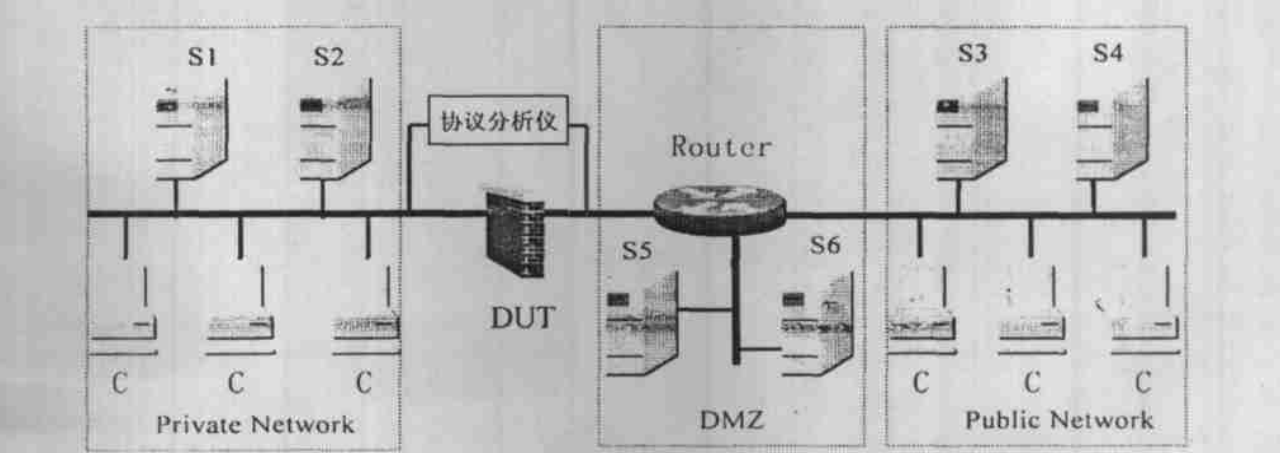


图 1 网络硬件平台

软件支持环境:支持系统运行的操作系统是 Windows NT 4.0 或 Windows98 或 Windows 2000.网络硬件平台如图 1 所示.图中,三个模拟网(以太网)分别代表内部网(private)、隔离区(DMZ)和外部网(pub-

lic).DUT 是待测防火墙,它是外部网、隔离区进入内部网的唯一通道.Router 是路由器.S1 和 S2、S3 和 S4、S5 和 S6 是六台服务器,分别由三台 SUN Ultra 机模拟,每一个物理客户机(C)是一台 Pentium 微机,

可以模拟 1 至 8(或更多)个虚拟客户机.S1、S3 和 S5 专门处理 FTP 服务请求,S2、S4 和 S6 则处理包括 FTP 和 WWW 的混合服务. 跨接在 DUT 两端的协议分析仪可用 HP 网间分析仪(Internet Adviser),使用它进行监测、统计及智能分析,有助于迅速诊断问题所在和观察网络的性能.

3 系统主要功能模块的实现

本系统采用微软公司的 Visual C++ 6.0 开发. 功能实现的总体思路是:在测试之前首先生成测试任务表,并以文件格式存储. 然后设置测试客户机的 IP 地址及客户机所在网段. 在开始测试时,先设置测试对象和存储测试数据的文件名. 管理器通过已设置的客户机 IP 地址与测试客户机建立 TCP 连接,管理器通过与客户机建立的 TCP 连接向客户机发送测试任务表、接收客户机传回的测试数据和向客户机发送测试命令,管理器把客户机传回的测试

数据存储至文件,测试完毕拆除 TCP 连接. 然后设置待分析测试对象测试数据的文件名和存储测试结果报告数据的文件名;读取测试对象数据进行分析;产生测试结果报告数据并对不同测试对象进行性能比较,最后打印测试数据及报表.

下面分别介绍防火墙性能测试系统的管理器、客户应用程序和通信线程应用程序的实现思路.

3.1 管理器程序的实现

服务器端的管理器程序中数据流的基本活动过程如图 2 所示. 开始测试前,首先要在管理器上设置好各种初始化参数,其中包括设置“测试客户机的 IP 地址及客户机所在网段”以及设置“测试对象和存储测试数据的文件名”. 设置完成后,开始测试. 然后由客户机将本机的测试数据收集到测试数据文件中,再传给管理器,管理器将对这些数据进行分析并形成测试结果报告,然后存储到测试结果报告数据文件中,供显示器显示或打印出测试结果的报告. 基本过程如下:

