

浅析网络防火墙*

陈素玲

(盐城市建委,江苏 盐城 224001)

摘 要 防火墙是一道竖在被保护的内部网和不安全网络之间的安全屏障。通过介绍防火墙的作用、系统构成和如何根据实际情况选择防火墙,使人们对防火墙技术有全面的了解。

关键词 网络; 防火墙; INTERNET

分类号 TP393.08 **文献标识码** C **文章编号** 1008-5092/(2000)01-0069-02

随着网络技术的发展,各种网上活动日益频繁,网络的应用越来越广泛,网络安全问题更显得重要^[1]。

1 防火墙的作用

防火墙是用来保护计算机系统免受黑客的骚扰与入侵。它如一道护栏隔在被保护的内部网和不安全网络之间,INTERNET 便是世界上最大的不安全网。现在的防火墙在被保护的内部网与INTERNET 之间,竖起一道安全屏障,用于增强内部网络安全性。

1.1 集中的网络安全

防火墙在被认为是安全和可信的内部网络和不那么安全和可信的INTERNET 之间提供了一个控制机制。防火墙允许网络管理员定义一个中心“阻塞点”来防止非法用户,如黑客、网络破坏者等进入内部网络。禁止存在安全脆弱性的访问进出网络,并抗击来自各种路线的攻击,能够简化网络的安全管理,保障网络的安全性。

1.2 产生安全报警

通过防火墙可以很方便地监视网络的安全性,并产生报警信号。网络管理员必须审查并记录所有通过防火墙的重要信息。如果网络管理员不能及时响应报警并审查常规记录,它就形同虚设。

1.3 部署 NAT

INTERNET 的迅猛发展使得有效的未被申请

的IP地址越来越少,这意味着想进入INTERNET的机构可能申请不到足够的IP地址来满足内部网络上用户的需要。为了连接到INTERNET,可以通过NAT(NETWORK ADDRESS TRANS LATOR 网络地址转换)来完成内部所有地址到外部注册地址的映射。防火墙是部署NAT的理想位置。

1.4 监视 INTERNET 的使用

防火墙是审查和记录内部对INTERNET使用的一个最佳地方,可以在此对内部访问INTERNET进行记录。

1.5 向外部发布信息的理想位置

防火墙也是非常理想的部署WWW服务器和FTP服务器的地点,还可以以防火墙进行配置,允许INTERNET访问上述服务器,而禁止对内部受保护的其它系统进行访问。

2 防火墙的分类

防火墙有以软件形式运行在普通计算机上的,也有以固件形式设置在路由器中的,具体的分类有三种:包过滤防火墙、应用级网关和状态监视器。

2.1 包过滤防火墙

在互联网这样的信息包交换网络上,所有往来的信息都被分割成许多一定长度的信息包,其中包括发送者的IP地址和接收者的IP地址。当这些包被送上互联网时,路由器会读取接收者的IP地址,并选择一条物理上的线路发送出去,信

* 收稿日期:1999-09-26

作者简介:陈素玲(1967-),女,江苏射阳县人。

息包可能以不同的线路抵达目的地,当所有的包抵达后会在目的地重新组装还原。包过滤式的防火墙会检查所有通过信息包里的 IP 地址,并按照系统管理员所给定的过滤规则过滤信息包。这种防火墙的用法很多,比如国家有关部门可以通过包过滤防火墙来禁止国内用户去访问那些违反我国有关规定或者“有问题”的国外站点。

2.2 应用级网关

应用级防火墙也常被人们称为代理服务器。包过滤防火墙可以按照 IP 地址来禁止未授权者的访问。但是它不适合公司用来控制内部人员访问外界的网络,对于这样的企业来说,应用级防火墙是更好的选择。应用级防火墙应用于特定的互联网服务,如超文本传输(HTTP),远程文件传输(FTP)等等。代理服务器通常运行在两个网络之间,它对于客户来说象真的服务器一样,而于外部的服务器来说,它又是一台客户机。当代理服务器接受到用户的请求后会检查用户请求的站点是否符合公司要求。

应用级网关比单一的过滤更为可靠,而且会详细地记录所有的访问状态信息。但是应用级网关也存在一些不足之处,首先,它会使访问速度变慢,因为它不允许用户直接访问网络。

2.3 电路层网关

电路层网关有一个特殊功能,它可以由应用层网关来完成。电路层网关只依赖于 ICP 连接并不进行任何附加的包处理或过滤。在 TELNET 的连接中电路层网关简单地进行了中继,并不做任何审查、过滤或协议管理。只是在内部连接和外部之间来回拷贝字节。但是由于连接似乎是起源于防火墙,其隐藏了受保护网络的有关信息。

3 防火墙的选择

一个好防火墙必须是建构在作业系统之前而不是在作业系统之上,所以作业系统可能有的漏洞并不会影响到一个好的防火墙系统所提供的安全性,防火墙应该提供给使用者不同平台的选择,由于防火墙并非完全由硬件所构成,所以作业系

