网络安全与防火墙

杨槟 (清华大学计算机系 100084)

Internet 以及 Intranet 的飞速发展,使得计算机网络一夜之间成了人们关心的热点。计算机网络给人们带来了巨大的利益。通信的手段不再只是电话,传真,而增加了更快捷和便宜的 E-mail, EDI 系统给网上贸易提供了可能。网络给人们带来了并即将带来更多的娱乐手段,人们通过网络看报纸杂志交友聊天,获取大量信息,而花费不多。通过网络召开电视会议,看电影听音乐....。所有这一切的发展正在并即将给人们的生活带来巨大的变化,人们处在一种惊喜之中。

然而这惊喜的背后,也有一些担忧。当人们通过计算机定货或拨出一大笔款项时,当人们打开自己的 Web 站点向世人展示时,当那些军事机要部门通过网络传递消息时,他们不免有些战战兢兢,计算机网络真的不会出错吗?会不会有人搞破坏呢?我的钱会不会被偷走?这些焦虑是可以理解的。

防火墙(Firewall)就是这样一种保护措施,它使用户可以安全地使用网络,更好地利用网络上的资源,而不必担心受到黑客(Hacker)的袭击。

近一两年来各种防火墙产品如雨后春笋,但就其基本概念主要有如下这些:

·包过滤技术 (IP filtering or packet filtering)。采用这种技术的防火墙产品,其原理在于监视并过滤网络上流入流出的 IP 包,拒绝发送那些可疑的包。由于 Internet 与 Intranet 的连接多数都要使用路由器,所以路由器成为内外通信的必经端口,那么路由器厂商在新型的路由器上增加 IP filtering 功能,即添加 Firewall 功能,这样的路由器也就成为 Screening Router 或称为 Circuit-level gateway。仅仅采用这种方式的 Firewall 是否足够安全呢?网络专家 Steven. M. Bellovin 说,这种方式的 Firewall 应该是足够安全的,但前提是配置合理。然而一个包过滤规则是否完全严密及必要是很难判定的,因而在安全要求较高的场合,通常还配合使用其他的技术来加强安全性。

·应用网关 Application gateway。通常由一台专用计算机来实现,这台机器是内外网络连接的桥梁,是内外联络的唯一途径,起着网关的作用,这台机器也被称为 Bastion Host, Duel-homed gateway。在应用网关上运行应用代理程序(Applicaiton Proxy),一方面代替原来的服务器程序,与客户程序建立连接,另一方面代替原来的客户程序,与服务器建立连接,使得合法用户可以通过应用网关安全地使用 Internet 服务,而对于非法用户的请求将不予理睬。常用的代理程序有 WWW proxy, E-mail proxy 等。

·其他常用的安全机制还有身份验证(Authentication),访问控制(Access Control),加密(Encryption)等。身份验证的目的主要是为了进一步证明用户的合法性,使用的手段有利用 UserID 和 Password,或利用 token 产生一个一次性的密码,更复杂的如 MIT 发明的 Kerberos。访问控制要用到身份验证的结果,根据用户的身份赋予其相应的权限。利用加密传输可以保证重要信息不外泄。即使黑客窃听到文件,也无法了解其内容。除此之外,日志(Log)、入侵侦察(Intrusion Detection)及报警(Alert)也是非常有效的手段。日志要详尽,不漏掉任何可疑信息,又要易读。而入侵侦察则可以保证在出现问题后及时报警,避免造成更大的损失。

如何实现一个防火墙呢?在实现一个防火墙之前,应当首先制定一个策略(Policy)。只有这个策略制定得合理有效,实现的防火墙才能起到安全保护的作用。否则策略本身就有漏洞,那么依据此而建立的防火墙又有什么安全可言?

尽管实现一个什么样的防火墙没有一定之规,但还是可以从总体上给出一个原则:

(1) 支持一条"禁止一切未明确允许的服务"规则;

(2) 在实现既定规则时不能漏掉任何一条;

(3) 只要适当修改规则,便可以适应新的服务和需求;

(4) 要具有或可以安装一个身份验证系统;

(5) 在包过滤时,可以对某个具体的机器系统允许或禁止;

(6) 包过滤模块的语言要灵活,易于编程,可以控制

尽可能多的属性;

(7) 对于需要的各种服务如 FTP, TELNET, SMTP, NNTP, HTTP, X, gopher 等要加相应的代理服务(proxy services);

