

McAfee®

personal**firewall**plus

使用手册

McAfee®

版权

版权所有 © 2005 McAfee, Inc. 保留所有权利。未经 McAfee, Inc. 或其供应商或子公司的书面许可, 不得以任何形式或手段将本出版物的任何内容复制、传播、转录、存储于检索系统或翻译成任何语言。

商标归属

ACTIVE FIREWALL, ACTIVE SECURITY (及片假名)、ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (特殊样式的 E)、DESIGN (特殊样式的 N)、ENTERCEPT, ENTERPRISE SECURECAST (及片假名)、EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD (及片假名)、GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE (及片假名)、MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS (及片假名)、NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN (及片假名)、WEBSCAN, WEBSHIELD (及片假名)、WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. 是 McAfee, Inc. 和 / 或其子公司在美国和 / 或其他国家或地区的注册商标或商标。安全图标为红色是 McAfee 品牌产品的特色。本文件中所有其他注册和未注册的商标均为其各自所有者专有。

许可信息

许可协议

致全体用户: 请仔细阅读与您所购买的许可相关的法律协议, 以了解使用许可软件的一般条款和条件。如果不清楚您购买的许可属于哪一类, 请查看软件包装盒中或购买产品时单易提供的销售文档以及与您所购买的或订单相关的其他文档, 这些文档既可以是小册子、产品光盘上的文件, 也可以是软件包下载网站提供的文件。如果您不同意该协议规定的所有条款和条件, 请勿安装本软件。根据情况, 您可以将产品退回 MCAFEE 或原购买处以获得全额退款。

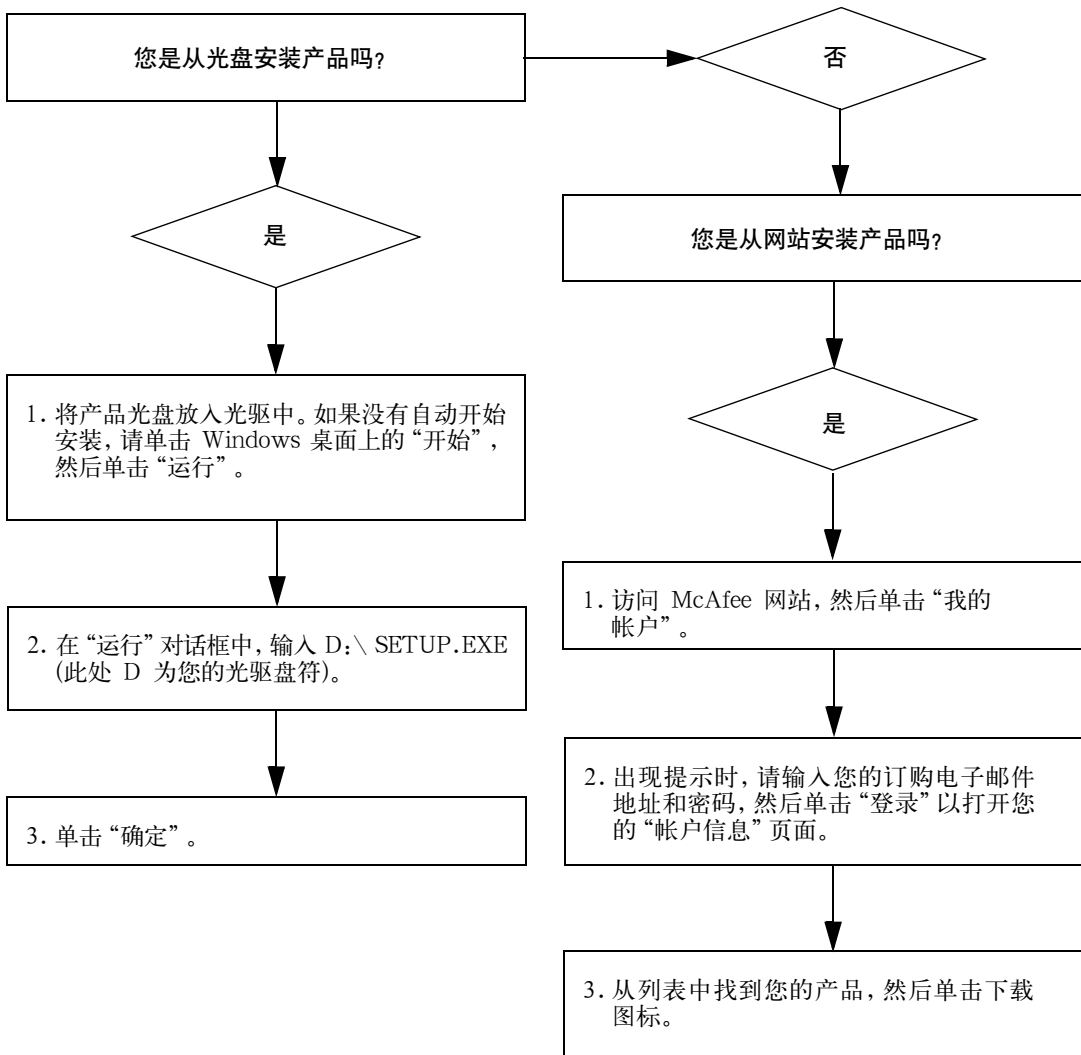
归属声明

本产品包括或可能包括:

