第 3 章　防火墙技术

随着计算机网络广泛应用于政治、军事、经济和科学技术各个领域，数据在存储和传输过程中可能被窃听、暴露或篡改，网络系统和应用软件也可能遭受黑客的恶意程序的攻击而使网络瘫痪。因此，计算机网络的安全非常重要。

在计算网络的安全中，保护网络数据和程序等资源，以免受到有意或无意地破坏或越权修改与占用，称为访问控制技术。实现访问控制技术最好的办法就是有一个好的安全策略，在这个安全策略上使用防火墙技术。

为实现网络安全，必须了解防火墙技术的体系结构，同时掌握常见的防火墙设备的配置方法。

本章的主要内容有：

- 防火墙的定义；
- 防火墙的功能与作用；
- 防火墙的类型；
- 防火墙的配置；
- 防火墙的实现策略；
- 防火墙的选择原则；
- Windows 自带防火墙和卡巴斯基个人防火墙的使用。

3.1　防火墙概述

3.1.1　什么是防火墙

古时候，人们常在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。现在，如果一个网络接到了 Internet 上面，它的用户就可以访问外部世界并与之通信。但同时，外部世界也同样可以访问该网络并与之交互。为安全起见，可以在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障。这道屏障的作用是阻断来自外部通过网络对本网络的威胁和入侵，提供扼守本网络的安全和审计的唯一关卡，它的作用与古时候的防火砖墙有类似之处，因此把这个屏障就叫做“防火墙”，如图 3-1 所示。

在网络中，防火墙是一种用来加强网络之间访问控制的特殊网络互连设备，如路由器、网关等。它对两个或多个网络之间传输的数据包和连接方式按照一定的安全策略进行检查，以决定网络之间的通信是否被允许。其中被保护的网络称为内部网络，另一方则称为外部网络或公用网络。它能有效地控制内部网络与外部网络之间的访问及数据传送，从而达到保护内部网络的信息不受外部非授权用户的访问和过滤不良信息的目的。

防火墙是一个或一组在两个网络之间执行访问控制策略的系统，包括硬件和软件，目的是保护网络不被可疑人侵扰。本质上，它遵从的是一种允许或阻止业务来往的网络通信安

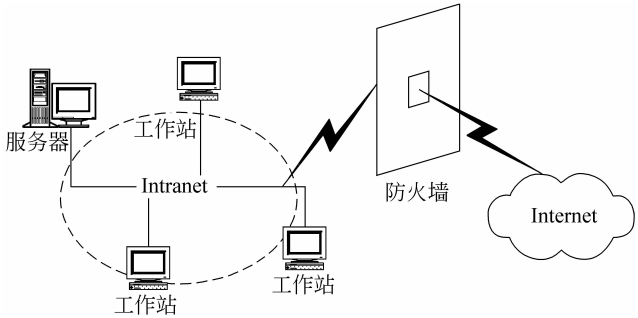

图 3-1　防火墙在网络中的位置

全机制，也就是提供可控的过滤网络通信，只允许授权的通信。

通常，防火墙就是位于内部网或 Web 站点与 Internet 之间的一个路由器或一台计算机，又称为堡垒主机。其目的如同一个安全门，为门内的部门提供安全，控制那些可被允许出入该受保护环境的人或物。就像工作在前门的安全卫士，控制并检查站点的访问者。

3.1.2　防火墙的功能

防火墙是由管理员为保护自己的网络免遭外界非授权访问但又允许与 Internet 连接而发展起来的。从网际角度来说，防火墙可以被看成是安装在两个网络之间的一道栅栏，根据安全计划和安全策略中的定义来保护其后面的网络。

由软件和硬件组成的防火墙应该具有以下功能：

(1) 所有进出网络的通信流都应该通过防火墙。

(2) 所有穿过防火墙的通信流都必须有安全策略和计划的确认和授权。

(3) 理论上说，防火墙是穿不透的。

利用防火墙能保护站点不被任意连接，甚至能建立跟踪工具，帮助总结并记录有关正在进行的连接资源、服务器提供的通信量以及试图闯入者的任何企图。

总之，防火墙是阻止外面的人对你的网络进行访问的任何设备，此设备通常是软件和硬件的组合体，它通常根据一些规则来挑选想要或不想要的地址。

随着 Internet 上越来越多的用户要访问 Web，运行例如 TELNET，FTP 和 Internet Mail 之类的服务，系统管理者和 LAN 管理者必须能够在提供访问的同时，保护他们的内部网，不给闯入者留有可乘之机。

