McAfee®
personalfirewallplus

User Guide

McAfee®

Issued November 2005 / McAfee® Personal Firewall Plus software

Quick Start Card

If you are installing your product from a CD or a Web site, print this convenient reference page.
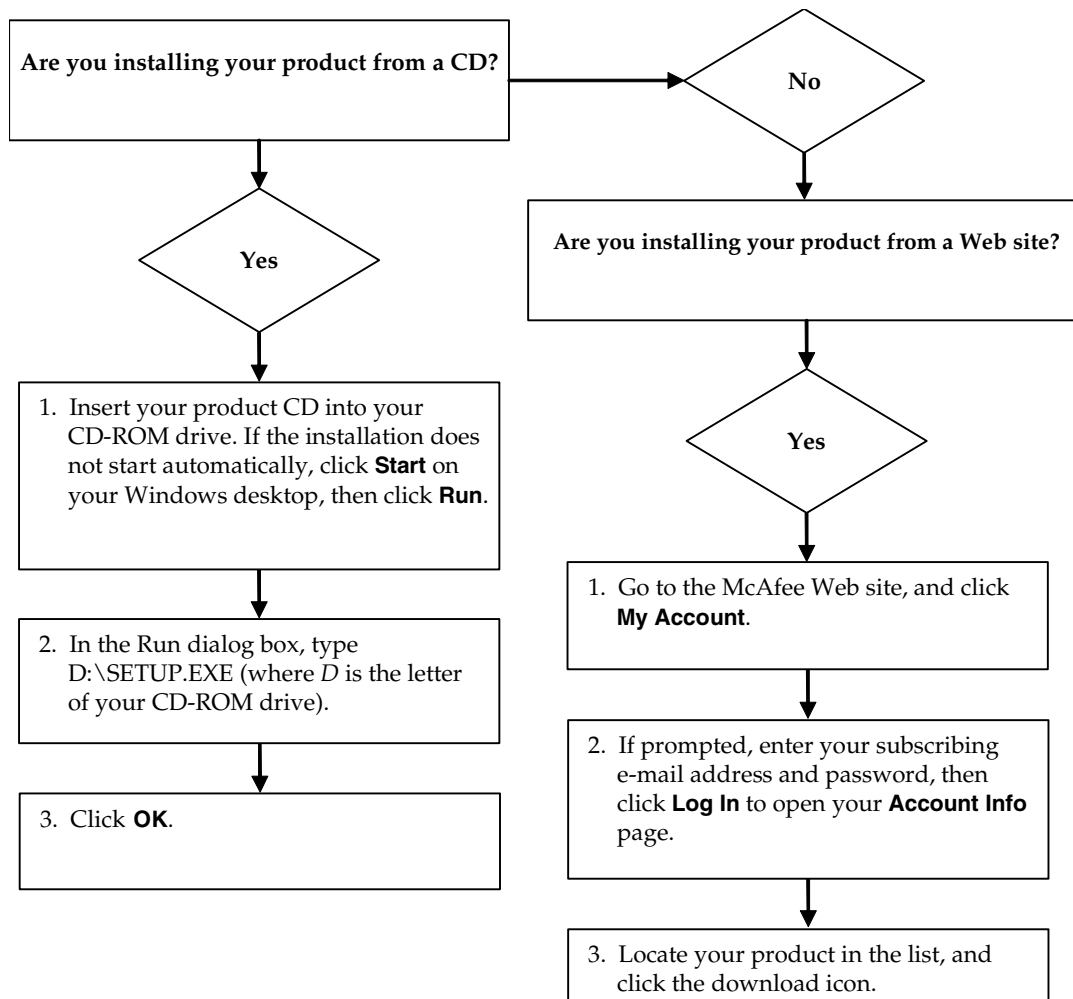
Are you installing your product from a CD? → **No**

Yes

1. Insert your product CD into your CD-ROM drive. If the installation does not start automatically, click **Start** on your Windows desktop, then click **Run**.

2. In the Run dialog box, type D:\SETUP.EXE (where *D* is the letter of your CD-ROM drive).

3. Click **OK**.

Are you installing your product from a Web site?

Yes

1. Go to the McAfee Web site, and click **My Account**.

2. If prompted, enter your subscribing e-mail address and password, then click **Log In** to open your **Account Info** page.

3. Locate your product in the list, and click the download icon.

For more information

To view the User Guides on the product CD, ensure that you have Acrobat Reader installed; if not, install it now from the McAfee product CD.

1 Insert your product CD into your CD-ROM drive.

2 Open Windows Explorer: Click **Start** on your Windows desktop, and click **Search**.

3 Locate the Manuals folder, and double-click the User Guide .PDF you want to open.

Registration benefits

McAfee recommends that you follow the easy steps within your product to transmit your registration directly to us. Registration ensures that you receive timely and knowledgeable technical assistance, plus the following benefits:

■ FREE electronic support

■ Virus definition (.DAT) file updates for one year after installation when you purchase VirusScan software

Go to http://www.mcafee.com/ for pricing of an additional year of virus signatures.

■ 60-day warranty that guarantees replacement of your software CD if it is defective or damaged

■ SpamKiller filter updates for one year after installation when you purchase SpamKiller software

Go to http://www.mcafee.com/ for pricing of an additional year of filter updates.

■ McAfee Internet Security Suite updates for one year after installation when you purchase MIS software

Go to http://www.mcafee.com/ for pricing of an additional year of content updates.

Technical Support

For technical support, please visit

http://www.mcafeehelp.com/.

Our support site offers 24-hour access to the easy-to-use Answer Wizard for solutions to the most common support questions.

Knowledgeable users can also try our advanced options, which include a Keyword Search and our Help Tree. If a solution cannot be found, you can also access our FREE Chat Now! and E-mail Express! options. Chat and e-mail help you to quickly reach our qualified support engineers through the Internet, at no cost. Otherwise, you can get phone support information at

http://www.mcafeehelp.com/.

Contents

Contents

Getting Started

1

Welcome to McAfee Personal Firewall Plus.

