McAfee®

Personal Firewall 2007

User Guide

Contents

CHAPTER 1

McAfee Personal Firewall

Personal Firewall 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.

In this chapter

Features

Personal Firewall provides complete inbound and outbound firewall protection and automatically trusts known good programs and helps blocks spyware, Trojans, and key loggers. Firewall allows you to defend against hacker probes and attacks, monitors Internet and network activity, alerts you to hostile or suspicious events, provides detailed information about Internet traffic, and complements antivirus defenses.

Standard and custom protection levels

Guard against intrusion and suspicious activity using Firewall's default protection settings or customize Firewall to your own security needs.

Real-time recommendations

Receive recommendations, dynamically, to help you determine whether programs should be granted Internet access or network traffic should be trusted.

Intelligent access management for programs

Manage Internet access for programs, through alerts and Event Logs, or configure access permissions for specific programs from Firewall's Program Permissions pane.

Gaming protection

Prevent alerts regarding intrusion attempts and suspicious activities from distracting you during full-screen gameplay and configure Firewall to display alerts following completion of the computer game.

Computer startup protection

Before Windows opens, Firewall protects your computer from intrusion attempts and unwanted programs and network traffic.

System service port control

System Service ports can provide a backdoor to your computer. Firewall allows you to create and manage open and closed system service ports required by some programs.

Manage computer connections

Trust and ban remote connections and IP addresses that can connect to your computer.

HackerWatch information integration

HackerWatch is a security information hub that tracks global hacking and intrusion patterns as well as providing the most up-to-date information about programs on your computer. You can view global security event and Internet port statistics.

Lockdown Firewall

Instantly block all inbound and outbound Internet traffic between your computer and the Internet.

Restore Firewall

Instantly restore the original protection settings for Firewall. If Personal Firewall exhibits undesirable behavior that you cannot correct, you can restore Firewall to its default settings.

Advanced Trojan detection

Combines program connection management with an enhanced database to detect and block potentially malicious applications, such as Trojans, from accessing the Internet and relaying your personal data.

Event logging

Specify whether you want to enable or disable logging and, when enabled, which event types to log. Event logging allows you to view recent inbound and outbound events. You can also view intrusion detected events.

Monitor Internet traffic

Review easy-to-read graphical maps showing the source of hostile attacks and traffic worldwide. In addition, locate detailed owner information and geographical data for originating IP addresses. Also analyze inbound and outbound traffic, monitor program bandwidth and program activity.

Intrusion prevention

Protect your privacy by providing intrusion prevention of possible Internet threats. Using heuristic-like functionality, McAfee provides a tertiary layer of protection by blocking items that display symptoms of attacks or characteristics of hacking attempts.

Sophisticated traffic analysis

Review both inbound and outbound Internet traffic and program connections, including those that are actively listening for open connections. This allows you to see and act upon programs that can be vulnerable to intrusion.

Starting Firewall

As soon as you install Firewall, your computer is protected from intrusion and unwanted network traffic. In addition, you are ready to handle alerts and manage inbound and outbound Internet access for known and unknown programs. Smart Recommendations and Standard security level are automatically enabled.

Although you can disable Firewall from the Internet & Network Configuration pane, your computer will no longer be protected from intrusion and unwanted network traffic, and you will be unable to effectively manage inbound and outbound Internet connections. If you must disable firewall protection, do so temporarily and only when necessary. You can also enable Firewall from the Internet & Network Configuration panel.

Firewall automatically disables Windows® Firewall and sets itself as your default firewall.

Note: To configure Firewall, open the Internet & Network Configuration pane.

Start firewall protection

Enabling firewall protection defends your computer from intrusion and unwanted network traffic and helps you manage inbound and outbound Internet connections.

To enable firewall protection:

1. On the McAfee SecurityCenter pane, do one of the following:
   - Click **Internet & Network**, and then **Configure**.
   - Click **Advanced Menu**, then **Configure** on the **Home** pane, and then point to **Internet & Network**.
2. On the **Internet & Network Configuration** pane, under **Firewall protection**, click **On**.