防火墙需要防范的 3 种基本进攻如下：

(1) 间谍：试图偷走敏感信息的黑客、入侵者和闯入者。

(2) 盗窃：盗窃对象包括数据、Web 表格、磁盘空间、CPU 资源、连接等。

(3) 破坏系统：通过路由器或主机/服务器蓄意破坏文件系统或阻止授权用户访问内部网(外部网)和服务器。

这里防火墙的作用是保护 Web 站点和公司的内部网，使之免遭 Internet 上各种危险的侵犯。

典型的防火墙建立在一个服务器/主机机器上，亦称“堡垒”，是一个多边协议路由器。这个堡垒由两个网络连接：一边与内部网相连，另一边与 Internet 相连。它的主要作用除

了防止未经授权的或来自对 Internet 访问的用户外，还应包括为安全管理提供详细的系统活动记录。在有的配置中，这个堡垒主机经常作为一个公共 Web 服务器或一个 FTP 或 E-mail 服务器使用。

通过在防火墙上运行的专门 HTTP 服务器，可使用“代理”服务器，以访问防火墙另一边的 Web 服务器。

防火墙的基本目的之一就是防止黑客侵扰站点。网络站点经常暴露于无数威胁之中，而防火墙可以帮助防止外部连接。此外，还应小心局域网内的非法 MODEM 连接，特别是当 Web 服务器在受保护的局域内时。

当 Web 站点置于内部网中时，也要提防内部袭击。对于这种情况，防火墙几乎无用。例如，若一个心怀不满的雇员拔掉 Web 服务器的插头，将其关闭，防火墙将对此无能为力。防火墙不是万无一失的，其目的只是加强安全性，而不是保证安全。

3.1.3 防火墙的优点

防火墙能够做什么呢？下面来讨论这个问题。

1. 防火墙能强化安全策略

因为在 Internet 上每天都有上百万的人浏览和交换信息，所以不可避免地会出现个别品德不良或违反 Internet 规则的人。防火墙是为了防止不良现象发生的“交通警察”，它执行网络的安全策略，仅仅允许经许可的、符合规则的请求通过。

2. 防火墙能有效地记录 Internet 上的活动

因为所有进出内部网信息都必须通过防火墙，所以防火墙非常适用收集网络信息。作为网间访问的唯一通路，防火墙能够记录内部网络和外部网络之间发生的所有事件。

3. 防火墙可以实现网段控制

防火墙能够用来隔开网络中某一个网段，这样它就能够有效地控制这个网段中的问题在整个网络中的传播。

4. 防火墙是一个安全策略的检查站

所有进出网络的信息都必须通过防火墙，这样防火墙便成为一个安全检查点，把所有可疑的访问拒之门外。

3.1.4 防火墙的特性

一个好的防火墙系统应具有以下 3 方面的特性。

- 所有在内部网络和外部网络之间传输的数据必须通过防火墙。
- 只有被授权的合法数据即防火墙系统中安全策略允许的数据可以通过防火墙。
- 防火墙本身不受各种攻击的影响。

同时，防火墙应具有的基本准则如下：

(1) 过滤不安全服务。

基于这个准则，防火墙应封锁所有信息流，然后对希望提供的安全服务逐项开放，把不安全的服务或可能有安全隐患的服务一律扼杀在萌芽之中。这是一种非常有效而实用的方法，只有经过仔细挑选的服务才能允许用户使用，从而形成十分安全的网络环境。

(2) 过滤非法用户和访问特殊站点。

基于这个准则，防火墙应先允许所有的用户和站点对内部网络进行访问，然后网络管理

员按照 IP 地址对未授权的用户或不信任的站点进行逐项屏蔽。这种方法构成了一种更为灵活的应用环境,网络管理员可以针对不同的服务面向不同的用户开放,也就是能自由地设置各个用户的不同访问权限。

3.1.5 防火墙的缺点

前面介绍了防火墙的优点,同时它也存在一些缺点。

1. 防火墙不能防范恶意的知情者

防火墙可以禁止用户通过网络传输机密信息,但用户可以不通过网络,比如将数据复制到磁盘或磁带上,然后放在公文包中带出去。如果入侵者是在防火墙内部,那么它也是无能为力的。内部用户可以不通过防火墙而偷窃数据、破坏硬件和软件等。对于内部的威胁只能通过加强管理来防范,如主机安全防范和用户教育等。

