第3章

软件防火墙、小型办公室防火墙和企业防火墙

章节目标

通过阅读本章内容以及完成练习，将能够做如下工作：

- 简述基本硬件及软件防火墙的种类。
- 了解个人防火墙的重要性。
- 区分流入与流出流量。
- 认清 IPTABLES 及访问控制列表(ACL)的功能。
- 用程序及外部扫描器测试防火墙。

3.1 概述

当今市场上可用的防火墙数量众多，使得选择一款防火墙变得很困难。本章概括主要的硬件防火墙及软件防火墙，以帮助用户了解可用的产品范围。虽然本书将会着重于开源 LEAF Bering 防火墙，但它并不适于所有环境。在具有很多要求的大型公司中，通常企业防火墙是唯一的实践解决方案。

访问控制列表及 IPTABLES 是决定网络数据包被接受还是拒绝的规则，是很多防火墙的基本构件。这些概念的理解对于成功配置防火墙是必须的，因此这里对这些概念的介绍将会为用户做好后续章节的准备。

在安装防火墙之前，做出向攻击开放的内部网络端口的基准报告是有益处的。有几种工具能帮助用户扫描网络，以确定哪个端口向 Internet 开放，能够确定防火墙是否正确配置及是否履行其既定任务。本章中将会提供几种在线及开源工具，用于扫描网络开放端口。

3.2 硬件和软件防火墙

当今市面上有众多的防火墙，并且，随着信息安全需求的增长，定期会出现新的防火墙。除了传统的企业防火墙，防火墙特性被合并到很多网络设备中，并且现在大部分操作系统还提供个人防火墙。对于想了解何种设备将提供所需要的保护级别的用户和管理员而言，可用防火墙解决方案的数量都是一个挑战。

防火墙的主要种类如下：

- 作为防火墙的路由器(数据包过滤器)。
- 独立代理，或者应用防火墙。
- 企业防火墙。
- 小型办公室/家庭办公室(Small Office/Home Office，SOHO)防火墙。
- 个人防火墙/基于主机的软件防火墙。

本节中简要介绍这些种类的防火墙。

为了选择适当的防火墙技术，应当牢记下列因素：

- 预算。
- 组织的规模及网络节点的数量。
- 所需要的保护级别。
- 入侵及数据丢失的风险。
- 所需的制造商支持级别。
- 安装及管理防火墙所需的时间。

当建立安全基础结构时，需要为网络安全考虑分层的实现方法。换句话说，可能有多种网络设备提供了用户计算机与 Internet 之间的某种级别的防火墙保护。这种分层的网络安全实现方法通常称为深度防御(defense in depth)或者深度安全(Northcutt 2003；Miles 2004)。随着对每一个防火墙种类的描述，知道防火墙如何与其他防御层如何联合提供更加完整的网络及计算机安全环境是很重要的。

3.2.1 防火墙作为路由器

路由器是一种具有两个或更多网络接口的设备，对每一个到达接口的数据包，它确定其应该输出的接口。虽然路由器不被认为是防火墙，但是大多数路由器都包含有过滤流入及流出数据包的功能。路由器检查数据包的首部，在流量进入网络时提供初始防御层。图 3.1 演示了在公司网络边缘将公司网络连接至 Internet 的作为边界设备的路由器。虽然路由器仅仅提供了无状态检查，但某些流量是恶意的，并且绝不应该通过此边界路由器。因此，该路由器应该配置为拒绝或者丢弃这些最具危险性的网络流量。

