第 3 章　防火墙概述

网络安全问题随着 Internet 带宽与电子商务的事务需求的增长变得日益重要。企业或个人越来越频繁地利用互联网进行交易，网络安全性成为了一个重要的问题。个人会用信用卡在网络上做交易，公司之间会在网络上做信息交换，一些重要资料会在网络上流动，这时个人或公司传送的资料就有可能被拦截、修改或盗用，而有些黑客为了试验自己的技术而入侵别人的计算机，严重的会使公司的网站破坏并毁掉顾客资料，以致影响到公司的利益或顾客的隐私及权利。防火墙的目的就是保护网络不被未经授权的使用者经由外界网络（如 Internet）不法侵入，为维护企业及个人的利益建立一道安全屏障。

3.1　防火墙的定义

防火墙是指隔离在本地网络与外界网络之间的一道防御系统，是这一类防范措施的总称。

防火墙的架构是一套独立的软、硬件配置。基本上是在一台服务器上，包括操作系统（Operation System，OS）及安装网络防火墙应用软件而构成的。它架构于互联网（Internet）与内部网络（Intranet）之间，是被运用于两个网络之间的安全屏障，作为内部与外部沟通的桥梁，也是企业网络对外接触的第一道大门。

在互联网上防火墙是一种非常有效的网络安全系统，通过它可以隔离风险区域（即 Internet 或有一定风险的网络）与安全区域（局域网）的连接，同时不会妨碍人们对风险区域的访问。防火墙可以监控进出网络的通信量，从而完成看似不可能的任务；仅让安全、核准了的信息进入，同时又抵制威胁的数据。随着安全性问题上的失误和缺陷越来越普遍，对网络的入侵不仅来自高超的攻击手段，也有可能来自配置上的低级错误或不合适的口令选择。因此，防火墙的作用是防止不希望的、未授权的通信进出被保护的网络，强化了网络安全政策。

一般的防火墙都可以达到以下目的：一是可以限制他人进入内部网络，过滤掉不安全服务和非法用户；二是防止入侵者接近防御设施；三是限定用户访问特殊站点；四是为监视 Internet 安全提供方便。由于防火墙假设了网络边界和服务，因此更适合于相对

独立的网络，如 Intranet 等种类相对集中的网络。防火墙正在成为控制对网络系统访问的非常流行的方法。目前，在 Internet 上的 Web 网站中，超过 1/3 的 Web 网站都是由某种形式的防火墙加以保护的，这是对黑客防范最严，安全性较强的一种方式，任何关键性的服务器，都建议放在防火墙之后。

防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，使 Internet 与 Intranet 之间建立起一个安全网关(Security Gateway)，从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成。

在互联网上防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域(即 Internet 或有一定风险的网络)与安全区域(局域网)的连接。所谓“防火墙”，是指一种将内部网和公众访问网(如 Internet)分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许“同意”的人和数据进入网络，同时将“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问网络。换句话说，如果不通过防火墙，公司内部的人就无法访问 Internet，Internet 上的人也无法和公司内部的人进行通信。

防火墙是设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合，如图 3-1 所示。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。

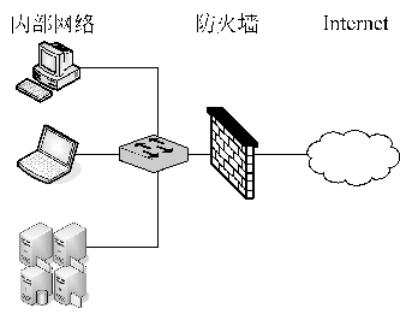

图 3-1　防火墙逻辑位置示意图

在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和 Internet 之间的任何活动，保证了内部网络的安全。防火墙可以是硬件型的，所有数据都首先通过硬件芯片监测；也可以是软件类型的，软件在电脑上运行并监控。其实硬件型也就是芯片里固化了的软件，但是它不占用计算机 CPU 处理时间，功能非常强大，处理速度很快，但对于个人用户来说软件型更加方便实在。