Stop firewall protection

Disabling firewall protection leaves your computer vulnerable to intrusion and unwanted network traffic. Without firewall protection enabled, you cannot manage inbound and outbound Internet connections.

To disable firewall protection:

1. On the McAfee SecurityCenter pane, do one of the following:
   - Click **Internet & Network**, and then **Configure**.
   - Click **Advanced Menu**, then **Configure** on the **Home** pane, and then point to **Internet & Network**.
2. On the **Internet & Network Configuration** pane, under **Firewall protection**, click **Off**.

Working with alerts

Firewall employs an array of alerts to help you manage your security. These alerts can be grouped into four basic types.

- Trojan Blocked alert
- Red alert
- Yellow alert
- Green alert

Alerts can also contain information to help the user decide how to handle alerts or get information about programs running on their computer.

About alerts

Firewall has four basic alert types. As well, some alerts include information to help you learn or get information about programs running on your computer.

Trojan Blocked alert

A Trojan appears to be a legitimate program, but can disrupt, damage, and provide unauthorized access to your computer. The Trojan alert appears when Firewall detects, then blocks, a Trojan on your computer, and recommends that you scan for additional threats. This alert occurs in every security level, except Open or when Smart Recommendations is disabled.

Red alert

The most common type of alert is the red alert, which generally requires a response from you. Because Firewall is, in some cases, unable to automatically determine a particular course of action for a program activity or network event, the alert first describes the program activity or network event in question followed by one or more options to which you must respond. If Smart Recommendations is enabled, programs are added to the Program Permissions pane.

The following alert descriptions are the most commonly encountered:

- **Program requests Internet access**: Firewall detects a program attempting to access the Internet.
- **Program has been modified**: Firewall detects a program that has changed in some way, perhaps as a result of an online update.
- **Program Blocked**: Firewall blocks a program because it is listed on the Program Permissions pane.

Depending on your settings and program activity or network event, the following options are the most commonly encountered:

- **Grant access**: Allow a program on your computer access to the Internet. The rule is added to the Program Permissions page.
- **Grant access once**: Allow a program on your computer to temporarily access the Internet. For example, the installation of a new program may require access once only.
- **Block access**: Prevent a program's access to the Internet.

- **Grant outbound-only access**: Allow an outbound connection to the Internet only. This alert typically appears when Tight and Stealth security levels are set.
- **Trust this network**: Allow inbound and outbound traffic from a network. The network is added to the Trusted IP Addresses section.
- **Do not trust this network at this time**: Block inbound and outbound traffic from a network.

Yellow alert

The yellow alert is a non-critical notification which informs you about a network event detected by Firewall. For example, the **New Network Detected** alert appears when Firewall is run for the first time or when a computer with Firewall installed is connected to a new network. You can choose to trust or not trust the network. If the network is trusted, Firewall allows traffic from any other computer on the network and is added to Trusted IP Addresses.

Green alert

In most cases, a green alert provides basic information about an event and does not require a response. Green alerts usually occur when Standard, Tight, Stealth, and Lockdown security levels are set. Green alert descriptions are as follows:

- **Program has been Modified**: Informs you that a program that you previously allowed access to the Internet has been modified. You can opt to block the program, but if you do not respond, the alert disappears from your desktop and the program continues to have access.
- **Program Granted Internet Access**: Notifies you that a program has been granted Internet access. You can opt to block the program, but if you do not respond, the alert disappears and the program continues to access the Internet.

User Assistance

Many Firewall alerts contain additional information to help you manage your computer's security, which includes the following:

- **Learn more about this program**: Launch McAfee's global security Web site to get information about a program that Firewall has detected on your computer.
- **Tell McAfee about this program**: Send information to McAfee about an unknown file that Firewall has detected on your computer.
- **McAfee recommends**: Advice about handling alerts. For example, an alert can recommend that you grant access for a program.