McAfee Personal Firewall Plus software offers advanced protection for your computer and your personal data. Personal Firewall establishes a barrier between your computer and the Internet, silently monitoring Internet traffic for suspicious activities.

With it, you get the following features:

■ Defends against potential hacker probes and attacks

■ Complements anti-virus defenses

■ Monitors Internet and network activity

■ Alerts you to potentially hostile events

■ Provides detailed information on suspicious Internet traffic

■ Integrates Hackerwatch.org functionality, including event reporting, self-testing tools, and the ability to email reported events to other online authorities

■ Provides detailed tracing and event research features

New features

■ **Improved Gaming Support**
McAfee Personal Firewall Plus protects your computer from intrusion attempts and suspicious activities during full-screen gameplay, but can hide alerts if it detects intrusion attempts or suspicious activities. Red alerts appear after you exit the game.

■ **Improved Access Handling**
McAfee Personal Firewall Plus lets users dynamically grant applications temporary access to the Internet. Access is restricted to the time the application launches until the time it closes. When Personal Firewall detects an unknown program, attempting to communicate with the Internet, a Red Alert provides the option to grant the application temporary access to the Internet.

■ **Enhanced Security Control**
Running the Lockdown feature in McAfee Personal Firewall Plus allows you to instantly block all incoming and outgoing Internet traffic between a computer and the Internet. Users can enable and disable Lockdown from three locations in Personal Firewall.

■ **Improved Recovery Options**
You can run Reset Options to automatically restore the default settings to Personal Firewall. If Personal Firewall exhibits undesirable behavior that you cannot correct, you can choose to undo your current settings and revert to the product's default settings.

■ **Internet Connectivity Protection**
To prevent a user from inadvertently disabling his or her Internet connection, the option to ban an Internet address is excluded on a Blue Alert when Personal Firewall detects an Internet connection originates from a DHCP or DNS server. If the incoming traffic does not originate from a DHCP or DNS server, the option appears.

■ **Enhanced HackerWatch.org Integration**
Reporting potential hackers is easier than ever. McAfee Personal Firewall Plus improves the functionality of HackerWatch.org, which includes event submission of potentially malicious events to the database.

■ **Extended Intelligent Application Handling**
When an application seeks Internet access, Personal Firewall first checks whether it recognizes the application as trusted or malicious. If the application is recognized as trusted, Personal Firewall automatically allows it access to the Internet so you do not have to.

■ **Advanced Trojan Detection**
McAfee Personal Firewall Plus combines application connection management with an enhanced database to detect and block more potentially malicious applications, such as Trojans, from accessing the Internet and potentially relaying your personal data.

■ **Improved Visual Tracing**
Visual Trace includes easy-to-read graphical maps showing the originating source of hostile attacks and traffic worldwide, including detailed contact/owner information from originating IP addresses.

■ **Improved Usability**
McAfee Personal Firewall Plus includes a Setup Assistant and a User Tutorial to guide users in the setup and use of their firewall. Although the product is designed to use without any intervention, McAfee provides users with a wealth of resources to understand and appreciate what the firewall provides for them.

■ **Enhanced Intrusion Detection**
Personal Firewall's Intrusion Detection System (IDS) detects common attack patterns and other suspicious activity. Intrusion detection monitors every data packet for suspicious data transfers or transfer methods and logs this in the event log.

■ **Enhanced Traffic Analysis**
McAfee Personal Firewall Plus offers users a view of both incoming and outgoing data from their computers, as well as displaying application connections including applications that are actively "listening" for open connections. This allows users to see and act upon applications that might be open for intrusion.

System requirements

■ Microsoft® Windows 98, Windows Me, Windows 2000, or Windows XP

■ Personal computer with Pentium-compatible processor
Windows 98, 2000: 133 MHz or higher
Windows Me: 150 MHz or higher
Windows XP (Home and Pro): 300 MHz or higher

■ RAM
Windows 98, Me, 2000: 64 MB
Windows XP (Home and Pro): 128 MB

■ 40 MB hard disk space

■ Microsoft® Internet Explorer 5.5 or later

> **NOTE**
> To upgrade to the latest version of Internet Explorer, visit the Microsoft web site at http://www.microsoft.com/.

Uninstalling other firewalls

Before you install McAfee Personal Firewall Plus software, you must uninstall any other firewall programs on your computer. Please follow your firewall program's uninstall instructions to do so.

> **NOTE**
> If you use Windows XP, you do not need to disable the built-in firewall before installing McAfee Personal Firewall Plus. However, we recommend that you do disable the built-in firewall. If you do not, you will not receive events in the Inbound Events log in McAfee Personal Firewall Plus.

Setting the default firewall

McAfee Personal Firewall can manage permissions and traffic for Internet applications on your computer, even if Windows Firewall is detected as running on your computer.

When installed, McAfee Personal Firewall automatically disables Windows Firewall and sets itself as your default firewall. You then experience only McAfee Personal Firewall functionality and messaging. If you subsequently enable Windows Firewall via Windows Security Center or Windows Control Panel, letting both firewalls run on your computer might result in partial loss of logging in McAfee Firewall as well as duplicate status and alert messaging.

> **NOTE**
> If both firewalls are enabled, McAfee Personal Firewall does not show all the blocked IP addresses in its Inbound Events tab. Windows Firewall intercepts most of these events and blocks those events, preventing McAfee Personal Firewall from detecting or logging those events. However, McAfee Personal Firewall might block additional traffic based upon other security factors, and that traffic will be logged.
>
> Logging is disabled in Windows Firewall by default, but if you choose to enable both firewalls, you can enable Windows Firewall logging. The default Windows Firewall log is C:\Windows\pfirewall.log

To ensure that your computer is protected by at least one firewall, Windows Firewall is automatically re-enabled when McAfee Personal Firewall is uninstalled.

If you disable McAfee Personal Firewall or set its security setting to **Open** without manually enabling Windows Firewall, all firewall protection will be removed except for previously blocked applications.