防火墙技术从诞生开始，就在一刻不停地发展着，各种不同结构不同功能的防火墙，构筑成网络上的一道道防御大堤。

3.2 防火墙的分类与技术

3.2.1 防火墙的分类

防火墙分类的方法很多，除了从形式上把它分为软件防火墙和硬件防火墙以外，还可以从技术上将其分为包过滤型、应用代理型和状态监视3类；从结构上又分为单一主机防火墙、路由集成式防火墙和分布式防火墙3种；按工作位置分为边界防火墙、个人防火墙和混合防火墙；按防火墙性能分为百兆级防火墙和千兆级防火墙两类；等等。虽然看似种类繁多，但这只是因为业界分类方法不同罢了，例如一台硬件防火墙就可能由于结构、数据吞吐量和工作位置而规划为“百兆级状态监视型边界防火墙”，因此这里主要介绍的是技术方面的分类，即包过滤型、应用代理型和状态监视型防火墙技术。

为了更有效率地对付网络上的各种不同攻击手段，防火墙也派分出几种防御架构。根据物理特性，防火墙分为两大类，硬件防火墙和软件防火墙。软件防火墙是一种安装在负责内外网络转换的网关服务器上或者独立的个人计算机上的特殊程序，它是以逻辑形式存在的，防火墙程序跟随系统启动，通过运行在Ring0级别的特殊驱动模块把防御机制插入系统关于网络的处理部分和网络接口设备驱动之间，形成一种逻辑上的防御体系。

在没有软件防火墙之前，系统和网络接口设备之间的通道是直接的，网络接口设备通过网络驱动程序接口(Network Driver Interface Specification，NDIS)把网络上传来的各种报文都忠实地交给系统处理，例如一台计算机接收到请求列出机器上所有共享资源的数据报文，NDIS直接把这个报文提交给系统，系统在处理后就会返回相应数据，在某些情况下会造成信息泄漏。而使用软件防火墙后，尽管NDIS接收到的仍然是原封不动的数据报文，但是在提交到系统的通道上多了一层防御机制，所有数据报文都要经过这层机制根据一定的规则判断处理，只有它认为安全的数据才能到达系统，其他数据则被丢弃。因为有规则提到“列出共享资源的行为是危险的”，因此在防火墙的判断下，这个报文会被丢弃，这样一来，系统接收不到报文，则认为什么事情也没发生过，也就不会把信息泄漏出去了。

软件防火墙工作于系统接口与NDIS之间，用于检查过滤由NDIS发送过来的数据，在无须改动硬件的前提下便能实现一定强度的安全保障，但是由于软件防火墙自身属于运行于系统上的程序，不可避免地需要占用一部分CPU资源维持工作，而且由于数据判断处理需要一定的时间，在一些数据流量大的网络里，软件防火墙会使整个系统工作效率和数据吞吐速度下降，甚至有些软件防火墙会存在漏洞，导致有害数据可以绕过它的防御体系，给数据安全带来损失，因此，许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施，而是使用看得见摸得着的硬件防火墙。

硬件防火墙是一种以物理形式存在的专用设备，通常架设于两个网络的驳接处，直接从网络设备上检查过滤有害的数据报文，位于防火墙设备后端的网络或者服务器接收到的是经过防火墙处理的相对安全的数据，不必另外分出 CPU 资源去进行基于软件架构的 NDIS 数据检测，可以极大地提高工作效率。

硬件防火墙一般是通过网线连接于外部网络接口与内部服务器或企业网络之间的设备，这里又另外派分出两种结构，一种是普通硬件级别防火墙，它拥有标准计算机的硬件平台和一些功能经过简化处理的 UNIX 系列操作系统和防火墙软件，这种防火墙措施相当于专门拿出一台计算机安装了软件防火墙，除了不需要处理其他事务以外，它毕竟还是一般的操作系统，因此有可能会存在漏洞和不稳定因素，安全性并不能做到最好；另一种是所谓的芯片级硬件防火墙，它采用专门设计的硬件平台，在上面搭建的软件也是专门开发的，并非流行的操作系统，因而可以达到较好的安全性能保障。

