防火墙在网络安全访问控制中的应用选择

吴子勤　刘笑军　滕建明

（蚌埠坦克学院训练部　**邮编** 233050）

摘要：随着 Internet 的应用日益普及，针对网络的攻击频率和密度也在显著增长，这给网络安全带来了越来越多的隐患。我们可以通过很多网络工具、设备和策略来保护不可信任的网络。其中防火墙是运用非常广泛和效果最好的选择。它设置在用户网络和外界之间的一道屏障，防止不可预料的、潜在的破坏侵入用户网络；在开放和封闭的界面上构造一个保护层，属于内部范围的业务，依照协议在授权许可下进行；外部对内部网络的访问受到的限制。

关键词：防火墙；网络安全；访问控制；应用选择

1　引言

过去，许多内联网访问 Internet 的基本方法是将本系统的内部网直接接入 Internet，这样内部网的每台计算机都可以获得完全的 Internet 服务。这样的连接在给用户带来方便的同时也使网络入侵者有机可乘。内部网的主机将毫无保护地暴露在 Internet 中，因此,分布在世界各地的任何一台 Internet 主机都可以直接对其进行访问,从而在安全上带来极大的危险。并且，入侵者的行动通常都是很难被察觉的，因此安全问题已经成为各内部网接入 Internet 之前必须要考虑的问题之一。目前，以防火墙为代表的被动防卫型安全保障技术已经被证明是一种较有效的防止外部入侵的措施。

从本质上，Internet 的安全性可以通过提供以下两方面的安全服务来达到：一是访问控制服务，用来保护计算机和联网资源不被非授权使用；二是通信安全服务，用来提供认证、数据机要性、完整性和各通信端的不可否认性服务。这两种服务的实现，主要依赖于防火墙技术和加密技术。

防火墙的概念实际上是借用了建筑学上的一个术语。建筑学中的防火墙是用来防止大火从建筑的一部分蔓延到另一部分而设置的阻挡机构。计算机网络上的防火墙是用来防止来自互联网的破坏，如黑客攻击、资源被盗用或文件被篡改等波及内部网络的危害。

防火墙的实质就是限制数据流通和允许数据流通。因此防火墙有两种对立的安全策略：

⑴允许没有特别拒绝的事情。这种情况下防火墙只拒绝了规定的对象，不属于拒绝范围以内的任何情况都被允许。这种策略对数据包的阻挡能力相对较小，所以安全性相对较弱。

⑵拒绝没有特别允许的事情。这种情况与前面一种情况正好相反，其拒绝能力强，它只接收被允许了的数据包，凡是在允许情况以外的数据包都将被拒绝。

总之，防火墙能增强机构内部网络的安全性。防火墙系统决定了外界的哪些人可以访问内部的哪些可以访问的服务，以及哪些外部服务可以被内部人员访问；要使一个防火墙有效，所有来自和通向外界的信息都必须经过防火墙，接受防火墙的检查；防火墙必须只允许授权的数据通过，并且防火墙本身也必须能够免于渗透。

2　防火墙的技术

防火墙的种类多种多样，在不同的发展阶段，采用的技术也各不相同。采用的不同技术，因而也就产生了不同类型的防火墙。

⑴从防火墙产品形态分类，防火墙可以分为如下 3 种：

软件防火墙　运行于特定的计算机上,它需要客户预先安装好的计算机操作系统的支持，一般来说，这台计算机就是整个网络的网关，俗称“个人防火墙”。

硬件防火墙　是指所谓的“硬件防火墙”。之“所谓”二字是针对芯片级防火墙说的。它们最大的差别在于是否基于专用的硬件平台。传统硬件防火墙一般至少应具备三个端口，分别接内网、外网和 DMZ（非军事化区），现在一些新的防火墙往往扩展了端口，常见的四端口防火墙一般将第 4 端口作为配置口、管理端口。

芯片级防火墙　基于专门的硬件平台及专用的操作系统。

(2)从防火墙所采用的技术不同，可以将防火墙分为如下 3 种类型：

“包过滤型”防火墙　是防火墙的初级产品，其技术依据是网络是的分包传输技术。网络上的数据都是以“包”为单位传输的，数据波被分割成一定大小的数据包，每一个数据包中都有一些特定信息，如数据的源地址、目标地址、TCP/UDP 源端口和目标端口等。

