文章编号:1005-0523(2001)04-0036-04

应用级防火墙测试规范的研究

汤文亮, 李正凡

(华东交通大学 电气信息工程学院,江西 南昌 330013)

摘要:应用级防火墙产品的产生是源于信息网络安全的需求,而测试为产品的评估和认可提供了最可信的依据,因此,有必要对这类产品的测试作较为深入的研究.本论文描述了测试应用级防火墙所依据的测试准则以及测试中常用的工具,并对应用级防火墙测试体系作了较详细的论述.

关 键 词:网络安全;防火墙;代理服务;测试

中图分类号:TP309.2 **文献标识码**:A

0 引 言

信息安全产品的可靠性直接影响着国家的安全利益和经济利益,必须由国家权威机构对其进行权威和公正的测试及评估,确认它们达到了所声称的安全性,即达到了一定的标准安全级别[1],以保证满足用户的安全需求.为了保证国家安全、维护主权的独立和完整,对希望进入我国信息安全领域的他国的安全产品或系统也必须经过我国测评认证机构进行评估和认可.

测试为评估提供最有力的、不可缺少的证据,对评估和认证的结果有决定性的作用.其目的是确定送检产品与有关标准相符合的程度,得到其它有关组织和测试实验室可广泛接受的检验报告.

防火墙测试技术在我国是一门新兴的技术,目前国内只有中国国家信息安全测评认证中心是测评认证的权威机构.作者曾在该中心工作年余,主要从事应用级防火墙的测试,在参考国外相关理论的基础上,提交了通用测试规范"根据低风险环境下应用级防火墙保护轮廓导出的测试要求"报批稿,并进一步研究了应用级防火墙的测试技术及方法.

虽然防火墙的体系结构和技术多种多样,但防火墙大致可分成三类:IP级防火墙、应用级防火墙及链路级防火墙.IP级防火墙又称为报文过滤(packet filter)防火墙.它通常实现在路由软件中,在为IP报文进行转发之前根据报文的源地址、宿地址及服务类别(端口号)来过滤报文.应用级防火墙又称为代理(proxy)防火墙.它一般针对某一特定的应用而使用特定的代理模块,并由用户端的代理客户(proxy client)和防火墙端的代理服务器(proxy server)两部分组成.当某远程用户想和一个配置了代理防火墙的内部网络建立联系时,此防火墙会阻塞这个远程联接,对流经它的业务流进行审计并执行详细的日志功能.如Telnet Proxy负责Telnet在防火墙上的转发,Http Proxy负责WWW,Ftp Proxy负责Ftp等,管理员可以根据自己的需要安装相应的代理.链路级防火墙的工作原理和组成结构与应用级防火墙相似,但它并不针对专门的应用协议,而是一种通用的TCP(UDP)连接中继服务.连接的发起方不直接与响应方建立连接,而是与链路级防火墙交互,由它再与响应方建立连接,并在此过程中完成用户鉴别.在随后的通信中维护数据的安全(如进行数据加密)及控制通信的进展.SOCKS就是一个典型的链路级防火墙.

1 应用级防火墙的安全技术要求

应用级防火墙作为一种计算机网络安全产品,其安全性必须达到一定的安全级别,以满足用户的安全需求.在设计应用级防火墙产品时,必须依据中华人民共和国国家标准信息技术《应用级防火墙的安全技术要求》中规定的安全技术要求.此标准规定应用级防火墙在低风险(敏感但无特定级别)环境下

收稿日期:2001-05-10;

作者简介:汤文亮(1969-),男,江西省南昌市人,华东交通大学讲师.

的最低安全要求,它明确指出应由防火墙防止的威胁,并定义了安全目标、使用环境以及功能要求和安全保证要求等,因此,对送检的应用级防火墙产品进行测试时必须参考这一标准[19].

下面简单介绍应用级防火墙应阻止的威胁、安全目标、安全功能要求及三者之间的关系[19].

1.1　安全威胁

符合《应用级防火墙的安全技术要求》的应用级防火墙应能阻止的威胁包括未授权逻辑访问、假冒网络地址攻击、针对内部网络的攻击、审计记录丢失或破坏、对防火墙的配置和其它与安全相关数据的更改以及绕开身份标识和鉴别机制等几种威胁[19].

另外,有些安全威胁必须通过物理控制、过程措施或者管理手段来对付[19]这些威胁是:被保护网上的恶意用户试图向外部用户提供信息、受保护网络上的恶意用户攻击同一网络上的计算机、攻击高层协议和服务以及截取传输信息[19].