Setting the security level

You can configure security options to indicate how Personal Firewall responds when it detects unwanted traffic. By default, the **Standard** security level is enabled. In **Standard** security level, when an application requests Internet access and you grant it access, you are granting the application Full Access. Full Access allows the application the ability to both send data and receive unsolicited data on non-system ports.

To configure security settings:

1   Right-click the McAfee icon 🅼 in the Windows system tray, point to **Personal Firewall**, then select **Options**.

2   Click the **Security Settings** icon.

3 Set the security level by moving the slider to the desired level.

The security level ranges from Lockdown to Open:

- ◆ **Lockdown —** All Internet connections on your computer are closed. You can use this setting to block ports you configured to be open in the System Services page.

- ◆ **Tight Security —** When an application requests a specific type of access to the Internet (for example, Outbound Only Access), you can allow or disallow the application an Internet connection. If the application later requests Full Access, you can then grant Full Access or restrict it to Outbound Only access.

- ◆ **Standard Security (recommended) —** When an application requests and then is granted Internet access, the application receives full Internet access to handle incoming and outgoing traffic.

- ◆ **Trusting Security —** All applications are automatically trusted when they first attempt to access the Internet. However, you can configure Personal Firewall to use alerts to notify you about new applications on your computer. Use this setting if you find that some games or streaming media do not work.

- ◆ **Open —** Your firewall is disabled. This setting allows all traffic through Personal Firewall, without filtering.

    NOTE
    Previously blocked applications continue to be blocked when the firewall is set to the **Open** or **Lockdown** security setting. To prevent this, you can either change the application's permissions to **Allow Full Access** or delete the **Blocked** permission rule from the **Internet Applications** list.

4 Select additional security settings:

    NOTE
    If your computer runs Windows XP and multiple XP users have been added, these options are available only if you are logged on to your computer as an administrator.

- ◆ **Record Intrusion Detection (IDS) Events in Inbound Events Log —** If you select this option, events detected by IDS will appear in the Inbound Events log. The Intrusion Detection System detects common attack types and other suspicious activity. Intrusion detection monitors every inbound and outbound data packet for suspicious data transfers or transfer methods. It compares these to a "signature" database and automatically drops the packets coming from the offending computer.

IDS looks for specific traffic patterns used by attackers. IDS checks each packet that your machine receives to detect suspicious or known-attack traffic. For example, if Personal Firewall sees ICMP packets, it analyzes those packets for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns.

 ◆ **Accept ICMP ping requests** — ICMP traffic is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. If you select this option, Personal Firewall allows all ping requests without logging the pings in the Inbound Events log. If you do not select this option, Personal Firewall blocks all ping requests and logs the pings in the Inbound Events log.

 ◆ **Allow restricted users to change Personal Firewall settings** — If you run Windows XP or Windows 2000 Professional with multiple users, select this option to allow restricted XP users to modify Personal Firewall settings.

 5 Click **OK** if you are finished making changes.

Testing McAfee Personal Firewall Plus

You can test your Personal Firewall installation for possible vulnerabilities to intrusion and suspicious activity.

To test your Personal Firewall installation from the McAfee system tray icon:

 ▪ Right-click the McAfee icon in the Windows system tray, and select **Test Firewall**.

Personal Firewall opens Internet Explorer and goes to http://www.hackerwatch.org/, a web site maintained by McAfee. Please follow the directions on the Hackerwatch.org Probe page to test Personal Firewall.

Using McAfee SecurityCenter

McAfee SecurityCenter is your one-stop security shop, accessible from its icon in your Windows system tray or from your Windows desktop. With it, you can perform these useful tasks:

 ▪ Get free security analysis for your computer.

 ▪ Launch, manage, and configure all your McAfee subscriptions from one icon.

 ▪ See continuously updated virus alerts and the latest product information.

 ▪ Get quick links to frequently asked questions and account details at the McAfee web site.

NOTE
For more information about its features, click **Help** in the **SecurityCenter** dialog box.

While SecurityCenter is running and all of the McAfee features installed on your computer are enabled, a red M icon appears in the Windows system tray. This area is usually in the lower-right corner of the Windows desktop and contains the clock.

If one or more of the McAfee applications installed on your computer are disabled, the McAfee icon changes to black .

To launch the McAfee SecurityCenter:

1   Right-click the McAfee icon , then select **Open SecurityCenter**.

To launch Personal Firewall from McAfee SecurityCenter:

1   From SecurityCenter, click the **Personal Firewall Plus** tab.

2   Select a task from the I want to menu.

To launch Personal Firewall from Windows:

1   Right-click the McAfee icon in the Windows system tray, then point to **Personal Firewall**.

2   Select a task.

Using McAfee Personal Firewall Plus　　　2

To open Personal Firewall:

- Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select a task.

About the Summary page

The Personal Firewall Summary includes four summary pages:

- ◆ Main Summary

- ◆ Application Summary

- ◆ Event Summary

- ◆ HackerWatch Summary

The Summary pages contain a variety of reports on recent inbound events, application status, and world-wide intrusion activity reported by HackerWatch.org. You will also find links to common tasks performed in Personal Firewall.

To open the Main Summary page in Personal Firewall:

■ Right-click the McAfee icon ![M] in the Windows system tray, point to **Personal Firewall**, then select **View Summary** (Figure 2-1).

Figure 2-1. Main Summary page

Click the following to navigate to different Summary pages:

Item	Description
Change View	Click **Change View** to open a list of Summary pages. From the list, select a Summary page to view.
Right arrow	Click the right arrow icon to view the next Summary page.
Left arrow	Click the left arrow icon to view the previous Summary page.
Home	Click the home icon to return to the **Main Summary** page.

The Main Summary page provides the following information:

Item	Description
Security Setting	The security setting status tells you the level of security at which the firewall is set. Click the link to change the security level.
Blocked Events	The blocked events status displays the number of events that have been blocked today. Click the link to view event details from the Inbound Event page.