所谓的边界防火墙、单一主机防火墙又是什么概念呢？所谓边界，就是指两个网络之间的接口处，工作于此的防火墙就被称为“边界防火墙”；与之相对的有“个人防火墙”，它们通常是基于软件的防火墙，只处理一台计算机的数据而不是整个网络的数据，现在一般家庭用户使用的软件防火墙就是这个分类了。而单一主机防火墙，就是最常见的一台台硬件防火墙了；一些厂商为了节约成本，直接把防火墙功能嵌进路由设备里，就形成了路由集成式防火墙。

下面介绍防火墙的基本分类。

1. 包过滤防火墙

第一代防火墙和最基本形式防火墙检查每一个通过的网络包，或者丢弃，或者放行，取决于所建立的一套规则，这称为包过滤防火墙。本质上，包过滤防火墙是多址的，表明它有两个或两个以上网络适配器或接口。例如，作为防火墙的设备可能有两块网卡(NIC)，一块连到内部网络，一块连到公共的 Internet。防火墙的任务，就是作为“通信警察”，指引包和截住那些有危害的包。

包过滤防火墙检查每一个传入包，查看包中可用的基本信息(源地址和目的地址、端口号、协议等)，然后，将这些信息与设立的规则相比较。如果已经设立了阻断 telnet 连接，而包的目的端口是 23 的话，那么该包就会被丢弃；如果允许传入 Web 连接，而目的端口为 80，则包就会被放行。

多个复杂规则的组合也是可行的。如果允许 Web 连接，但只针对特定的服务器，目的端口和目的地址二者必须与规则相匹配，才可以让该包通过。

最后，可以确定当一个包到达时，如果有理由让该包通过，就要建立规则来处理它。

建立一个包过滤防火墙规则的例子如下。

对来自专用网络的包，只允许来自内部地址的包通过，因为其他包包含不正确的包头部信息。这条规则可以防止网络内部的任何人通过欺骗性的源地址发起攻击。而且，如果黑客对专用网络内部的机器具有了不知从何得来的访问权，这种过滤方式可以阻止黑客从网络内部发起攻击。

在公共网络，只允许目的地址为 80 端口的包通过。这条规则只允许传入的连接为 Web 连接，也允许与 Web 连接使用相同端口的连接，所以它并不是十分安全的。

丢弃从公共网络传入的包，而这些包都有网络内的源地址，从而减少 IP 欺骗性的攻击。

丢弃包含源路由信息的包，以减少源路由攻击。要记住，在源路由攻击中，传入的包包含路由信息，它覆盖了包通过网络应采取的正常路由，可能会绕过已有的安全程序。通过忽略源路由信息，防火墙可以减少这种方式的攻击。

2. 状态/动态检测防火墙

状态/动态检测防火墙，试图跟踪通过防火墙的网络连接和包，这样防火墙就可以使用一组附加的标准，以确定是否允许和拒绝通信。它是在使用了基本包过滤防火墙的通信上应用一些技术来做到这点的。

当包过滤防火墙见到一个网络包，包是孤立存在的。它没有防火墙所关心的历史或未来。允许和拒绝包的决定完全取决于包自身所包含的信息，如源地址、目的地址、端口号等。包中没有包含任何描述它在信息流中的位置的信息，则该包被认为是无状态的，它仅是存在而已。

检查一个有状态的包防火墙跟踪的不仅是包中包含的信息。为了跟踪包的状态，防火墙还记录有用的信息以帮助识别包，例如已有的网络连接、数据的传出请求等。

如果传入的包包含视频数据流，防火墙可能已经记录了有关信息，是关于位于特定 IP 地址的应用程序最近向发出包的源地址请求视频信号的信息。如果传入的包是要传给发出请求的相同系统，防火墙进行匹配，包就可以被允许通过。

一个状态/动态检测防火墙可截断所有传入的通信，而允许所有传出的通信。因为防火墙跟踪内部出去的请求，所有按要求传入的数据被允许通过，直到连接被关闭为止。只有未被请求的传入通信被截断。

如果在防火墙内运行一台服务器，配置就会变得稍微复杂一些，但状态包检测是有效且能适应的技术。例如，可以将防火墙配置成只允许从特定端口进入的通信，只可传到特定服务器。如果正在运行 Web 服务器，防火墙只将 80 端口传入的通信发送到指定的 Web 服务器。

