第18章 防 火 墙

作者：Tim Parker

本章内容包括：

- 使网络安全
- 使用防火墙
- 安全服务
- 建造自己的防火墙
- 使用商业防火墙软件

如果没有听说过诸如防火墙、网关或代理服务器等这些术语，讨论网络、互联网络和Internet在一定程度上将是不可能的。读者已经了解了网关及其功能，但是本书还未涉及到有关防火墙和代理服务器的内容。虽然防火墙和 TCP/IP实际上并没太大关系，但是它们可以用于基于TCP/IP的网络和Internet。

因此，花一点时间来解释防火墙和代理服务器的功能，以及它们在 TCP/IP网络内工作的过程是值得的。本章和第19章将讨论如下问题：保护网络、隐藏信息以及防止数据破坏。

18.1 使网络安全

防火墙和代理服务器，以及加密和认证 (下一章内容)，都是为了保护数据安全而设计的。如果用户的电子邮件或网关中没有有价值的数据，为什么还要为安全问题而困扰呢？原因很简单：如果用户联接到Internet，那么Internet就有一条到用户的联接。在用户做 double-take之前，要考虑其结果意味着，如果条件合适的话， Internet上的某个人可以访问用户网络。如果用户网关没有设置安全，世界上任何一个和 Internet相联的人都会使用TCP/IP经过网关到达用户网络上的任何一台计算机。用户可能在网络的某个地方存储了不想让其他人看到的数据，因此要考虑安全问题来防止Internet上的其他用户访问网络内部。

设置网络安全实际上是想努力达到两个保护目的 (间接地达到第三个目的)。两个保护是指数据保护(存储在网络中)和设备保护(和网络相联的任何东西)。如果黑客访问设备，可能会造成损害。对数据而言也是一样。用户不想让自己的重要文件作为电子邮件附件散布到整个Internet上。间接的保护是指声誉保护，既指个人声誉，也指公司声誉。像 IBM和HP这样的大公司，如果它们的所有内部文档可以自由获得，看起来有点不妙。

一个最常见的安全问题前面已经提及 —— 某个人通过Internet访问用户网络。这样非授权的入侵正是要求良好安全机制的主要原因。入侵者或黑客能侵入用户网络内部、搜索用户数据、对数据进行任意修改，并且可以导致用户系统上的物理损坏。

黑客可以通过多种方式侵入网络内部，从利用已知的操作系统和应用程序漏洞到用甜言蜜语套得用户的登录名和口令。网络安全的基本作用 (也就是防火墙的基本作用)就是防止非授权入侵。

另一个安全问题称为服务拒绝。当黑客妨碍用户正确使用自身计算机时就发生这种攻击。

服务拒绝有多种形式。Internet上能找到的典型例子是湮灭一种服务 (如email、FTP站点或Web服务器)。湮灭意味着向这种服务发大量的数据使得服务器崩溃或使服务时间加长。黑客通常使用电子邮件湮灭，在这种攻击中，每隔一小时就有成千上万的电子邮件消息发送到目标电子邮件服务器上。服务器处于忙乱状态最终使邮件系统不可用。相同的技术适合于绝大多数的TCP/IP程序，如FTP、Telnet以及Web服务器。服务拒绝的另一方面和重路由有关—不是访问一台机器上的某个特定服务，而是被重路由到另一地方。

有几种方法用来保护用户网络、数据以及服务。许多人依靠匿名或隐藏技术。原因是如果不知道用户网络及其内容，网络就是安全的。当然，这是错误的安全措施，因为有许多方法可以让用户并不能隐藏太长时间。很自然的一个假设是：如果用户认为黑客不会找到他们感兴趣的数据，就不会打扰他。绝大多数黑客想要做的就是要找到用户数据。

最广泛使用的安全形式称为主机安全，主机安全对网络上的每台机器单独进行安全保护。当用户设置Windows访问允许权限时，就要依赖于主机安全，对于设置 UNIX文件和目录访问允许权也是这样。虽然主机安全能用于保护单机安全，但是认为单机安全整个网络就安全的想法是不正确的。整个网络可能对黑客开放。同时，因为主机安全并不适合于所有机器，黑客可以利用一个弱安全机器上的服务达到访问强安全机器的目的，而不会出现任何问题。