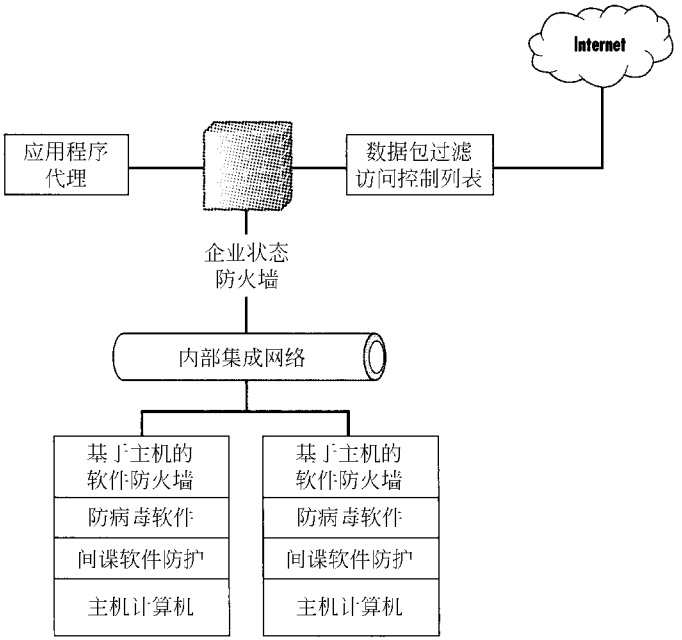

图 3.1　网络图：路由器及企业防火墙

路由器使用访问控制列表(ACL)查看每一个进入及离开给定路由器接口的数据包的 IP 首部信息。管理员必须创建一个列表来过滤流入流量，并且创建一个单独的列表来过滤流出流量。不要求一个接口既包含输入规则又包含输出规则；然而，如果一个端口含有其中一个，那么它通常会含有另一个。通过在路由器中配置访问控制列表，即应用了第一层防御。访问列表将保证尽可能最早拒绝某种流量再进入网络。

ACL 是实用的，但既然路由器不是被设计为完成网络防火墙功能，它们就不含有良好设计的更新控制列表的界面，这样使得使用路由器用于进一步的初始层防御变得不方便。随着 ACL 中条目数量的增长，管理该列表所需要的时间也在增加。不恰当的访问列表配置也能影响路由器的性能，所以，考虑在路由器中放置何种规则是重要的。

因此，路由器应该用于提供对不应进入网络的恶意及欺骗性网络流量的初始层防；使用另一种工具或产品做其他防火墙功能。

3.2.2　独立代理或者应用程序防火墙

第二层防御通常包括应用防火墙或者代理(proxies)。代理是为诸如 HTTP、SMTP、ARP 或者 FTP 等特定协议量身打造的特殊防火墙。通常，通过缓存结果，及过滤发往应被阻塞的服务器的请求。或可能提供恶意内容的服务器请求，代理服务器提高性能。Squid (www. squid-cache. org)开源代理服务器可以与本书所用的防火墙一起使用。

这种类型防火墙有一个很好的实例，就是 Web 服务器代理。所有来自于内部网络上的客户机，发送至 80 端口上的 Web 服务请求都被送到代理中。该代理可能检查 HTTP 协议载荷的内容(通常是对一个 Web 页面的 GET 请求)以保证请求的安全性。如果该请求通过了各种检测，就会转发至实际的 Web 服务器上。既然代理服务器实际上向 Web 服务器发送该请求，而不是客户机，所以响应也送回至代理服务器。接着，代理服务器验证该数据包是有效的 HTTP 响应，检查负载中的恶意代码，并且向内部网络中的客户机发送该数据包。

现在很多防火墙内置有代理特性，有时也称为应用程序网关或者内容过滤功能。它们比代理服务器更进一步，并且在负载内部查找单词、短语或恶意脚本以决定是允许还是拒绝该流量。

3.2.3 企业防火墙

虽然本书的重点内容是开源防火墙，但是，理解商用企业防火墙的重要性也是很重要的。企业防火墙执行了一系列广泛的功能，并且提供了管理界面，以协助更新和维护防火墙的日常任务。企业防火墙的设计基础是作为网络安全关口。这些产品提供了在很多开源解决方案中不曾出现的增强特性、管理能力及专有选项功能。当选择企业防火墙时，需要认真评估该组织的需求，及此防火墙如何满足这些需求。选择过程不应仅仅包含技术能力，还包含对问题的支持及响应时间。

当前市场上有几款企业防火墙，它们分为软件防火墙与硬件防火墙。用户购买软件防火墙并在维护的硬件上安装该软件。硬件防火墙通常是网络设备，生产商在一个单独的、集成的包装箱中提供该硬件及其软件。如果有配置硬件的资深经历，并且喜欢加载自己的软件，那么一款软件防火墙也许是最好的选择。如果用户更愿意依靠制造商为硬件及软件提供支持，那么，一款硬件防火墙将会提供更加彻底的解决方案。

下面提供了当前可用的很多企业级硬件及软件防火墙。

- 软件防火墙(运行于现有的计算机上)。
  - Checkpoint Firewall 1
  - Microsoft ISA Server
  - Symantec Enterprise
- 硬件防火墙(专用设备)。
  - Cisco PIX 防火墙
  - Nokia(运行 Checkpoint Firewall 1)
  - SonicWall
  - NetScreen
  - Watchguard

