使用 TTPlatForm 的防火墙自动测试系统

Automated Testing of Firewall Using TTPlatForm

蒋 凡 张 辉 （中国科学技术大学 计算机科学与技术系 安徽合肥 230027）

摘要：防火墙自动测试对提高防火墙测试的效率具有很大的意义。在一致性测试框架上，使用 TTCN－3 测试语言，我们实现 TTCN－3 测试平台 TTPlatForm，提出了一种有效解决防火墙自动测试的方法。它人工干预少，测试结构灵活，测试套开发方便。

关键词：防火墙测试 测试自动化 TTCN－3 TTPlatForm

1 引言

如何保证信息资源的安全是一个很重要的问题。现在常用的保护手段是防火墙。对某个防火墙产品，确定其是否符合相关的技术标准，功能是否完备，是一个产品级的测试问题；当一个防火墙应用到某个系统环境中之后，更需要关注是它的配置是否真正达到了防范的目的。

目前，防火墙功能测试大部分属于产品级的测试，采用的方法都是采用非标准化的方法搭建测试环境，按照测试标准，用手工的方式切换测试场景进行测试。

通过研究我们发现，大部分的防火墙功能测试可以采用自动化的方式进行。利用策略、工具以及产品等减少非技术性（unskilled）、重复性（repetitive）、冗长（redundant）的测试活动的人工介入[1]，可以节省人力和物力，提高测试效率。

2 防火墙测试概述

防火墙的测试方法主要是由防火墙测试的目的来决定的。对防火墙功能测试而言，主要采用黑盒测试的测试方法。一般防火墙功能测试的模型与流程如下：

在防火墙的两侧分别架设下测试器（LT，用作主测试器）和上测试器（UT，用作采集器）。

由于防火墙两端的节点都可以主动向另一端的节点发起通信，故需要考虑两种测试流程：

a）LT 作为主测试端，向防火墙发出测试报文，目的地址为 UT；UT 截取/采集所收到的报文（该报文为 LT 通过 FW 发送给 UT 的报文），回传给 LT，由 LT 比较判断结果是否正确；如果 UT 未收到相应的报文，则表示超时或者数据包被防火墙丢弃。这种情况用作 LT 端主动发起通信，UT 被动接收。

b）LT 依然用作主测试端。不同之处在于 LT 先和 UT 同步通信，同步通信结束后由 UT 主动发送测试报文，LT 截取/采集收到的报文，进行判断。这种情况用作 UT 主动发起通信，LT 用作被动接收。

在具体的防火墙配置中，防火墙为这两种情况都需要配置策略，在测试的时候这两种情况都需要考虑到。

3 自动化测试的考虑和 TTCN－3

自动化就是将测试工具集成到测试环境中，使得测试的执行、记录和结果比较减少人的干预。一般说来，企图实现所有测试工作的自动化通常都不是很有成效，而且兴许是不可能或不合理。

自动化测试中很重要的两个环节是测试内容的选取和测试工具的使用。

自动化测试的主要候选对象就是那些需要重复执行的测试任务，再就是那些需要很大的人力和物力投入而且自动化成本不太高的测试项目。以包过滤防火墙为例，大部分的规则都可以通过简单的脚本来实现测试，相对于手动测试，有很大的优势。

测试工具的选取则直接关系到自动化测试的效益和代价。一般说来，没有一个测试工具能够满足所有的测试要求，如果对于如何使用工具没有一个清楚的

策略的话，将会导致选择错误的工具，这对测试没有任何好处。选取测试工具的另一个原则是易用性和易维护性，选择容易使用的测试工具，可以在很大程度上节省人力投入；当测试环境变更后，只对测试脚本做较少的改动。

自动化测试的实现方法最常见的是[录制/播放](Capture/Play)，不过代价比较大，而且维护不易，一般不予推荐。现在用得比较多的是采用数据驱动(Data-Driven)的测试方法，将"输入数据/预期结果"与测试脚本分离，开发相对通用的测试脚本，面对不同的需求，变更"输入资料/预期结果"的数据。比较常用的数据驱动方法有 Function Decomposition 和 Key-Word Driven[2](或称为 Test Plan Driven)。