Item	Description
Application Rule Changes	The application rule status displays the number of application rules that have been changed recently. Click the link to view the list of allowed and blocked applications and to modify application permissions.
What's New?	**What's New?** shows the latest application that was granted full access to the Internet.
Last Event	**Last Event** shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Daily Report	**Daily Report** displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click the link to view event details from the Inbound Event page.
Active Applications	**Active Applications** displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view firewall activity and perform tasks.

To view the Application Summary page:

1   Right-click the McAfee icon **M** in the Windows system tray, point to **Personal Firewall**, then select **View Summary.**

2   Click **Change View**, then select **Application Summary**.

The Application Summary page provides the following information:

Item	Description
Traffic Monitor	The **Traffic Monitor** shows inbound and outbound Internet connections over the last fifteen minutes. Click the graph to view traffic monitoring details.
Active Applications	**Active Applications** shows the bandwidth use of your computer's most active applications during the last twenty-four hours. **Application**—The application accessing the Internet. **%**—The percentage of bandwidth used by the application. **Permission**—The type of Internet access that the application is allowed. **Rule Created**—When the application rule was created.
What's New?	**What's New?** shows the latest application that was granted full access to the Internet.

Item	Description
Active Applications	**Active Applications** displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view application status and perform application-related tasks.

To view the Event Summary page:

1 Right-click the McAfee icon ![M] in the Windows system tray, point to **Personal Firewall**, then select **View Summary.**

2 Click **Change View**, then select **Event Summary**.

The Event Summary page provides the following information:

Item	Description
Port Comparison	**Port Comparison** shows a pie chart of the most frequently attempted ports on your computer during the past 30 days. You can click a port name to view details from the Inbound Events page. You can also move your mouse pointer over the port number to see a description of the port.
Top Offenders	**Top Offenders** shows the most frequently blocked IP addresses, when the last inbound event occurred for each address, and the total number of inbound events in the past thirty days for each address. Click an event to view event details from the Inbound Events page.
Daily Report	**Daily Report** displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click a number to view the event details from the Inbound Events log.
Last Event	**Last Event** shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view details of events and perform event-related tasks.

To view the HackerWatch Summary page:

1 Right-click the McAfee icon ![M] in the Windows system tray, point to **Personal Firewall**, then select **View Summary.**

2 Click **Change View**, then select **HackerWatch Summary.**

The HackerWatch Summary page provides the following information.

Item	Description
World Activity	**World Activity** shows a world map identifying recently blocked activity monitored by HackerWatch.org. Click the map to open the Global Threat Analysis Map in HackerWatch.org.
Event Tracking	**Event Tracking** shows the number of inbound events submitted to HackerWatch.org.
Global Port Activity	**Global Port Activity** shows the top ports, in the past 5 days, that appear to be threats. Click a port to view the port number and port description.
Common Tasks	Click a link in **Common Tasks** to go to HackerWatch.org pages where you can get more information on world-wide hacker activity.

About the Internet Applications page

Use the Internet Applications page to view the list of allowed and blocked applications.

To launch the Internet Applications page:

■ Right-click the McAfee icon ![M] in the Windows system tray, point to **Personal Firewall**, then select **Applications** (Figure 2-2).
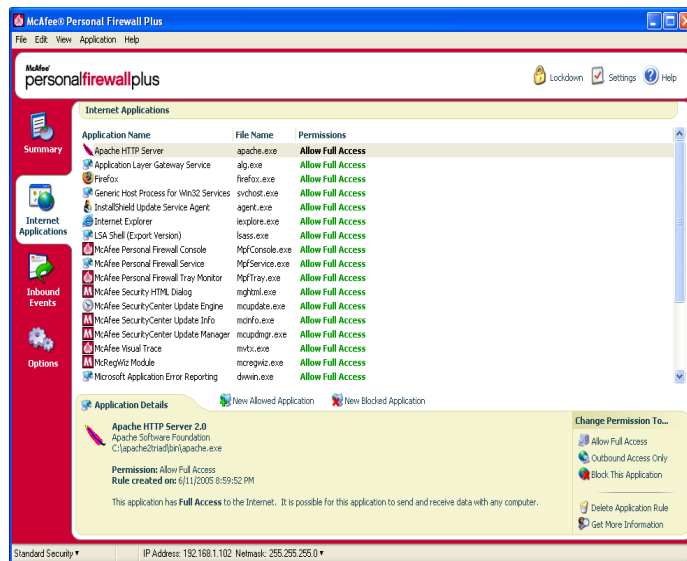
Figure 2-2. Internet Applications page

The Internet Applications page provides the following information:

■ Application names

■ File names

■ Current permission levels

■ Application details: application name and version, company name, path name, permission, timestamps, and explanations of permission types.

Changing application rules

Personal Firewall lets you change access rules for applications.

To change an application rule:

1   Right-click the McAfee icon, point to **Personal Firewall**, then select **Internet Applications**.

2   In the **Internet Applications** list, right-click the application rule for an application, and select a different level:

   ◆   **Allow Full Access —** Allow the application to establish outbound and inbound Internet connections.

   ◆   **Outbound Access Only —** Allow the application to establish an outbound Internet connection only.

   ◆   **Block This Application —** Disallow the application Internet access.

      NOTE
      Previously blocked applications continue to be blocked when the firewall is set to the **Open** or **Lockdown**. To prevent this from, you can either change the application's access rule to **Full Access** or delete the **Blocked** permission rule from the **Internet Applications** list.

To delete an application rule:

1   Right-click the McAfee icon ![M] in the Windows system tray, point to **Personal Firewall**, then select **Internet Applications**.

2   In the **Internet Applications** list, right-click the application rule, then select **Delete Application Rule**.

The next time the application requests Internet access, you can set its permission level to re-add it to the list.

Allowing and blocking Internet applications

To change the list of allowed and blocked Internet applications:

1   Right-click the McAfee icon ![M] in the Windows system tray, point to **Personal Firewall**, then select **Internet Applications**.

2   On the Internet Applications page, click one of the following options:

   ◆   **New Allowed Application** — Allow an application full Internet access.

   ◆   **New Blocked Application** — Disallow an application Internet access.

   ◆   **Delete Application Rule** — Remove an application rule.

