防火墙安全测试研究

虞平 丁伟[1]

（东南大学计算机系，210096 南京）

【摘要】

本文研究了防火墙的安全测试问题，提出了三测试种防火墙策略配置的方案，即单点测试、内外部合作测试和协同测试。描述了这三种测试方案的具体算法，并出了它们之间的关系。在文章的结尾，对防火墙测试同端口扫描进行了比较。

【关键词】

防火墙 配置 检测

【中图分类号】

TP393

Firewall security test

Yu Ping, Ding Wei

(Southeast University, Computer Science Dept., 210096 Nanjing, P.R.China)

【Abstract】

In this paper, three schemas are provided to test the firewall configuration, that is, single point test, cooperative test between inside and outside, and collaborative test. This paper describes the detailed algorithm and gives the relations among the three schemas. At the end of the paper, the difference between firewall test and port scan is described.

【Key words】

firewall configuration test

1 引言

网络安全日益受到社会的关注，越来越多的单位建立了防火墙系统。在实际使用中，会出现防火墙配置错误、策略意外变更或失效等情况。本文对防火墙策略的检测方法进行了研究，以便使防火墙的配置者能尽快发现防火墙配置中的错误和最新的更改情况。

无法保证防火墙的管理员对防火墙的配置和修改都是符合要求的。防火墙策略检测的目的是发现防火墙配置中的错误，消除隐患。为确保一个防火墙系统能按要求工作，应对当前的防火墙策略进行检查。本文将研究检测防火墙实施效果的基本思路如下：

将防火墙看成一台报文过滤设备，测试机向防火墙发送给定特征的网络探测报文，分析收到的回应报文，以判断当前的过滤策略，为了提高测试的准确度，多台测试机协同测试。

---

[1]作者简介：虞平，硕士研究生，主要研究方向为网络安全。

丁伟，东南大学计算机系教授主要研究方向包括网络测量、网络管理、网络安全等。

定稿日期：2002-06-07

2 防火墙策略测试方案研究

防火墙是用来限制一部分网络与 Internet 其它部分网络之间数据的自由流动的一种屏障设施。可以认为防火墙将网络分为了内部网和外部网。为了全面的检测防火墙的功能，应当在内部网和外部网中均放置测试机进行探测实验。由于内部网中可能包括多个子网，各子网的防火墙配置策略不尽相同，因而，为了准确的探测各子网的防火墙策略，需要在各子网中也放置一台测试机。本文将讨论探测模型的三种方案，即单点探测、内外部合作探测、以及协同探测。

2.1 单点探测

单点探测是整个探测模型的基础。在单点探测模型中，存在三个对象机，即测试机，防火墙和被探测主机。单点探测就是测试机向被探测主机发送具有特定特征的探测报文，并分析接收到的响应，从而得出防火墙的配置策略。（如图 1 所示）

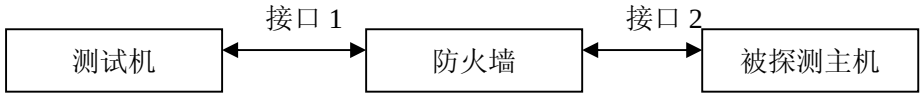

图 1 单点探测的系统结构图

在测试机和被探测主机之间的防火墙存在两个接口，接口 1 和接口 2，每个接口均可有两个方向的防火墙动作，因而从检测系统到被探测主机之间的最多可有 4 种防火墙策略，任何一个接口的任何一个方向为“拒绝”均导致检测系统无法访问被探测主机的某一服务。测试机向被探测主机发送的报文如果没有正常的回应，测试机认为防火墙过滤了这个报文，但测试机无法明确知道在哪个接口的哪个方向上过滤了这个报文。因此测试机只能将这 16 种情况视为两种情况，1：允许 2：拒绝。因而这仅是一种防火墙功能性测试，是以外人的眼光来看防火墙系统的工作状况。

单点测试模型的目标就是准确的获取防火墙的配置情况。为了达到这个目标，采用如下步骤：

步骤一：

向防火墙后的主机发送正常的 TCP 报文 *SYN* 报文，端口号为 *port*。如果收到该主机回应的 *ACK* 或 *RST* 报文，则防火墙一定允许 *port* 端口的报文通过；而如果收到了 ICMP 的 Unreachable 报文，则防火墙一定不允许 *port* 端口的报文通过。长时间没有得到回应，置 *port* 端口的过滤情况不明，使用步骤二进行测试。

步骤二

测试机向防火墙发送 TCP 或 UDP 报文，这个报文的 TTL 值正好在穿越该防火墙时为 0。如果防火墙允许这个报文通过，则测试机会收到一个 TTL 过期的 ICMP 报文。如果不允许该类型的报文通过，有些防火墙会向测试机发送地址不可达的信息；而有些防火墙丢弃该报文后不作任何回应，以上的行为均能明确的判断出防火墙对该报文的过滤策略。