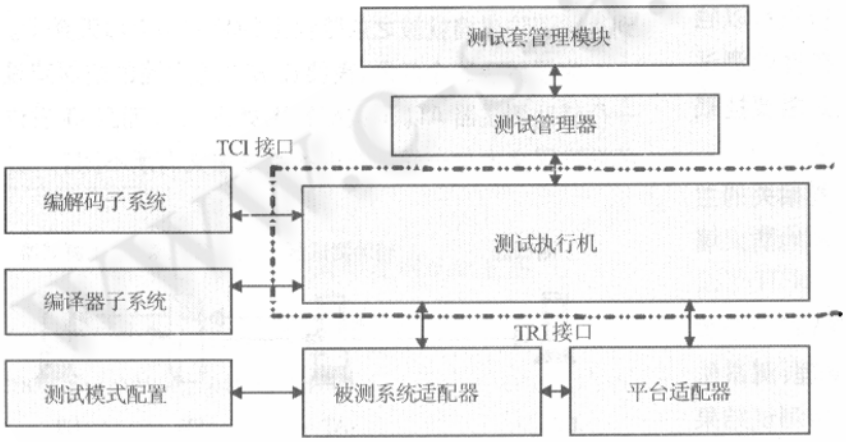

图 1　TTPlatForm 体系结构

TTCN-3[7](Testing and Test Control Notation Version 3)是新一代的测试语言规范，是一种标准化的测试描述语言。TTCN-3 语言由 ETSI(欧洲电信标准局)制定，现已被 ISO 接纳为国际标准(Z.140 系列)，该语言力求适应测试需求的不断变化，为像 ODP、CORBA、TINA、DCE 等新的软件架构，以及下一代网络协议提供新的测试概念，测试架构和功能强大的测试规范描述手段。TTCN-3 不仅适用于一致性测试，也适用于网络性能测试。和其它性能测试工具比较起来，基于 TTCN3 的性能测试系统有以下优点：

(1) TTCN3 支持外部自定义函数，使用户编写性能测试中各种压力模型变得更加简单。

(2) TTCN3 支持定时器的启动、停止、读取当前时间等操作，这使得性能测试中确定网络事件产生的时序变得更加方便。

(3) TTCN3 提供了一种可编程，动态可配置的性能测试结构，并发测试组件可以产生大流量的数据流，这为性能测试提供了充足的数据参考。

(4) TTCN3 类似高级语言，开发测试套方便、简洁，开发出的测试套可读性强，同时具有良好的可维护性。

利用 TTCN-3 的这些特点，我们设计并研制了防火墙测试系统平台 TTPlatForm。TTPlatForm 工具使用"Key-Word Driven"的方法来实现防火墙的自动测试。

4　防火墙测试系统的设计

在一致性测试框架[3,4]上，参考 TTCN-3 的核心标准[7,8,9]，设计并实现了防火墙测试系统 TTPlatForm，下面介绍 TTPlatForm 的体系结构和各模块的实现机制。

如图 1 所示，TTPlatForm 主要包括编译器子系统(TC)，执行机子系统(TE)，编解码子系统(TCD)，平台适配器(PA)，被测系统适配器(SA)，测试配置模块(CC)，测试管理器(TM)，测试套管理子系统(TSM)。

编译器子系统(TC)：编译器子系统将 TTCN-3 核心语言格式的抽象测试套转化为 CPP 语言格式，调用 C++ 编译器生成执行器(TE)可以调用执行的目标代码(DLL 格式)。

执行机子系统(TE)：通过执行编译器(TC)生成的测试例目标代码，完成对被测系统的测试，计算出测试判决，并保存测试结果和测试日志，供实时和事后分析。

编解码子系统(CD)：一致性测试系统中的 CD 模块用于将 TTCN-3 或 ASN.1 值转换成二进制码流，或者将被测系统反馈回来的码流还原成 TTCN-3 或 ASN.1 的值。在 TTPlatForm 中，CD 主要负责将测试套中定义的消息包转换成测试过程中实际需要发送的数据格式，相对于一致性测试系统，TTPlatForm 中的 CD 模块功能更为简单。