防火墙的作用

我们应该注意的安全级别应该是网络安全。这意味着首先要使所有到网络的访问点安全，之后再依赖内部主机安全。网络安全的重要组成部分是防火墙 —— 一台作为网络和 Internet之间接口的机器，主要和安全相关。防火墙有几项功能：

- 限制只能访问网络的一些地点。
- 防止非授权用户得到网络访问权。
- 强制流量只能从特定的安全点去向 Internet。
- 防止服务拒绝攻击。
- 限制Internet用户在网络上的行为。

防火墙并不限于网络和 Internet的联接。防火墙也用于远程访问服务器 (拨入访问)和网络与网络的联接。防火墙的全部思想在于在一个或多个特定点提供进出网络的通道，而在这些地方设置了访问和服务控制。

18.2 使用防火墙

许多人认为防火墙是一台机器，有一些网络是这种情况。专用的单机防火墙仅仅作为网络的安全网关。另一种情况是，一台机器可以只运行专用的防火墙软件，而不运行其他软件。然而，防火墙这一术语和所执行的功能关系更紧密一些，而不是指物理设备。防火墙可以由一起工作的几台机器组成，共同控制网络和 Internet之间的联接。许多不同的程序可以用于提供这些防火墙服务，防火墙也可能执行许多任务，而不仅仅限于监控网络访问。

防火墙并不是十分安全的。防火墙一般是脆弱的，因为黑客可以利用防火墙设计中的漏洞。而且，防火墙实现通常比较昂贵并需要一些时间来安装和配置。然而，网络从防火墙获得的好处大大超过其问题。

防火墙可以做许多事情。它能为网络提供安全的单访问点。所以用户可以在一个地方改变设置而无需改动每台机器 (比如，可以禁用匿名 FTP)。防火墙能在网络范围内加强安全，比

如防止网络中的每个人都有权访问某些 Internet资源。防火墙并不能为用户做每一件事情，用户确实也需要了解这些限制。防火墙只擅长于网络和 Internet之间的联接。防火墙并不能阻止网络内的一些用户对其他机器进行攻击。防火墙不能保护用户网络免受侵入，如果网络具有其他联接方式，比如一台 Windows PC使用一台调制解调器通过 ISP联到Internet上(联接不经过防火墙，因此绕过了防火墙提供的安全控制)。并且防火墙不能防止许多常见的 Internet问题，如病毒和特洛伊木马。

在一个网络上实现防火墙有两种基本方法：

- 利用基本的网络服务建造自己的防火墙。
- 购买商业产品。

后者容易得多，但花费更多。为 UNIX机开发的典型防火墙软件，至多可以卖到 10 000美元，且服务于小型网络。随着网络尺寸的增长，防火墙软件的费用会成 10倍的增加。购买商业防火墙软件包的好处很简单：绝大部分工作已经为客户做好了。用户只需使用菜单来选择允许和拒绝的服务，防火墙软件会为用户完成具体工作。建造自己的防火墙意味着使用位于网络和Internet之间机器上的设置来执行相同的任务。每一项服务必须手工地设置为允许访问或不允许访问。比如，对一台 UNIX机器而言，这意味着和网络配置文件以及像 /etc/services这样的文件打交道，来拒绝一些网络服务访问请求。建造自己的防火墙会花更长的时间、需要更多专业知识，以及需要多次实验。而另一方面，用户无需花费大量金钱购买防火墙软件。

当通过手工或商业产品安装了防火墙之后，用户就可以获得多方面的安全保护。是否选择所有实现依赖于用户本身。然而，用户应该知道其中的一些方面，如代理服务器和报文过滤器。下面几节会更详细地讨论这些技术。

18.2.1 代理服务器

代理服务器位于网络和 Internet之间，接收、分析服务请求，并在允许的情况下对其进行转发。代理服务提供服务的替代连接，就像一个代理一样。比如，网络内部的一个用户想要远程登录到Internet上的一台主机，代理服务器会接收用户请求，决定是否准许其到远程的连接，之后建立自身与远程目标主机之间及自身与用户之间的 Telnet会话。作为中介，代理服务器隐藏了关于用户的一些信息，但仍然允许服务通过它来进行。代理服务器处理服务和应用，因此通常称为应用级网关。