步骤三

本步骤的思想是测试机向被探测主机发送一个构造的错误报文，如 IP 长度错误、IP 选项错误、不合法的 IP 域等，如果这个报文能顺利的到达被探测主机，被探测主机会向测试机发送一个 ICMP 报文，以告知测试机某个错误。在已知子网 ICMP 不被禁止的情况下，可

以利用这个方法测试一个报文与防火墙内的主机之间的是否可达，即测试一个报文从测试机出发，经过接口 1 和接口 2 到达被探测主机的能力。

这个步骤的缺点是在防火墙本身检测错误报文的情况下，探测结果没有意义。

单点测试是功能最弱的一种测试技术，它仅能把 16 种可能的防火墙配置可能分为 2 种。因此对防火墙配置的认识比较模糊。但它防火墙系统没有任何要求，简单，易行。它是下面将要提到的防火墙策略测试的基础。

2.2 内外部合作探测

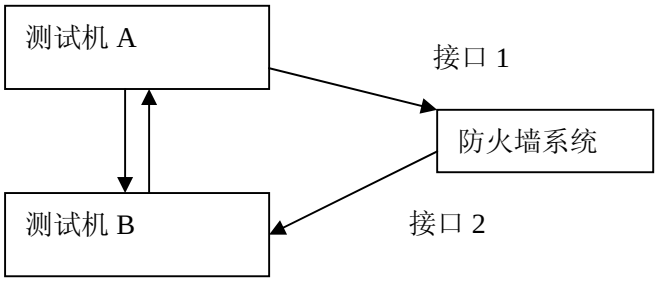

图 2 内外合作探测模型系统图

多点合作探测的原理是在防火墙的内外部各设一台测试机，两测试机之间要求是可以通信的（如图 2）。测试机 A 向测试机 B 发送探测报文的步骤是：

（1） 把将要发送的报文 *packet* 内容告诉 B

（2） 通过防火墙把报文 *packet* 发送给 B。

（3） 询问 B 是否收到了报文 *packet*。

（4） 检查自己有没有收到报文 *packet* 的回应报文 *packet*

（5） 分析，并得到防火墙的策略。

相对单点测试而言，内外部合作探测有两个优越性：

1. 增加了单工这一测度
   测试机可以知道报文是否安全的到达了被探测主机。
2. 可以双向测试
   测试机可以对称测试

2.3 协同探测

单点测试和内外部合作测试的共同点是测试工作量大。以测端口的可达性为例，一个完备的测试方案应包括对所有端口的策略测试。为了在短时间内得到防火墙的过滤策略，可以使用协同的探测技术。协同探测将功能探测系统分为 2 层，即子网间协同层和子网内协同层。在子网间协同层设立一个探测中心，各子网的探测结果均向探测中心报告。

2.3.1 子网间的协同处理

一般来说，防火墙的配置策略是基于子网的，即在相同的子网内，防火墙策略一般相同，(特定主机的特定端口除外)，不同子网的防火墙策略不同，因此一个完备的防火墙探测系统的粒度是子网。应该在每个需要探测的子网内分布一个或多个测试机。每个子网的测试机得到本子网的防火墙策略，再向探测中心报告。

在不设防火墙的情况下，每个子网都直接和探测中心联络。但是防火墙的存在可能导致了一部分子网的探测机无法和探测中心联系。这种情况下，子网探测机只能向它能联络到的

其他子网探测机通信，通过它把本子网的防火墙探测结果报送探测中心。为此，子网测试机需要知道它可达的其他子网的测试主机。在实际使用中，可以静态配置，也可以让子网测试机具备简单的拓扑发现能力，即在测试某一个端口报文的时候，顺便看一下上层的语义，以得到这是否是一台和它一样进行功能测试的机器。

当各子网的测试机掌握了它可达的其他子网测试机后，应用内外部合作探测技术，它可以得到本子网和其他子网之间的防火墙配置情况。

2.3.2 子网内协同处理

在一个子网内，为提高测试速度，可设定多台测试机。利用子网内的拓扑发现技术，测试机之间可以相互感知。根据某种策略（如 IP 最小原则），可选出子网的测试领导，也可人为指定。测试领导负责子网间的协同处理，即子网间协同处理的参加者都为子网的测试领导。测试领导同时负责本子网内的探测任务分工，即把一个测试任务切成多个独立的任务。子网测试机在完成了自己分配的任务后向子网领导报告结果。如果测试领导失效，则在一定的超时后选出新的子网领导。

3 结论

本文研究了防火墙测试算法，提供了三个测试方案，在这三个方案里，单点测试是最基本的防火墙测试方法。内外部合作测试使用了单点测试的技术，同时加入了测试机之间的通信机制，因而结果更准确。协同测试是在前两者的基础上的测试，具有不同子网的协同工作能力，从而能认识防火墙针对不同子网的策略。

【参考文献】

【1】 MountAraratBlossom, Firewall penetration testing, mountararatblossom@usa.net