- OpenSSL Project 为 OpenSSL 工具包开发的软件 (<http://www.openssl.org/>)。 • Eric A. Young 编写的加密软件 and 由 Tim J. Hudson 编写的软件。 • 一些根据 GNU 通用公共许可 (GPL) 或其他类似自由软件许可 (允许用户复制、修改和重新发布某些程序或程序的某些部分以及取得源代码) 授权 (或再授权) 用户使用的软件程序。 GPL 规定对于任何 GPL 软件, 在发布时除可执行二进制文件外, 还必须向用户提供源代码。对于涉及到的所有 GPL 软件, 其源代码均可在这张光盘中找到。如果任何自由软件许可要求 McAfee 提供比本协议所赋予的使用、复制或修改软件程序更广泛的权利, 则这些权利将优先于此处提及的权利和限制。 • Henry Spencer 原创的软件, Copyright © 1992, 1993, 1994, 1997 Henry Spencer。 • Robert Nordier 原创的软件, Copyright 1996-7 Robert Nordier。 • Douglas W. Sauder 编写的软件。
- Apache Software Foundation (<http://www.apache.org/>) 开发的软件。您可以在如下位置找到该软件的许可协议: www.apache.org/licenses/LICENSE-2.0.txt。 Copyright © 1992, 1993, 1994, 1997 Henry Spencer。 • Robert Nordier 原创的软件, Copyright 1996-7 Robert Nordier。 • Douglas W. Sauder 编写的软件。
- International Components for Unicode ("ICU"), Copyright © 1995-2002 International Business Machines Corporation 及其他公司。 • CrystalClear Software Inc. 开发的软件, Copyright © 2000 CrystalClear Software, Inc.。 • FEAD® Optimizer® 技术, Copyright Netopsystems AG, Berlin, Germany。 • Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. 和 / 或 Outside In® HTML Export, © 2001 Stellent Chicago, Inc.。 • Thai Open Source Software Center Ltd. 和 Clark Cooper 拥有版权的软件, © 1998, 1999, 2000。 • Expat 维护人员拥有版权的软件。 • University of California 校委会拥有版权的软件, © 1989。 • Gunnar Ritter 拥有版权的软件。 • Sun Microsystems® Inc. 拥有版权的软件, © 2003。 • Gisle Aas 拥有版权的软件, © 1995-2003。 • Michael A. Chase 拥有版权的软件, © 1999-2000。 • Neil Winton 拥有版权的软件, © 1995-1996。 • RSA Data Security, Inc. 拥有版权的软件, © 1990-1992。 • Sean M. Burke 拥有版权的软件, © 1999, 2000。 • Martijn Koster 拥有版权的软件, © 1995。 • Brad Appleton 拥有版权的软件, © 1996-1999。 • Michael G. Schwern 拥有版权的软件, © 2001。 • Graham Barr 拥有版权的软件, © 1998。 • Larry Wall 和 Clark Cooper 拥有版权的软件, © 1998-2000。 • Frodo Looijaard 拥有版权的软件, © 1997。 • Python Software Foundation 拥有版权的软件, Copyright © 2001, 2002, 2003。该软件的许可协议可在 www.python.org 中找到。 • Beman Dawes 拥有版权的软件, © 1994-1999, 2002。 • Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek 编写的软件, © 1997-2000 University of Notre Dame。 • Simone Bordet 和 Marco Craverio 拥有版权的软件, © 2002。 • Stephen Purcell 拥有版权的软件, © 2001。 • Indiana University Extreme! 实验室 (<http://www.extreme.indiana.edu/>) 开发的软件。
- International Business Machines Corporation 及其他公司拥有版权的软件, © 1995-2003。 • University of California of the Berkeley 及其合作伙伴开发的软件。 • Ralf S. Engelschall <rse@engelschall.com> 为 mod_ssl 项目 (<http://www.modssl.org/>) 开发的软件。 • Kevin Henney 拥有版权的软件, © 2000-2002。 • Peter Dimov 和 Multi Media Ltd. 拥有版权的软件, © 2001, 2002。 • David Abrahams 拥有版权的软件, © 2001, 2002。请参阅 <http://www.boost.org/libs/bind/bind.html> 上的文档。 • Steve Cleary, Beman Dawes, Howard Hinnant 和 John Maddock 拥有版权的软件, © 2000。 • Boost.org 拥有版权的软件, © 1999-2002。 • Nicolai M. Josuttis 拥有版权的软件, © 1999。 • Jeremy Siek 拥有版权的软件, © 1999-2001。 • Daryle Walker 拥有版权的软件, © 2001。 • Chuck Allison 和 Jeremy Siek 拥有版权的软件, © 2001, 2002。 • Samuel Krempp 拥有版权的软件, © 2001。请访问 <http://www.boost.org> 以获取更新、文档和修订历史记录。 • Doug Gregor (gregod@cs.rpi.edu) 拥有版权的软件, © 2001, 2002。 • Cadenza New Zealand Ltd. 拥有版权的软件, © 2000。 • Jens Maurer 拥有版权的软件, © 2000, 2001。 • Jaakko Jarvi (jaakko.jarvi@cs.utsu.fi) 拥有版权的软件, © 1999, 2000。 • Ronald Garcia 拥有版权的软件, © 2002。 • David Abrahams, Jeremy Siek 和 Daryle Walker 拥有版权的软件, © 1999-2001。 • Stephen Cleary (shammah@voyager.net) 拥有版权的软件, © 2000。 • Housemarque Oy <<http://www.housemarque.com>> 拥有版权的软件, © 2001。 • Paul Moore 拥有版权的软件, © 1999。 • Dr. John Maddock 拥有版权的软件, © 1998-2002。 • Greg Colvin 和 Beman Dawes 拥有版权的软件, © 1998, 1999。 • Peter Dimov 拥有版权的软件, © 2001, 2002。 • Jeremy Siek 和 John R. Bandela 拥有版权的软件, © 2001。 • Joerg Walter 和 Mathias Koch 拥有版权的软件, © 2000-2002。

快速入门卡

如果要从光盘或网站安装产品，为了方便起见，请打印下面的参考页面。



McAfee 保留随时更改升级和支持计划及策略的权利，恕不另行通知。McAfee 及其产品名称是 McAfee, Inc. 和 / 或其子公司在美国和 / 或其他国家或地区的注册商标。
© 2005 McAfee, Inc. 保留所有权利。

获取更多信息

要查看产品光盘中的《使用手册》，请确保已安装了 Acrobat Reader；如果尚未安装，请立即从 McAfee 产品光盘中安装。

- 1 将产品光盘放入光驱中。
- 2 打开 Windows 资源管理器：在 Windows 桌面上，单击“开始”，然后单击“搜索”。
- 3 找到 Manuals 文件夹，然后双击要打开的使用手册 PDF 文件。

注册的好处

McAfee 建议您按照产品中的简易步骤直接向我们发送注册信息。注册不仅可以确保用户收到及时、专业的技术帮助，而且还具有以下好处：

- 免费的电子支持。
- 购买和安装 VirusScan 软件之后提供为期一年的病毒特征码 (.DAT) 文件更新。
请访问 <http://www.mcafee.com/> 以了解续订一年病毒特征码的价格。
- 为期 60 天的担保，如果软件光盘存在缺陷或受损，可以保证进行更换。

- 购买和安装 SpamKiller 软件之后提供为期一年的 SpamKiller 过滤器更新。

请访问 <http://www.mcafee.com/> 以了解续订一年过滤器更新的价格。

- 购买和安装 MIS 软件之后提供为期一年的 Internet Security Suite 更新。

请访问 <http://www.mcafee.com/> 以了解续订一年内容更新的价格。

技术支持

要获得技术支持，请访问

<http://www.mcafeehelp.com/>。

我们的支持站点提供 24 小时访问服务，您可以通过简单易用的“应答向导”获得常见技术支持问题的解答。

经验丰富的用户还可以选用我们的高级选项，其中包括“关键字搜索”和“帮助树”。如果找不到答案，还可以使用我们提供的“免费聊天室！”和“电子邮件支持！”选项。聊天和电子邮件功能可以帮助您通过 Internet 快速联系到我们的资深的技术支持工程师，以获取免费支持。此外，还可以从以下网站获得电话支持信息：

<http://www.mcafeehelp.com/>。

目录

快速入门卡	iii
1 入门	7
新功能	7
系统要求	9
卸载其他防火墙	9
设置默认防火墙	9
设置安全级别	10
测试 McAfee Personal Firewall Plus	11
使用 McAfee SecurityCenter	12
2 使用 McAfee Personal Firewall Plus	13
关于摘要页面	13
关于 Internet 应用程序页面	17
更改应用程序规则	18
允许和阻止 Internet 应用程序	18
关于入站事件页面	19
了解事件	20
显示入站事件日志中的事件	22
响应入站事件	24
管理入站事件日志	27
关于警报	29
红色警报	29
绿色警报	34
蓝色警报	36
索引	37

欢迎使用 McAfee Personal Firewall Plus。

McAfee Personal Firewall Plus 软件可以为您的计算机和个人数据提供高级保护。它可以在您的计算机和 Internet 之间构筑一道屏障，悄无声息地监测 Internet 通讯是否存在可疑活动。

该软件提供了以下功能：

- 抵御可能出现的黑客探测和攻击
- 协助防护病毒
- 监控 Internet 和网络活动
- 通知可能有害的事件
- 提供有关可疑 Internet 通讯的详细信息
- 集成 Hackerwatch.org 功能，包括事件报告、自检工具以及将报告的事件以电子邮件方式发送给其他在线机构
- 提供详细的跟踪和事件分析功能

新功能

- **增强的游戏体验**
玩全屏游戏时，McAfee Personal Firewall Plus 不仅可以帮助计算机抵御入侵企图和可疑活动的威胁，而且还可以在检测到入侵企图或可疑活动时隐藏警报。退出游戏后才显示红色警报。
- **增强的访问处理**
McAfee Personal Firewall Plus 可以动态地为应用程序授予临时 Internet 访问权限。仅限应用程序在启动后和关闭前这段时间进行访问。当 Personal Firewall 检测到试图与 Internet 进行通讯的未知程序时，会在红色警报中提供为该应用程序授予临时 Internet 访问权限的选项。
- **增强的安全控制**
McAfee Personal Firewall Plus 的“锁定”功能可以立即阻止您的计算机的所有入站和出站 Internet 通讯。在 Personal Firewall 中，用户可以从三个位置启用和禁用“锁定”。

