电子科技大学学报社科版　2002 年(第Ⅳ卷)　第 1 期　信息科学

Journal of UESTC (social sciences edition) Mar.2002,vol.4,No.1

网络安全与防火墙技术*,**

□郝玉洁　[电子科技大学　成都　610054]

□常　征　[成都信息工程学院　成都　610041]

[摘　要]　防火墙是网络安全的关键技术,其核心思想是在不安全的网络环境中构造一个相对安全的子网环境。本文讨论了实现防火墙的主要技术手段,重点阐述了现行防火墙的功能、类型、安全措施以及防火墙技术的发展。

[关键词]　防火墙;　包过滤;　代理服务器

[中图分类号]TN711　　[文献标识码]A　　[文章编号]1008－8105(2002)01－0005－(03)

随着 Internet 的迅速发展,人们可以通过互联网进行购物、银行转账等许多商业活动,全球电子交易一体化将成为可能。但是,开放的系统必然存在众多潜在的安全隐患,网络犯罪的递增、大量黑客网站的诞生,促使人们思考网络的安全性问题。黑客与反黑客、破坏与反破坏的斗争仍将继续。安全技术作为一个独特的领域越来越受到人们的关注。各种网络安全工具也跟着在市场上被炒得火热,最受人注目的当属网络安全工具中最早成熟,最早产品化的网络防火墙产品了。

一、防火墙及安全功能

当一个网络接上 Internet 之后,系统的安全除了考虑计算机病毒、系统的健壮性之外,更主要的是防止非法用户的入侵,保护一个网络不受来自另一个网络的攻击。通常,被保护的网络属于我们自己,或者是我们负责管理的,而所要防备的网络则是一个外部的网络,该网络是不可信赖的,因为可能有人会从该网络上对我们的网络发起攻击,破坏网络安全。

防火墙是位于两个信任程度不同的网络之间(如企业内部网络和 Internet 之间)的软件或硬件设备的组合,对网络之间的通信进行控制,通过强制实施统一的安全策略,防止对重要信息资源进行非法存取和访问,达到保护系统安全的目的。防火墙(firewall)处于企业或网络群体计算机与外界通道(Internet)之间,限制外界用户对内部网络进行访问并具备管理内部用户访问外界网络的权限。能有效地监控内部网和 Internet 之间的活动,保证内部网络的安全,使企业的网络规划清晰明了,识别并屏蔽非法请求,有效防止跨越权限的数据访问。它既可以是非常简单的过滤器,也可能是精心配置的网关,监测并过滤所有内部网和外部网之间的信息交换。防火墙保护着内部网络的敏感数据不被窃取和破坏,并记录内外通信的有关状态信息日志,如通信发生的时间和进行的操作等等。新一代的防火墙甚至可以阻止内部人员将敏感数据向外传输。目前,全球连入 Internet 的计算机中约有 1/3 是处于防火墙保护之下。

一般来说,防火墙具有以下几种功能:

第一,强化安全策略,过滤掉不安全服务和非法用户,即过滤进、出网络的数据;管理进、出网络的访问行为;拒绝发往或者来自所选网点的请求通过防火墙。

第二,监视网络的安全性,并报警。

第三,利用网络地址转换(NAT)技术,将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来,用来缓解地址空间短缺的问题。

第四,防火墙是进出信息都必须通过的关口,适合收集关于系统和网络使用和误用的信息。利用此关口,防火墙能在网络之间进行记录。是审计和记录 Internet 使用费用的一个最佳地点。网络管理员可以在此提供 Internet 连接的费用情况,查出潜在的带宽瓶颈位置,并能够依据本机构的核算模式提供部门级的计费。