2. 防火墙不能防范不通过它的连接

防火墙能够有效地防止通过它进行信息传输,但它不能防止不通过它的信息传输。例如,如果允许对防火墙后面的内部系统进行拨号访问,那么防火墙绝对没有办法阻止入侵者进行拨号入侵。

3. 防火墙不能防止利用标准网络协议中的缺陷进行的攻击

一旦防火墙允许某些标准网络协议,就不能防止利用协议缺陷的攻击,如 DoS(denial of service,拒绝服务)或者 DDoS(distributed denial of service,分布式拒绝服务)进行的攻击。

4. 防火墙不能防范病毒

防火墙不能防范网络上或 PC 中的病毒。虽然许多防火墙可以扫描所有通过它的信息,以决定是否允许它通过,但这种扫描是针对源地址、目标地址和端口号,而不是数据的具体内容。即使是先进的数据包过滤系统,也难以防范病毒,因为病毒的种类太多,而且病毒可以通过许多种手段隐藏在数据中。

防火墙要检测随机数据中的病毒十分困难,它要求:

(1) 确认数据包是程序的一部分。

(2) 确定程序的功能。

(3) 确定病毒引起的改变。

事实上,大多数防火墙采用不同的方式来保护不同类型的机器。当数据在网络上进行传输时,要被打包并经常被压缩,这样便给病毒带来了可乘之机。无论防火墙是多么安全,用户只能在防火墙后面清除病毒。

5. 防火墙不能防备全部的威胁

防火墙被用来防备已知的威胁,一个很好的防火墙设计方案可以防备新威胁,但没有一个防火墙能自动地防御所有新的威胁。

3.2 防火墙的分类

目前,根据防火墙在 ISO/OSI 模型中的逻辑位置和网络中的物理位置及其所具备的功能,可以将其分为两大类,即基本型防火墙和复合型防火墙。基本型防火墙有包过滤路由器

和应用型防火墙两种。复合防火墙将以上两种基本型防火墙结合使用，主要包括主机屏蔽防火墙、子网屏蔽防火墙和分布式防火墙。

下面对这 5 种防火墙进行论述。

3.2.1 包过滤路由器

包过滤路由器(packet filters)在一般路由器的基础上增加了一些新的安全控制功能，是一个检查通过它的数据包的路由器。包过滤路由器的标准由网络管理员在网络访问控制表(access control list)中设定，以检查包的源地址、目的地址及每个 IP 包的端口。它是在 7 层协议的下 3 层中实现的，包的类型可以拦截和登录，因此，此类防火墙易于实现对用户透明的访问，且费用较低，如图 3-2 所示。但包过滤路由器无法有效地区分同一 IP 地址的不同用户，因此安全性较差。

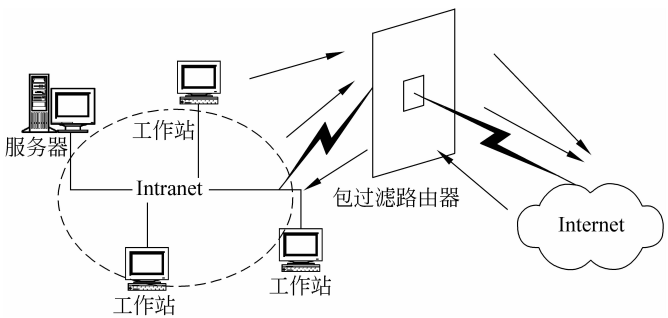

图 3-2 使用包过滤路由器进行数据包过滤

防火墙通常就是一个具备包过滤功能的简单路由器，支持 Internet 安全。这是使 Internet 连接更加安全的一种简单方法，因为包过滤是路由器的固有属性。

包是网络上信息流动的单位。在网上传输的文件一般在发出端被划分成一串数据包，经过网上的中间站点，最终传到目的地，然后这些数据包中的数据又重新组成原来的文件。

每个数据包有两个部分：数据部分和包头。包头中含有源地址和目标地址等信息。

包过滤一直是一种简单而有效的方法，通过拦截数据包，读出并拒绝那些不符合标准的包头，过滤掉不应入站的信息。

包过滤器又称为筛选路由器，它通过将包头信息和管理员设定的规则表比较，如果有一条规则不允许发送某个包，路由器将它丢弃。

包过滤规则一般基于部分的或全部的包头信息，例如对于 TCP 包头信息为：IP 协议类型、IP 源地址、IP 目标地址、IP 选择域的内容、TCP 源端口号、TCP 目标端口号和 TCP ACK 标识，其中 TCP ACK 标识指出这个包是否是连接中的第一个包，是否是对另一个包的响应。