Managing informational alerts

Firewall allows you to display or hide informational alerts during certain events.

Display alerts while gaming

By default, Firewall prevents informational alerts from appearing during full-screen gameplay. However, you can configure Firewall to show informational alerts during gameplay when Firewall detects intrusion attempts or suspicious activity.

To show alerts during gameplay:

1. On the Common Tasks pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the SecurityCenter Configuration pane, click **Alerts**.
4. Click **Advanced**.
5. On the **Alert Options** pane, select **Show informational alerts when gaming mode is detected**.

Hide informational alerts

Informational alerts notify you about events that do not require your immediate attention.

To hide informational alerts:

1. On the Common Tasks pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the SecurityCenter Configuration pane, click **Alerts**.
4. Click **Advanced**.
5. On the **SecurityCenter Configuration** pane, click **Informational Alerts**.
6. On the **Informational Alerts** pane, do one of the following:
   - Select an alert type to hide.
   - Select **Hide informational alerts** to hide all informational alerts.
7. Click **OK**.

CHAPTER 2

Configuring Firewall protection

Firewall offers a number of methods to manage your security and to tailor the way you want to respond to security events and alerts.

After you install Firewall for the first time, your level of protection is set to Standard security. For most, this setting meets all their security needs. However, Firewall provides other levels, ranging from highly restrictive to highly permissive.

Firewall also offers you the opportunity to receive recommendations on alerts and Internet access for programs.

In this chapter

Managing Firewall security levels

You can configure security levels to control the degree to which you want to manage and respond to alerts when Firewall detects unwanted network traffic and inbound and outbound Internet connections. By default, Standard security level is enabled.

When Standard security level is set and Smart Recommendations is enabled, red alerts provide the options to grant or block access for unknown or modified programs. When known programs are detected, green informational alerts appear, and access is automatically granted. Granting access allows a program to create outbound connections and to listen for unsolicited incoming connections.

Generally, the more restrictive a security level (Stealth and Tight), the greater the number of options and alerts that are displayed and which, in turn, must be handled by you.

Firewall employs six security levels. Starting from the most restrictive to the least, these levels include the following:

- **Lockdown**: Blocks all Internet connections.
- **Stealth**: Blocks all inbound Internet connections.
- **Tight**: Alerts require your response to every inbound and outbound Internet connection request.
- **Standard**: Alerts notify you when unknown or new programs require Internet access.
- **Trusting**: Grants all inbound and outbound Internet connections and automatically adds them to the Program Permissions pane.
- **Open**: Grants all inbound and outbound Internet connections.

Firewall also allows you to immediately reset your security level to standard from the Restore Firewall Protection Defaults pane.

Set security level to Lockdown

Setting the firewall's security level to Lockdown blocks all inbound and outbound network connections, including access to Web sites, e-mail, and security updates. This security level has the same result as removing your connection to the Internet. You can use this setting to block ports you set to open on the System Services pane. During Lockdown, alerts can continue to prompt you to block programs.

To set the firewall's security level to Lockdown:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Lockdown** displays as the current level.
3. Click **OK**.

Set security level to Stealth

Setting the firewall's security level to Stealth blocks all inbound network connections, except open ports. This setting completely hides your computer's presence on the Internet. When the security level is set to Stealth, the firewall alerts you when new programs attempt outbound Internet connections or receive inbound connection requests. Blocked and added programs appear on the Program Permissions pane.

To set the firewall's security level to Stealth:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Stealth** displays as the current level.
3. Click **OK**.

Set security level to Tight

When you set the security level to Tight, Firewall informs you when new programs attempt outbound Internet connections or receive inbound connection requests. Blocked and added programs appear on the Program Permissions pane. When the security level is set to Tight, a program only requests the type of access it requires at that time, for example outbound-only access, which you can either grant or block. Later, if the program requires both an inbound and an outbound connection, you can grant full access for the program from the Program Permissions pane.

To set the firewall's security level to Tight:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Tight** displays as the current level.
3. Click **OK**.