(8) 对于拨入用户集中管理,进行过滤,并做好日志

通常来说,自己实现一个防火墙的成本可能不比买产品的费用低,而且考虑到可靠性及稳定性,还是购买一个信得过的产品比较好。

现有的防火墙产品非常之多,产品五花八门,但其用到的主要技术上面都已叙述了。

美国国家计算机安全协会(The National Computer Security Association)是一个国家性组织,它为许多公司的防火墙产品做测试,而防火墙生产厂家也将 NCSA 认证当作是一种荣誉。

NCSA 开发了一个无偏见的可发展的标准来定义一个好的防火墙。其测试主要从安全性及功能性两方面来进行测试。安全的防火墙才可能是好的,而如果加了防火墙,Internet 服务就要受到限制,这必然也会使用户不满意,因而好的功能,快的 throughput 都会是用户考虑的因素。

在这众多的产品中,介绍以下几种。

1. TurnStyle Firewall System

ASG 公司的 TurnStyle Firewall System 的核心是一个高性能的包过滤模块,另外,ASG 与 ActivCard Network Inc. 有很好的合作关系,使用该公司的 authentication token 可以增加 User Authentication 功能,增强 Firewall 的功能,提高安全性。该系统的工作平台是 486 或奔腾,NetBSD 操作系统,或 SunSparc 服务器,SunOS 4.1.3 操作系统,或 DEC Alpha 服务器,使用 OSF/1 或 Digital UNIX 操作系统。其 GUI 的用户界面易于配置,另外由于其在网络层实现防火墙,因而其速度好,另外可有效地防止伪造 IP 地址(IP spoofing)。

2. Borderware Firewall Server 3.0.1

Border Network 公司的 Borderware Firewall Server 3.0.1 是一种总控开关式的防火墙,并具有 Plug - and - Play 的特性,与网关系统合而为一,有基于 Web 的远程管理器,可以实现先进的 VPN(Virtual Private Network)和 SSN(Secure Server Network),其特点可概括为:

·简单、集中化的管理;

·VPN 加密和身份验证(支持 DES, RC5 利用身份验证可使内部 VPN 与 Internet 外部服务共存);

·安全的服务器;

·增强的性能;

·综合的审计日志;

·易于使用,模块化可适应各种网络要求。

除 Border Network 公司外,Secure Computing Corporation 公司, Webster Network Strategies 以及 Enigma Logic Inc 公司也支持 Border ware Firewall Server。其中 Secure Computing Corporation 的 SidewiderTM Enterprise Security Server 曾多次获奖。该公司有多年为美国政府研究开发网络系统安全的经验,现在其产品也应用于美国及各国的政府中,Webster 公司提供一种监视过滤流过的 Internet Packet 的访问信息及内容的软件。而 Enigma 公司在加密方法方面有很丰富的经验,其主要在 Authentication 及报警、病毒防御等方面有杰出贡献。

3. Checkpoint Firewall - 1

在防火墙行业中最出色的一个是 Checkpoint 公司。其 Firewall - 1 是一个非常有效、高性能的防火墙产品。Checkpoint 公司的防火墙已经经历了多年的考验,是一种透明实时的解决方案。其所获得的奖励及认证也是最多的。在 Data Communication 所做的测试中,其性能明显优于其他产品,速度最快,高居榜首。Chechpoint 的防火墙涉及包过滤、应用代理、网络地址变换等技术,并采用先进的用户认证、加密功能以及友好的用户界面。Sun, HP, Ubnetworks, Oracle 等公司利用 Checkpoint Firewall - 1 来解决网络安全问题。该产品还作为 Sun 公司的 Solstice Firewall - 1 出售。

4. Digital's Firewall Service

Digital's Firewall Service 包括咨询、安装软件、硬件、培训、技术支持等。标准的 Digital's Firewall Service 包括三台机器,Gatekeeper, Gate 和 Mailgate。Gatekeeper 位于外部网络,Mailgate 位于内部,而 Gate 位于内外网络之间。构成一个 Screend Subnet,将内部网络独立出来。

5. Gauntlet Internet Firewall

Gauntlet 是一个 Bastion - Host 系统。运行于 Pentium - Powered 平台,BSD Unix 。

Gauntlet 包括一个 完整性检查(integrity checker)、报警 (configurable alarms)、审计 (audit tool)、用户身份确证并包含了基于令牌的一次性密码(Token - Based One - time Password)。 (来稿时间:1996 年 10 月)