- **改进的恢复选项**

可以运行“重置选项”自动恢复 Personal Firewall 的默认设置。如果 Personal Firewall 中出现无法纠正的不当行为，则可以选择撤消当前设置并恢复产品的默认设置。
- **保护 Internet 连接**

为防止用户无意中禁用 Internet 连接，Personal Firewall 在检测到由 DHCP 或 DNS 服务器发起的 Internet 连接时，会在蓝色警报中隐藏禁止 Internet 地址的选项。如果入站通讯不是由 DHCP 或 DNS 服务器发起的，则会显示此选项。
- **增强的 HackerWatch.org 集成**

报告黑客行为比以往任何时候都方便。McAfee Personal Firewall Plus 改进了 HackerWatch.org 的功能，其中包括将可能有害的事件提交给数据库。
- **增强的智能应用程序处理**

当应用程序试图访问 Internet 时，Personal Firewall 会首先检查该应用程序是可信应用程序还是恶意应用程序。如果是可信应用程序，Personal Firewall 将自动允许其访问 Internet，其间无须用户执行任何操作。
- **先进的特洛伊木马程序检测**

McAfee Personal Firewall Plus 将应用程序连接管理与增强的数据库相结合，以检测并阻止更多可能有害的应用程序（如特洛伊木马程序）访问 Internet 和传播您的个人数据。
- **改进的 Visual Trace**

Visual Trace 中包含易于阅读的地图，可以显示全球范围的恶意攻击和通讯的来源，包括始发 IP 地址的联系人 / 所有者的详细信息。
- **便于使用**

McAfee Personal Firewall Plus 中的设置助理和使用教程可指导用户设置和使用防火墙。虽然设计该产品的目的是在不进行任何干预的情况下使用，但 McAfee 还是为用户提供了大量的资源以了解和评估防火墙所提供的功能。
- **增强的入侵检测**

Personal Firewall 的入侵检测系统 (IDS) 可以检测常见的攻击模式和其他可疑活动。入侵检测将监视每个数据包中是否存在可疑的数据或数据传输方式，并将此信息记录到事件日志中。
- **增强的通讯流量分析**

McAfee Personal Firewall Plus 不仅为用户提供计算机的入站和出站数据视图，而且还显示应用程序连接，包括当前正在“侦听”网络连接的应用程序。这样，用户就可以查看可能会受到攻击的应用程序，并采取相应措施。

系统要求

- Microsoft® Windows 98、Windows Me、Windows 2000 或 Windows XP
- 使用 Pentium 兼容处理器的个人计算机
Windows 98 和 Windows 2000: 133 MHz 或更高
Windows Me: 150 MHz 或更高
Windows XP (家庭版和专业版): 300 MHz 或更高
- RAM
Windows 98、Windows Me 和 Windows 2000: 64 MB
Windows XP (家庭版和专业版): 128 MB
- 40 MB 硬盘空间
- Microsoft® Internet Explorer 5.5 或更高版本

注意

要升级到 Internet Explorer 的最新版本, 请访问 Microsoft 网站 <http://www.microsoft.com/>。

卸载其他防火墙

在安装 McAfee Personal Firewall Plus 软件之前, 必须卸载计算机上的所有其他防火墙程序。请按照防火墙程序的卸载说明进行操作。

注意

在 Windows XP 上安装 McAfee Personal Firewall Plus 之前, 无需禁用内置防火墙。不过, 我们建议您禁用内置防火墙。否则, McAfee Personal Firewall Plus 的入站事件日志不会记录事件。

设置默认防火墙

即使检测到计算机上正在运行 Windows 防火墙, McAfee Personal Firewall 也可以管理计算机上 Internet 应用程序的权限和通讯。

McAfee Personal Firewall 在安装后会自动禁用 Windows 防火墙, 并将自身设置为默认防火墙。此后, 您只能使用 McAfee Personal Firewall 的功能和消息。如果以后通过 Windows Security Center 或 Windows 控制面板启用了 Windows 防火墙, 两个防火墙同时在计算机上运行可能会导致 McAfee Firewall 中的部分记录丢失, 并显示重复的状态和警报消息。

注意

如果同时启用两个防火墙，McAfee Personal Firewall 不会在“入站事件”选项卡中显示所有已阻止的 IP 地址。Windows 防火墙会拦截其中大多数事件，并阻止 McAfee Personal Firewall 检测或记录这些事件。不过，McAfee Personal Firewall 可能会基于其他安全因素阻止其他通讯，并记录该通讯。

默认情况下，Windows 防火墙日志处于禁用状态，但如果选择启用两个防火墙，则会启用 Windows 防火墙日志。默认的 Windows 防火墙日志为 C:\Windows\pfirewall.log。


为确保计算机至少受到一个防火墙的保护，在卸载 McAfee Personal Firewall 后，系统会自动重新启用 Windows 防火墙。

如果禁用 McAfee Personal Firewall 或者将其安全设置设定为“开放”，而没有手动启用 Windows 防火墙，除以前阻止的应用程序外，防火墙将不提供任何保护。

设置安全级别

可以配置安全选项以指示 Personal Firewall 在检测到有害通讯时如何进行响应。默认情况下，系统将启用“标准”安全级别。在“标准”安全级别中，如果允许应用程序访问 Internet，则会为其授予“完全访问权限”。“完全访问权限”允许应用程序同时在非系统端口上发送数据和接收未经请求的数据。

配置安全设置：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“选项”。
- 2 单击“安全设置”图标。
- 3 通过将滑块移动到所需的级别来设置安全级别。

安全级别的范围从“锁定”到“开放”：

- ◆ **锁定** — 关闭计算机上的所有 Internet 连接。可以使用此设置阻止在“系统服务”页面中配置为开放的端口。
- ◆ **严格** — 应用程序请求特定类型的 Internet 访问权限（如“仅出站访问”）时，可以允许或禁止应用程序建立 Internet 连接。如果应用程序以后请求“完全访问权限”，既可以为其授予“完全访问权限”，也可以将其限制为“仅出站访问”。
- ◆ **标准** — 如果在应用程序发出请求时为其授予 Internet 访问权限，应用程序将获得入站和出站通讯的完全 Internet 访问权限。
- ◆ **信任** — 在所有应用程序首次试图访问 Internet 时，系统将自动信任它们。另外，可以配置 Personal Firewall 使用警报来通知您有关计算机上新应用程序的信息。如果发现某些游戏或流媒体无法正常运行，请使用此设置。
- ◆ **开放** — 禁用防火墙。此设置允许所有通讯通过 Personal Firewall，不进行任何过滤。

注意

将防火墙的安全设置设置为“开放”或“锁定”后，系统将连续阻止以前被阻止的应用程序。为了避免出现这种情况，可以将应用程序的权限更改为“允许完全访问”，或从“Internet 应用程序”列表中删除“已阻止”权限规则。

4 选择其他安全设置：

注意

对于添加了多个 XP 用户的 Windows XP 系统，只有以管理员身份登录计算机时，才能使用这些选项。

- ◆ **在入站事件日志中记录入侵检测 (IDS) 事件** — 如果选择此选项，入站事件日志将显示 IDS 检测到的事件。入侵检测系统会检测常见的攻击类型和其他可疑活动，并监测每个入站和出站数据包中是否存在可疑的数据或数据传输方式。它会将这些数据包与“签名”数据库进行比较，然后自动丢弃恶意数据包。

IDS 将查找攻击者使用的特定通讯模式。为了检测可疑通讯或网络攻击，IDS 会检查您的计算机收到的每个数据包。例如，如果 Personal Firewall 收到 ICMP 数据包，它会将 ICMP 通讯与已知攻击模式进行比较来分析这些数据包是否存在可疑的通讯模式。