Set security level to Standard

Standard is the default and recommended security level.

When you set the firewall's security level to Standard, Firewall monitors inbound and outbound connections and alerts when new programs attempt Internet access. Blocked and added programs appear on the Program Permissions pane.

To set the firewall's security level to Standard:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Standard** displays as the current level.
3. Click **OK**.

Set security level to Trusting

Setting the firewall's security level to Trusting allows all inbound and outbound connections. In Trusting security, the firewall automatically grants access for all programs, and adds them to the list of allowed programs on the Program Permissions pane.

To set the firewall's security level to Trusting

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Trusting** displays as the current level.
3. Click **OK**.

Configuring Smart Recommendations for alerts

You can configure Firewall to include, exclude, or display recommendations in alerts regarding programs which attempt to access the Internet.

Enabling Smart Recommendations helps you decide how to handle alerts. When Smart Recommendations is enabled (and the security level is Standard), the Firewall automatically grants or blocks known programs, and alerts you and recommends a course of action when it detects unknown and potentially dangerous programs.

When Smart Recommendations is disabled, the Firewall neither grants or blocks Internet access automatically nor recommends a course of action.

When Firewall is configured to display Smart Recommendations only, an alert prompts you to grant or block access, but suggests a course of action.

Enable Smart Recommendations

Enabling Smart Recommendations helps you decide how to handle alerts. When Smart Recommendations is enabled, the Firewall automatically grants or blocks programs, and alerts you about unrecognized and potentially dangerous programs.

To enable Smart Recommendations:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under **Smart Recommendations**, select **Enable Smart Recommendations**.
3. Click **OK**.

Disable Smart Recommendations

When you disable Smart Recommendations, alerts exclude assistance about handling alerts and managing access for programs. If Smart Recommendations is disabled, the firewall continues to grant and block programs, and alerts you about unrecognized and potentially dangerous programs. And, if it detects a new program that is suspicious or is known to be a possible threat, Firewall automatically blocks the program from accessing the Internet.

To disable Smart Recommendations:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under **Smart Recommendations**, select **Disable Smart Recommendations**.
3. Click **OK**.

Display Smart Recommendations only

Displaying Smart Recommendations helps you decide how to handle alerts regarding unrecognized and potentially dangerous programs. When Smart Recommendations is set to **Display Only**, information about handling alerts is shown, but unlike the **Enable Smart Recommendations** option, the recommendations displayed are not automatically applied and programs' access are not automatically granted or blocked. Instead, alerts provide recommendations to help you decide to grant or block programs.

To display Smart Recommendations only:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under **Smart Recommendations**, select **Display Only**.
3. Click **OK**.

Optimizing Firewall security

There are many ways the security of your computer can be compromised. For example, some programs can attempt to connect to the Internet before Windows® starts. In addition, sophisticated computer users can ping your computer to determine whether it is connected to a network. Firewall allows you to defend against both types of intrusion by allowing you to enable boot time protection and to block ICMP ping requests. The first setting blocks programs from accessing the Internet as Windows starts and the second blocks ping requests that help other users detect your computer on a network.

Standard installation settings include automatic detection for the most common intrusion attempts, such as Denial of Service attacks or exploits. Using the standard installation settings ensures that you are protected against these attacks and scans; however, you can disable automatic detection for one or more attacks or scans on the Intrusion Detection pane.

Protect your computer during startup

Firewall can protect your computer as Windows starts up. Boot time protection blocks all new programs that have not been previously granted and require access to the Internet. After Firewall is launched, it displays relevant alerts for programs that had requested Internet access during startup, which you can grant or block. To use this option, your security level must not be set to Open or Lockdown.

To protect your computer during startup:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under Security Settings, select **Enable boot time protection**.
3. Click **OK**.

Note: Blocked connections and intrusions are not logged while boot time protection is enabled.

Configure ping request settings

Computer users can use a ping tool, which sends and receives ICMP Echo Request messages, to determine whether a given computer is connected to the network. You can configure Firewall to prevent or allow computer users to ping your computer.