第五,可以连接到一个单独的网络上,在物理上与内部网络隔开,并部署 WWW 服务器和 FTP 服务器,作为向外部发布内部信息的地点。

二、防火墙的结构

目前防火墙主要采用的是包过滤防火墙、应用级网关和

* [收稿日期]　2001－04－11

** [作者简介]　郝玉洁(1961—)女,北京市人,电子科技大学计算机学院教师,副教授;常征(1962—)男,成都信息工程学院副研究员.

状态监视器：

(一)包过滤防火墙

内部网络↔过滤器(Filter)↔路由器(Router)↔Internet

又叫网络级防火墙,因为它是工作在网络层。

所有往来的信息在 Internet 网络上,被分割成许多定长的信息包,包含发送者和接收者的 IP 地址信息。路由器读取信息包接收者的 IP 并选择一条合适的物理线路发送出去,经由不同的路线抵达目的地,并重新组装还原。包过滤式防火墙可以提供内部信息以说明通过的连接状态和一些数据流的内容,把判断的信息同规则表进行比较,是否同意或拒绝包的通过。具体的说,包过滤式的防火墙会检查所有通过的信息包中 IP 地址,并按照系统管理员所给定的过滤规则进行过滤。如果防火墙设定某一 IP 地址为不适宜访问的话,从这个地址来的所有信息都会被防火墙屏蔽掉。

这种结构由路由器和 Filter 共同完成,实现对外界计算机访问内部网络在 IP 地址或者域名上的限制,以及内部网络访问 Internet。路由器仅对筛选主机的特定的 PORT 上数据通讯加以路由,而 Filter 主机则执行筛选、过滤、验证及其安全监控,很大程度隔断内外网络间的不正常的访问登陆。

包过滤防火墙对用户来说是透明的,处理速度快且易于维护。但包过滤路由器通常没有用户的使用记录,不能得到入侵者的攻击记录。“IP 地址欺骗”和“同步风暴”便是黑客用于攻击包过滤防火墙比较常用的手段。同时,包过滤防火墙相对而言配置比较繁琐。它阻挡非法用户进入内部网络,但无法告诉何人进入你的系统;它可以阻止外部对内部网络的访问,对内部之间的访问却不做任何限制。包过滤另一个关键的弱点就是不能在用户级别上进行过滤,即不能鉴别不同的用户和防止 IP 地址盗用。

(二)应用级网关

内部网络↔代理网关(Proxy Gateway)↔Internet

应用级网关主要工作在应用层,又称为应用级防火墙。就是通常我们提到的代理服务器。这种方式是内部网络与 Internet 不直接通讯。它适用于特定的 Internet 服务,如 HTTP、FTP 等等。代理服务器通常运行在两个网络之间,具有双重身份。对客户来说像是一台真的服务器,对于外界的服务器来说,又是一台客户机。用户对某站点的访问请求可以通过代理服务器进行。如果用户访问该站点得到许可,代理程序使用代理地址(因而隐藏了内部的网络地址)发送请求,当从 Internet 服务器上收到响应时,代理服务器会检查信息包的数据部分确信这个内容是所期望的回应。若有命令或数据可疑,代理服务器会放弃这个信息包。否则,就会用它自己的地址作为源地址来创建一个新的信息包,把结果送回到内部客户端。这里,代理应用程序不但检查信息包头信息,同时检查了 IP 信息包的数据部分。代理服务器通常都拥有一个高速缓存,存储用户经常访问的站点内容,当有用户要访问相同站点时,服务器将缓存内容发出,无须到访问的站点,节省了时间和网络资源,使之成为内部网络与外部网络之间的防火墙,挡在内部用户和外界之间。从外部只能看到代理服务器而无法获知任何的内部资源,诸如用户的 IP 地址等。代理服务器担当了局域网与 Internet 之间的中间人详细地记录所有的访问状态信息。受保护网内部用户想对外部网访问时,也需先登录到防火墙上,再向外提出请求,这样从外部网向内就只能看到防火墙,由于外部系统与内部服务器之间没有直接的数据通道,外部的恶意侵害也就很难伤害到内部网络。

