试论计算机防火墙技术及其应用

冯思毅
（河北工程大学 教育技术中心，河北 邯郸 056038）

[摘 要]随着科技的发展，人们可以在网上完成各种交易，避免了现金交易的繁琐。但是网络在为人们带来便利的同时也带来了隐患，资金的流动不再可见，资金的安全也变得难以保障，因而网络安全开始变得更加重要。从防火墙的概念、分类、优劣势等方面出发，讨论计算机防火墙技术的应用。

[关键词]计算机；财产安全；防火墙；应用
doi:10.3969/j.issn.1673-9477.2015.01.037
[中图分类号]G64 [文献标识码]A [文章编号]1673-9477(2015)01-113-02

网络的发展让人们得以在世界上任何有网络的地方运用电脑对自己的财产进行操作，避免了现金交易的风险，也让电商这一行业得以异军突起，只要在电脑前下单，想要的东西就能在不久后送达。网络为人们生活带来便利的同时，利用网络技术进行犯罪的事情也开始日渐凸显。由于网络的特殊性，人们需要借助计算机防火墙对个人财产进行保护。

一、防火墙的概念

计算机网络防火墙技术是软件和硬件结合起来形成的、在专用网络和公用网络之间、个人网络与他人网络之间的界面上构造的保护屏障。这个屏障是在不同网络间建立网关，以帮助使用者的电脑过滤网络上的病毒等危害计算机安全的信息，保护用户财产的安全。

防火墙主要包括以下四部分：验证工具、访问规则、应用网关以及包过滤。而其主要功能主要体现在访问控制和内容控制，防火墙可以自动过滤不安全的服务或者不安全的站点，监控 Internet 安全和预警的方便端点，以保证内部网络的安全性，可以说防火墙是连接计算机与外部网络的桥梁。

二、防火墙的分类

（一）包过滤防火墙

包过滤防火墙是最基础的防火墙，电脑及路由器都自带有包过滤功能。网络上的所有数据传递都是以数据包的形式进行的，包过滤就是解析数据包中标识发送者的 IP、端口号等信息，已确认数据是否安全，如果某一 IP 地址被认为是不安全的，那么来自这一 IP 地址的所有数据包都会被过滤掉。

包过滤型防火墙又可以分为无状态包过滤和有状态包过滤。无状态包过滤是根据包头部的信息来判断数据包的安全与否，这是最原始的判断方法，其弊端也很明显，判断的依据很不充分，只有特别明显的错误才能被识别。有状态包过滤则可以检查包内所有信息，以此来判断数据能否通过。有状态包过滤的缺点是对每一个数据包的解析和比对会占用大量的时间和运行空间，影响电脑的响应速度。不过由于其在处理数据时的简易性和可读性，目前仍然被计算机操作人员广泛使用。

（二）代理服务型防火墙

代理服务器相当于在用户和外部网络之间设立了一个中转站，用户的数据包先到中转站，然后由中转站发往外部网络，运用代理服务器，数据包的内容会有所改变，从而起到保护用户计算机的目的，而这种防火墙的弱点同样是对于数据的处理需要占用大量的资源。

（三）复合型防火墙

复合型防火墙是代理型防火墙和包过滤型防火墙的有机结合，复合型防火墙的防护效果要由于两者。复合型防火墙又可以划分为屏蔽主机防火墙体系结构和屏蔽子网防火墙体系结构，屏蔽主机防火墙体系结构是在内部网络中设置堡垒机，堡垒机是外部网络唯一能够访问的节点。而屏蔽子网防火墙体系是将堡垒机安装在子网内，使这一子网与外界网络分离，确保子网不受未授权外部用户的攻击。

