防火墙的安全分析及构筑建议

马志强[1]， 门 健[2]， 蔡 勇[2]
(1 海军工程大学，湖北 武汉 430033;2.空军工程大学 电讯工程学院，陕西 西安 710077)

摘 要:简要介绍了目前防火墙所采用的三种应用技术:包过滤技术,应用层网关,代理服务。讨论了包过滤、代理、双穴主机防火墙的特点。对防火墙的安全性进行了详细分析,指出了目前防火墙技术存在的问题和局限性,在此基础上提出了新一代防火墙的构筑建议。

关键词:防火墙;应用技术;安全性;建议
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1009-3516(2001)03-86-88

随着计算机工业的迅速发展,网络的应用越来越普及,网络用户的数量也以惊人的速度增长。迅速发展的网络在给人们的生活、工作带来了巨大方便的同时,也带来了一些不容忽视的问题,网络信息的安全问题就是其中最重要的问题之一。很多企事业单位和政府部门在解决面临的网络安全问题时,都把构筑一个有效的防火墙系统作为安全策略的重要组成部分。

1 防火墙技术及特性

由于网络中通信的交互性,在网络内部用户访问外部世界的同时,外部世界也可以访问该网络。为阻断来自外部网络对本网络的威胁和入侵,可在该网络与 Internet 中插入一个中介系统,竖起一道安全屏障。这一中介系统叫防火墙或防火墙系统。防火墙系统可以是路由器,也可以是个人机、主系统或者是一批主系统。

1.1 防火墙的应用技术

防火墙的应用技术主要有三种:包过滤技术,应用层网关,代理服务。

1)包过滤技术:是在网络中的适当位置按照预先设定的过滤原则过滤数据包。只有满足过滤原则的数据包才被转发到相应的目的端口,那些不符合过滤原则的数据包会被从信息中过滤掉。这是一种基于网络层的安全技术,对于应用层的黑客行为是无能为力的。

2)应用层网关:是在网络应用层上建立协议过滤和转发功能。它针对特定的网络应用服务协议使用指定的数据过滤逻辑,并在过滤的同时,对数据包进行必要的分析、登记和统计,形成报告。能够记录和控制所有进出通信业务。它的主要缺点是:对提供的大部分服务都需要专业化的用户程序或不同的用户接口。

3)代理服务:是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术。代理服务器接收客户请求后会检查验证其合法性,如其合法,代理服务器取回所需的信息再转发给客户,从而将内部系统与外界隔离开来。代理服务器的优点在于可以将被保护网络内部的结构屏蔽起来。此外,代理服务还可以用于实施较强的数据流监控、过滤、记录和报告等功能。新型的代理服务——网络地址转换服务(NAT)可以屏蔽内部网络的 IP 地址,使网络结构对外部来讲是不可见的。

1.2 几类主要防火墙比较

目前的防火墙产品主要有以下三种类型:

1)包过滤防火墙:包过滤防火墙设置在网络层,可以在路由器上实现包过滤。首先应建立一定数量的访问控制表,访问控制表是以其收到的数据包头信息为基础而建成的。信息包头含有数据包源 IP 地址、目

收稿日期:2000-09-06
作者简介:马志强(1968-),男,山东乳山人,讲师,主要从事自动控制与网络安全研究.

的IP地址、传输协议类型(ICP、UDP、ICMP等)、协议源端口号、协议目的端口号、连接请求方向、ICMP报文类型等。当一个数据包满足访问控制表中的规则时,则允许数据包通过,否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问,也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包,无法实施对应级协议的处理。

2)代理防火墙:代理防火墙又称应用层网关防火墙,它由代理服务器和过滤路由器组成,是目前较流行的一种防火墙。过滤路由器负责网络互连,并对数据进行严格选择,然后将筛选过的数据传送给代理服务器。代理服务器起到外部网络申请访问内部网络的中间转接作用,其功能类似于一个数据转发器,它主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时,代理服务器接受申请,然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务,如果接受,它就向内部网络转发这项请求。

3)双穴主机防火墙:该防火墙是用主机来执行安全控制功能。一台双穴主机配有多个网卡,分别连接不同的网络。双穴主机从一个网络收集数据,并且有选择地把它发送到另一个网络上。内部网和外部网的用户可通过双穴主机的共享数据区传递数据,从而保护了内部网络不被非法访问。

一个防火墙系统往往是多种防火墙技术的有机组合。但至少应该包括过滤路由器和代理两个部件。

2　防火墙的安全性分析

2.1　对防火墙安全性的几点认识

1)正确选用、合理配置防火墙并不容易。建立合理的防护系统,配置有效的防火墙应遵循如下四个步骤:风险分析;需求分析;确立安全政策;选择准确的防护手段,并使之与安全政策保持一致。然而,多数防火墙的设立没有或很少进行充分的风险分析和需求分析,而只是根据不很完备的安全政策选择了一种似乎能"满足"需要的防火墙。

2)防火墙的失效状态急需关注。评价防火墙性能时,不仅要看它工作是否正常,能否阻挡或捕捉到恶意攻击和非法访问的蛛丝马迹,而且要看到一旦防火墙被攻破,它的状态如何?按级别来分,它有以下四种状态:未受伤害能够继续正常工作;关闭并重新启动,同时恢复到正常工作状态;关闭并禁止所有的数据通行;关闭并允许所有的数据通行。前两种状态比较理想,而第四种最不安全。但是许多防火墙由于没有条件进行失效状态测试和验证,无法确定其失效状态等级,因此网络存在安全隐患。