- ◆ **接受 ICMP Ping 请求** — ICMP 通讯主要用于执行跟踪和 Ping。在开始通讯之前，通常使用 Ping 来执行快速测试。如果正在使用或已使用过对等文件共享程序，您可能会发现其他计算机经常 Ping 您的计算机。如果选择此选项，Personal Firewall 将允许所有 Ping 请求，而不会在入站事件日志中记录 Ping。如果没有选择此选项，Personal Firewall 将阻止所有 Ping 请求，并在入站事件日志中记录 Ping。
- ◆ **允许受限用户更改 Personal Firewall 设置** — 在包含多个用户的 Windows XP 或 Windows 2000 Professional 上，请选择此选项以允许受限用户修改 Personal Firewall 设置。

5 完成更改后，单击“确定”。

测试 McAfee Personal Firewall Plus

通过测试 Personal Firewall，可以了解系统在抵御入侵和可疑活动方面可能存在的不足。

从 McAfee 系统任务栏图标测试 Personal Firewall：

- 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“测试防火墙”。

Personal Firewall 将打开 Internet Explorer，并访问由 McAfee 维护的网站 <http://www.HackerWatch.org>。请按照 [Hackerwatch.org Probe](http://www.HackerWatch.org) 页面中的说明来测试 Personal Firewall。


使用 McAfee SecurityCenter


McAfee SecurityCenter 是您的一站式安全商店，可以从 Windows 系统任务栏图标或从 Windows 桌面来访问。它可以执行以下任务：

- 免费的计算机安全分析。
- 通过一个图标启动、管理和配置所有 McAfee 产品。
- 查看连续更新的病毒警报和最新的产品信息。
- 快速链接到 McAfee 网站以查看常见问题和帐户详细信息。

注意

要了解有关其功能的更多信息，请单击“SecurityCenter”对话框中的“帮助”。

如果正在运行 SecurityCenter 并且启用了计算机上安装的所有 McAfee 功能，Windows 系统任务栏中将显示一个红色 M 图标 。任务栏通常位于 Windows 桌面的右下角，并且包含时钟。

如果禁用了计算机上安装的一个或多个 McAfee 应用程序，McAfee 图标将变为黑色 。


启动 McAfee SecurityCenter：

- 1 右键单击 McAfee 图标 ，然后选择“打开 SecurityCenter”。

从 McAfee SecurityCenter 中启动 Personal Firewall：

- 1 从 SecurityCenter 中单击“Personal Firewall Plus”选项卡。
- 2 从“我想”菜单中选择一项任务。


从 Windows 中启动 Personal Firewall：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标 ，然后指向“Personal Firewall”。
- 2 选择一项任务。

使用 McAfee Personal Firewall Plus

2

打开 Personal Firewall:

- 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向 “Personal Firewall”，然后选择某项任务。

关于摘要页面

Personal Firewall 摘要包括以下四个摘要页面:

- ◆ 主摘要
- ◆ 应用程序摘要
- ◆ 事件摘要
- ◆ HackerWatch 摘要

摘要页面包含各种报告，其内容与最新入站事件、应用程序状态以及 HackerWatch.org 所报告的全球范围的入侵活动有关。这里还有指向 Personal Firewall 中执行的常见任务的链接。

在 Personal Firewall 中打开“主摘要”页面：





- 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“查看摘要”（图 2-1）。



图 2-1. “主摘要”页面

要浏览不同的摘要页面，请单击以下按钮：


项目	描述
更改视图	单击“更改视图”可以打开“摘要”页面列表。从列表中选择要查看的摘要页面。
 右箭头	单击右箭头图标可以查看下一个“摘要”页面。
 左箭头	单击左箭头图标可以查看上一个“摘要”页面。
 主页	单击主页图标可以返回“主摘要”页面。

“主摘要”页面提供了以下信息：

项目	描述
安全设置	安全设置状态显示防火墙的安全级别。单击此链接可以更改安全级别。
阻止的事件	阻止的事件状态显示今天已阻止的事件数量。单击此链接可以从“入站事件”页面中查看事件的详细信息。
应用程序规则更改	应用程序规则状态显示最近更改的应用程序规则的数量。单击此链接可以查看允许和阻止的应用程序列表或修改应用程序权限。
最新信息	“最新信息”显示最新授予 Internet 完全访问权限的应用程序。

项目	描述
最新事件	“最新事件”显示最新的入站事件。可以单击链接以跟踪事件或信任 IP 地址。通过信任 IP 地址可以允许计算机接收来自特定 IP 地址的所有通讯。
日常报告	“日常报告”显示 Personal Firewall 今天、本周和本月所阻止的入站事件数量。单击此链接可以从“入站事件”页面中查看事件的详细信息。
活动中的应用程序	“活动中的应用程序”显示当前在计算机上运行并访问 Internet 的应用程序。单击某个应用程序可以查看该应用程序所连接的 IP 地址。
常见任务	单击“常见任务”中的链接可以转到 Personal Firewall 页面，并从中查看防火墙活动和执行任务。


查看“应用程序摘要”页面：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“查看摘要”。
- 2 单击“更改视图”，然后选择“应用程序摘要”。

“应用程序摘要”页面提供了以下信息：

项目	描述
通讯流量监视器	“通讯流量监视器”显示过去 15 分钟内的入站和出站 Internet 连接。单击图像可以查看更详细的通讯流量监视信息。
活动中的应用程序	“活动中的应用程序”显示过去 24 小时内计算机中最活跃的应用程序的带宽使用情况。 应用程序 — 访问 Internet 的应用程序。 % — 应用程序的宽带使用百分比。 权限 — 允许应用程序采用的 Internet 访问类型。 规则创建时间 — 创建应用程序规则的时间。
最新信息	“最新信息”显示最新授予 Internet 完全访问权限的应用程序。
活动中的应用程序	“活动中的应用程序”显示当前在计算机上运行并访问 Internet 的应用程序。单击某个应用程序可以查看该应用程序所连接的 IP 地址。
常见任务	单击“常见任务”中的链接可以转到 Personal Firewall 页面，并从中查看应用程序状态和执行与应用程序有关的任务。


查看“事件摘要”页面：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“查看摘要”。
- 2 单击“更改视图”，然后选择“事件摘要”。

“事件摘要”页面提供了以下信息：

项目	描述
端口比较	“端口比较”显示在过去 30 天内访问次数最多的计算机端口的饼形图。可以单击某个端口名称，从“入站事件”页面中查看其详细信息。还可以将鼠标指针移到端口号上，以查看该端口的说明。
首要入侵者	“首要入侵者”显示受阻次数最多的 IP 地址、每个地址最后一次入站事件的时间以及过去 30 天内每个地址入站事件的总数。单击某个事件可以从“入站事件”页面中查看其详细信息。
日常报告	“日常报告”显示 Personal Firewall 今天、本周和本月所阻止的入站事件数量。单击某个数字可以从入站事件日志中查看事件的详细信息。
最新事件	“最新事件”显示最新的入站事件。可以单击链接以跟踪事件或信任 IP 地址。通过信任 IP 地址可以允许计算机接收来自特定 IP 地址的所有通讯。
常见任务	单击“常见任务”中的链接可以转到 Personal Firewall 页面，并从中查看事件详细信息和执行与事件有关的任务。

查看 HackerWatch 摘要页面：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“查看摘要”。
- 2 单击“更改视图”，然后选择“HackerWatch Summary”。


HackerWatch 摘要页面提供了以下信息：

项目	描述
World Activity (全球活动)	“World Activity”（全球活动）中的世界地图可反映 HackerWatch.org 监测到的最近阻止的活动。单击该地图可以打开 HackerWatch.org 中的全球病毒威胁分析图。
Event Tracking (事件跟踪)	“Event Tracking”（事件跟踪）显示向 HackerWatch.org 提交的入站事件数。
Global Port Activity (全球端口活动)	“Global Port Activity”（全球端口活动）显示过去 5 天内受到威胁次数最多的端口。单击某个端口可以查看端口号和端口说明。
Common Tasks (常见任务)	单击“Common Tasks”（常见任务）中的链接可转到 HackerWatch.org 页面，并从中获取全球范围内黑客活动的更多信息。