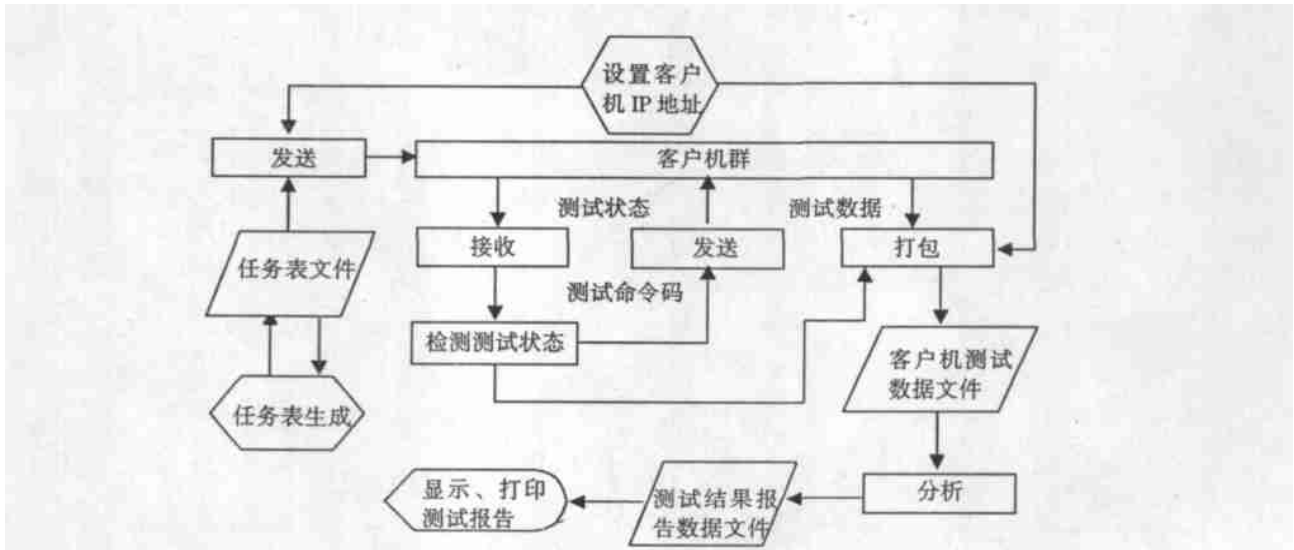


图 2 管理器程序中数据流的基本活动过程

- 1) 启动本测试系统后,在尚未开始对待测应用代理防火墙进行测试之前,必须对管理器进行参数设置.使用 OnTestParaSet()生成测试任务表,并以文件格式存储.
- 2) 使用 OnTestSetClientIp()设置测试客户机的 IP 地址.
- 3) 开始测试时,使用 OnTestStart()设置测试对象和存储测试数据的文件名,然后开始测试.
- 4) 开始测试后,管理器利用预先已设置好的客户机 IP 地址与测试客户机建立 TCP 连接,管理器通过与客户机建立的 TCP 连接向客户机发送测试任

- 务表、向客户机发送测试开始命令;管理器再接收客户机传回的测试数据,把客户机传回的测试数据存储至文件中;系统会根据设置的客户机最大模拟虚拟机数目和设置的重复测试次数对测试对象进行多次测试,当测试次数达到要求时,系统自动发送中止测试命令来结束测试,并拆除 TCP 连接.
- 5) 分析测试对象的测试数据.在源文件列表中选择待分析的测试数据的文件名一,并给出一个用来存储分析结果的文件名二.这样在读取测试对象数据进行分析后,测试结果存入文件名二中.
- 6) 最后,系统调用 OnDraw()来显示、OnPrint()

来打印测试结果.

在这里仅给出步骤一中的测试任务表生成程序:

```
void CFwtestDoc::OnTestParaSet()  
{  
    CString szFile ; //存储任务表文件名  
    BOOL bFlag ; //从文件中读取测试参数是否成功标志  
    CPropertySheet sheet(IDS __SET __PARA __CAPTION);  
    if ( useProxy == 1 )  
        szFile = "Proxy.data"; //应用代理的存储任务表文件  
    else szFile = "PktFlt.data"; //包过滤防火墙的存储任务表文件  
    bFlag = ReadTestParaFromFile( szFile ); //从文件中读取任务表中的测试参数  
  
    if( sheet.DoModal() == IDOK )  
    {  
        WriteTestParaToFile( szFile );  
        //写测试参数及服务器的设置到任务表存储文件中  
    }  
    return ;  
}
```

3.2 客户端程序的实现

客户端应用程序的主要作用是保持与管理器之间的通信,接收从管理器传送来的测试任务表;记录和计算测试数据;发送测试数据至管理器.为便于理解,仍可参考图 2 的管理器程序程序中数据流的基本活动过程.

客户端应用程序的实现主要步骤:

- 1) 填写协议参数,这些参数主要有:FTP 协议参数、HTTP 协议参数及临时参数;
- 2) 创建文件映射,映射至内存以填充参数;
- 3) 发送 Buffer 中存储的 size 个字节的数据;
- 4) 测试全部客户终端.

值得一提的是,在创建测试客户机方法 CreateTestClients()中调用了创建进程 CreateProcess()函数,而该方法以可执行文件的方式调用通信线程应用程序 fwtester.exe,其实现方法如下:

```
char szProgram[] = "fwtester.exe";  
CreateProcess( szProgram,
```

```
szCommand, // Window 消息句柄作为命令行.  
NULL, NULL, FALSE, 0, NULL, NULL,  
&startUpInfo, &procInfo )
```

3.3 通信线程程序的实现

通信线程程序被编译成可执行文件为客户端应用程序所调用.它的主要作用是在客户端与真实服务器(Web 服务器或 FTP 服务器)之间进行通信.例如它建立与 FTP 服务器(或代理服务器)的连接并登录到服务器上,通过控制通道发送和接收命令,在数据通道上传送或接收数据等等.通信线程程序所用到的函数包括针对 FTP 协议的和 HTTP 协议而言的.而对于 HTTP 协议的方法与上面的类似,在此就不一一列出了.