平台适配器(PA)：是与操作系统密切相关的功能

模块。在测试过程中，PA 用于协助执行机实现定时器功能以及远程配置防火墙功能。在防火墙测试中，定时器机制提供启动定时器，停止定时器，读取定时器等操作。

被测系统适配器（SA）：SA 是防火墙测试里比较重要的模块，也将是防火墙测试时使用最多的一个模块，因为防火墙测试的基本方法都是通过发送特定格式和组合的数据到实际防火墙中。数据如何收发，数据收发采用什么通信协议，都在 SA 中体现。在 TTPlatForm 中，SA 用于处理测试系统与被测系统之间的数据通信，SA 与测试系统中的执行机通过 TRI 接口连接，执行机不再参与实际的网络通信而是将报文交给 SA，SA 再将报文按被测系统可识别的格式封装后通过实际网络线路发送出去，接收时也类似，这使得执行机可以独立于特定的被测协议实现，具有通用性。在性能测试过程中无论是采用何种连接，该测试系统只需要挂载不同的 SA 模块就能进行测试。

测试模式配置（CC）：是防火墙测试配置相关的主要模块，主要用来配置测试机是用来进行本地防火墙测试还是远程防火墙测试。

测试管理器（TM）：在 TTPlatForm 中，TM 是一个管理界面，支持抽象测试套编写、测试文件管理、测试例选择功能。同时，TTPlatForm 的 TM 模块支持测试结果数据的收集和保存，测试结果的在线和离线分析。

测试套管理子系统（TSM）：管理一些常用的防火墙测试套，用户可以将开发测试过的测试套保存下来，在实际测试时可以通过 TM 动态选择执行，完成所需要的测试。在 TTPlatForm 中，实现了防火墙包过滤检测的常用抽象测试套，TSM 中的测试套用数据库进行简单的管理，可进行修改、删除、更新等操作。

TTPlatForm 进行防火墙测试的基本过程如下：

编写抽象测试套。使用 TTCN3 语言编写符合 TTCN3 语言规范的抽象测试套。使用 TTPlatForm 调试修改抽象测试套，使之满足所需要的测试要求。

加载所需的被测系统适配器 SA。方便测试过程中发送和接收实际的数据包。

调用测试配置模块 CC，选择当前运行的测试模式。

执行抽象测试套。开始实际的测试，执行抽象测试套。TTE 将在线记录测试结果数据，并交给 TTM 显示和保存，以供实时和事后分析使用。

结果统计和分析。对测试过程中收集数据进行统计分析，得到系统的配置性能。

5　防火墙测试流程研究

防火墙测试主要分两种，防火墙置于局域网内的本地防火墙测试和防火墙不在本网的远程防火墙测试，本地测试环境瞎防火墙测试相对简单，可以使 LT、FW、UT 均互相连接，丢包的可能性非常低。

远程防火墙测试与本地防火墙测试的主要区别在于 LT 与被测防火墙之间可能存在许多的其它网络节点，比如路由器，其它防火墙等。如果直接发送测试报文到远程防火墙，则可能存在的问题是这些测试报文还没有到达被测防火墙就被之前路径上的其它防火墙丢弃了。

为了解决这个问题，需要在被测防火墙的前面架设一个辅助测试器 AT（测试配置图如图二），而且 LT 发送的测试报文也与一般情况下的测试报文有所不同。

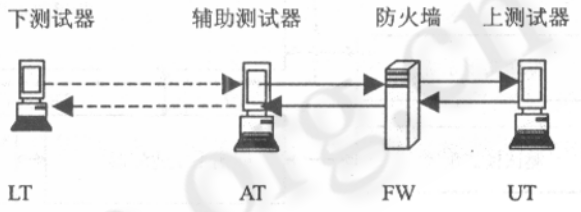

图 2　远程防火墙测试配置图

（1）在一般情况下，LT 发送的测试报文的为普通的测试报文，而在这种情况下需要将测试报文封装成目的地址为 AT 的普通数据报文。

（2）LT 在发送测试报文前需要与 AT 进行协调，保证测试的正确性。

（3）AT 收到 LT 发送过来的测试报文后，去掉封装，取出测试报文，再发送给防火墙进行测试。当然，AT 和 UT 也需要进行同步协调。

（4）AT 收到 UT 的返回报文，或者某个时间段后还没有收到 UT 的返回报文，封装返回报文并发送给 LT，或者直接发送超时报文给 LT，由 LT 做出测试判决。