另外状态/动态检测防火墙可提供的其他一些额外的服务如下。

(1) 将某些类型的连接重定向到审核服务中去。例如，专用 Web 服务器的连接，在 Web 服务器连接被允许之前，被发送到 SecutID 服务器(使用一次性口令)。

(2) 拒绝携带某些数据的网络通信，例如，带有附加可执行程序的传入电子消息，或包含 ActiveX 程序的 Web 页面。

跟踪连接状态的方式取决于包通过防火墙的类型。

(1) TCP 包。当建立起一个 TCP 连接时，通过的第一个包被标有包的 SYN 标志。一般情况下，防火墙会丢弃所有外部的连接企图，除非用已经建立起来的某条特定规则来处理它们。对内部的连接试图连到外部主机，防火墙会注明连接包，允许响应及随后再连

接两个系统之间的包，直到连接结束为止。在这种方式下，传入的包只有在它是响应一个已建立的连接时，才会被允许通过。

(2) UDP 包。UDP 包比 TCP 包简单，因为它们不包含任何连接或序列信息，只包含源地址、目的地址、校验和携带的数据。信息的缺乏使得防火墙很难确定包的合法性，因为没有打开的连接可以测试传入的包是否应该被允许通过。可是，防火墙跟踪连接状态的方式可以确定。对传入的包，若它所使用的地址和 UDP 包携带的协议与传出的连接请求匹配，该包就被允许通过。和 TCP 包一样，UDP 包会被允许通过，是响应传出的请求或已经建立了指定的规则来处理它。

对其他种类的包，情况和 UDP 包类似。防火墙仔细地跟踪传出的请求，记录下所使用的地址、协议和包的类型，然后对照保存过的信息核对传入的包，以确保这些包是被请求的。

3. 应用程序代理防火墙

应用程序代理防火墙实际上不允许在它连接的网络之间直接通信。它是接受来自内部网络特定用户应用程序的通信，再建立单独的公共网络服务器连接。网络内部的用户不直接与外部的服务器通信，所以服务器不能直接访问内部网的任何一部分。

另外，如果不为特定的应用程序安装代理程序代码，这种服务是不会被支持的，不能建立任何连接。这种建立方式拒绝任何没有明确配置的连接，从而提供了额外的安全性和控制性。

例如，一个用户的 Web 浏览器可能在 80 端口，但也经常可能是在 1080 端口，连接到了内部网络的 HTTP 代理防火墙。防火墙会接受这个连接请求，并把它转到所请求的 Web 服务器。这种连接和转移对该用户来说是透明的，因为它完全是由代理防火墙自动处理的。代理防火墙通常支持的一些常见的应用程序有 HTTP、HTTPS/SSL、SMTP、POP3、IMAP、NNTP、TELNET、FTP 和 IRC。

应用程序代理防火墙可以配置成允许来自内部网络的任何连接，它也可以配置成要求用户认证后才建立连接。要求认证的方式有只为已知的用户建立连接的限制，为安全性提供了额外的保证。如果网络受到危害，这个特征使得从内部发动攻击的可能性大大减少。

4. NAT

讨论到防火墙的主题，就一定要提到有一种路由器，尽管从技术上讲它根本不是防火墙。网络地址转换(NAT)协议将内部网络的多个 IP 地址转换到一个公共地址发送到 Internet 上。

NAT 经常用于小型办公室、家庭等网络，多个用户分享单一的 IP 地址，并为 Internet 连接提供一些安全机制。

当内部用户与一个公共主机通信时，NAT 追踪是哪一个用户发送的请求，修改传出的包，这样包就像是来自单一的公共 IP 地址，然后再打开连接。一旦建立了连接，在内部

计算机和 Web 站点之间来回流动的通信就都是透明的了。

当从公共网络传来一个未经请求的传入连接时，NAT 有一套规则来决定如何处理它。如果没有事先定义好的规则，NAT 只是简单地丢弃所有未经请求的传入连接，就像包过滤防火墙所做的那样。