对于任何防火墙解决方案，企业防火墙配置是关键。大多数企业防火墙依赖于规则的配置，并且，如果未经适当培训，配置会非常复杂难于理解。因而，培训是使防火墙发挥最大

作用的要点。

最后，企业防火墙可能十分昂贵，这取决于网络规模的大小。因此，认真分析特性是很重要的。

3.2.4　SOHO 防火墙

随着远程通信的不断流行，很多人在家庭中建立了办公室。小型办公室/家庭办公室(SOHO)路由器能够作为防火墙及路由器，为家庭网络提供第一层安全防御。SOHO 防火墙设备，有时称为个人防火墙设备(Personal Firewall Appliance；Wack 2002)，可用来保护家庭网络。如图 3.2 所示，SOHO 路由器通常作为家庭网络网关接入 Internet 而起作用。

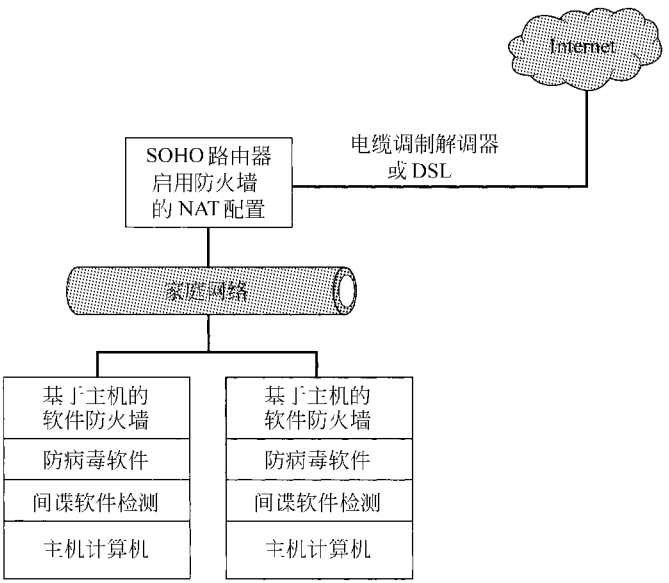

图 3.2　SOHO 防火墙图解

作为 SOHO 防火墙及企业防火墙的 Linux 防火墙。开源 Linux 防火墙在 SOHO 中开始流行。有了对作为 Linux 内核一部分的 netfilter 的介绍，将此功能加入任何基于 Linux 平台的系统中是简单的。对于防火墙功能及路由功能，在 Linux 内核的使用，已经发展到了甚至诸如 Linksys 这样的公司，都在它们的某些产品中使用了内嵌版 Linux 内核的地步(www. linksys. com/support/gpl. asp)。开源、基于 Linux 的防火墙的主要优势是其完整的可配置性及可加入的选项数量。如果某些功能未能提供，在开源社区中，可能会有可用的程序包加入到防火墙中去。

由于其低廉的日常开销及专用目的，这些基于 Linux 的防火墙能够在人们认为不适合使用的计算机——具有低速 CPU 及很少内存的计算机中运行。

在 SOHO 环境中，使用非商业（例如开源）Linux 防火墙的主要劣势是，需要一名能够构造所需的安装媒介（光盘、硬盘等）及具有网络详尽知识的技术专家，来配置这些防火墙。大部分开源 Linux 防火墙软件包都不包含为新接触网络人士准备的界面友好的安装向导，也不包含用于管理防火墙的直观 GUI 界面。

本书的目的是使用一款基于 Linux 的防火墙，介绍网络安全的基本原理，并且帮助用户学习配置防火墙。其余章节将逐渐加深难度指导用户实践，让 SOHO 用户从防火墙中得到最流行的功能。第 7 章将说明 Linux 防火墙如何作为完整的 SOHO 防火墙解决方案而起作用。第 8 章将介绍 VPN 的附加功能，及展示开源 Linux 防火墙如何缩放，以适应企业防火墙的等级。

以小型办公室环境为目的的商用防火墙。SOHO 环境使用的商用防火墙可在几家提供低价（50 美元～300 美元）设备的公司中找到。它们的主要优势是设备的“即插即用”特性及最小限度的、易于理解的配置选项。SOHO 路由器和防火墙的最主要劣势是它们缺乏复杂特性，例如内容检查。面向 SOHO 市场的低价商用防火墙可能缺少 VPN 能力，以及对诸如 NetMeeting H.323 连接这样的高级应用的支持。然而，随着这些设备越来越流行，这些特性甚至会逐渐加入相对不昂贵的设备中。