为什么使用代理服务器？假设用户正在从事一项高度保密的项目，那么用户就想对外(Internet)隐藏关于其所在网络的信息 —— IP地址、用户登录名等等。如果用户通过 Internet建立了与远程主机的 telnet会话，用户的IP地址就会包含在报文中被传输。得到 IP地址，黑客就能确定用户网络的大小，特别是当他们看到大量不同的 IP地址经过时。代理服务器会把用户地址改成自己的地址，使用一个内部表来解析到正确目的地的进出报文。对于外面的人而言，只有一个IP地址(代理服务器的IP地址)可见。

代理服务器总是用软件来实现，并且不必是防火墙软件包的组成部分，但一般的防火墙软件包却包含代理服务器。绝大多数商业防火墙包含代理服务功能。绝大多数代理服务器软件不仅仅作为用户的代理；它们也能控制使用哪个应用并且能阻止一些进出的数据。

如果用户正在建造自己的防火墙，有许多软件包设计允许用户来完成这一工作。最有名的是SOCKS，SOCKS允许应用程序和代理变换软件包一起工作。另一个有名的软件包是 TIS

FWTK(可信任信息系统 Internet防火墙开发工具包)，TIS FWTK为许多TCP应用(如FTP和Telnet)提供代理服务器。

18.2.2 报文过滤器

报文过滤器系统允许报文有选择地从用户网络进入 Internet，或从Internet进到用户网络。换句话说，报文过滤器允许一些报文被过滤掉，不被发送，而另一些报文却可以无阻碍地进出网络。报文由创建它们的应用程序类型标识 (正如读者在前面章中所见，一些信息包含在头中)。TCP/IP报文头包含源和目的 IP地址、源和目的端口 (用于识别应用程序)、协议 (TCP、UDP或ICMP)，以及其他信息。如果用户决定阻止所有的 FTP报文进出网络，报文过滤器会检查所有端口号为 20和21的报文，并阻止其通过。报文过滤可以由防火墙软件或路由器进行。在后一种情况下，路由器被称为筛分路由器 (screening router)。

标准路由器和筛分路由器的不同之处在于二者检查报文的方式。普通路由器只是查看 IP地址并把报文发送到至目的地的正确路径上。筛分路由器检查报文头，不仅要决定怎样对其进行路由，还要基于一些规则决定是否应对其进行路由。

读者可能认为通过改变端口号，可绕过报文过滤系统；这在一定程度上是可能做到。然而，由于报文过滤器软件位于用户网络中，它也能决定报文进出的接口，因此，即使 TCP端口不一样，报文过滤软件有时照样可以正确地过滤报文。

用户可以采用多种方式使用报文过滤软件。最常见的用法是简单地阻止一种服务，如 FTP或Telnet。用户也可以指定允许或不允许通过的机器。比如，使用者发现某个特定网络是许多问题的来源，就可以告诉报文过滤软件抛弃所有从那个网络发来的报文，这要依赖于 IP地址。在极端情况下，用户可以阻止所有服务，或只允许一个服务如电子邮件通过过滤器。

18.3 使服务安全

安装防火墙的一个关键是决定哪些服务允许通过网络到 Internet的联接，哪些要受到限制。用户是否打算允许外部网络来的 FTP请求联到内部机器上？如果是 Web请求又如何处理？这一节会仔细地讨论防火墙上使用的基本服务及其主要安全问题。读者可以基于自身网络要求决定是否应该允许或拒绝服务。

大多数网络防火墙缺省设置，允许 6种服务通过：

- 电子邮件(SMTP)
- HTTP(万维网访问)
- FTP
- Telnet(远程访问)
- Usenet(NNTP)
- DNS(主机名查找)

这6项服务不是没有安全问题，这将在以下几节中看到。

18.3.1 电子邮件(SMTP)

电子邮件是Internet上使用最广泛的服务，并且用户不大会限制通过防火墙的电子邮件访问。面对黑客攻击，电子邮件并不脆弱，其问题主要出在电子邮件附件可能包含病毒或其他