About the Inbound Events page

Use the Inbound Events page to view the Inbound Events log, generated when Personal Firewall blocks unsolicited Internet connections.

To launch the Inbound Events page:

■ Right-click the McAfee icon 🅼 in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events** (Figure 2-3).
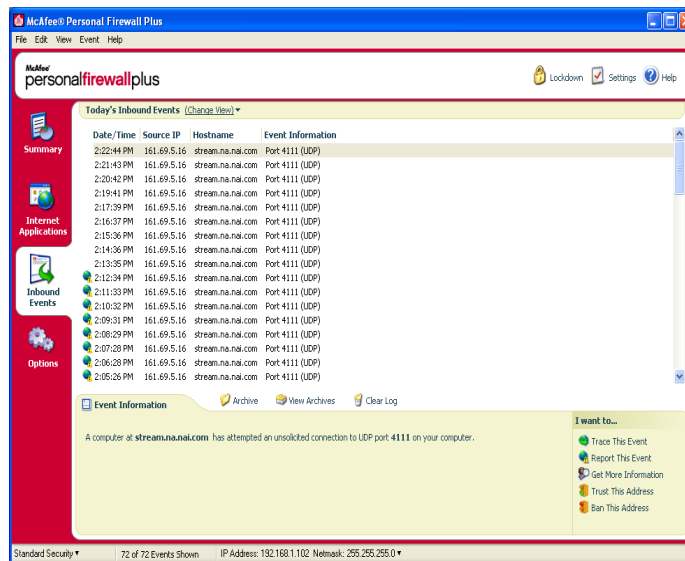
Figure 2-3. Inbound Events page

The Inbound Events page provides the following information:

■ Timestamps

■ Source IPs

■ Hostnames

■ Service or application names

■ Event details: connection types, connection ports, host name or IP, and explanations of port events

Understanding events

About IP addresses

IP addresses are numbers: four numbers each between 0 and 255 to be precise. These numbers identify a specific place that traffic can be directed to on the Internet.

IP address types

Several IP addresses are unusual for various reasons:

Non-routable IP addresses — These are also referred to as "Private IP Space." These IP addresses cannot be used on the Internet. Private IP blocks are 10.x.x.x, 172.16.x.x - 172.31.x.x, and 192.168.x.x.

Loop-back IP addresses — Loop-back addresses are used for testing purposes. Traffic sent to this block of IP addresses comes right back to the device generating the packet. It never leaves the device, and is primarily used for hardware and software testing. The Loop-Back IP block is 127.x.x.x.

Null IP address — This is an invalid address. When detected, Personal Firewall indicates that the traffic used a blank IP address. Frequently, this indicates that the sender is deliberately obscuring the origin of the traffic. The sender will not be able to receive any replies to their traffic unless the packet is received by an application that understands the contents of the packet that will include instructions specific to that application. Any address that starts with 0 (0.x.x.x) is a null address. For example, 0.0.0.0 is a null IP address.

Events from 0.0.0.0

If you see events from IP address 0.0.0.0, there are two likely causes. The first, and most common, is that your computer has received a badly formed packet. The Internet isn't always 100% reliable, and bad packets can occur. Since Personal Firewall sees the packets before TCP/IP can validate them, it might report these packets as an event.

The other situation occurs when the source IP is spoofed, or faked. Spoofed packets can be a sign that someone is scanning your computer for Trojans. Personal Firewall blocks this kind of activity, so your computer is safe.

Events from 127.0.0.1

Events will sometimes list their source IP as 127.0.0.1. This is called a loopback address or localhost.

Many legitimate programs use the loopback address for communication between components. For example, you can configure many personal E-mail or Web servers through a Web interface. To access the interface, you type "http://localhost/" in your Web browser.

Personal Firewall allows traffic from these programs, so if you see events from 127.0.0.1, it is likely that the source IP address is spoofed, or faked. Spoofed packets are usually indicate that another computer is scanning yours for Trojans. Personal Firewall blocks such intrusion attempts, so your computer is safe.

Some programs, notably Netscape 6.2 and higher, require you to add 127.0.0.1 to the Trusted IP Addresses list. These programs' components communicate between each other in such a manner that Personal Firewall cannot determine if the traffic is local or not.

In the example of Netscape 6.2, if you do not trust 127.0.0.1, then you will not be able to use your buddy list. Therefore, if you see traffic from 127.0.0.1 and all of the applications on your computer work normally, then it is safe to block this traffic. However, if a program (like Netscape) experiences problems, add 127.0.0.1 to the Trusted IP Addresses list in Personal Firewall.

If placing 127.0.0.1 in the trusted IP list fixes the problem, then you need to weigh your options: if you trust 127.0.0.1, your program will work, but you will be more open to spoofed attacks. If you do not trust the address, then your program will not work, but you will remain protected against certain malicious traffic.

Events from computers on your LAN

Events can be generated from computers on your local area network (LAN). To show that these events are generated by your network, Personal Firewall displays them in green.

In most corporate LAN settings, you should select **Make all computers on your LAN Trusted** in the Trusted IP Addresses options.

In some situations, your "local" network can be as dangerous than the Internet, especially if your computer runs on a high-bandwidth DSL or cable modem based network. In this case, do not to select **Make all computers on your LAN Trusted**. Instead, add the IP addresses of your local computers to the Trusted IP Addresses list.

Events from private IP addresses

IP addresses of the format 192.168.xxx.xxx, 10.xxx.xxx.xxx, and 172.16.0.0 - 172.31.255.255 are referred to as non-routable or private IP addresses. These IP addresses should never leave your network, and can be trusted most of the time.

The 192.168.xxx.xxx block is used with Microsoft Internet Connection Sharing (ICS). If you are using ICS, and see events from this IP block, you might want to add the IP address 192.168.255.255 to your Trusted IP Addresses list. This will trust the entire 192.168.xxx.xxx block.

If you are not on a private network, and see events from these IP ranges, the source IP address might be spoofed, or faked. Spoofed packets are usually signs that someone is scanning for Trojans. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe.