关于 Internet 应用程序页面

可以使用“Internet 应用程序”页面查看允许和阻止的应用程序列表。

启动“Internet 应用程序”页面：

- 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“应用程序”（图 2-2）。

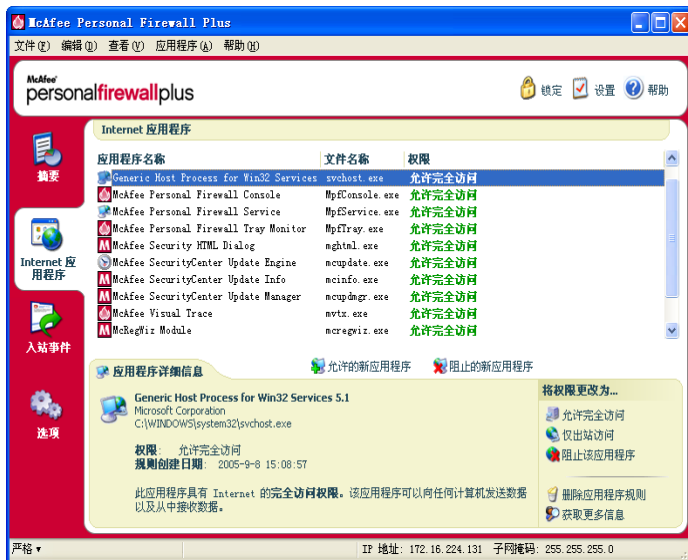


图 2-2. “Internet 应用程序”页面

“Internet 应用程序”页面提供了以下信息：

- 应用程序名称
- 文件名
- 当前权限级别
- 应用程序详细信息：应用程序名称及版本、公司名称、路径名称、权限、时间戳和权限类型说明。

更改应用程序规则

在 Personal Firewall 中，可以更改应用程序的访问规则。


更改应用程序规则：

- 1 右键单击 McAfee 图标，指向“Personal Firewall”，然后选择“Internet 应用程序”。
- 2 在“Internet 应用程序”列表中，右键单击某个应用程序的应用程序规则，然后选择不同的级别：
 - ◆ **允许完全访问** — 允许应用程序建立出站和入站 Internet 连接。
 - ◆ **仅出站访问** — 仅允许应用程序建立出站 Internet 连接。
 - ◆ **阻止此应用程序** — 禁止应用程序访问 Internet。

注意

将防火墙设置为“开放”或“锁定”后，系统将阻止以前被阻止的应用程序。为了避免出现这种情况，可以将应用程序的访问规则更改为“完全访问”，或从“Internet 应用程序”列表中删除“已阻止”权限规则。


删除应用程序规则：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“Internet 应用程序”。
- 2 在“Internet 应用程序”列表中，右键单击应用程序规则，然后选择“删除应用程序规则”。

下次应用程序请求访问 Internet 时，可以设置权限级别以将其重新添加到列表中。

允许和阻止 Internet 应用程序


更改允许和阻止的 Internet 应用程序列表：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“Internet 应用程序”。
- 2 在“Internet 应用程序”页面上，单击下面某个选项：
 - ◆ **允许的新应用程序** — 允许应用程序具有完全的 Internet 访问权限。
 - ◆ **阻止的新应用程序** — 禁止应用程序访问 Internet。
 - ◆ **删除应用程序规则** — 删除某个应用程序规则。

关于入站事件页面

使用“入站事件”页面可以查看入站事件日志，该日志是在 Personal Firewall 阻止未经请求的 Internet 连接时生成的。

启动“入站事件”页面：

- 右键单击 Windows 系统任务栏中的 McAfee 图标 ，指向“Personal Firewall”，然后选择“入站事件”（图 2-3）。

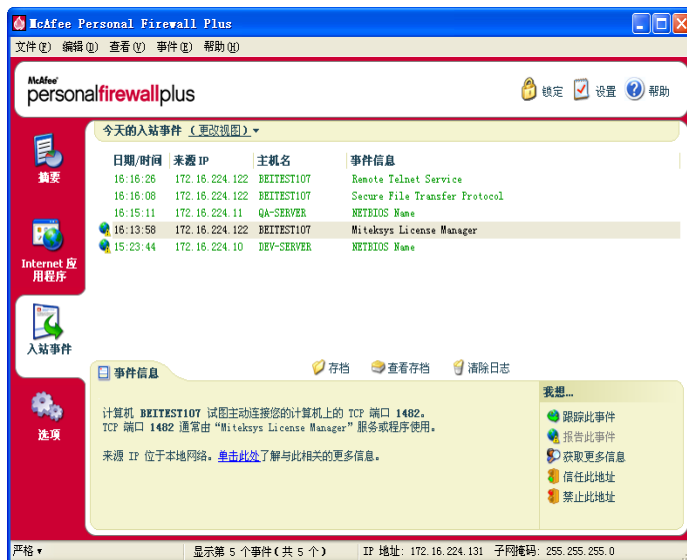


图 2-3. “入站事件”页面

“入站事件”页面提供了以下信息：

- 时间 / 日期
- 来源 IP
- 主机名
- 服务或应用程序名称
- 事件信息：连接类型、连接端口、主机名或 IP 以及端口事件说明

了解事件

关于 IP 地址

IP 地址是一些数字：准确地说，是四个介于 0 和 255 之间的数字。这些数字用于确定将通讯发送到 Internet 上的特定位置。

IP 地址类型

出于各种原因，有些 IP 地址并不常用：

无法路由的 IP 地址 — 又称“专用 IP 空间”。这些 IP 地址无法在 Internet 上使用。专用 IP 的范围是 10.x.x.x、172.16.x.x - 172.31.x.x 和 192.168.x.x。

环回 IP 地址 — 环回地址用于测试目的。发送到该 IP 地址块的通讯将立即返回给生成数据包的设备。它绝不会脱离设备，因此主要用于硬件和软件测试。环回 IP 的范围是 127.x.x.x。

空 IP 地址 — 这是无效的地址。检测到该地址时，Personal Firewall 将指出通讯使用的是空 IP 地址。它通常表明发送者蓄意隐藏通讯来源。除非收到数据包的应用程序了解数据包内容并且知道其中包含该应用程序的特定指令，否则发送者将无法收到任何答复。所有以 0 开头的地址 (0.x.x.x) 都是空地址。例如，0.0.0.0 即为空 IP 地址。

来自 0.0.0.0 的事件

如果您看到来自 IP 地址 0.0.0.0 的事件，可能有两个原因。第一个原因也是最常见的原因是，您的计算机收到格式错误的数据包。Internet 并不总是百分之百可靠的，有时也会出现错误的数据包。因为 Personal Firewall 在 TCP/IP 验证数据包之前检测这些数据包，所以可能会报告有关这些数据包的事件。

另外一种情况是，源 IP 地址是伪造的或是虚假的。伪造的数据包表明有人正在扫描您的计算机以查找特洛伊木马程序。Personal Firewall 会阻止此类活动，因此您的计算机是安全的。

来自 127.0.0.1 的事件

有时，事件会将源 IP 显示为 127.0.0.1。该地址又称环回地址或 localhost。

很多合法程序都使用环回地址来进行组件间通讯。例如，可以通过 Web 界面来配置许多个人电子邮件或 Web 服务器。要访问该界面，需要在 Web 浏览器中输入“http://localhost/”。

不过，Personal Firewall 允许来自这些程序的通讯，因此，如果出现来自 127.0.0.1 的事件，很可能意味着源 IP 地址是伪造的或是虚假的。伪造的数据包通常表明另一台计算机正在扫描您的计算机以查找特洛伊木马程序。Personal Firewall 会阻止此类入侵企图，因此您的计算机是安全的。

有些程序（比如 Netscape 6.2 和更高版本）要求您将 127.0.0.1 添加到“信任的 IP 地址”列表中。这些程序的组件彼此之间以一种 Personal Firewall 无法判定的方式进行通讯。