包过滤型防火墙的优点是逻辑简单，实施费用低廉，对网络的影响较小，有较强的透明性。并且它的工作与应用层无关，无须改动任何客户机和主机上的应用程序，易于安装和使用。其弱点是：配置基于包过滤方式的防火墙，需要对 IP、TCP、UDP、ICMP 等各种协议有深入的了解，否则容易出现因配置不当带来的问题；不提供用户的鉴别机制。

“代理型”防火墙　也称为代理服务器，它的安全性要高于包过滤型产品，并开始向应用层发展。

“监测型”防火墙　就是对包过滤技术的增强。这种防火墙采用了一个在网关上执行网络安全策略的软件引擎，称之为监测模块。它工作在链路层和网络层之间，对网络通信的各层实施监测分析，提取相关的通信和状态信息，并在动态连接表中进行状态及上下文信息的存储和更新，这些表被持续更新，为下一个通信检查提供累积的数据。

(3)从网络结构来分类，可以将防火墙分为以下 4 类型：

网络级防火墙 是基于源地址和目的地址、应用研究或协议，以及每个 IP 包的商品来做出通过与否的判断。

应用级网关　通常也称为应用代理服务器。它工作于 OSI 模型的应用层。在外部网络向内部网络或内部网络向外部网络申请服务时起到转接作用。

其工作过程为：首先，它对该用户的身份进行验证。若为合法用户，则把请求转发给真正的某个内部网络的主机，同时监控用户的操作，拒绝不合法的访问。当内部网络向外部网络申请服务时，代理服务器的工作过程刚好相反。应用网关代理的优点是易于配置，界面友好；不允许内外网主机的直接连接；可以提供比包过滤更详细的日志记录。

电路级网关　用来监控信任的客户机或服务器与不受信任的主机间的 TCP 握手信息，这样来决定该会话是否合法，电路级网关是在 OSI 模型中会话层上来过滤数据包，这样比包过滤防火墙要高两层。

规则检查型防火墙　该防火墙结合了包过滤防火墙、电路级网关和应用级网关的特点。它同包过滤防火墙一样，规则检查防火墙能够在 OSI 网络层上通过 IP 地址和端口号，过滤进出的数据包。

(4)从防火墙应用部署位置来分，可将防火墙分为 3 种类型：

边界防火墙　这是最为传统的那种，它们位于内、外网络的边界，所起的作用是对内、外网络实施隔离，保护边界内部网络。

个人防火墙　安装于单台主机中，防护的也只是单台主机，应用于广大的个人用户。

混合式防火墙　可以说就是“分布式防火墙”或者“嵌入式防火墙”，它是一套防火墙系统，由若干个软、硬组成，分布于内、外网络边界和内部各主机之间，既对内、外部网络之间进行通信过滤，又对网络内部各主机间的通信进行过滤。

另外，新近推出的自适应代理(Adaptive Proxy)防火墙技术，本质上也属于代理服务技术，但它也结合了动态包过滤（状态检测）技术。组成这种类型防火墙的基本要素有两个：动态包过滤器与自适应代理服务器。它结合了代理服务防火墙的安全性和包过滤防火墙的高

速度等优点，在保证安全性的基础上将代理服务器防火墙的性能提高 10 倍以上。

3　防火墙的应用选择

在防火墙与网络的选择上，有以下 3 种结构：双宿主主机模式、屏蔽主机模式和屏蔽子网模式。

(1)双宿主主机模式

这种防火墙系统由一台特殊主机来实现。这台主机拥有两个不同的网络接口：一端接外部网络，一端接需要保护的内部网络，故被称为双宿主主机，也成为双宿主网关。防火墙不使用包过滤规则,而是通过在外部网络和被保护的内部网络之间设置这个网关(双宿主网关)，隔断 IP 层之间的直接传输。被保护网络中的主机与该网关可以通信，外部网络中主机也能与该网关通信，但是两个网络中的主机不能直接通信，两个网络之间的通信通过应用层数据共享或应用层代理服务来实现，其配置实现如图 01 所示。