包过滤的一个重要的局限是它不能分辨好的和坏的用户，只能区分好的数据包和坏的数据包。包过滤只能工作在有黑白分明安全策略的网中，即内部人是好的，外部人是可疑的。

不幸的是，包过滤不能有效到足以保证站点的安全。站点受到许多新的协议的威胁，它们能毫不费力地通过那些过滤器。例如，对于 FTP 协议，包过滤就不十分有效，因为为完成

数据传输，FTP 允许连接外部服务器并使连接返回到端口 20。这甚至成为一条规则附加于路由器之上，即内部网络机器上的端口 20 可用于探查外部情况。黑客们很容易“欺骗”这些路由器。而防火墙则使这些“欺骗”变得困难，并且几乎不可能实现。在决定实施防火墙计划之前，先要决定使用哪种类型的防火墙及其设计。

3.2.2 应用型防火墙

应用型防火墙(application gateway，又称双宿主网关或应用层网关)的物理位置与包过滤路由器一样，但它的逻辑位置在 OSI 7 层协议的应用层上，所以主要采用协议代理服务(proxy services)，就是在运行防火墙软件的堡垒主机(bastion host)上运行代理服务程序 Proxy。应用型防火墙不允许网络间的直接业务联系，而是以堡垒主机作为数据转发的中转站。堡垒主机是一个具有两个网络界面的主机，每一个网络界面与它所对应的网络进行通信。它既能作为服务器接收外来请求，又能作为客户机转发请求。如果认为信息是安全的，那么代理就会将信息转发到相应的主机上，用户只能够使用代理服务器支持的服务。在业务进行时，堡垒主机监控全过程并完成详细的日志(log)和审计(audit)，这就大大地提高了网络的安全性。应用型防火墙易于建立和维护，造价较低，比包过滤路由器更安全，但缺少透明性。

应用型防火墙控制对应用程序的访问，即允许访问某些应用程序而阻止访问其他应用程序。采用的方法是在应用层网关上安装代理(proxy)软件，每个代理模块分别针对不同的应用。例如，远程登录代理 Telnet Proxy 负责 Telnet 在防火墙上的转发，文件传输代理 FTP Proxy 负责 FTP 等。管理员可以根据需要安装相应的代理，以控制对应应用程序的访问。各个代理模块相互无关，即使某个代理模块的工作发生问题，只需将它拆卸，不会影响其他代理模块的正常工作，从而保证了防火墙的安全性。

管理员通过配置访问控制表中的规则，决定内、外部网络的哪些用户可以使用应用层网关中的哪个代理模块连接到哪个目的站点。

实际上，应用型防火墙是运行服务器代理软件的计算机，通常叫做“堡垒主机”(bastion host)。由于它采用了一系列安全措施，因而能抵御各种攻击。

(1) 应用层网关运行的是一个安全的操作系统，避免了一般操作系统的脆弱性。

(2) 除安装代理模块外，还安装了用户认证模块，能对用户的身份进行认证。一般采用客户机/服务器方式，根据用户所在网络的安全级别采用不同的认证方法。可卸掉一切多余的服务。

(3) 应用层网关除安装代理模块外，还维持自己的用户库和对象库。用户库保存了用户名、用户的认证方式和用户的管理级别等信息。对象库则保存有管理员定义的主机名、主机组、网络和网关等信息。