以 Netscape 6.2 为例，如果不信任 127.0.0.1，您将无法使用好友名单。因此，如果出现来自 127.0.0.1 的通讯，并且计算机上的所有应用程序均正常运行，则可以放心地阻止该通讯。然而，如果某个程序（如 Netscape）出现问题，请在 Personal Firewall 的“信任的 IP 地址”列表中添加 127.0.0.1。

如果将 127.0.0.1 添加到信任的 IP 列表中可以解决问题，则需要权衡所作出的选择：如果信任 127.0.0.1，程序将正常运行，但是您更容易受到欺骗攻击。如果不信任该地址，程序将无法正常运行，但是您的计算机能够抵御某些恶意通讯。

来自 LAN 计算机的事件

可以创建来自局域网 (LAN) 计算机的事件。Personal Firewall 用绿色表示来自当前网络的事件。

在大多数公司的 LAN 设置中，应该在“信任的 IP 地址”选项中选择“信任 LAN 上的所有计算机”。

在某些情况下，“本地”网络可能与 Internet 一样危险，尤其当您的计算机处于基于高带宽 DSL 或电缆调制解调器的网络上时。此时，请勿选择“信任 LAN 上的所有计算机”。而应将本地计算机的 IP 地址添加到“信任的 IP 地址”列表中。

来自专用 IP 地址的事件

采用 192.168.xxx.xxx、10.xxx.xxx.xxx 和 172.16.0.0 - 172.31.255.255 格式的 IP 地址称为无法路由的地址或专用 IP 地址。这些 IP 地址绝不会脱离您的网络，因此，大多数情况下可以信任这些地址。

192.168.xxx.xxx 块用于 Microsoft Internet 连接共享 (ICS)。如果正在使用 ICS，并且出现来自该 IP 块的事件，则可能需要将 IP 地址 192.168.255.255 添加到“信任的 IP 地址”列表中。此操作将信任整个 192.168.xxx.xxx 块。

如果没有使用专用网络，但出现来自该 IP 范围的事件，则源 IP 地址可能是伪造的或是虚假的。伪造的数据包通常表明有人正在扫描特洛伊木马程序。切记，Personal Firewall 会阻止该尝试，因此您的计算机是安全的。

由于专用 IP 地址在不同网络中代表不同的计算机，所以报告这些事件没有任何作用，因此不需要这样做。

显示入站事件日志中的事件

入站事件日志可以通过多种方式来显示事件。默认视图仅显示当天发生的事件。此外，还可以查看过去一周内发生的事件或者查看完整的日志。

在 Personal Firewall 中，还可以显示特定日期、特定 Internet 地址（IP 地址）的入站事件，或者显示包含相同事件信息的事件。

要查看某个事件的信息，请单击该事件，然后查看“事件信息”窗格中的信息。

显示今天的事件

使用此选项查看当天的事件。

显示今天的事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在入站事件日志中，右键单击某个条目，然后单击“显示今天的事件”。

显示本周的事件

使用此选项查看每周的事件。

显示本周的事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在入站事件日志中，右键单击某个条目，然后单击“显示本周的事件”。

显示完整的入站事件日志

使用此选项查看所有事件。

显示入站事件日志中的所有事件：

- 1 右键单击 McAfee 图标，指向“Personal Firewall”，然后单击“入站事件”。
- 2 在入站事件日志中，右键单击某个条目，然后单击“显示完整的日志”。

入站事件日志将显示入站事件日志中的所有事件。

显示特定日期的事件

使用此选项查看特定日期的事件。

显示某天的事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在入站事件日志中，右键单击某个条目，然后单击“仅显示此日期的事件”。

显示特定 Internet 地址的事件

使用此选项查看来自特定 Internet 地址的其他事件。

显示某个 Internet 地址的事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后单击“入站事件”。
- 2 在入站事件日志中，右键单击某个条目，然后单击“仅显示此 Internet 地址的事件”。

显示具有相同事件信息的事件

使用此选项查看入站事件日志中与所选事件具有相同“事件信息”列信息的事件。您可以了解事件发生的次数，以及事件来源是否相同。“事件信息”列提供事件的说明以及使用该端口的常用程序或服务（如果已知）的说明。

显示具有相同事件信息的事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后单击“入站事件”。
- 2 在入站事件日志中，右键单击某个条目，然后单击“仅显示包含相同事件信息的事件”。

响应入站事件

除了查看入站事件日志中事件的详细信息外，还可以对入站事件日志中的事件执行 IP 地址可视化跟踪，或者在防黑客在线社区 HackerWatch.org 网站中获取事件详细信息。

跟踪选定事件

可以尝试为入站事件日志中的事件执行 IP 地址可视化跟踪。

跟踪选定事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在入站事件日志中，右键单击要跟踪的事件，然后单击“跟踪选定事件”。也可以双击某个事件以跟踪该事件。

默认情况下，Personal Firewall 使用内置的 Personal Firewall Visual Trace 程序来启动可视化跟踪。

从 HackerWatch.org 获取建议

从 HackerWatch.org 获取建议：

- 1 右键单击 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在“入站事件”页面中选择事件条目，然后在“我想”窗格中单击“获取更多信息”。

将启动默认 Web 浏览器并打开 HackerWatch.org，您可以在其中检索有关该事件类型的信息并获取有关是否报告事件的建议。

报告事件

报告您认为是攻击计算机的事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 单击要报告的事件，然后在“我想”窗格中单击“报告此事件”。

Personal Firewall 将使用您的唯一 ID 向 HackerWatch.org 报告事件。

注册 HackerWatch.org

首次打开“摘要”页面时，Personal Firewall 会联系 HackerWatch.org 以生成您的唯一用户 ID。如果您是老用户，系统将自动验证您的注册信息。如果您是新用户，则必须输入昵称和电子邮件地址，然后单击 HackerWatch.org 发送的确认电子邮件中的验证链接，才能使用该网站中的过滤 / 发送电子邮件功能。

无需验证您的用户 ID 即可向 HackerWatch.org 报告事件。然而，要过滤事件并以电子邮件方式将其发送给朋友，您必须注册该服务。

注册该服务后，我们就可以跟踪您提交的内容，并且如果 HackerWatch.org 需要您提供更多信息或采取进一步的措施，我们可以向您发送通知。由于我们必须在确认收到的任何信息后才能使用该信息，所以也会要求您进行注册。

提供给 HackerWatch.org 的所有电子邮件地址都是保密的。如果 ISP 请求获得其他信息，则会通过 HackerWatch.org 发送该请求；但您的电子邮件地址绝不会被公开。

信任地址

可以使用“入站事件”页面将 IP 地址添加到“信任的 IP 地址”列表中，从而建立永久性连接。

如果“入站事件”页面中的事件包含需要允许的 IP 地址，则可以让 Personal Firewall 始终允许来自该地址的连接。

将 IP 地址添加到“信任的 IP 地址”列表中：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 右键单击要信任其 IP 地址的事件，然后单击“信任来源 IP 地址”。

确保“信任此地址”对话框中显示的 IP 地址是正确的，然后单击“确定”。该 IP 地址将添加到“信任的 IP 地址”列表中。

验证是否添加了该 IP 地址：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“选项”。
- 2 单击“信任的和禁止的 IP”图标，然后单击“信任的 IP 地址”选项卡。

在“信任的 IP 地址”列表中，该 IP 地址处于选中状态。

禁止地址

如果入站事件日志中显示某个 IP 地址，则表明阻止了来自该地址的通讯。因此，除非计算机包含借助“系统服务”功能故意打开的端口，或者计算机包含有权接收通讯的应用程序，否则禁止某个地址并不会提供额外的保护。