恶意程序。这并不意味着电子邮件是安全服务。

大多数邮件系统使用简单邮件传输协议 (SMTP)实现。SMTP自身没有安全问题，但处理SMTP的服务器存在安全问题。SMTP服务器处理邮件时，会作为超级用户或邮件寻址的目的用户身份出现。一名聪明的黑客会利用允许权的这一变化。更进一步，大多数常见的 SMTP服务器只发送邮件，通常运行于UNIX环境下。发送邮件程序有许多已知的安全漏洞。这些漏洞必须由管理员通过安装补丁程序来防止被黑客利用。

18.3.2 HTTP：万维网

实际上，世界上的每个网络都具有 Internet访问权，而且用户很可能对内部网络访问Internet时通过防火墙不作任何限制。允许从内部网络访问 Web并不会造成很大的安全危险，而对下载的文件或带有恶意设计的Java小程序却要小心，接收机上最好有病毒检测程序。

重要的是允许Internet用户进入用户网络访问Web服务器，这会引起真正的安全问题，避免安全问题的最好方法是使用一台单独的主机，不经过防火墙提供 Web服务。现在绝大多数可用的Web服务器都很安全(虽然有一些已知的能被黑客所利用的漏洞)。另一个重要的安全考虑是加载在服务器上的任何扩展功能，如通用网关接口 (CGI)，必须注意文件访问权安全。

18.3.3 FTP

文件传输协议(FTP)在Internet上广泛使用，在安全方面与电子邮件差不多。然而，具有从Internet下载文件的功能意味着所下载的文件可能含有各种程序，如病毒和欺骗程序，这样的程序会把网络信息发送给黑客。FTP服务自身相当安全，然而有许多已知的漏洞，系统管理员必须要通过安装补丁程序来弥补，安装的补丁程序要依赖于 FTP版本。

FTP更重要的问题是匿名FTP，匿名FTP允许任何人以匿名用户名访问FTP服务器。对FTP服务器的匿名访问必须要严格控制，否则一名知识丰富的黑客能很容易地利用服务器。

最后，用户不应允许在网络和 Internet接口处使用普通FTP(TFTP)。只有很少的一些应用程序使用TFTP并且这些程序不大可能在网络范围内使用。

18.3.4 Telnet

Telnet广泛使用，允许用户和位于远处的另一台机器相联，操作起来就像直接相联一样。Telnet程序和协议本身是相当安全的，不易受黑客攻击，但是 Telnet有一个主要的不足：所有的信息以非加密的方式传送。Telnet是以明文的方式发送登录名和口令，这样使得黑客可以解释和利用这些信息。认证协议可以用于解决这一问题，但是 Telnet经常被各种方式所利用，因为所有信息都要往返于客户机和服务器之间。

Berkeley程序(rlogin、rsh、exec等等)经常用于代替Telnet。这个程序依赖于可信任的主机，但这种方法并不是在整个 Internet上都有效。Berkeley r-系列程序非常容易被黑客攻击，很不安全，并且不应允许这些程序通过防火墙。

18.3.5 Usenet:NNTP

网络新闻传输协议 (NNTP)是最广泛使用的用于发送和接收新闻组邮件的方式。如果用户想在网络中接受这一协议，就必须仔细地规划，考虑 NNTP的安全性。NNTP非常容易被黑客

所利用，从而对内部网络进行访问。幸运的是，使 NNTP安全很容易，因为NNTP主机之间的通信在每次会话中几乎都是相同的。

对新闻用户，特别是大型组织内的用户而言，一个更重要的问题是要让内部的私有新闻不要传输到Internet上。用户也可以限制传进来的新闻为某种特定类型。可以配置 NNTP，使某一新闻组被接收或被拒绝。

18.3.6 DNS

DNS是大型网络的完整组成部分，运行在 Internet主机上用于查找。DNS自身通常没有安全问题，但是DNS所依赖的协议可能成为问题。可以设置认证方法来验证请求的真实性且没有误导。绝大多数情况下，DNS是相当安全的。