Linksys、NETGEAR 和 D-Link 是提供面向 SOHO 市场设备的少数制造商。伴随着宽带连接和 802.11 无线网络的提出和增加，这些设备中的很多已经变得十分容易负担。通常，购买这些设备的用户不会检查是否包含防火墙功能，或者仅仅是不开启该功能。大部分制造商当前默认启用防火墙，如果用户不需要该功能时，可以关闭它。

3.3 个人防火墙：基于主机的软件防火墙

使用深度防御（或者分层安全）方法，本地网络可以通过企业防火墙、家庭办公室防火墙或者一组具有限制的路由器 ACL 过滤器，从 Internet 中保护起来。然而，这并不能保护主机不受内部网络攻击。公司职员或者在校生可能在该组织的安全范围内，在任何媒介中引入安全威胁，这些媒介包括下载的光盘映像、软盘及来自其家庭的 ZIP 磁盘。将威胁引入组织中的另一个可能是通过笔记本电脑。随着移动计算的便携性和功能性的提高及宽带连接的广泛出现，笔记本电脑经常在公司防火墙的保护之外被使用。通过这两种情况中的任一种，安全威胁都会被带入到安全范围内。

这些威胁包含病毒及蠕虫，近年来，它们频繁安装特洛伊木马（Trojan horse）或者后门程序，不断寻找其他计算机进行感染。通常，这些特洛伊木马的“主人”载体甚至不清楚他的计算机已经被感染。在这种情况下，任何接入到与被感染计算机相同 IP 子网的计算机都有被攻击的风险。图 3.3 演示了在主机中软件防火墙的重要性。

近几年来，很多大学遇到了这样的情况，学生携带在家里被感染的台式或者笔记本电脑

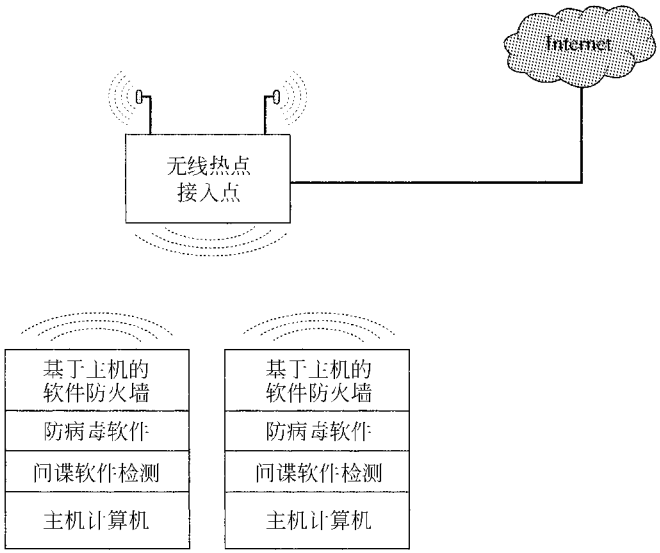

图 3.3　在无线环境中的深度防御

返校，这是内部网络攻击风险的一个体现。实际上，所有大学住宅楼都提供连接至校园网及 Internet 的 IP 子网。这些住宅楼 IP 子网通常为整个建筑物所提供，路由器用来分隔各个 IP 子网。如果一名学生带回一台已感染病毒的计算机，无论大学有多少防火墙及过滤器，如果网络根据建筑物来划分子网，那么，它们都不能阻止该计算机攻击其所在建筑物中的每一台计算机的企图。在同一子网内，其他计算机唯一的防护就是本地安装的个人防火墙。

为了阻止这类情况，所有用户都应当使用软件提供有效保护。建议如下：

- 基于主机的个人防火墙——监控流入连接，仅允许被认可的数据包或者来自已建立连接的返回流量。优秀的软件防火墙还检查并且阻止不恰当的对外连接。
- 防病毒软件——依靠已知的病毒特征数据库，检查计算机中的文件，检测及删除被感染文件。此类软件需要每周更新数据库以保持有效。
- 间谍软件防护软件——阻止弹出式广告、浏览器劫持及其他可能发送个人信息至中央服务器的恶意软件。类似于防病毒软件，此类软件必须定期更新，以检测新的漏洞。
- （可选）入侵检测软件。