统所提供的功能以及执行效率一定会影响到整体的表现,而使用者的操作意愿及熟悉程度也是必须考虑的重点。另外,一个好的防火墙应该能为使用者提供完善的后继支援能力。有新的产品出现,就有人会研究新的破解方法。所以,一个好的防火墙提供者就必须要有有一个庞大的组织作为使用者安全的后盾。

在选择防火墙时,应注意到以下几个方面:

3.1 防火墙的管理难易度

防火墙的管理难易程度是防火墙能否达到目的的主要因素之一。若其管理过于困难,需具备完整的知识及不易除错等,将造成设定上的错误,反而不能达到其功能。

3.2 防火墙自身的安全性

防火墙是限制互访,保护内部网的守护者,同时也是网络上的主机之一,也可能存在安全问题,如其不能确保自身安全,则控制功能再强,也终究不能完全保护内部网络。

3.3 防火墙保护网络的整体性

防火墙应以保护整体网络为基本要求,它所保护的是全部的 INTERNET。在 INTERNET 中把对外提供各种服务的服务器分散于许多操作平台上,也是一种分散不安全因素的有效办法。因为,防火墙建立在操作系统之前,能够弥补操作系统的不足。

3.4 防火墙的软件功能及执行效率

防火墙并非全由硬件构成,所以软件所提供的功能及执行效率会影响防火墙的整体表现。防火墙还应同时具备检查、认证、警告、记录的功能,可事先为使用者可能遇到的困难提出解决方案,如信息加密解密的问题。另外,防火墙还应提供多平台的执行方式,以符合不同网络环境的需求。

INTERNET 防火墙是对内部网络安全采取的防护措施,它不是解决所有网络安全问题的万能法宝,而只是网络安全策略中的一个组成部分。但在当今 INTERNET 世界中,防火墙是有其存在的价值的,并且随着 INTERNET 基础技术的发展,防火墙技术也将相应地得到更新。

参 考 文 献

- 1 张月琳. 环球信息网应用指南[M]. 南京: 南京大学出版社, 1997.

(下转第 75 页)

故交错级数 $\sum_{n=1}^{\infty} (-1)^{n-1} \frac{(2n-1)!!}{(2n)!!}$ 收敛。

于是 $\lim_{n \rightarrow \infty} \frac{(2n-1)!!}{(2n)!!} = 0$

例2 判别交错级数 $\sum_{n=1}^{\infty} (-1)^{n-1} \frac{a(a+d) \cdots [a+(n-1)d]}{b(b+d) \cdots [b+(n-1)d]}$ ($a > 0, b > 0, d > 0$) 的敛散性。

解: $r = \lim_{n \rightarrow \infty} n \left(\frac{a_n}{a_{n+1}} - 1 \right) = \lim_{n \rightarrow \infty} \frac{(b-a)n}{a+nd} = \frac{b-a}{d}$

由定理可得:

当 $0 < \frac{b-a}{d} < 1$, 即 $a < b < a+d$ 时, 原级数条件收敛;

当 $\frac{b-a}{d} > 1$, 即 $b > a+d$ 时, 原级数绝对收敛;

当 $\frac{b-a}{d} = 1$, 即 $b = a+d$ 时, 原级数收敛。此时, 原级数即为 $\sum_{n=1}^{\infty} (-1)^{n-1} \frac{a}{a+nd}$, 故条件收敛;

当 $\frac{b-a}{d} < 0$, 即 $b < a$ 时, 原级数发散;

当 $\frac{b-a}{d} = 0$, 即 $b = a$ 时, 原级数为 $\sum_{n=1}^{\infty} (-1)^{n-1}$, 发散。

综上所述, 原级数

当 $b \leq a$ 时, 发散;

当 $a < b \leq a+d$ 时, 条件收敛;

当 $b > a+d$ 时, 绝对收敛。

上述例子表明本文所给出的新的判别定理, 对某些级数应用起来显得很方便。

参 考 文 献

- 1 华东师范大学数学系. 数学分析[M]. 北京: 高等教育出版社, 1980.
- 2 吉米多维奇. 数学分析习题集题解(四)[M]. 费定晖, 周学圣编译. 济南: 山东科学技术出版社, 1980.

A Criterion for Convergence of Alternate Series

Luo Rujia

(Lianyungang Vocational College, Jiangsu Lianyungang 222001, PRC)

Abstract In this paper, we present a new sometimes very effective, criterion for convergence of alternate series.

Keywords alternate series; convergence; criterion; theorem

(上接第70页)

A Narrow Analysis about Firewall

Chen Shulin

(Yancheng building commission of the city and
countryside, Jiangsu Yancheng 224001, PRC)

Abstract Firewall is a safety screen setting between the inter Net and the unsafety Net Through the introduction of the use and system constitution of the Firewall, and how to choose it according to the actualities, people can know more about this new knowledge-Firewall.

Keywords Net; Firewall; INTERNET