Since private IP addresses refer to different computers depending on what network you are on, reporting these events will have no effect, so there's no need to do so.

Showing events in the Inbound Events log

The Inbound Events log displays events in a number of ways. The default view limits the view to events which occur on the current day. You can also view events that occurred during the past week, or view the complete log.

Personal Firewall also lets you display inbound events from specific days, from specific Internet addresses (IP addresses), or events that contain the same event information.

For information about an event, click the event, and view the information in the **Event Information** pane.

Showing today's events

Use this option to review the day's events.

To show today's events:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2   On the Inbound Events log, right-click an entry, then click **Show Today's Events**.

Showing this week's events

Use this option to review weekly events.

To show this week's events:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2   On the Inbound Events log, right-click an entry, then click **Show This Week's Events**.

Showing the complete Inbound Events log

Use this option to review all events.

To show all of the events in the Inbound Events log:

1   Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.

2   On the Inbound Events log, right-click an entry, then click **Show Complete Log**.

The Inbound Events log displays all events from the Inbound Events log.

Showing events from a specific day

Use this option to review events from a specific day.

To show a day's events:

1 Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2 On the Inbound Events log, right-click an entry, then click **Show Only Events From this Day**.

Showing events from a specific Internet address

Use this option to review other events which originate from a particular Internet address.

To show events of an Internet address:

1 Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and click **Inbound Events**.

2 On the Inbound Events log, right-click an entry, then click **Show Only Events From Selected Internet Address**.

Showing events that share identical event information

Use this option to review other events in the Inbound Events log that have the same information in the Event Information column as the event you selected. You can find out how many times this event happened, and if it is from the same source. The Event Information column provides a description of the event and, if known, the common program or service that uses that port.

To show events that share identical event information:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and click **Inbound Events**.

2   On the Inbound Events log, right-click an entry, then click **Show Only Events with the same Event Information**.

Responding to inbound events

In addition to reviewing details about events in the Inbound Events log, you can perform a Visual Trace of the IP addresses for an event in the Inbound Events log, or get event details at the anti-hacker online community HackerWatch.org web site.

Tracing the selected event

You can try to perform a Visual Trace of the IP addresses for an event in the Inbound Events log.

To trace a selected event:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Inbound Events**.

2   On the Inbound Events log, right-click the event you want to trace, then click **Trace Selected Event**. You can also double-click an event to trace an event.

By default, Personal Firewall begins a Visual Trace using the integrated Personal Firewall Visual Trace program.

Getting advice from HackerWatch.org

To get advice from HackerWatch.org:

1   Right-click the McAfee icon, point to **Personal Firewall**, and select **Inbound Events**.

2   Select the event's entry on the Inbound Events page, then click **Get More Information** on the **I want to** pane.

Your default Web browser launches and opens the HackerWatch.org to retrieve information about the event type, and advice about whether to report the event.

Reporting an event

To report an event that you think was an attack on your computer:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Inbound Events**.

2   Click the event you want to report, then click **Report This Event** in the **I want to** pane.

Personal Firewall reports the event to the HackerWatch.org using your unique ID.

Signing up for HackerWatch.org

When you first open the Summary page, Personal Firewall contacts HackerWatch.org to generate your unique user ID. If you are an existing user, your sign-up is automatically validated. If you are a new user, you must enter a nickname and email address, then click the validation link in the confirmation email from HackerWatch.org to be able to use the event filtering/e-mailing features at its web site.

You can report events to HackerWatch.org without validating your user ID. However, to filter events and email events to a friend, you must sign up for the service.

Signing up for the service allows your submissions to be tracked and lets us notify you if HackerWatch.org needs more information or further action from you. We also require you to sign up because we must confirm any information we receive for that information to be useful.

All email addresses provided to HackerWatch.org are kept confidential. If a request for additional information is made by an ISP, that request is routed through HackerWatch.org; your email address is never exposed.

Trusting an address

You can use the Inbound Events page to add an IP address to the Trusted IP Addresses list to allow a permanent connection.

If you see an event in the Inbound Events page that contains an IP address that you need to allow, you can have Personal Firewall allow connections from it at all times.

To add an IP address to the Trusted IP Addresses list:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Inbound Events**.

2   Right-click the event whose IP address you want trusted, and click **Trust the Source IP Address**.

Verify that the IP address displayed in the Trust This Address dialog is correct, and click **OK**. The IP address is added to the Trusted IP Addresses list.

To verify that the IP address was added:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Options**.

2   Click the **Trusted & Banned IPs** icon, then the **Trusted IP Addresses** tab.

The IP address appears checked in the Trusted IP Addresses list.

Banning an address

If an IP address appears in your Inbound Events log, this indicates that traffic from that address was blocked. Therefore, banning an address adds no additional protection unless your computer has ports that are deliberately opened through the System Services feature, or unless your computer has an application that has permission to receive traffic.

Add an IP address to your banned list only if you have one or more ports that are deliberately open and if you have reason to believe that you must block that

If you see an event in the Inbound Events page that contains an IP address that you want to ban, you can configure Personal Firewall to prevent connections from it at all times.

You can use the Inbound Events page, which lists the IP addresses of all inbound Internet traffic, to ban an IP address that you suspect is the source of suspicious or undesirable Internet activity.

To add an IP address to the Banned IP Addresses list:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2   The Inbound Events page lists the IP addresses of all inbound Internet traffic. Select an IP address, and then do one of the following:

   ◆   Right-click the IP address, and then select **Ban the Source IP Address**.

   ◆   From the **I want to** menu, click **Ban This Addres**s.

3   In the Add Banned IP Address Rule dialog, use one or more of the following settings to configure the Banned IP Address rule:

   ◆   **A Single IP Address**: The IP address to ban. The default entry is the IP address that you selected from the Inbound Event page.

   ◆   **An IP Address Range**: The IP addresses between the address you specify in From IP Address and the IP address you specify in To IP Address.

◆ **Make this rule expire on**: Date and time in which the Banned IP Address rule expires. Select the appropriate drop down menus to select the date and the time.