这些软件包通常是截然不同的独立软件，但是，很多制造商都提供捆绑所有这三项功能的软件套件。

当潜在有可疑程序活动时，这些安全软件包通常会提供通告消息对话框，如图 3.4 所示。然而，对于最终用户来说，这些消息通常是难以理解的。大多数用户并不是安全专家，当对话框询问一个端口或应用程序是否应被阻塞时，用户并不知道如何应对。用户

对一个对话框的应对，意味着他知道虽然被感染但仍保持安全状态，与新病毒或木马之间的区别。

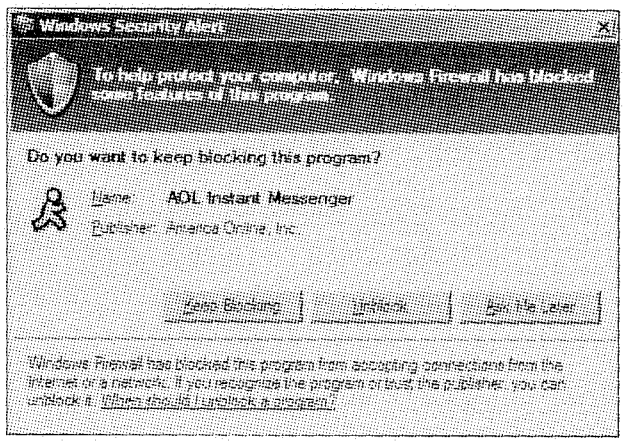

图 3.4 Windows XP Security Alert(安全警告)

与企业防火墙及路由器 ACL 过滤器不同，软件防火墙直接影响最终用户。公司或者组织中负责网络及信息安全的专业人士具有配置必要的软件防火墙规则及培训用户群体的关键职责。

应当告诉用户认真解读来自安全软件的对话框消息。如果该信息与用户知道应当运行的应用程序或者与所单击链接相关联的话，那么允许它就可能是安全的。例如，在图 3.4 中，用户刚刚启动了 AOL Instant Messenger。Windows 防火墙已经检测到了一个进入端口连接，给用户三个选择：Keep Blocking(保持阻塞)，Unblock(不阻塞)或 Ask Me Later(以后再问)。该消息对于用户而言，理解和响应起来都足够简单，但是，如果该应用程序没有被明确标识为 AOL Instant Messenger，用户可能就会发现它很难解读。

另一个难以理解的消息的例子如图 3.5 所示。这个消息来自于 Microsoft Access，它警告不安全的表达式——宏或者其他属于 Access 数据库内部的函数未被阻止。我们使用本例说明两个问题：

- 难以理解的警告消息。
- 没有防火墙能够阻止的安全威胁：蠕虫、病毒或者其他在诸如 Word 或者 Access 等常用 Microsoft Office 应用程序内部的不安全表达式。

由于几个原因，该消息令人感到迷惑。首先，用户被告知要阻止不安全的表达式，必须安装 Jet Expresss Service Pack 8。其次，有关导致可疑问题出现的数据库详细信息："C:\Program Files …Do you want to open this file(你是否想打开此文件)?"。没有 Yes(是)和 No(否)按钮，而是 Hide Help(隐藏帮助)及 Open in Help Window(在帮助窗口中打开)按钮呈现给用户。Yes(是)和 No(否)选择位于对话框的最底部。

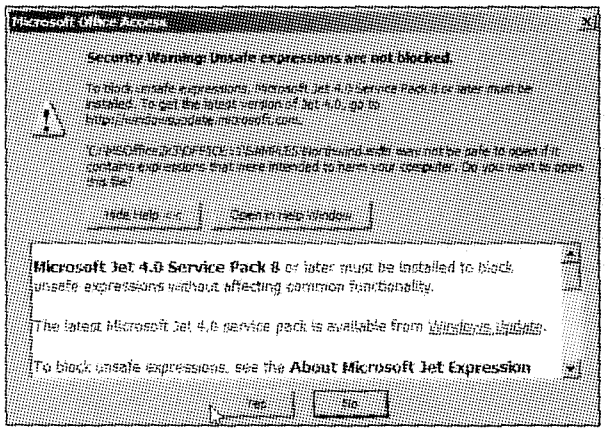

图 3.5　Microsoft Access 2003 不安全表达式警告

图 3.5 所示信息如不断重复，那么，对任何用户而言，都会感到厌烦。另一方面，如果可能，还要禁止通知成功阻止了每一个威胁的消息，这样用户就不会被过多打扰。

当今市场上有很多个人防火墙，可任意挑选。在选择一款个人防火墙时，应重点考虑其提供的功能水平。最低程度上，它应该包含流入和流出过滤(Granger 2003)；更加高级的防火墙可能包含基于主机的入侵检测功能，以提供对更加复杂的攻击的额外保护。