应用级网关的不足之处:因为不允许用户直接访问网络,导致访问速度变慢。而且应用级网关需要对每一个特定的 Internet 服务安装相应的代理服务软件,用户不能使用未被服务器支持的服务,对每一类服务要使用特殊的客户端软件,每一种协议都需要相应的代理软件,使用时工作量大,效率明显不如网络级防火墙,尤其是并非所有的 Internet 应用都可以使用代理服务器。

(三)状态监测防火墙

这种防火墙具有非常好的安全特性,它使用了一个在网关上执行网络安全策略的软件模块,称之为监测引擎。动态设置包过滤规则,避免了静态包过滤所具有的问题。监测引擎在不影响网络正常运行的前提下,采用抽取有关数据的方法对网络通信的各层实施监测,抽取状态信息,并保存起来作为以后执行安全策略的参考。采用这种技术的防火墙对通过其建立的每一个连接都可以进行跟踪,并且根据需要可动态地在过滤规则中增加或更新条目。监测引擎支持多种协议和应用程序,可以很容易地实现应用和服务的扩充。与前两种防火墙不同,当用户访问请求到达网关的操作系统前,状态监视器要抽取有关数据进行分析,结合网络配置和安全规定做出接纳、拒绝、身份认证、报警或给该通信加密等处理动作。

状态监测防火墙对违反访问安全规定的,禁止通行,做好相关状态的日志记录,并将对网络的恶意入侵记录在案,同时会监测无连接状态的远程过程调用(RPC)和用户数据报(UDP)之类的端口信息。这种防火墙无疑是相对可靠和比较安全的,但也会降低网络的速度。配置相对复杂。

三、防火墙的安全措施

作为一种安全防护设备,防火墙在网络中自然是众多攻击者的目标,各种安全措施是防火墙的必备功能。在 Internet 环境中针对防火墙的攻击方法很多,下面介绍几种常用安全措施。

(一)防电子欺骗

IP 假冒是指一个非法的主机假冒内部的主机地址,骗取服务器的“信任”,从而达到对网络的攻击目的。防电子欺骗功能是保证数据包的 IP 地址与网关接口相符,防止通过修改 IP 地址的方法进行非授权访问,对可疑信息进行鉴别,并向网络管理员报警。

(二)抗特洛伊木马攻击

安全防火墙是建立在可靠的操作系统之上的,其安全内

电子科技大学学报社科版　2002 年(第Ⅳ卷)　第 1 期　信息科学

Journal of UESTC (social sciences edition) Mar.2002,vol.4,No.1

核中不能执行下载的程序,可防止特洛伊木马的发生。但是,由于内部用户可通过防火墙下载程序,并可以执行下载的程序,所以就防火墙而言,自身能抗特洛伊木马的攻击,但无法使其保护的某个主机也能防止特洛伊木马或类似的攻击。

(三)网络地址转移

目前,市场上流行许多网络安全性分析工具,它们通常供管理人员用于分析网络安全。使用这些工具,管理人员能较方便地探测到内部网络的安全缺陷和弱点所在。然而,这些工具也成为了恶意入侵者窥视网络或从事破坏的首选。例如 :许多网站免费赠送 SATAN 软件,Internet Scanner 可从市面上购买,这些分析工具给网络安全构成了直接威胁。地址转移是对 Internet 隐藏内部地址,防止内部地址公开,使网络安全分析工具无法从外部对内部网进行分析。这一功能可以克服 IP 寻址方式的诸多限制,完善内部寻址模式。把未注册 IP 地址映射成合法地址,就可以对 Internet 进行访问。

(四)开放式结构设计

开放式结构设计使得防火墙与相关应用程序和外部用户数据库的连接相当容易,典型的应用程序连接如财务软件包、病毒扫描、登录分析等。

(五)邮件技术

外部网络向防火墙保护的内部网络发送邮件,由于只知道防火墙的 IP 地址和域名,就只能送到防火墙上。这时防火墙对邮件进行检查,只有当发送邮件的源主机是被允许通过的,防火墙才对邮件的目的地址进行转换,送到内部的邮件服务器,由其进行转发。