- 对于 FTP 协议,其主要实现过程如下:
- 1) 创建 CFTPWnd 的消息句柄(handlers);
 - 2) 建立与 FTP 服务器(或代理服务器)的连接;
 - 3) 登录服务器.测试分组过滤防火墙时,使用匿名登录,但对于测试的防火墙是应用级防火墙时则是使用有效的用户 ID 和口令来进行登录的.
 - 4) 在控制通道上发送命令,创建 Socket 侦听,发送数据通道所需的命令;
 - 5) 开始另一次 FTP 测试或开始新一轮 FTP 测试;
 - 6) 结束一次 FTP 测试;
 - 7) 接收 FTP 数据,把数据写入一个文件中.

4 系统设计策略及系统特点

基于以上的防火墙性能测试系统的需求及设计目标,该系统的基本设计策略是:以真实的业务为依据,选择有代表性的、关键的业务操作设计测试案例,以评价防火墙系统的当前性能;通过自动负载测试,在一台或几台 PC 机上模拟成百或上千的虚拟用户同时执行业务,重复执行和运行测试,可以确认性能瓶颈并优化和调整应用.

除了电子邮件以外,HTTP、FTP 是 Internet/Intranet 网上服务中广泛应用的两种服务,因此选择这两种服务类型具有代表性.对于使用了应用代理防火墙的网络环境而言,使用匿名 FTP 是无法登录到远程的 FTP 服务器上的,必须先登录到应用代理防火墙,而且需要预先设置好服务器的用户帐号、口令.超文本传输协议(HTTP)是当前运行最多的协议,它本身是安全的,但它提供的相关服务影响了它的安全性.

系统提供了灵活的基础数据和系统管理设置的功能. 基础数据及代码设置是系统所用到的基础数据代码及其相应的基础信息. 通过基础数据设置, 形成公用参数库, 可以保证系统公用数据的完整性和一致性. 在系统设置方面, 实现程序关键信息参数化, 可大大减少数据的录入量, 提高系统的运行效率, 增强系统的可维护性, 同时能够根据实际情况进行相应参数设置, 更方便准确的模拟真实环境. 例如, 可根据 Internet 上多个站点公布的统计数据来选择网上较频繁访问的服务类型. 通过搭建网络硬件平台, 对网上流量进行适当分配, 尽可能模拟 Internet 网上真实环境, 从而对防火墙产品的性能进行更准确的测试.

5 结束语

防火墙测试技术是一项全新的技术, 尤其是在利用自主开发的软件系统对防火墙的性能进行测试, 目前我国尚无成熟产品出现. 我们开发的这个防火墙性能测试系统能够在模拟真实环境下对防火墙进行“每秒的处理连接速率”、“最大并发连接总数”、“有无防火墙的性能下降百分比”以及“启用和禁用 NAT 功能后的性能下降百分比”等几种重要

的性能参数的测试. 防火墙性能测试系统的各项功能有待完善, 系统本身的性能有待进一步提高, 例如目前尚未集成防火墙抗攻击能力测试性能测试, 仅预留了扩展接口. 但相比诸多公司和评测机构仅能作基准测试而言, 该系统具有真实环境测试所具有的各种优势, 提供了防火墙在网络的真实运行状态的一个绝对评价, 其测试出的性能参数更能反映出防火墙在真实网络应用中的实际性能.

该系统现正用于某安全产品测评认证中心的测试工作中, 取得了良好的效果. 实践证明, 使用这个系统对被测产品进行测试是可行且有效的, 随着系统的进一步改进和完善, 必将对今后的测试工作具有更高的实用价值以及对测试研究具有更大的参考价值.

参考文献:

- [1] 张林辉. 防火墙性能测试浅析[EB/OL]. <http://www.re-alneter.com>, 2004-2-3.
- [2] 潘永花, 张峰, 宋丽娜. 12 款防火墙比较评测报告[EB/OL]. http://www.ccw.com.cn/applic/prod/htm2003/20030115_1460e_2.asp, 2004-1-24.
- [3] 汤文亮, 李正凡. 应用级防火墙测试规范研究[J]. 华东交通大学学报, 2001.

Design and Implementation of a Kind of Firewall Performance Testing System Based on Simulated Real World Testing

TANG Wen-liang, YUAN Ke-feng, DING Zhen-fan

(School of Information Eng., East China Jiaotong University, Nanchang 330013, China)

Abstract: The Performance testing of Firewall offers consumers a good guidance to choose and buy this kind of products or to configure their firewalls correctly. In this paper, a Firewall Performance Testing System based on simulated real world testing is introduced as a tool of testing firewall's performance, and the implementation of this system is discussed in detail.

Key words: network security; firewall; performance testing; real world testing