1.2　安全目标

安全目标包括信息技术安全目标和非信息技术安全目标[19].符合《应用级防火墙的安全技术要求》的应用级防火墙应达到的信息技术安全目标包括:访问仲裁目标、管理员访问目标、个体身份记录目标、防火墙的自保护目标及审计目标[19].

非信息技术安全目标是指除防火墙技术要求之外还需满足的要求[19].它们不是依靠防火墙安全策略来实现,而是通过采用物理的、过程的或管理的方法来达到安全目标[19].它们是:安装与操作控制目标、物理控制目标及授权管理人员培训目标[19].

1.3　安全功能要求

本节提出了符合《应用级防火墙的安全技术要求》的应用级防火墙必须满足的功能要求[19]安全功能主要分为五大类,分别是用户数据保护、表识与鉴别、密码支持、可信安全功能保护及安全审计等,各类均有一个或数个功能组件[19].具体的安全功能要求见表 1[19].

表 1　功能要求

功能分类	功能组件	
用户数据保护	FDP ACC.2	完整的客体访问控制
	FDP ACF.4	访问授权与拒绝
	FDP AFC.2	多种安全属性访问控制
	FDP SAM.1	资源分配时对遗留信息的充分保护
	FDP SAM.1	管理员属性修改
	FDP SAQ.1	管理员属性查询
标识与鉴别	FIA ADA.1	授权管理员、可信主机和用户鉴别数据初始化
	FIA ADP.1	授权管理员、可信主机和用户鉴别数据的基本保护
	FIA AFL.1	鉴别失败的基本处理
	FIA ATA.1	授权管理员、可信主机、主机和用户属性初始化
	FIA ATD.2	授权管理员、可信主机、主机和用户唯一属性定义
	FIA UAU.1	授权管理员的基本鉴别
	FIA UAU.2	单一使用的鉴别机制
	FIA UID.2	授权管理员、可信主机、主机和用户唯一身份标识
密码支持	FCS_COP.2	符合规定的加密操作
可信安全功能保护	FPT RVM.1	防火墙安全策略的不可旁路性
	FPT SEP.1	安全功能区域分隔
	FPT TSA.2	区分安全管理角色
	FPT TSM.1	管理功能
安全审计	FAU GEN.1	审计数据生成
	FAU MGT.1	审计跟踪管理
	FAU POP.1	可理解的格式
	FAU PRO.1	限制审计跟踪访问
	FAU SAR.1	限制审计查阅
	FAU SAR.3	可选择查阅审计
	FAU STG.3	防止审计数据丢失

1.4 安全目标、安全功能与威胁三者之间的关系

在表 1 中列出了信息技术功能要求的各种功能分类和功能组件，对于每个组件分别必须达到一定的安全目标[19].而要达到某一安全目标必须防止相应的安全威胁[19].例如，"用户数据保护类"的一个安全功能组件"完整的客体访问控制"用于定义防火墙的访问控制功能，它直接支持访问仲裁安全目标[19].而要达到支持访问仲裁安全目标，防火墙必须具有访问控制功能并能够防止这样三种威胁：第一，假冒网络地址攻击；第二，针对内部网络的攻击；第三，对防火墙的配置和其它与安全相关数据的更改[19].

2 应用级防火墙的测试要求

应用级防火墙的测试要求给测评人员提供了测试的指南，并保证测评时所采用的评估标准一致[19].

测试要求中每一项要求包括输入、设计分析和测试三个操作部分[19].为了证实应用级防火墙的安全功能是否真正达到访问仲裁安全目标，送检产品供应商必须提供相关的文档资料，这就是输入部分的内容[19].设计分析部分的内容描述的是测试人员在测试之前的种种要求[19].而测试部分是对测试人员实际测试的要求[19].

表 1 中的每项功能要求，从"完整的客体访问控制"到"防止审计数据丢失"，都有相应的测试要求[19].限于论文的篇幅，下面仅以"用户数据保护"功能类中的"完整的客体访问控制"功能组件的要求为例，简略地描述测试要求[19].为了便于理解下文，我们首先了解两种策略的概念，一种是"无鉴别的端到端策略"，是指一个内部或外部网络上的主体直接通过评估目标(TOE，在此指待测防火墙) 发送数据流到一个外部或内部网络上的客体；另一种是"有鉴别的端到端策略"，它是指一个内部或外部网络上的主体在发送数据流之前，必须通过 TOE 的鉴别后，才能传到一个外部或内部网络上的客体[19].