(六)内部防火墙

传统的防火墙设置在内外网络边界,然而日益发展的电子商务要求商务伙伴之间在一定权限下可以进入到彼此的内部网络,这样一来,企业网的边界日趋模糊,来自于内外部的各种安全隐患对防火墙提出了更高的要求。

在实际环境中,80%的攻击和越权访问来自于内部,也就是说,边界防火墙在对付网络安全的主要威胁时束手无策。由于检查机制集中在网络边界,造成了网络访问的瓶颈问题,影响了网络的工作效率,同时防火墙本身的安全机制对整个系统影响至关重要,一旦出现问题或被攻克,整个内部网络将会完全暴露在外部攻击者面前。针对传统边界防火墙的弱点,“分布式防火墙”可能是解决问题的首选了。

在“分布式防火墙”系统中,处于内外部网之间的防火墙仍然监控和保护内部网络;主机防火墙对于网络中(内部和外部网络)的服务器和桌面机进行防护;中心管理是“分布式防火墙”的核心,统一策划和管理作为安全监测机制的每个防火墙,它们根据安全性的不同要求布置在网络中任何需要的位置上,同时,安全策略的分发及日志的汇总都是中心管理应具备的功能。

建造“分布式防火墙”加强了对来自内部攻击的防范,提供了多层次立体的防范体系,实施全方位的安全策略,消除了结构性瓶颈问题,提高了系统性能。

四、防火墙发展展望

今后,防火墙技术的发展要求防火墙采用多级过滤措施,并辅以鉴别手段,使过滤深度不断加强,从目前的地址、服务过滤,发展到 URL(页面)过滤、关键字过滤和对 Active X、Java 等的过滤,并逐渐有病毒清除功能,安全管理工具、可疑活动的日志分析工具不断完善,对网络攻击的检测和告警将更加及时和准确。

现行操作系统自身往往存在许多安全漏洞,而运行在操作系统之上的应用软件和防火墙也不例外,一定会受到这些安全漏洞的影响和威胁。因此,其运行机制是防火墙的关键技术之一。为保证防火墙自身的安全和彻底堵住因操作系统的漏洞而带来的各种安全隐患,防火墙的安全监测核心引擎可以采用嵌入操作系统内核的形态运行,直接接管网卡,将所有数据包进行检查后再提交操作系统。

建立“以防火墙为核心的网络安全体系”,将防火墙与网络入侵监测系统 IDS、病毒检测等相关安全系统联合起来,充分发挥各自的长处,协同配合,就能共同建立一个有效的安全防范体系。这就是说,相关专业检测系统专职于某一类安全事件的检测,一旦发现安全事件,立即通知防火墙。因此,充分发挥各专业厂商的技术优势,形成有机的整体安全系统,这样的安全系统不但有效,而且具有一定的智能。

Network Security And Firewall Technology

Hao Yujie

(UESTC　Chengdu　610054)

Abstract　The firewall is the linchpin upon which network security depends. This article mainly deals with the functions、types and safeguards of the present firewall and its development as well.

Key Words　Firewall;　Package filter;　Proxy

网络安全与防火墙技术

作者： 郝玉洁， 常征
作者单位： 郝玉洁(电子科技大学,成都,610054)， 常征(成都信息工程学院,成都,610041)
刊名： 电子科技大学学报(社会科学版)
英文刊名： JOURNAL OF UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA
年，卷(期)： 2002,4(1)
被引用次数： 22次

本文读者也读过(10条)