仅当一个或多个端口被蓄意打开，而且确信必须阻止某个地址访问打开的端口时，才应该将该 IP 地址添加到禁止的地址列表中。

如果“入站事件”页面中的事件包含要禁止的 IP 地址，则可以将 Personal Firewall 配置为始终禁止来自该地址的连接。

“入站事件”页面列出了所有 Internet 入站通讯的 IP 地址，可以使用该页面禁止可疑的或有害的 Internet 活动的源 IP 地址。

将 IP 地址添加到“禁止的 IP 地址”列表中：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 “入站事件”页面列出了所有 Internet 入站通讯的 IP 地址。选择一个 IP 地址，然后执行下面某项操作：
 - ◆ 右键单击该 IP 地址，然后选择“禁止来源 IP 地址”。
 - ◆ 在“我想”菜单中，单击“禁止此地址”。
- 3 在“添加禁止的 IP 地址规则”对话框中，使用以下一个或多个设置来配置“禁止的 IP 地址”规则：
 - ◆ **单个 IP 地址：**要禁止的 IP 地址。默认条目是在“入站事件”页面中选择的 IP 地址。
 - ◆ **IP 地址范围：**介于“自 IP 地址”和“至 IP 地址”之间的 IP 地址。
 - ◆ **规则在此时间过期：**“禁止的 IP 地址”规则的过期日期和时间。选择相应的下拉菜单以选择日期和时间。
 - ◆ **描述：**（可选）描述新规则。
 - ◆ 单击“确定”。
- 4 在对话框中，单击“是”确认设置，或单击“否”返回“添加禁止的 IP 地址规则”对话框。

如果 Personal Firewall 检测到来自禁止的 Internet 连接的事件，则将根据在“警报设置”页面中设定的方法发出警报。

验证是否添加了该 IP 地址：

- 1 单击“选项”选项卡。
- 2 单击“信任的和禁止的 IP”图标，然后单击“禁止的 IP 地址”选项卡。

在“禁止的 IP 地址”列表中，该 IP 地址处于选中状态。

管理入站事件日志

可以使用“入站事件”页面来管理入站事件日志中的事件，这些事件是在 Personal Firewall 阻止未经请求的 Internet 通讯时生成的。

保存入站事件日志

可以通过保存当前入站事件日志来保存所有记录的入站事件，包括日期和时间、源 IP、主机名、端口和事件信息。应该定期保存入站事件日志，以防入站事件日志变得太大。

保存入站事件日志：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在“入站事件”页面上，单击“存档”。
- 3 在“保存日志”对话框中，单击“是”继续执行操作。
- 4 单击“保存”在默认位置保存存档，或者浏览到要保存存档的位置。

注意：默认情况下，Personal Firewall 会自动保存入站事件日志。在“事件日志设置”页面中，选中或清除“自动保存记录的事件”可启用或禁用该选项。

查看保存的入站事件日志

可以查看以前保存的任何入站事件日志。保存的存档包括事件的日期和时间、源 IP、主机名、端口和事件信息。

查看保存的入站事件日志：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在“入站事件”页面上，单击“查看存档”。
- 3 选择或浏览存档文件名称，然后单击“打开”。

清除入站事件日志

可以清除入站事件日志中的所有信息。

警告：一旦清除了入站事件日志，就无法对其进行恢复。如果您认为以后还需要使用该事件日志，则应将其存档。

清除入站事件日志：

- 1 右键单击 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在“入站事件”页面上，单击“清除日志”。
- 3 单击对话框中的“是”以清除日志。

将事件复制到剪贴板

可以将事件复制到剪贴板，以便使用记事本将其粘贴到文本文件中。

将事件复制到剪贴板：

- 1 右键单击 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 右键单击入站事件日志中的事件。
- 3 单击“将事件文本复制到剪贴板”。
- 4 启动“记事本”。
 - ◆ 在命令行中输入 notepad，或者单击 Windows “开始”按钮，指向“程序”，然后指向“附件”。选择“记事本”。
- 5 单击“编辑”，然后单击“粘贴”。事件文本将出现在记事本中。重复此步骤，直到复制完所有需要的事件为止。
- 6 将记事本文件保存到安全的地方。

删除选定事件

可以从入站事件日志中删除事件。

从入站事件日志中删除事件：

- 1 右键单击 Windows 系统任务栏中的 McAfee 图标，指向“Personal Firewall”，然后选择“入站事件”。
- 2 在“入站事件”页面上，单击要删除的事件条目。
- 3 在“编辑”菜单中，单击“删除选定事件”。该事件将从入站事件日志中删除。

关于警报

强烈建议您熟悉使用 Personal Firewall 时遇到的各种警报类型。请查看以下可能出现的警报类型以及可以选择的处理方式，以便对警报做出适当的处理。

注意

警报上的建议可帮助您决定如何处理警报。要在警报上显示建议，请单击“选项”选项卡，单击“警报设置”图标，然后从“智能建议”列表中选择“使用智能建议”（默认设置）或“仅显示智能建议”。

红色警报

红色警报包含需要立即处理的重要信息：

- **Internet 应用程序已阻止** — 如果 Personal Firewall 阻止应用程序访问 Internet，则会显示该警报。例如，如果出现特洛伊木马程序警报，McAfee 将自动拒绝该程序访问 Internet，并建议您对计算机进行病毒扫描。
- **应用程序要访问 Internet** — Personal Firewall 在检测到来自新应用程序的 Internet 通讯或网络通讯时显示该警报。
- **应用程序已修改** — Personal Firewall 在检测到以前允许访问 Internet 的应用程序已修改时显示该警报。如果最近没有升级该应用程序，则为修改后的应用程序授予 Internet 访问权限时要慎重。
- **应用程序请求服务器访问权限** — Personal Firewall 在检测到以前允许访问 Internet 的应用程序请求作为服务器访问 Internet 时显示该警报。

注意

Windows XP SP2 的默认“自动更新”设置将自动为计算机上运行的 Windows 操作系统和其他 Microsoft 程序下载和安装更新，而不会通知您。使用 Windows 静默更新对应用程序进行修改后，下次运行该 Microsoft 应用程序时，将显示 McAfee Personal Firewall 警报。

重要信息

对于需要访问 Internet 以获取在线产品更新的应用程序（如 McAfee 服务），必须为其授予访问权限，以使它们保持最新状态。

Internet 应用程序已阻止警报

如果出现特洛伊木马程序警报（图 2-4），Personal Firewall 将自动拒绝该程序访问 Internet，并建议您对计算机进行病毒扫描。如果未安装 McAfee VirusScan，您可以启动 McAfee SecurityCenter。



图 2-4. “Internet 应用程序已阻止”警报

查看事件的简要说明，然后选择以下选项：

- 单击“了解更多信息”，通过入站事件日志获取有关事件的详细信息（详细信息，请参阅第 19 页的“关于入站事件页面”）。
- 单击“启动 McAfee VirusScan”，对计算机进行病毒扫描。
- 单击“继续进行操作”，不执行任何操作。
- 单击“授予出站访问权限”，允许建立出站连接（“严格”安全级别）。

应用程序要访问 Internet 警报

如果在“安全设置”选项中选择“标准”或“严格”安全级别，则 Personal Firewall 在检测到新应用程序或修改后的应用程序的 Internet 通讯或网络通讯时将显示警报（图 2-5）。



图 2-5. “应用程序要访问 Internet” 警报

如果显示的警报建议要慎重对待应用程序对 Internet 的访问，则可以单击“单击此处以了解更多信息”来了解有关该应用程序的详细信息。只有将 Personal Firewall 配置为使用“智能建议”时，警报中才会显示此选项。

McAfee 有时可能无法识别试图获取 Internet 访问权限的应用程序（图 2-6）。

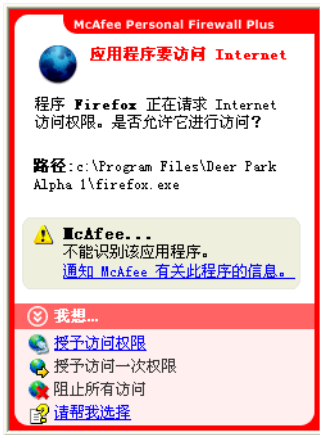


图 2-6. “无法识别的应用程序” 警报

因此，McAfee 无法给出如何处理该应用程序的建议。可以单击“通知 McAfee 有关此程序的信息”，向 McAfee 报告该应用程序。此时会出现一个网页，询问有关该应用程序的信息。请填写您知道的所有信息。