可是，就像对包过滤防火墙一样，可以将 NAT 配置为接受某些特定端口传来的传入连接，并将它们送到一个特定的主机地址。

3.2.2 防火墙的技术

传统意义上的防火墙技术分为 3 大类：包过滤(Packet Filtering)、应用代理(Application Proxy)和状态监视(Stateful Inspection)。无论一个防火墙的实现过程多么复杂，归根结底都是在这 3 种技术的基础上进行功能扩展的。

1. 包过滤技术

包过滤是最早使用的一种防火墙技术，它的第一代模型是静态包过滤(Static Packet Filtering)，使用包过滤技术的防火墙通常工作在 OSI 模型中的网络层(Network Layer)上，后来发展更新的动态包过滤(Dynamic Packet Filtering)增加了传输层(Transport Layer)，简而言之，包过滤技术工作的地方就是各种基于 TCP/IP 协议的数据报文进出的通道，它把这两层作为数据监控的对象，对每个数据包的头部、协议、地址、端口、类型等信息进行分析，并与预先设定好的防火墙过滤规则(Filtering Rule)进行核对，一旦发现某个包的某个或多个部分与过滤规则匹配并且条件为“阻止”的时候，这个包就会被丢弃。适当地设置过滤规则可以让防火墙工作得更安全有效，但是这种技术只能根据预设的过滤规则进行判断，一旦出现一个没有在设计人员意料之中的有害数据包请求，整个防火墙就形同虚设了。人们也许会想，自行添加不行吗？但是别忘了，应该为普通计算机用户考虑，并不是所有人都了解网络协议，如果防火墙工具出现了过滤遗漏问题，他们只能等着被入侵了。一些公司采用定期从网络升级过滤规则的方法，这个创意固然可以方便一部分家庭用户，但是对相对比较专业的用户而言，却不见得就是好事，因为他们可能会有根据自己的机器环境设定和改动规则，如果这个规则刚好和升级后的规则发生冲突，用户就该郁闷了，而且如果两条规则冲突了，防火墙会不会当场崩溃？也许就因为考虑到这些因素，至今没见过有多少个产品会提供过滤规则更新功能的，这并不能和杀毒软件的病毒特征库升级原理相提并论。为了解决这种鱼与熊掌的问题，人们对包过滤技术进行了改进，这种改进后的技术称为动态包过滤(市场上存在一种基于状态的包过滤防火墙技术，即 Stateful-based Packet Filtering，它们其实是同一类型)，与它的前辈相比，动态包过滤功能在保持着原有静态包过滤技术和过滤规则的基础上，会对已经成功与计算机连接的报文传输进行跟踪，并且判断该连接发送的数据包是否会对系统构成威胁，一旦触发其判断机制，防火墙就会自动产生新的临时过滤规则或者对已经存在的过滤规则进行修改，从而阻止该有害数据的继续传输，但是由于动态包过滤需要消耗额外的资源和时间来提取数

据包内容进行判断处理，所以与静态包过滤相比，它会降低运行效率，但是静态包过滤已经几乎退出市场了，能选择的，大部分也只有动态包过滤防火墙了。

2. 应用代理技术

由于包过滤技术无法提供完善的数据保护措施，而且一些特殊的报文攻击仅仅使用过滤的方法并不能消除危害（如 SYN 攻击、ICMP 洪水等），因此人们需要一种更全面的防火墙保护技术，在这样的需求背景下，采用应用代理（Application Proxy）技术的防火墙诞生了。代理服务器作为一个为用户保密或者突破访问限制的数据转发通道，在网络上应用广泛。一个完整的代理设备包含一个服务端和客户端，服务端接收来自用户的请求，调用自身的客户端模拟一个基于用户请求的连接到目标服务器，再把目标服务器返回的数据转发给用户，完成一次代理工作过程。应用代理防火墙，实际上就是一台小型的带有数据检测过滤功能的透明代理服务器（Transparent Proxy），但是它并不是单纯地在一个代理设备中嵌入包过滤技术，而是一种被称为应用协议分析（Application Protocol Analysis）的新技术。