To configure your ICMP ping requests setting:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, under **Security Settings**, do one of the following:
   - Select **Allow ICMP ping requests** to allow detection of your computer on the network using ping requests.
   - Clear **Allow ICMP ping requests** to prevent detection of your computer on the network using ping requests.
3. Click **OK**.

Configure intrusion detection

Intrusion detection (IDS) monitors data packets for suspicious data transfers or transfer methods. IDS analyzes traffic and data packets for specific traffic patterns used by attackers. For example, when Firewall detects ICMP packets, it analyzes these for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns. Firewall compares packets to a signature database and, if suspicious or harmful, drops the packets from the offending computer, and then optionally logs the event.

Standard installation settings include automatic detection for the most common intrusion attempts, such as Denial of Service attacks or exploits. Using the standard installation settings ensures that you are protected against these attacks and scans; however, you can disable automatic detection for one or more attacks or scans on the Intrusion Detection pane.

To configure intrusion detection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Intrusion Detection**.
3. Under **Detect Intrusion Attempts**, do one of the following:
   - Select a name to automatically detect the attack or scan.
   - Clear a name to disable automatic detection of the attack or scan.
4. Click **OK.**

Configure Firewall Protection Status settings

SecurityCenter tracks problems that are part of your overall computer Protection Status. However, you can configure Firewall to ignore specific problems on your computer which can affect your Protection Status. You can configure SecurityCenter to ignore when Firewall is set to Open security level, when the Firewall service is not running, and when an outbound-only firewall is not installed on your computer.

To configure Firewall Protection Status settings:

1. On the Common Tasks pane, click **Advanced Menu**.
2. Click **Configure**.
3. On the SecurityCenter Configuration pane, click **Alerts**.
4. Click **Advanced**.
5. On the Common Tasks pane, click **Advanced Menu**.
6. Click **Configure**.
7. On the SecurityCenter Configuration pane, click **Protection Status**.
8. Click Advanced.
9. In the Ignored Problems pane, select one or more of the following options:
   - **Firewall is set to Open security level.**
   - **Firewall service is not running.**
   - **Outbound firewall is not installed on your computer.**
10. Click **OK**.

Locking and restoring Firewall

Lockdown is helpful when handling computer-related emergencies, for users who need to block all traffic to isolate and troubleshoot a problem on their computer, or for those who are uncertain, and need to determine, how to manage a program's access to the Internet.

Lock Firewall instantly

Locking down Firewall instantly blocks all inbound and outbound network traffic between your computer and the Internet. It stops all remote connections from accessing your computer and blocks all programs on your computer from accessing the Internet.

To instantly lock Firewall and block all network traffic:

1. On the Home or Common Tasks panes with the **Basic** or **Advanced Menu** enabled, click **Lockdown Firewall**.
2. On the Lockdown Firewall pane, click **Lockdown**.
3. On the dialog, click **Yes** to confirm that you want to instantly block all inbound and outbound traffic.

Unlock Firewall instantly

Locking down Firewall instantly blocks all inbound and outbound network traffic between your computer and the Internet. It stops all remote connections from accessing your computer and blocks all programs on your computer from accessing the Internet. After you Lockdown Firewall, you can unlock it to allow network traffic.

To instantly unlock Firewall and allow network traffic:

1. On the Home or Common Tasks panes with the **Basic** or **Advanced Menu** enabled, click **Lockdown Firewall**.
2. On the Lockdown Enabled pane, click **Unlock**.
3. On the dialog, click **Yes** to confirm that you want to unlock Firewall and allow network traffic.

Restore Firewall settings

You can quickly restore Firewall to its original protection settings. This sets your security level to standard, enables Smart Recommendations, resets trusted and banned IP addresses, and removes all programs from the Program Permissions pane.