18.4 建造用户自己的防火墙

用户能够建造自己的 Internet防火墙，但是这需要关于操作系统和 TCP/IP的丰富知识。Windows 95和Windows 98由于操作系统自身的设计提供很少的防火墙功能。UNIX和Windows NT好一些，但是Windows NT比UNIX更难配置。

在大多数情况下，用户不想在网络中使用的服务，就应停止，并且要配置防火墙防止黑客得到防火墙自身的访问权。即使知道什么是必须的，建造自己的防火墙也需要一段时间才能完成。

18.5 使用商业防火墙软件

在市场上有许多防火墙软件包，并且这些软件包通常非常贵。一个比较好的防火墙 (作者使用的一个软件包)是Cyberguard公司的Cyberguard软件。这个防火墙可以运行在 Windows NT或UNIX平台上(开始在UNIX下，最近移植到NT上)。Cyberguard受欢迎因为它不仅是曾被测试过的一个最安全的防火墙，同时也因为它很容易安装、配置、管理。

注意 为了得到关于Cyberguard更多的信息，可以访问公司的 Web站点http:// www.cyberguard.com。读者可以发现关于软件包的描述以及几本白皮书。要想得到关于防火墙和安全问题的信息，访问CERT(计算机紧急问题应答组)站点：http://www.cert.org。

在Windows NT服务器上安装和配置Cyberguard特别容易，简单的网络配置可以不到 15分钟就能完成。Cyberguard工作在双穴主机上，一条连接到内部网，一条连接到 Internet(既可以是直接相连也可以通过ISP)。在安装软件包的时候，Cyberguard让用户在三种缺省的安全配置中选择一种，如图18-1所示。

在选择了一种缺省设置之后，用户可以通过不同的屏幕检查所有的设置并验证这些选项。图18-2显示了一个设置屏幕，通过选择可以影响 NT帐号和口令。

选择缺省设置之后，Cyberguard会重启Windows NT服务器，之后保护就起作用了。作为管理员，可以修改防火墙的任何一方面设置，图 18-3显示了报文过滤规则设置屏幕可以让管理员指出什么样的报文可以通过，什么样的报文不允许通过。正如读者所见，Cyberguard很好地利用了Windows对话框简化了通常复杂的过程。