3.3.1　Windows XP Firewall

了解了连接至 Internet 计算机上本地软件防火墙的普遍需求，Microsoft 集成了一款基于软件的防火墙作为其 Windows XP 操作系统的一部分。最初的 Windows XP 版本包含了 Internet 连接防火墙(Internet connection Firewall，ICF)。随着 Windows XP SP2 的出现，ICF 被 Windows Firewall 所取代。安装了 Windows XP SP2，Windows Firewall 就在所有计算机上默认启动，如图 3.6 所示。

Windows Firewall 是一款状态软件防火墙，它检查所有的流入流量。用户通过管理界面指定允许通过防火墙的端口及应用程序。Windows Firewall 并不检查或限制流出流量。

Windows Firewall 在为用户提供基于主机的软件防火墙方面迈出了第一步。如果公司、组织或者个人不能负担购买及支持更加高级的基于主机的防火墙软件，那么，Windows Firewall 是优秀的免费替代品。虽然它提供的配置数量没有其他安全制造商所提供的那么多，但提供了流入流量的保护。

在 Control Panel(控制面板)中的 Security Center(安全中心)图标中可找到 Windows Firewall 配置屏幕，在运行有 Windows XP SP2 及其以后版本的计算机中都有它。还可以通过单击 Network Connections(网络连接)页面中 Change Windows Firewall(更改

Windows Firewall)设置图标,找到 Windows Firewall 的配置屏幕。

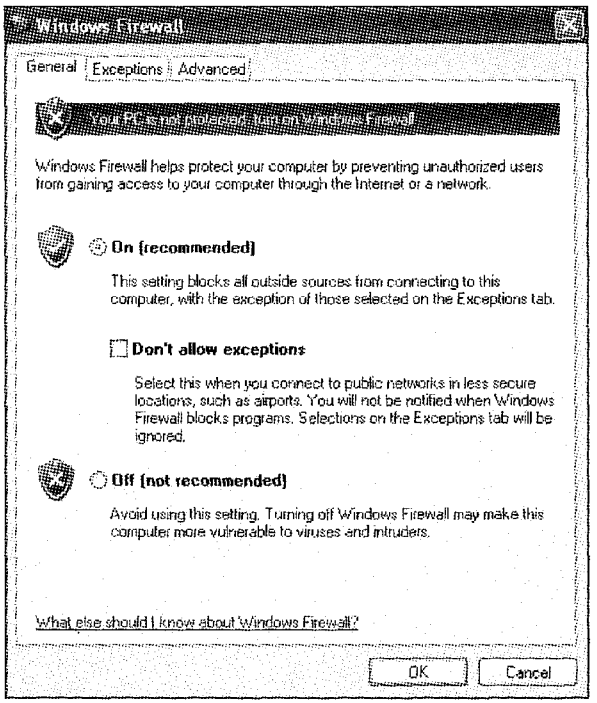

图 3.6 Windows Firewall 主页面

如图 3.7 所示,Windows Firewall 配置屏幕中的 Exceptions(例外)选项卡列出了为特定的端口和应用程序构造的例外选项。

- 不是完全开放一个端口,如果该端口能够与特定的应用程序相联系,那么该访问更应该被限制。
- 如果有必要开放一个应用程序或端口,将其限制为仅对需要明确访问的子网开放。在程序或服务中选择 Edit(编辑),之后选择 Change Scope(更改范围)即可。
- 如果不使用远程协助,则禁止它。
- 如果可能,禁止文件和打印机共享,因为这个服务经常被滥用。如果共享是绝对必要的,尝试更改范围,并且仅仅允许从 My network(subnet)only(仅我的网络(子网))访问,如图 3.8 所示。

在图 3.6 的 Advanced(高级)选项卡中,单击 Settings(设置)按钮,显示日志及 ICMP 的细节。默认设置日志在 Windows Firewall 上被禁止。然而,如果不时常查看日志,用户会发现,确定防火墙是否正常发挥作用是很困难的。因此,最好是启用 Dropped Packets(被丢弃数据包)日志记录。请注意,本日志文件的默认路径为 C:\Windows\pfirewall.log。