1) 要求：防火墙的安全功能应在以下方面执行"无鉴别的端到端策略"：

[主体：未经防火墙鉴别的主机]；

[客体：内部或外部网上的主机]；

[以及安全功能策略(SFP) 所包括的主体、客体的所有操作][19].

2) 输入：供应商应该提供文档描述以下内容：

(1) 能够把未经鉴别的主机标识为一个主体的数据包参数，如：网络地址、主机名字、网络标识符、连接标识；

(2) 如何识别一个未经鉴别的主机是内部网或外部网中的客体，以及如何识别一个主机是内部网中已被鉴别的(信任) 主机；

(3) 评估目标(TOE) 能够对下列服务严格执行"无鉴别的端到端策略"：

两台未鉴别的外部主机，

一台未鉴别的外部主机向一个未经鉴别的内部主机请求服务，

一台未鉴别的外部主机向一内部可信主机请求服务；

(4) 如果一个外部未经鉴别的主机具有一个内部主机的源地址，防火墙如何判断

其唯一标识，而且该对此种情形作出何种反应；

(5) 明确在一个未经鉴别的外部主机与另一个主机(未经鉴别的外部主机、内部主机或可信主机) 之间所允许的所有操作[19].

3) 设计分析：基于上述要求，评估者需要：

(1) 理解由一个作为主体的未经鉴别的主机向一个内部或外部网络中的主机提出服务请求中哪些是合法的；

(2) 标识(或证实厂商的标识) 所有的服务类型，理解未鉴别主机采用的访问控制策略，以及知道如何标识客体；

(3) 理解一个请求与一个未经鉴别的主机之间的联系；

(4) 判定在内外网络上的一鉴别主机与其它主机(未鉴别的或是可信主机) 之间的许可操作是否全部符合安全功能策略[19].

在进行设计分析的过程中，评估者需要核查以下内容：安全目标(ST)，评估目标安全策略(TSP)，功能说明(FSPEC) 和高层次设计(HLD) 文档[19].

4) 测试：该项目的评估测试是通过分析来进行的，需要：

(1) 证实未经鉴别的主机是唯一标识的；

(2) 证实内部网络或外部网络上未经鉴别的主机能够被唯一地辨别；

(3) 核查防火墙如何处理对每一种服务的访问；

(4) 证实在一台未鉴别主机和其他的内部或外部网络上的主机(未鉴别的或可信的) 之间，所有允许的操作与 SFP 是一致的[19].

测试需要查阅的文件有：功能详细说明书(FSPEC)，测试范围分析，测试计划，测试过程，以及测试结果[19].

3 应用级防火墙的测试体系

应用级防火墙的测试必须以应用级防火墙的安全技术要求和测试要求两准则为指导，对送检产品的各项测试指标进行客观的测试[19].测试内容是针对特定的送检产品而言的，即设计开发出来的产品(系统)的本身决定了需要测试的内容[19].

在测试之前，先要熟悉送检产品的产品性能、技术特点、系统构成和操作使用等基本情况[19].其次，修改测试模板并根据测试轮廓选择测试工具、搭建测试平台[19]然后，开始具体的测试[19]测试后填写好的测试工作单上的所有内容构成了测试的基本数据，依据这些数据来撰写出测试报告[19].

实际测试主要包括三大类测试，它们分别是：功能测试、性能测试和安全测试[19]下面拟对这类测试项目进行简略描述，并简单介绍一些常用的测试工具[19].

3.1 功能测试

应用级防火墙产品的功能测试项目是针对送检产品的功能而言的，不同供应商提供的产品(系统)功能各异[19]测试人员必须对送检产品《功能详细说明书》中所声称的各项功能进行详细的测试[19]例如代理服务器的待测功能一般有：管理工具、管理用户鉴别、代理规则管理及代理服务、代理用户管理、系统日志与审计、拨号代理、虚拟网络、联机帮助等[19].

3.2 性能测试

应用级防火墙的性能测试大致包括如下测试项：

1) 吞吐率：对于稳定的网络负载，单位时间内所能够转发的最大数据量[19].

2) 延迟：在某特定吞吐率下，被测设备引起的数据帧延迟时间[19].即从某数据帧的最后一位数据到达被测设备开始，到此帧的第一位数据从被测设备输出的这段时间[19].