HackerWatch 员工将使用其他分析工具来分析您提交的信息，以确定是否应在已知应用程序数据库中列出该应用程序；如果列出的话，同时还会提供 Personal Firewall 对该应用程序的处理办法。

查看事件的简要说明，然后选择以下选项：

- 单击“授予访问权限”，允许应用程序建立出站和入站 Internet 连接。
- 单击“授予访问一次权限”，允许应用程序建立临时的 Internet 连接。仅限应用程序在启动后和关闭前这段时间进行访问。
- 单击“阻止所有访问”，禁止建立 Internet 连接。
- 单击“授予出站访问权限”，允许建立出站连接（“严格”安全级别）。
- 单击“请帮我选择”，查看有关应用程序访问权限的联机帮助。

应用程序已修改警报

如果在“安全设置”选项中选择“信任”、“标准”或“严格”安全级别，则 Personal Firewall 在检测到以前允许访问 Internet 的应用程序已修改时将显示警报（图 2-7）。如果最近没有升级该应用程序，则为修改后的应用程序授予 Internet 访问权限时要慎重。



图 2-7. “应用程序已修改”警报

查看事件的简要说明，然后选择以下选项：

- 单击“授予访问权限”，允许应用程序建立出站和入站 Internet 连接。
- 单击“授予访问一次权限”，允许应用程序建立临时的 Internet 连接。仅限应用程序在启动后和关闭前这段时间进行访问。
- 单击“阻止所有访问”，禁止建立 Internet 连接。
- 单击“授予出站访问权限”，允许建立出站连接（“严格”安全级别）。
- 单击“请帮我选择”，查看有关应用程序访问权限的联机帮助。

应用程序请求服务器访问权限警报

如果在“安全设置”选项中选择“严格”安全级别，则 Personal Firewall 在检测到以前访问过 Internet 的应用程序请求作为服务器访问 Internet 时将显示警报（图 2-8）。

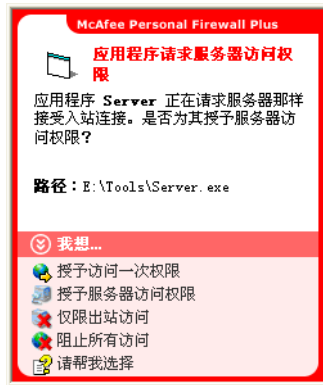


图 2-8. “应用程序请求服务器访问权限”警报

例如，如果 MSN Messenger 请求在聊天过程中发送文件的服务器访问权限，则会显示一条警报。

查看事件的简要说明，然后选择以下选项：

- 单击“授予访问一次权限”，为应用程序授予临时的 Internet 访问权限。仅限应用程序在启动后和关闭前这段时间进行访问。
- 单击“授予服务器访问权限”，允许应用程序建立出站和入站 Internet 连接。
- 单击“仅限出站访问”，禁止建立入站 Internet 连接。
- 单击“阻止所有访问”，禁止建立 Internet 连接。
- 单击“请帮我选择”，查看有关应用程序访问权限的联机帮助。

绿色警报

绿色警报用于通知 Personal Firewall 中的事件，例如已自动授予 Internet 访问权限的应用程序。

程序已被允许访问 Internet — Personal Firewall 在自动为所有新应用程序授予 Internet 访问权限时显示该警报（“信任”安全级别）。修改后的应用程序可能会将规则修改为自动允许应用程序访问 Internet。

程序已被允许访问 Internet 警报

如果在“安全设置”选项中选择“信任”安全级别，Personal Firewall 将自动为所有新应用程序授予 Internet 访问权限，并且使用警报通知您（图 2-9）。



图 2-9. “程序已被允许访问 Internet”警报

查看事件的简要说明，然后选择以下选项：

- 单击“查看应用程序日志”，通过 Internet 应用程序日志获取有关事件的详细信息（详细信息，请参阅第 17 页的“关于 Internet 应用程序页面”）。
- 单击“关闭此警报类型”，防止出现此类警报。
- 单击“继续进行操作”，不执行任何操作。
- 单击“阻止所有访问”，禁止建立 Internet 连接。

应用程序已修改警报

如果在“安全设置”选项中选择“信任”安全级别，Personal Firewall 将自动为所有已修改的应用程序授予 Internet 访问权限。请查看事件的简要说明，然后选择以下选项：

- 单击“查看应用程序日志”，通过 Internet 应用程序日志获取有关事件的详细信息（详细信息，请参阅第 17 页的“关于 Internet 应用程序页面”）。
- 单击“关闭此警报类型”，防止出现此类警报。
- 单击“继续进行操作”，不执行任何操作。
- 单击“阻止所有访问”，禁止建立 Internet 连接。

蓝色警报

蓝色警报包含不需要进行响应的信息。

- **已阻止连接尝试** — Personal Firewall 在阻止不必要的 Internet 通讯或网络通讯时显示该警报（“信任”、“标准”或“严格”安全级别）。

已阻止连接尝试警报

如果选择“信任”、“标准”或“严格”安全级别，Personal Firewall 在阻止不希望出现的 Internet 通讯或网络通讯时将显示警报（图 2-10）。

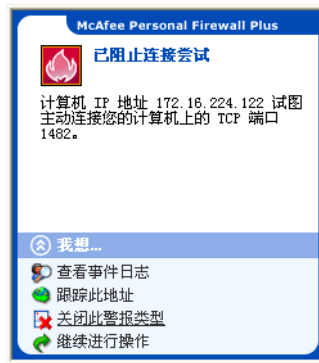


图 2-10. “已阻止连接尝试”警报

查看事件的简要说明，然后选择以下选项：

- 单击“查看事件日志”，通过 Personal Firewall 入站事件日志获取有关事件的详细信息（详细信息，请参阅第 19 页的“关于入站事件页面”）。
- 单击“跟踪此地址”，为该事件执行 IP 地址可视化跟踪。
- 单击“禁止此地址”，禁止该地址访问您的计算机。该地址将添加到“禁止的 IP 地址”列表中。
- 单击“信任此地址”，允许该 IP 地址访问您的计算机。
- 单击“继续进行操作”，不执行操作。

索引

B

报告事件, 24

C

测试 Personal Firewall, 11

G

跟踪事件, 24

H

HackerWatch.org

报告事件, 24

建议, 24

注册, 24

J

Internet 应用程序

更改应用程序规则, 18

关于, 17

允许和阻止, 18

IP 地址

关于, 20

禁止, 25

信任, 25

警报

Internet 应用程序已阻止, 29

已阻止连接尝试, 36

应用程序请求服务器访问权限, 29

应用程序已修改, 29

允许的新应用程序, 34

K

快速入门卡, iii

M

McAfee SecurityCenter, 12

默认防火墙, 设置, 9

P

Personal Firewall

测试, 11

使用, 13

R

入门, 7

S

事件

保存事件日志, 27

报告, 24

导出, 28

复制, 28

跟踪

查看保存的事件日志, 27

了解, 19

更多信息, 24

关于, 19

HackerWatch.org 建议, 24

环回, 20

来自 0.0.0.0, 20

来自 127.0.0.1, 20

来自 LAN 计算机, 21

来自专用 IP 地址, 21

清除事件日志, 27

删除, 28

显示

本周的, 22

今天的, 22

具有相同事件信息的, 23

来自某个地址的, 23

某一天的, 22

所有, 22

响应, 24

事件日志

查看, 27

管理, 27

关于, 19

W

Windows 防火墙, 9

Windows 自动更新, 29

X

系统要求, 9

显示事件日志中的事件, 22

卸载

 其他防火墙, 9

新功能, 7

Z

摘要页面, 13