(4) 应用网关能记录通过它的一些信息，如什么样的用户在什么时间连接了什么站点。这样就为识别网络间谍提供了有价值的信息。

代理工作时，用户首先与代理服务器建立连接，然后将目的站点告知代理，对于合法的请求，代理以应用层网关的身份与目的站建立连接，而代理则在这两个连接上转发数据。

由以上所述可见，应用层网关防火墙能针对各种服务进行全面控制，支持身份认证，提供详细的审计功能和方便的日志分析工具，比分组过滤路由器更容易配置和测试。但是不

透明，要求用户改变使用习惯。

3.2.3 主机屏蔽防火墙

包过滤路由器虽有较好的透明性，但无法有效地区分同一 IP 地址的不同用户；应用型防火墙可以提供详细的日志及身份验证，但又缺少透明性。因此，在实际应用中，往往将两种防火墙技术结合起来，以取长补短，主机屏蔽防火墙(screened host firewall)就是其中的一种。

主机屏蔽防火墙是由一个只需单个网络端口的应用型防火墙和一个包过滤路由器组成。将它物理地连接在网络总线上，它的逻辑功能仍工作在应用层上，所有业务通过它代理服务。Intranet 不能直接通过路由器和 Internet 相联系，数据包要通过路由器和堡垒主机两道防线。这个系统的第一个安全设施是过滤路由器，对到来的数据包而言，首先要经过包过滤路由器的过滤，过滤后的数据包被转发到堡垒主机上，然后由堡垒主机上应用服务代理对这些数据包进行分析，将合法的信息转发到 Intranet 的主机上。外出的数据包首先经过堡垒主机上的应用服务代理检查，然后被转发到包过滤路由器，最后由包过滤路由器转到外部网络上。主机屏蔽防火墙设置了两层安全保护，因此相对比较安全。另外，主机屏蔽防火墙也容易配置，但它对路由器的路由表要求较高。

3.2.4 子网屏蔽防火墙

子网屏蔽防火墙(screened subnet firewall)的保护作用比主机屏蔽防火墙更进了一步，它在被保护的 Intranet 与 Internet 之间加入了一个由两个包过滤路由器和一台堡垒机组成的子网。被保护的 Intranet 与 Internet 不能直接通信，而是通过各自的路由器和堡垒机打交道。两台路由器也不能直接交换信息。

子网屏蔽防火墙是较为安全的一种防火墙体系结构。它具有主机屏蔽防火墙的所有优点，并且比之更加优越。它与主机屏蔽防火墙不同，如果堡垒主机受到破坏，入侵者只能访问到子网。由于子网和 Intranet 之间还存在一个包过滤路由器，因此，入侵者只能有限地访问 Intranet。虽然子网屏蔽防火墙很优越，但实现的代价也高。它不易配置且增加了堡垒机转发数据的复杂性，同时，网络的访问速度也要减慢，其费用也明显高于以上几种防火墙。

3.2.5 分布式防火墙

分布式防火墙(distributed firewall)是近年来发展起来的一种新型的防火墙体系结构，它将传统的防火墙技术和分布式网络应用进行了有机结合，具有广泛的研究和应用前景。

前述几种防火墙技术统称为传统的防火墙技术，尽管依然是现代计算机网络安全防范的主要技术，但是它存在的不足也是显而易见的：

(1) 防外不防内。就是只对来自外部网络的通信进行检测，而对受保护的内部网络(或网段)中的用户通信不做任何防御。防火墙系统针对的是来自系统外部的攻击，一旦外部入侵者进入了系统，他们便不受任何阻拦。这就使得防火墙的应用受到很大制约，因为现代企业内部网络中的大部分安全威胁还是来自内部网络的。

(2) 结构性限制。传统的防火墙也称为边界防火墙，其工作机理依赖于网络的物理拓扑结构。而现代企业越来越多地成为跨区域的大型企业，企业内部网已成为一个逻辑概念，

用传统的防火墙已经不能满足分布式网络的安全需求。

(3) 效率问题。传统防火墙把检查机制集中在网络的边界节点,所以防火墙容易成为网络的瓶颈,网络应用的日益复杂不断加大防火墙的处理压力。

1999 年,分布式防火墙的概念首次在美国 AT&T 实验室提出,并得到了迅速发展和应用。分布式防火墙系统主要分为以下 3 部分。

(1) 网络防火墙。负责内外网络之间不同安全区域的划分,承担着与传统防火墙相似的功能,但是,增加了一种用于对内部子网之间的安全防护,这样使分布式防火墙实现了对内部网络的安全管理功能。