3) 丢帧率：在某特定吞吐率下，被测设备所丢失的帧数占所有应转发帧数的百分比[19].

4) 最大并发连接数：对应用级防火墙而言，被测设备所能连续支持的服务请求和应答连接的最大并发数[19].

5) 每秒最大连接数：对应用级防火墙而言，被测设备在 1 秒钟内所能支持的最大并发连接数[19].

6) 事务处理速率：对于特定的网络负载，单位时间内通过被测产品的事务处理个数[19].一个事务定义为从客户机提交一个服务申请开始，到得到应用服务器回答结束为止[19].

7) 代理规则数：代理服务器所能支持的最大规则数[19].

3.3 安全测试

应用级防火墙产品必须通过安全测试[19].安全测试分为例行测试、攻击测试以及安全检测三类，其测试内容如图 1 所示[19].

3.4 常见的测试工具

测试工具包括软件工具和硬件设备[19].常见的软

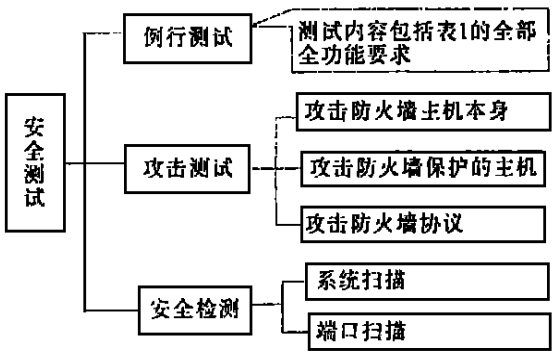

图1　安全测试的测试内容

件工具包括：第一，共享软件：ISS Internet Scanner SAFEsuite、SATAN(安全管理员的网络分析工具)、CRACK、NSS(网络安全扫描器)等；第二，自主开发的安全测试软件如防火墙安全保护轮廓综合测试系统等；第三，对于与加密强度、Tempest 等有关的测试内容委托国家有关职能部门专门的检测机构检测[19].常见的硬件设备有：Internet Advisor (HP)、SmartBits(NetCom)、ATM 交换机、路由器、交换机、集线器(HUB)等[19].

4 结论

要确认应用级防火墙达到了供应商所声称的安全性或安全级别，测试人员必须以它的安全技术要求和测试要求两准则为指导，系统地进行功能测试、性能测试和安全测试，得到国内外有关组织和测试实验室可以广泛接受的测试报告并提交给安全产品认证委员会进行下一步的认证[19].本文作者在中国国家信息安全测评认证中心工作期间，利用以上的测试体系及规范单独测试了邮电部数据所的 PROXY 98 多面手代理服务器和中科院计算所的 ERCIST 防火墙系统中的代理防火墙，并参与了多种防火墙产品的测试，主要有华堂防御系统(上海市外高桥保税区网络发展有限公司)和天网防火墙系统(广州新月通信技术有限公司)等[19]实践证明了该测试规范的系统性和有效性[19].

(下转第 68 页)

系统工程学报,1998(1):81～88.
[6] 张尧庭.成分数据统计分析导论[M].北京:科学出版社,2000.

Exploration on Portfolio Decision-making Model with Continuous Compound Interest under E-V Risk

LAN Rong

(Personnel Division, East China Jiaotong University, Nanchang 330013, China)

Abstract: Based on the returns of portfolio investment caculated by continuous compound interest, we study the decision-making model for portfolio investment under E-V risk and come up with a method for caculating optimal investment proportional coefficient.

Key words: continuous compound interest; E-V risk; portfolio investment

(上接第 39 页)

参考文献:
[1] Willian M.Daley, Gary R.Bachula, Robert E.Hebner. Inerner security policy: a technical guide [J]. Information Technology Laboratory Computer Security Devision, January 6, 1998.
[2] 舒若平,朱孝明,等译. D.Brent Chapman & Elizabeth D.Zwicky. 构筑因特网防火墙[M]. 北京:电子工业出版社, 1998.

A Research on the Criterion of Testing Application Level Firewall

TANG Wen-liang, LI Zheng-fan

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

Abstract: Application-level firewalls come from the requirements of information network security. Their test on firewall provide the most creditable data to evaluate the security of products. In this paper, the common testing criteria, on which the testing application level firewalls are based, and normal tools used in the process of testing, are introduced. And then the issues of testing application-level firewalls are discussed in detail.

Keywords: network security; firewall; Proxy service; testing