“应用协议分析”技术工作在 OSI 模型的最高层——应用层上，在这一层里能接触到的所有数据都是最终形式，也就是说，防火墙“看到”的数据和用户看到的是一样的，而不是一个个带着地址端口协议等原始内容的数据包，因而它可以实现更高级的数据检测过程。整个代理防火墙把自身映射为一条透明线路，在用户方面和外界线路看来，它们之间的连接并没有任何阻碍，但是这个连接的数据收发实际上是经过了代理防火墙转向的，当外界数据进入代理防火墙的客户端时，“应用协议分析”模块便根据应用层协议处理这个数据，通过预置的处理规则查询这个数据是否会产生危害，由于这一层面对的已经不再是组合有限的报文协议，所以防火墙不仅能根据数据层提供的信息判断数据，更能像管理员分析服务器日志那样“看”内容辨危害。而且由于工作在应用层，防火墙还可以实现双向限制，在过滤外部网络有害数据的同时也监控着内部网络的信息，管理员可以配置防火墙实现一个身份验证和连接时限的功能，进一步防止内部网络信息泄漏的隐患。最后，由于代理防火墙采取是代理机制进行工作，内外部网络之间的通信都需先经过代理服务器审核，通过后再由代理服务器连接，根本没有给分隔在内外部网络两边的计算机直接会话的机会，可以避免入侵者使用“数据驱动”攻击方式（一种能通过包过滤技术防火墙规则的数据报文，但是当它进入计算机处理后，却变成能够修改系统设置和用户数据的恶意代码）渗透内部网络，可以说，应用代理是比包过滤技术更完善的防火墙技术。

但是，似乎任何东西都不可能逃避墨菲定律的制约，代理型防火墙的结构特征偏偏正是它最大的缺点，由于它是基于代理技术的，通过防火墙的每个连接都必须建立在为之创建的代理程序进程上，而代理进程自身是要消耗一定时间的，更何况代理进程里还有一套复杂的协议分析机制在同时工作，于是数据在通过代理防火墙时就会不可避免地发生数据迟滞现象，换个形象的说法，每个数据连接在经过代理防火墙时都会先被请进保安室喝杯茶搜搜身再继续赶路，而保安的工作速度并不能很快。代理防火墙是以牺牲速度为代价换取了比包过滤防火墙更高的安全性能的，在网络吞吐量不是很大的情况下，也许用户

不会察觉到什么，然而到了数据交换频繁的时刻，代理防火墙就成了整个网络的瓶颈，而且一旦防火墙的硬件配置支撑不住高强度的数据流量而罢工，整个网络可能就会因此瘫痪了。所以，代理防火墙的普及范围还远远不及包过滤型防火墙，所以就目前整个庞大的软件防火墙市场来说，代理防火墙很难有立足之地。

3. 状态监视技术

这是继包过滤技术和应用代理技术后发展的防火墙技术，它是 CheckPoint 技术公司在基于包过滤原理的动态包过滤技术发展而来的，与之类似的有其他厂商联合发展的深度包检测(Deep Packet Inspection)技术。这种防火墙技术通过一种被称为状态监视的模块，在不影响网络安全正常工作的前提下采用抽取相关数据的方法对网络通信的各个层次实行监测，并根据各种过滤规则做出安全决策。

状态监视技术在保留了对每个数据包的头部、协议、地址、端口、类型等信息进行分析的基础上，进一步发展了会话过滤(Session Filtering)功能，在每个连接建立时，防火墙会为这个连接构造一个会话状态，里面包含了这个连接数据包的所有信息，以后这个连接都基于这个状态信息进行，这种检测的高明之处是能对每个数据包的内容进行监视，一旦建立了一个会话状态，则此后的数据传输都要以此会话状态作为依据，例如：一个连接的数据包源端口是 8000，那么在以后的数据传输过程里防火墙都会审核这个包的源端口还是不是 8000，否则这个数据包就被拦截，而且会话状态的保留是有时间限制的，在超时的范围内如果没有再进行数据传输，这个会话状态就会被丢弃。状态监视可以对包内容进行分析，从而摆脱了传统防火墙仅局限于几个包头部信息的检测弱点，而且这种防火墙不必开放过多端口，进一步杜绝了可能因为开放端口过多而带来的安全隐患。