◆ **Description**: Optionally describe the new rule.

◆ Click **OK**.

4 In the dialog box, click **Yes** to confirm your setting. Click **No** to return to the Add Banned IP Address Rule dialog.

If Personal Firewall detects an event from a banned Internet connection, it will alert you according to the method you specified on the Alert Settings page.

To verify that the IP address was added:

1 Click the **Options** tab.

2 Click the **Trusted & Banned IPs** icon, then click the **Banned IP Addresses** tab.

The IP address appears checked in the Banned IP Addresses list.

Managing the Inbound Events log

You can use the Inbound Events page to manage the events in the Inbound Events log generated when Personal Firewall blocks unsolicited Internet traffic.

Archiving the Inbound Events log

You can archive the current Inbound Events log to save all of the logged inbound events, including their date and times, source IPs, hostnames, ports, and event information. You should archive your Inbound Events log periodically to prevent the Inbound Events log from growing too large.

To archive the Inbound Events log:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2   On the Inbound Events page, click **Archive**.

3   On the Archive Log dialog, click **Yes** to proceed with the operation.

4   Click **Save** to save the archive in the default location, or browse to a location where you want to save the archive.

Note: By default, Personal Firewall automatically archives the Inbound Events log. Check or clear **Automatically archive logged events** in the Event Log Settings page to enable or disable the option.

Viewing an archived Inbound Events log

You can view any Inbound Events log that you previously archived. The saved archive includes date and times, source IPs, hostnames, ports, and event information for the events.

To view an archived Inbound Events log:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2   On the Inbound Events page, click **View Archives**.

3   Select or browse for the archive file name and click **Open**.

Clearing the Inbound Events log

You can clear all information from the Inbound Events log.

> **WARNING: Once you clear the Inbound Events log, you cannot recover it. If you think you will need the Events Log in the future, you should archive it instead.**

To clear the Inbound Events log:

1   Right-click the McAfee icon, point to **Personal Firewall**, then select **Inbound Events**.

2   On the Inbound Events page, click **Clear Log**.

3   Click **Yes** in the dialog to clear the log.

Copying an event to the Clipboard

You can copy an event to the clipboard so that you can paste it in a text file using Notepad.

To copy events to the clipboard:

1   Right-click the McAfee icon, point to **Personal Firewall**, then select **Inbound Events**.

2   Right-click the event in the Inbound Events log.

3   Click **Copy Selected Event to Clipboard**.

4   Launch Notepad.

   ◆   Type `notepad` on the command line or click the Windows **Start** button, point to **Programs**, then **Accessories**. Select **Notepad**.

5   Click **Edit**, and then click Paste. The event text appears in Notepad. Repeat this step until you have all of the necessary events.

6   Save the Notepad file in a safe place.

Deleting the selected event

You can delete events from the Inbound Events log.

To delete events from the Inbound Events log:

1   Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2   Click the event's entry on the Inbound Events page that you want to delete.

3   On the Edit menu, click **Delete Selected Event**. The event is deleted from the Inbound Events log.

About alerts

We strongly recommend that you become familiar with the types of alerts you will encounter while using Personal Firewall. Review the following types of alerts that can appear and the possible responses you can choose, so that you can confidently respond to an alert.

> **NOTE**
> Recommendations on alerts help you decide how to handle an alert. For recommendations to appear on alerts, click the **Options** tab, click the **Alert Settings** icon, then select either **Use Smart Recommendations** (the default) or **Display Smart Recommendations only** from the **Smart Recommendations** list.

Red alerts

Red alerts contain important information that requires your immediate attention:

- **Internet Application Blocked** — This alert appears if Personal Firewall blocks an application from accessing the Internet. For example, if a Trojan program alert appears, McAfee automatically denies this program access to the Internet and recommends that you scan your computer for viruses.

- **Application Wants to Access the Internet —** This alert appears when Personal Firewall detects Internet or network traffic for new applications.

- **Application Has Been Modified —**This alert appears when Personal Firewall detects that an application, previously allowed to access the Internet, has changed. If you have not recently upgraded the application, be careful about granting the modified application access to the Internet.

- **Application Requests Server Access —** This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has requested Internet access as a server.

> **NOTE**
> The Windows XP SP2 default Automatic Updates setting downloads and installs updates for the Windows OS and other Microsoft programs running on your computer without messaging you. When an application has been modified from one of Windows silent updates, McAfee Personal Firewall alerts appear the next time the Microsoft application is run.

> **IMPORTANT**
> You must grant access to applications that require Internet access for online product updates (such as McAfee services) to keep them up-to-date.

Internet Application Blocked alert

If a Trojan program alert appears (Figure 2-4), Personal Firewall automatically denies this program access to the Internet and recommends that you scan your computer for viruses. If McAfee VirusScan is not installed, you can launch McAfee SecurityCenter.
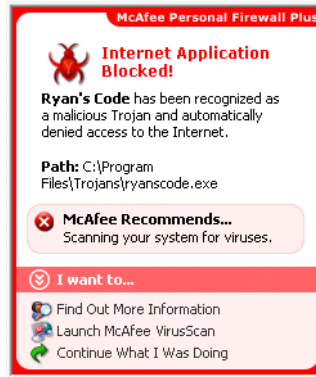
Figure 2-4. Internet Application Blocked alert

View a brief description of the event, then choose from these options:

- Click **Find Out More Information** to get details about the event through the Inbound Events log (see *About the Inbound Events page* on page 22 for details).

- Click **Launch McAfee VirusScan** to scan your computer for viruses.

- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

- Click **Grant Outbound Access** to allow an outbound connection (**Tight** security).

Application Wants to Access the Internet alert

If you selected **Standard** or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-5) when it detects Internet or network connections for new or modified applications.

Figure 2-5. Application Wants to Access the Internet alert

If an alert appears recommending caution in allowing the application Internet access, you can click **Click here to learn more** to get more information about the application. This option appears on the alert only if Personal Firewall is configured to use Smart Recommendations.