1. 网络安全之防火墙技术[期刊论文]-黑龙江科技信息2009(32)
2. 李艳玲. 国增平 防火墙技术在计算机网络安全中的应用研究[期刊论文]-黑龙江科技信息2009(22)
3. 潘晓雷. 杨眉. 李文璞. 简卓为 网络信息安全中的密码技术[期刊论文]-现代电子技术2001(1)
4. 李慧敏. Li Huimin 防火墙技术综述[期刊论文]-计算机光盘软件与应用2011(5)
5. 曹建文. 柴世红 防火墙技术在计算机网络安全中的应用[期刊论文]-甘肃科技纵横2005,34(6)
6. 防火墙技术在计算机网络安全中的应用研究[期刊论文]-大科技·科技天地2011(3)
7. 吕精巧. LV Jing-qiao 浅析网络安全与防火墙技术[期刊论文]-内蒙古科技与经济2009(6)
8. 康丽. KANG Li 论网络安全与防火墙技术[期刊论文]-内蒙古科技与经济2009(3)
9. 何小虎 网络安全与防火墙技术[期刊论文]-黑龙江科技信息2010(23)
10. 项阳 网络安全与防火墙技术[期刊论文]-湖南大众传媒职业技术学院学报2006,6(4)

引证文献(22条)

1. 郭兆丰. 徐兴元. 邢静宇 Snort在入侵检测系统中的应用[期刊论文]-大众科技 2007(8)
2. 方明. 刑远秀 防火墙技术在图书馆网络中的应用[期刊论文]-中国水运（理论版） 2006(12)
3. 邓平. 赵祖应 基于双防火墙的企业网安全设计与实现[期刊论文]-办公自动化（综合版） 2010(7)
4. 李义飞. 杨秋翔 防火墙数据包过滤规则问题探讨[期刊论文]-计算机安全 2007(5)
5. 李强 高校录取中心信息安全策略[期刊论文]-石家庄学院学报 2007(6)
6. 高峰. 许南山 防火墙包过滤规则问题的研究[期刊论文]-计算机应用 2003(z1)
7. 范秉琪. 朱晓东. 马鸿雁. 王杰 基于数据挖掘的网络入侵检测系统的设计与应用[期刊论文]-河南理工大学学报（自然科学版） 2006(3)
8. 汪洪. 杜小勤. 徐军利 公共娱乐服务场所安防系统技术方案[期刊论文]-计算机应用研究 2004(3)
9. 范秉琪. 朱晓东 基于数据挖掘的网络入侵检测系统的设计与应用[期刊论文]-河南科技学院学报（自然科学版） 2006(1)
10. 聂应高 试论图书馆网络安全的防火墙技术比较[期刊论文]-咸宁学院学报 2004(4)
11. 刘强 防火墙技术和安全措施[期刊论文]-商丘师范学院学报 2003(5)
12. 冉晓旻 网络攻击的自动追踪[期刊论文]-网络安全技术与应用 2002(12)
13. 郑晓霞 网络安全技术的研究[期刊论文]-电脑知识与技术 2009(35)
14. 徐兴元. 郭兆丰. 潘晓东 入侵检测系统研究进展[期刊论文]-电光与控制 2007(5)
15. 孔中明. 田玉玲 矿区局域网安全防范技术研究[期刊论文]-煤 2010(3)
16. 王喆 校园网络安全技术的研究[期刊论文]-天津职业院校联合学报 2007(2)
17. 林启招. 李勤文. 赵广 实时监视招办网站及其数据的程序设计与实现[期刊论文]-计算机与现代化 2011(3)
18. 吴文艳 基于透明代理和SSO单点登录技术的信息安全系统[学位论文]硕士 2005
19. 李雄伟. 于明. 周希元 信息网络对抗技术概论(连载二)[期刊论文]-无线电工程 2004(10)

20. 孔琳俊 校园网络安全分析及安全体系方案设计[学位论文]硕士 2006

21. 邹英成 网络安全技术及其在园区网中的应用研究[学位论文]硕士 2005

22. 张震 基于主机防火墙SNETMAN的研究和应用[学位论文]硕士 2005