(2) 主机防火墙。为了扩大防火墙的应用范围,在分布式防火墙系统中设置了主机防火墙。主机防火墙驻留在主机中,并根据相应的安全策略对网络中的服务器及客户端计算机进行安全保护。具体分为主机驻留和嵌入操作系统内核两种方式。主机驻留是指防火墙驻留在主机的内存中,对主机进行实时的安全保护,只负责对本地主机进行安全保护,不信赖除本地主机外的其他主机。嵌入操作系统内核方式主要防范由于操作系统自身存在的安全漏洞而引起的安全问题,直接接管网卡,检查进入操作系统的所有数据包。

(3) 中心管理服务器。是整个分布式防火墙的管理核心,负责安全策略的指定、分发及日志收集和分析等工作。

分布式防火墙不仅保留了传统防火墙的优点,同时还解决了传统防火墙在应用中存在的不足。加强了对来自内部网络的攻击防范,克服了结构性瓶颈问题,有效地解决了主机托管后,跨地区网络使用和管理的不安全性,支持虚拟专用网(VPN)和移动计算等应用。

3.3 防火墙的安全标准

在设计防火墙时,除了安全策略以外,还要确定防火墙类型和拓扑结构。一般来说,防火墙被设置在可信赖的内部网络和不可信赖的外部网络之间。防火墙相当于一个控流器,可用来监视或拒绝应用层的通信业务。防火墙也可以在网络层和传输层之间运行,在这种情况下,防火墙检查进入和离去的报文分组的 IP 和 TCP 头部,根据预先设计的报文分组过滤规则来拒绝或允许报文分组通过。

防火墙技术发展很快,但是现在标准尚不健全,导致各大防火墙产品供应商生产的防火墙产品兼容性差,给不同厂商的防火墙产品的互连带来了困难。为了解决这个问题,目前已提出了以下两个标准:

(1) RSA 数据安全公司与一些防火墙的生产厂商(如 Sun Microsystem 公司、Checkpoint 公司、TIS 公司等)以及一些 TCP/IP 协议开发商(如 FTP 公司等)提出了 Secure/WAN(S/WAN)标准。它能使在 IP 层上由支持数据加密技术的不同厂家生产的防火墙和 TCP/IP 协议具有互操作性,从而解决了建立虚拟专用网(VPN)的一个主要障碍,此标准包含以下两个部分。

- 防火墙中采用的信息加密技术一致,即加密算法、安全协议一致,使得遵循此标准生产的防火墙产品能够实现无缝互连,但又不失去加密功能。
- 安全控制策略的规范性、逻辑上的正确合理性,避免了由于各大防火墙厂商推出的防火墙产品在安全策略上的漏洞而对整个内部保护网络产生的危害。

(2) 美国国家计算机安全协会 NCSA(national computer security association)成立的防火墙开发商(FWPD,firewall product developer)联盟制定的防火墙测试标准。

3.4 在网络中配置防火墙

防火墙的配置是非常重要的。必须保证网络支持的协议能够通过防火墙,尤其是使得使用 TCP 协议 53 端口的域名系统协议(domain name system protocol)能够通过防火墙。否则,组织内部的机器就不能解析防火墙外的机器的名字。同样地,如果想让防火墙内外的机器能够通信的话,也得保证防火墙外的机器能够访问相应的 DNS 服务器,这样它们才能解析防火墙内的主机地址。

实现防火墙一个通常的办法是拒绝绝大部分的从防火墙外发起到防火墙内的机器的连接。当然特定的机器除外,这种机器是被严格保证安全的。

必须严格限制从防火墙内发起到防火墙外的连接,必须对这种连接特别小心。必须明白谁会对网络构成威胁,以及什么会对你构成威胁。禁止从内部发起的连接即意味着内部网连接到的主机可能就是潜在的威胁。当然如果防火墙允许任何协议通过的话,一个恶意的内部人员很容易攻破防火墙。

防火墙作为网络安全的一种防护手段,有多种实现方式。建立合理的防护系统,配置有效的防火墙应遵循如下 4 个基本步骤:

(1) 风险分析。

(2) 需求分析。

(3) 确立安全政策。

(4) 选择准确的防护手段,并使之与安全政策保持一致。

3.4.1 包过滤路由器的配置与实现

包(分组)过滤路由器是最简单也是最常见的防火墙,它位于内部网络和外部网络之间,除具有路由功能外,还可以再装上分组过滤软件,利用分组过滤规则完成基本的防火墙功能。

这种配置的优点如下:

(1) 容易实现,费用少,如果被保护网络与外界之间已经有一个独立的路由器,那么只需简单地加一个分组过滤软件便可保护整个网络。

(2) 分组过滤在网络层实现,不要求改动应用程序,也不要求用户学习任何新的东西,用户感觉不到过滤服务器的存在,因而使用方便。

其缺点是:

(1) 没有或有很少的日志记录能力,因此网络管理员很难确定系统是否正在被入侵或已经被入侵了。

(2) 规则表随着应用的深化会很快变得很大而且复杂,这样不仅规则难以测试,而且规则结构出现漏洞的可能性也会增加。

(3) 这种防火墙的最大弱点是依靠一个单一的部件来保护系统,一旦部件出现问题,会使网络的大门敞开,而用户可能还不知道。

当前，几乎所有的分组过滤装置（筛选路由器或分组过滤网关）都按如下方式操作。

（1）对于分组过滤装置的有关端口必须设置分组过滤准则，也称为分组过滤规则。

（2）当一个分组到达过滤端口时，将对该分组的头部进行分析。大多数分组过滤装置只检查 IP，TCP 或 UDP 头部内的字段。

（3）分组过滤规则按一定的顺序存储。当一个分组到达时，将按分组规则的存储顺序依次运用每条规则对分组进行检查。

（4）如果一条规则阻塞传递或接收一个分组，则不允许该分组通过。

（5）如果一条规则允许传递或接收一个分组，则允许该分组通过。

（6）如果一个分组不满足任何规则，则该分组被阻塞。

从规则(4)和规则(5)，可以看到将规则按适当的顺序排列是非常重要的。在配置分组过滤规则时一个常犯的错误就是将分组过滤规则按错误的顺序排列。如果一个分组过滤规则排序有错，就有可能拒绝进行某些合法的访问，而又允许访问本想拒绝的服务。规则(6)遵循以下原则：未被明确允许的就将被禁止。

这是一个在设计安全可靠的网络时应该遵循的失效安全原则；与之相对的是一种宽容的原则，即：没有被明确禁止的就是允许的。

如果采用后一种思想来设计分组过滤规则，就必须仔细考虑分组过滤规则没有包括的每一种可能的情况来确保网络的安全。当一个新的服务被加入到网络中时，可以很容易地遇到没有规则与之相匹配的情况。在这种情况下，不是先阻塞该服务，从而听取用户因为合法的服务被阻塞而抱怨，然后再允许该服务，而是可以以网络安全风险为代价来允许用户自由地访问该服务，直到制定了相应的安全规则为止。

3.4.2 应用型防火墙的配置与实现

应用型防火墙又称双宿主网关，使用双宿主主机实现。双宿主网关仅用一个代理服务器，代理服务器就是安装于双宿主主机的代理服务器软件。双宿主主机是一台有两块接口卡(NIC)的计算机，每一块接口卡有一个 IP 地址，如图 3-3 所示。如果 Internet 上的一台计算机想与 Intranet 上的一个工作站通信，它必须与双宿主主机上能“看到”的 IP 地址联系，代理服务器软件通过另一块网卡(NIC)启动到对方网络的连接。应该指出的是，在建立双宿主主机时，应该关闭操作系统的路由功能，否则从一块网卡(NIC)到另一块网卡的通信会绕过代理服务器软件，而使双宿主网关失去“防火”作用。Smart Wall 网关就是一个双宿主主机。

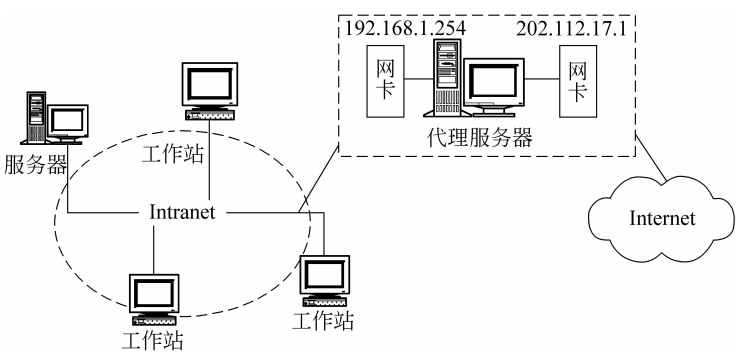

图 3-3 应用型防火墙的配置