由于状态监视技术相当于结合了包过滤技术和应用代理技术，因此是最先进的，但是由于实现技术复杂，在实际应用中还不能做到真正的完全有效的数据安全检测，而且在一般的计算机硬件系统上很难设计出基于此技术的完善防御措施。

4. 技术展望

防火墙作为维护网络安全的关键设备，在目前采用的网络安全的防范体系中，占据着举足轻重的地位。伴随计算机技术的发展和网络应用的普及，越来越多的企业与个体都遭遇到不同程度的安全难题，因此市场对防火墙的设备需求和技术要求都在不断提升，而且越来越严峻的网络安全问题也要求防火墙技术有更快的提高，否则将会在面对新一轮入侵手法时束手无策。

多功能、高安全性的防火墙可以让用户网络更加无忧，但前提是要确保网络的运行效率，因此在防火墙发展过程中，必须始终将高性能放在主要位置，目前各大厂商正在朝这个方向努力，而且丰富的产品功能也是用户选择防火墙的依据之一，一款完善的防火墙产品，应该包含访问控制、网络地址转换、代理、认证、日志审计等基础功能，并拥有有自己特色的安全相关技术，如规则简化方案等，明天的防火墙技术将会如何发展，请拭目以待。

3.2.3　防火墙的功能

1. 防火墙是网络安全的屏障

一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性,并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙,所以网络环境变得更安全。例如:防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络,这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击,如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置,能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比,防火墙的集中安全管理更经济。例如:在网络访问时,一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上,而是集中在防火墙上。

3. 对网络存取和访问进行监控审计

如果所有的访问都经过防火墙,那么,防火墙就能记录下这些访问并作出日志记录,同时也能提供网络使用情况的统计数据。当发生可疑动作时,防火墙能进行适当的报警,并提供网络是否受到监测和攻击的详细信息。另外,收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击,并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分,可实现内部网重点网段的隔离,从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者,隐私是内部网络非常关心的问题,一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣,甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节的如 Finger、DNS 等服务。Finger 显示了主机上所有用户的注册名、真名,最后登录时间和使用的 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度,这个系统是否有用户正在连线上网,这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络中的 DNS 信息,这样一台主机的域名和 IP 地址就不会被外界所了解。

除了安全作用,防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN,将企事业单位在地域上分布在全世界各地的 LAN 或专用子网,有机

地联成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

3.3 防火墙相关知识

下面介绍防火墙的发展历程。

第一代防火墙技术几乎与路由器同时出现，采用了包过滤（Packet Filter）技术。图 3-2 所示为防火墙技术的简单发展历史。

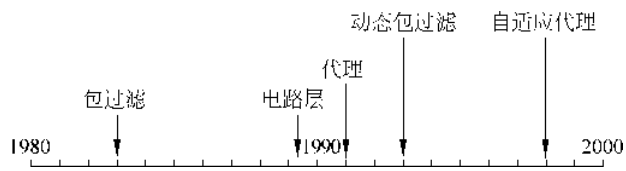

图 3-2 防火墙技术的简单发展历史

1. 第一代：静态包过滤

静态包过滤防火墙根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括 IP 源地址、IP 目标地址、传输协议（TCP、UDP、ICMP 等）、TCP/UDP 目标端口、ICMP 消息类型等。包过滤类型的防火墙要遵循的一条基本原则是最小特权原则，即明确允许那些管理员希望通过的数据包，禁止其他的数据包。主要针对网络层，如图 3-3 所示。

图 3-3 简单包过滤防火墙

防火墙最基本的功能：根据 IP 地址作转发判断。由于黑客可以采用 IP 地址欺骗技术，伪装成合法地址的计算机就可以穿越信任这个地址的防火墙了。根据地址的转发决策机制还是最基本和必需的，另外要注意的是，不要用 DNS 主机名建立过滤表，对 DNS 的伪造比 IP 地址欺骗要容易得多。

2. 第二代：动态包过滤

动态包过滤防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的