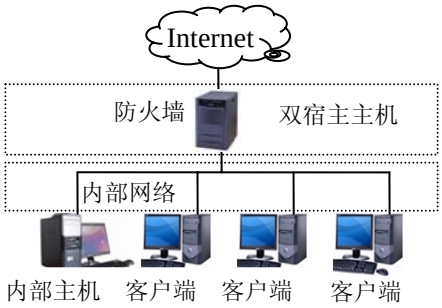

图 01 双宿主主机体系结构

(2)屏蔽主机模式

屏蔽主机防火墙由一台过滤路由器和一台堡垒主机组成，其配置实现如图 02 所示。在这种配置中，堡垒主机配置在内部网络上，过滤路由器则放置在内部网络和外部网络之间。在路由器上进行安装，使得外部网络的主机只能访问该堡垒主机，而不能直接访问内部网络的其他主机。内部网络在向外通信时，也必须首先到达堡垒主机，由该堡垒主机来决定是否允许访问外部网络。这样，堡垒主机成为内部网络与外部网络通信的唯一通道。

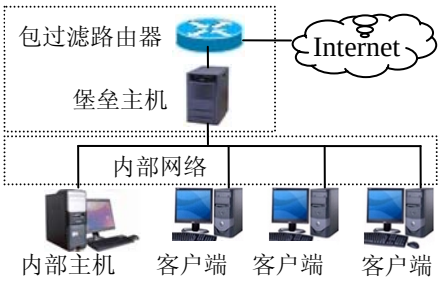

图 02 屏蔽主机体系结构

堡垒主机是运行代理软件的计算机，它暴露在被保护的网络之外，入侵者如果穿透了过滤路由器，必须首先把该主机攻克，才能够进入到内部网络。

(3)屏蔽子网模式

屏蔽子网防火墙是目前流行的一种结构，其配置实现如图 03 所示。采用了两个包过滤路由器和一个堡垒主机，在内外部网络之间建立一个被隔离的子网，定义为“非军事区”，有时也称作周边网，用于放置堡垒主机、WEB 服务器、Mail 服务器等公用服务。内部网络和外部网络均可访问屏蔽子网，但禁止它们穿过子网通信。在这一配置中，即使堡垒主机被入侵者控制，内部网络仍受到内部包过滤路由器的保护。

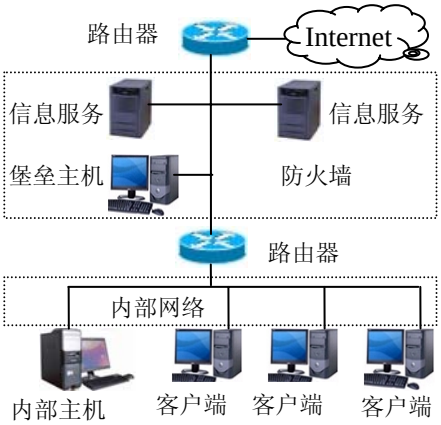

图 03 屏蔽子网体系结构

屏蔽子网防火墙的主要优点是它又提供了一层保护。一个入侵者必须通过两个路由器和一个应用网关，这比起屏蔽主机防火墙来要困难得多。

4 结束语

Internet 防火墙不仅仅是路由器、堡垒主机或任何提供网络安全的设备的组合，它更是安全策略的一个部分。安全策略建立了全方位的防御体系来保护机构的信息资源，所有可能受到网络攻击的地方都必须以同样安全级别加以保护。仅设立防火墙系统，而没有全面的安全策略，那么防火墙就形同虚设。防火墙是一种综合性的技术，涉及计算机网络技术、密码技术、安全技术、软件技术、国际标准化组织（ISO）的安全规范以及安全操作系统等方面。防火墙作为内部网与外部网之间的一种访问控制设备，常常安装在内部网和外部网交界点上。在实际的应用中，如果认为单纯地采用防火墙后网络将变得绝对安全，将是很幼稚的。

参考文献

1 张敏波．网络安全实战详解．北京：电子工业出版社，2008
2 谭方勇．网络安全技术实用教程．北京：中国电力出版社，2008
3 王高平．网络与应用教程．北京：清华大学出版社，2007
4 丁建立．网络安全．武汉：武汉大学出版社，2007
5 黄淑华．计算机网络技术教程．北京：机械工业出版社，2004