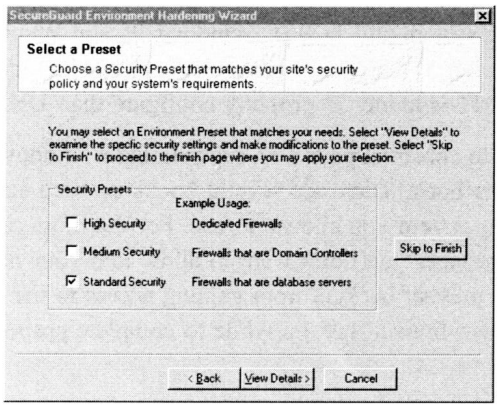

图18-1 3种Cyberguard缺省设置包含了大多数Windows NT设置，这个界面称为SecureGuard

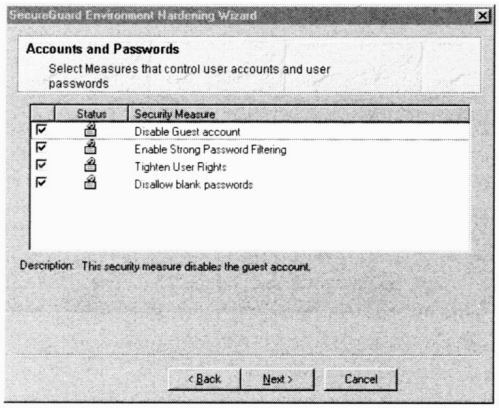

图18-2 选择一个Cyberguard缺省设置会出现一系列这样的界面用于修改特定项

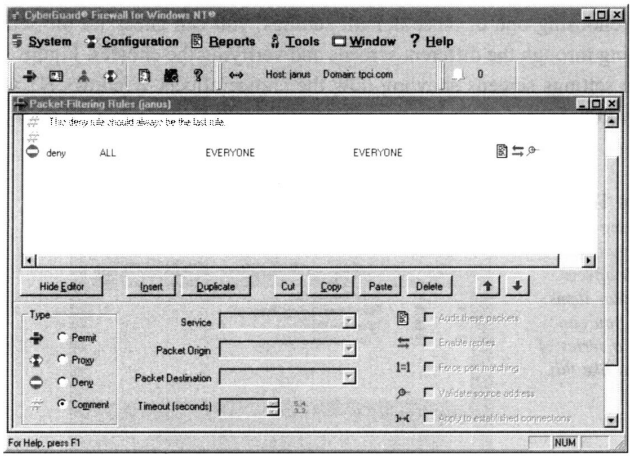

图18-3 Cyberguard报文过滤对话框允许用户设置对进出报文的处理

代理服务器的行为也可以容易地设置。图 18-4显示了Cyberguard的代理服务器对话框。选择使用的代理就是简单地选择列表中的一项。在这个图中，正在设置 FTP代理服务。

Cyberguard所擅长的另一方面是DNS服务。如图18-5所示，用户可以容易地设置DNS，甚至可以指定网络中的区。

有许多其他的防火墙商业软件包。许多的网络相关杂志中有关于防火墙常规的测试结果。如果用户正寻找商业防火墙，要仔细进行研究，因为防火墙的质量有很大不同，价格也相差很大。

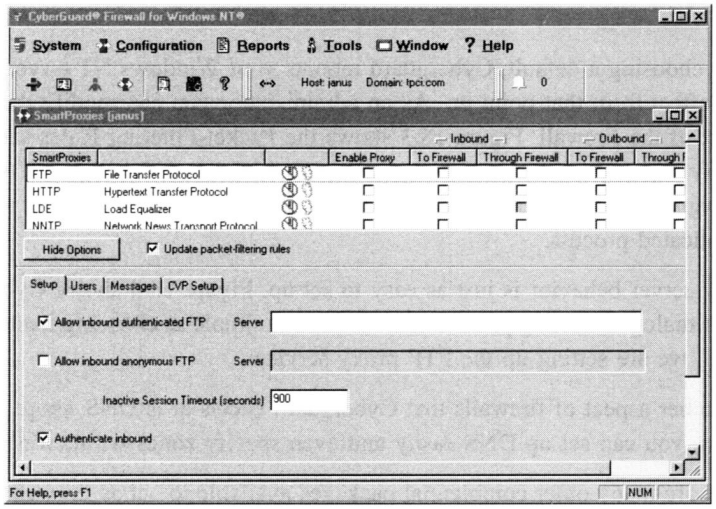

图18-4 Cyberguard代理服务窗容易理解，使用简单

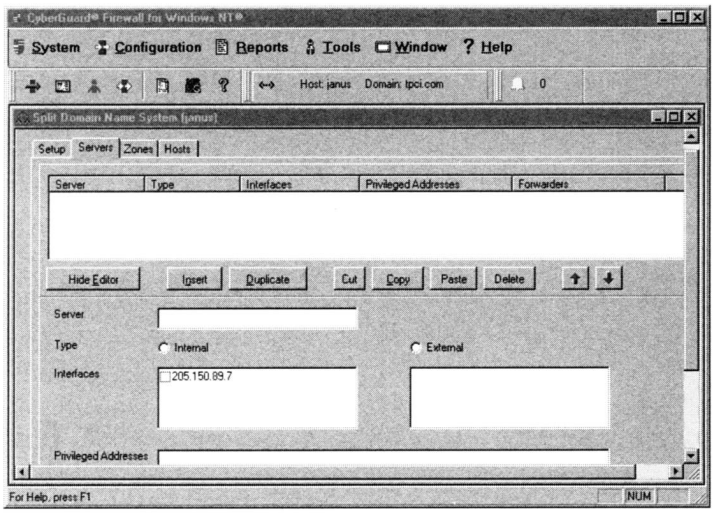

图18-5 通过Cyberguard GUI设置DNS

18.6 小结

这一章解释了什么是防火墙，防火墙的功能及其基本作用。用户已经看到代理服务器和报文过滤器是如何工作的。下一章会继续 IP安全这一内容，在下一章读者会了解包括密码和认证在内的一些主题。