3)防火墙的动态维护很有必要。防火墙安装和投入使用后,要想充分发挥它的安全防护作用,必须对它进行跟踪和维护,要与商家保持密切的联系。

4)防火墙的全面测试验证难以实现。防火墙能否起到防护作用,最根本、最有效的证明方法是对其进行测试,甚至站在"黑客"的角度采用各种手段对防火墙进行攻击,然而具体执行时难度较大。

2.2　防火墙的局限性

1)防火墙只是提供了对网络边缘的防卫,不能防止内部的攻击。

2)防火墙不能防止怀有恶意的代码:病毒和特洛伊木马。虽然有些防火墙可以检查病毒和特洛伊木马,但它只能阻挡已知的恶毒程序,这就可能让新的特洛伊木马溜进来。

3)大多数的产品还停留在需要网络管理员手工建立的水平上。

4)防火墙受到测试和验证等各方面的限制,因此很难证明防火墙的防护能力及失效状态能否满足安全政策的需要。

5)防火墙强迫绝大多数出入的信息都必须经过这个唯一的检查点,所以造成安全和速度不能兼得的局面,防火墙成为一个信息流量的阻塞点。

6)在设计防火墙的安全策略时,要在安全性和灵活性上做以取舍,可能会导致网络使用上的不方便。

3　新一代防火墙的构筑建议

新一代防火墙技术应全面考虑网络的安全、操作系统的安全、应用程序的安全、用户的安全、数据的安全,五者综合应用。在产品及功能上,要摆脱目前对子网或内部网管理方式的依赖,向远程上网集中管理方

式发展,并逐渐具备强大的病毒扫除功能;适应 IP 加密的需求,开发新型安全协议,建立专用网(VPN);推广单向防火墙;增强对网络攻击的检测和预警功能;完善安全管理工具,特别是可疑活动的日志分析工具,这是新一代防火墙在编程技术上的革新。新一代防火墙应具有两个或三个独立的网卡,内外两个网卡不作 IP 转化而串接与于内部与外部之间,另一个网卡专门用于对服务器的保护。它应具有以下特点:

1)应与安全操作系统合而为一。防火墙厂商具有系统的源代码,去掉系统中不安全的因素以及不必要的特征,实现安全内核。

2)利用多级过滤技术,保证系统的安全性和防护水平。在分组过滤一级,过滤掉所有的源路由分组和假冒的 IP 源地址;在应用网关一级,能利用 FTP,SMTP 等各种网关,控制和监测 Internet 提供的所有通用服务;在电路网关一级,实现内部主机与外部站点的透明连接,并对服务的通行严格控制。

3)利用网络地址转换(NAT)技术,使外部网络无法了解内部网络。利用网络地址转换(NAT)技术,允许内部网络使用自己编制的 IP 地址和专用网络。

4)利用安全服务器网络(SSN)技术,在内外网络系统中建立一个"隔离区",进一步保护内部网络。所谓安全服务器网络技术,就是利用一块网卡将对外服务器作为一个独立网络处理,对外服务器既是内部网络的一部分,又与内部网关完全隔离。对 SSN 上的主机即可单独管理,也可设置成 FTP,Telnet 等方式从内部网上管理。SSN 方法要比传统的"隔离区"(DMZ)要好的多,因为在 SSN 与内部网络之间都有一层防火墙防护,而 DMZ 只是一种内、外部网络网关之间存在的一种防火墙方式。一旦攻破,前者的内部网络仍会处于防火墙的保护之下,而后者则暴露于攻击之下。

5)用户鉴别和加密。新一代防火墙应该有对用户进行认证的机制,并对不同的用户赋予相应的权限,信息在 Internet 上传输时,应利用"虚拟专网"(Virtral Private Network)技术对信息进行加密传输。为了解决防火墙不能防范内部的攻击的缺点,应在内部网络上实现加密传输,但这一切对于内部用户应是透明的。

6)审计和警报。新一代防火墙应能对一切恶意的攻击进行审计,并发出警报。

随着 Internet 在我国的迅速发展,防火墙技术引起了各方面的广泛关注。目前使用较多的,是在路由器上采用分组过滤技术提供安全保证。防火墙技术还处在一个发展阶段,仍有许多问题有待解决。

参考文献:

[1] Internet Security System Internet Scanner[EB/OL]. http://www.iss.net,2000.

[2] 黄允聪,严望佳. 防火墙的选型、配置、安装和维护[M]. 北京:清华大学出版社,1999.

Analysis of the Security and the Advice for Constructing of Firewall

MA Zhi-qiang[1], MEN Jian[2], CAI Yong[2]

(1. Naval University of Engineering, Wuhan 430033, China; 2. The Telecommunication Engineering Institute of the Air Force Engineering University, Xi'an 710077, China)

Abstract: This paper briefly explicates three kinds of common application technology: package filtering, application gateway and the proxy service, and discusses the characteristics of the firewall of package filtering, the proxy and the dual hole main stations. Especially we point out the localization of the technology of firewall after the analysis of the security of the firewall. On the basis of it an advice of the new generation firewall is given.

Key words: firewall; application technology; security; advice