三、防火墙的应用

防火墙，顾名思义，其功能在于“防火”，防火墙能够作为网络安全的屏障，强化网络安全策略，可以配置 WWW 服务和 FTP 服务，方便用户对于此类

[投稿日期]2015-01-15
[作者简介]冯思毅（1984-），男，河北邯郸人，硕士生，研究方向：计算机应用。

服务器的访问，也能够禁止相关服务器的访问，以保护用户计算机。

如今黑客运用的攻击方式多种多样，主要有以下几种：病毒、口令字、IP 地址。针对不同的网络攻击方式，防火墙都有相应的反制措施。

（一）对于病毒的处理

在部分防火墙产品上自带有扫描病毒的功能，能够对接收的数据包进行筛选和侦察，但是由于病毒的日新月异，往往防火墙只能防一时的病毒，对于之后更先进的病毒基本无防护能力。而黑客常用的方法一是将病毒伪装成某种文件或者应用程序，用户在不知情的情况下下载文件或者安装应用程序会使病毒直接进入电脑内网。方法二是利用软件一次性发送成千上万条含有恶意代码的邮件，造成恶意代码的爆炸式传播。对于上述问题，可以设置防火墙到较强的等级，对于未经许可就运行的后台程序，一律禁止运行，以防止信息泄露。

（二）对于口令字的处理

口令字是相当于打开防火墙的钥匙，黑客如果掌握了口令字，就能在用户的计算机中为所欲为。因此对于口令字的攻击也是流行的网络攻击手法之一，黑客往往采用穷举和嗅探来获取防火墙口令字。嗅探是通过侦查来获取主机给防火墙的口令字，而穷举是将所有可能的口令字集合起来一个个测试，直至找出正确的口令字。对于此类问题，可以设置防火墙采用一次性口令或者让主机和防火墙通过不可侦测的单独接口进行通信。

（三）对于 IP 地址的处理

上文提到防火墙对于数据包的识别有时候是只根据包头部的信息判断是否拦截，因此如果黑客通过代理服务器把自己的 IP 地址设置成与内部网络的 IP 地址，就能够避过防火墙的检测，从而进入内部网盗取用户的信息。对于此种网络攻击，有两种解决方法：

1.将计算机的适配器地址（MAC）与计算机的 IP 地址进行绑定，拥有对应 MAC 地址的用户才能访问被绑定的 IP 地址，当然这种方式只适用于静态 IP,对于动态 IP 则要采用另一种方法。

2.反向过滤技术（rp-filter）。系统在接收到一个 IP 包后，检查该 IP 是不是合乎要求，不合要求的 IP 包会被系统丢弃，也就是对于 IP 包设置唯一的网口，只识别来自这个网口的 IP 包，这种方法能够有效避免黑客的网络攻击。

五、小结

互联网的发展让黑客的网络攻击手段更加灵活和隐蔽，而与此同时人们越来越趋向于利用网络来进行一切消费，以此来获取更大的便利，网络犯罪的隐蔽性让人们对于在网络层面的财产的保护更加关注，因此对于计算机防火墙的要求也越来越高。相信随着科技的发展，防火墙能够真正为用户防止一切攻击，保护用户的合法财产不受侵害。

参考文献：

[1]吉中云. 试论防火墙在计算机网络系统中的应用[J]. 电子制作，2012(8):29.

[2]赵俊. 浅谈计算机防火墙技术与网络安全[J]. 成都航空职业技术学院学报：综合版，2012,28(4):50-52.

[3]姜瑞云，冯立刚，赵丽萍. 网络社会与人的社会化[J]. 河北工程大学学报（社会科学版），2009(2):75-76,74.

[责任编辑 王云江]

On the computer firewall technology and its application

FENG Si-yi

(Educational Technology Center, Hebei University of Engineering, Handan, 056038)

Abstract: With the development of science, we can make various transactions online, avoiding the complicated procedure in the currency transaction. While the internet brings risk together with convenience. There is no more currency transfer, but the security of fund is no longer guaranteed. It is most important to make a secure internet environment. This paper makes a discussion of the concept, classification, advantage and disadvantage of firewall, to give an application proposal of computer firewall.

Key words: computer; property security; firewall; application