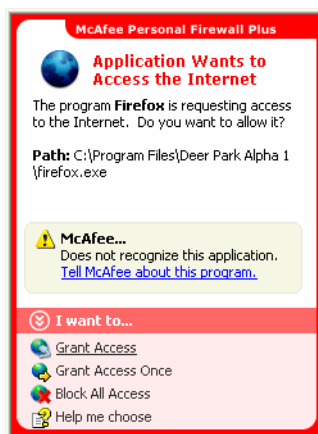McAfee might not recognize the application trying to gain Internet access (Figure 2-6).

Figure 2-6. Unrecognized Application alert

Therefore, McAfee cannot give you a recommendation on how to handle the application. You can report the application to McAfee by clicking **Tell McAfee about this program**. A web page appears and asks you for information related to the application. Please fill out as much information as you know.

The information you submit is used in conjunction with other research tools by our HackerWatch operators to determine whether an application warrants being listed in our known applications database, and if so, how it should be treated by Personal Firewall.

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application an outbound and inbound Internet connection.

- Click **Grant Access Once** to grant the application a temporary Internet connection. Access is limited to the time the application launches to the time it closes.

- Click **Block All Access** to prohibit an Internet connection.

- Click **Grant Outbound Access** to allow an outbound connection (**Tight** security).

- Click **Help me choose** to view online Help about application access permissions.

Application Has Been Modified alert

If you selected **Trusting**, **Standard**, or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-7) when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, be careful about granting the modified application access to the Internet.

Figure 2-7. Application Has Been Modified alert

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application an outbound and inbound Internet connection.

- Click **Grant Access Once** to grant the application a temporary Internet connection. Access is limited to the time the application launches to the time it closes.

- Click **Block All Access** to prohibit an Internet connection.

- Click **Grant Outbound Access** to allow an outbound connection (**Tight** security).

- Click **Help me choose** to view online Help about application access permissions.

Application Requests Server Access alert

If you selected **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 2-8) when it detects that an application you have previously allowed to access the Internet has requested Internet access as a server.
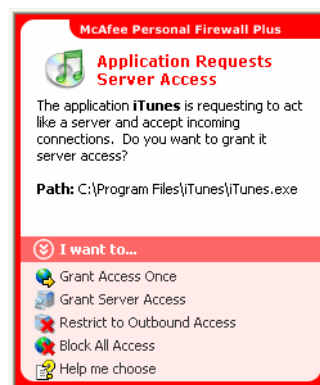
Figure 2-8. Application Requests Server Access alert

For example, an alert appears when MSN Messenger requests server access to send a file during a chat.

View a brief description of the event, then choose from these options:

- Click **Grant Access Once** to allow the application temporary Internet access. Access is limited to the time the application launches to the time it closes.

- Click **Grant Server Access** to allow the application an outbound and inbound Internet connection.

- Click **Restrict to Outbound Access** to prohibit an incoming Internet connection.

■ Click **Block All Access** to prohibit an Internet connection.

■ Click **Help me choose** to view online Help about application access permissions.Green alerts

Green alerts

Green alerts notify you of events in Personal Firewall, such as applications that have been automatically granted Internet access.

Program Allowed to Access the Internet — This alert appears when Personal Firewall automatically grants Internet access for all new applications, then notifies you (**Trusting** Security). An example of a modified application is one with modified rules to automatically allow the application Internet access.

Application Allowed to Access the Internet alert

If you selected **Trusting** security in the Security Settings options, Personal Firewall automatically grants Internet access for all new applications, then notifies you with an alert (Figure 2-9).
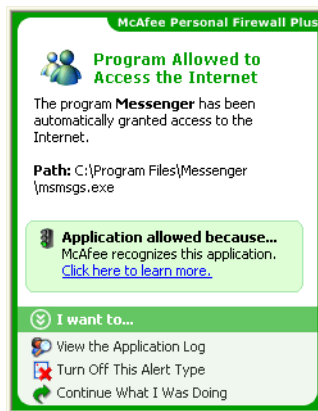
Figure 2-9. Program Allowed to Access the Internet

View a brief description of the event, then choose from these options:

■ Click **View the Application Log** to get details about the event through the Internet Applications Log (see *About the Internet Applications page* on page 20 for details).

■ Click **Turn Off This Alert Type** to prevent these types of alerts from appearing.

■ Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

■ Click **Block All Access** to prohibit an Internet connection.

Application Has Been Modified alert

If you selected **Trusting** security in the Security Settings options, Personal Firewall automatically grants Internet access for all modified applications. View a brief description of the event, then choose from these options:

- Click **View the Application Log** to get details about the event through the Internet Applications Log (see *About the Internet Applications page* on page 20 for details).

- Click **Turn Off This Alert Type** to prevent these types of alerts from appearing.

- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

- Click **Block All Access** to prohibit an Internet connection.

Blue alerts

Blue alerts contain information, but require no response from you.

■ **Connection Attempt Blocked —** This alert appears when Personal Firewall blocks unwanted Internet or network traffic. (Trusting, Standard, or Tight Security)

Connection Attempt Blocked alert

If you selected **Trusting**, **Standard**, or **Tight** security, Personal Firewall displays an alert (Figure 2-10) when it blocks unwanted Internet or network traffic.
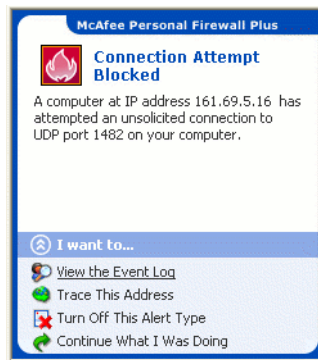
Figure 2-10. Connection Attempt Blocked alert

View a brief description of the event, then choose from these options:

■ Click **View the Event Log** to get details about the event through the Personal Firewall Inbound Events log (see *About the Inbound Events page* on page 22 for details).

■ Click **Trace This Address** to perform a Visual Trace of the IP addresses for this event.

■ Click **Ban This Address** to block this address from accessing your computer. The address is added to the Banned IP Addresses list.

■ Click **Trust This Address** to allow this IP address to access your computer.

■ Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done

Index