AT 和 UT 的功能都比较简单，如果远程的环境允许，实现远程加载是比较容易的。LT 的报文封装功能需要测试模式配置（CC）和编解码子系统（CD）合作实现。

6 使用 TTCN－3 工具进行防火墙自动测试

为了说明 TTPlatForm 进行性防火墙测试的基本流程，同时验证使用 TTPlatForm 系统进行防火墙测试的可行性。下面以是本地测试环境为测试实例，讲解从测试配置，测试套开发，测试执行，测试结果收集和整理的完整过程。

测试配置：LT 和 UT 是两台笔记本，被测对象是一台 Linux 主机，上面加载了 IPTables 配置的防火墙。具体连接图如下图 3 所示。

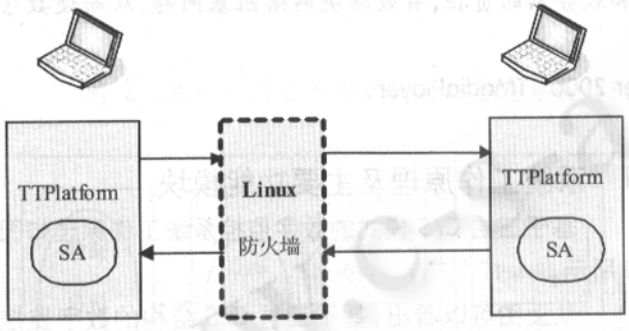

图 3 防火墙实验环境测试配置图

下面是防火墙测试套的代码片断：

```
module Firewall_Testing_Suite{
    ……
  external function CtrlPack( charstring s) return char-
string;
  //用来远程配置防火墙规则的外部函数，需要在 PA
中实现对应配置操作
  testcase firewall_testing_001( ) runs on FirewallTest-
ingMtcType system FirewallTestingSystemInterface{
  map( mtc:PCO1,system:I1) ;
  map( mtc:PCO2,system:I2) ;
  PCO2. send( "1") ;
  T1. start( MAXTIME_1) ;
  alt{ [ ]PCO2. receive( "2") {
      //判断同步是否成功
      T1. stop;
      CtrlPack( "Firewall - A OUTPUT - p ALL - s *
* * -j ACCECPT") ;
      //配置防火墙规则
      PCO1. send( packet1) ;
      T1. start 1( MAXTIME_2) ;
      alt{ [ ]PCO1. receive( packet2) {
        T1. stop;
        //发送测试报文并成功获得返回
        setverdict( pass) ; }
      [ else] { setverdict( fail) ;
        stop; } } }
  ……
  }
  control
    {
    execute( firewall_testing_001( ) ) ;
    }
}
```

7 结束语

在一致性测试框架上，使用 TTCN－3 测试语言，设计并实现了防火墙测试系统 TTPlatForm，并给出了该系统在进行防火墙自动测试时的基本过程。实际测试验证了 TTPlatForm 在进行防火墙自动测试时，具有人工干预少，测试结构灵活，开发测试套方便简洁，测试套易维护等优点。

参考文献

1 Dawn Haynes. The Rational Edge －June 2001－ Automated Testing：A Silver Bullet? Cem Kane's Web site.

2 Keith Zambelic. Totally Data－Driven Automated Testing，
http://www.sqa－test.com/w_paper1.html

3 D. Rayner，. OSI Conformance Testing，Computer Networks and ISDN，Systems Volume 14 ，? Issue 1 ? (March 1987).

4 ITU－T. Recommendation X.290. OSI Conformance Testing Methodology and Framework for Protocol Recommendations for ITU－T Applications － General Concepts，1995.

5 蒋凡、季向东、曾凡平，TTCN－3 测试系统的设计与实现，《计算机工程》.