To restore Firewall to its original settings:

1. On the Home or Common Tasks panes with the **Basic** or **Advanced Menu** enabled, click **Restore Firewall Defaults**.
2. On the Restore Firewall Protection Defaults pane, click **Restore Defaults**.
3. On the Restore Firewall Protection Defaults dialog, click **Yes** to confirm that you want to restore the firewall configuration to its default settings.

Set security level to Open

Setting the firewall's security level to Open allows the firewall to grant access to all inbound and outbound network connections. To grant access for previously blocked programs, use the Program Permissions pane.

To set the firewall's security level to Open:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Security Level pane, move the slider so that **Open** displays as the current level.
3. Click **OK**.

Note: Previously blocked programs continue to be blocked when the firewall security level is set to **Open**. To prevent this, you can change the program's rule to **Full Access**.

CHAPTER 3

Managing programs and permissions

Firewall allows you to manage and create access permissions for existing and new programs that require inbound and outbound Internet access. Firewall allows you to grant full or outbound-only access for programs. You can also block access for programs.

In this chapter

Granting Internet access for programs

Some programs, like Internet browsers, need to access the Internet to function properly.

Firewall allows you use the Program Permissions page to:

- Grant access for programs
- Grant outbound-only access for programs
- Block access for programs

You can also grant full and outbound-only access from the Outbound Events and Recent Events log.

Grant full access for a program

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can modify these permissions.

To grant a program full Internet access:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program with **Blocked** or **Outbound-Only Access**.
4. Under **Action**, click **Grant Full Access**.
5. Click **OK**.

Grant full access for a new program

Many programs on your computer require inbound and outbound access to the Internet. Firewall includes a list of programs that are automatically allowed full access, but you can add a new program and change its permissions.

To grant a new program full Internet access:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the **Firewall** pane, click **Program Permissions**.
3. Under **Program Permissions**, click **Add Allowed Program**.
4. On the **Add Program** dialog browse for and select the program you want to add.
5. Click **Open**.
6. Click **OK**.

   The newly added program appears under **Program Permissions**.

Note: You can change the permissions of a newly added program as you would an existing program by selecting the program, and then clicking **Grant Outbound-Only Access** or **Block Access** under **Action**.

Grant full access from the Recent Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Recent Events log and grant it full Internet access.

To grant a program full access from the Recent Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under Recent Events, select the event description, and then click **Grant Full Access**.
3. In the Program Permissions dialog, click **Yes** to confirm that you want to grant the program full access.

Related topics

- View outbound events (page 54)

Grant full access from the Outbound Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Outbound Events log and grant it full access to the Internet.

To grant a program full Internet access from the Outbound Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.
4. In the Outbound Events pane, select a source IP address, and then click **Grant access**.
5. On the Program Permissions dialog, click **Yes** to confirm that you want to grant the program full Internet access.

Related topics

- View outbound events (page 54)

Granting outbound-only access for programs

Some programs on your computer only require outbound access to the Internet. Firewall allows you to grant programs outbound-only access to the Internet.

Grant outbound-only access for a program

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can modify these permissions.

To grant a program outbound-only access:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program with **Blocked** or **Full Access**.
4. Under **Action**, click **Grant Outbound-Only Access**.
5. Click **OK**.

Grant outbound-only access from the Recent Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Recent Events log and grant it outbound-only Internet access.

To grant a program outbound-only access from the Recent Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under Recent Events, select the event description, and then click **Grant Outbound-Only Access**.
3. In the Program Permissions dialog, click **Yes** to confirm that you want to grant the program outbound-only access.

Related topics

- View outbound events (page 54)

Grant outbound-only access from the Outbound Events log

Many programs on your computer require inbound and outbound access to the Internet. You can select a program from the Outbound Events log and grant it outbound-only Internet access.

To grant a program outbound-only access from the Outbound Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.
4. In the Outbound Events pane, select a source IP address, and then click **Grant outbound-Only Access**.
5. In the Program Permissions dialog, click **Yes** to confirm that you want to grant the program outbound-only access.

Related topics

- View outbound events (page 54)

Blocking Internet access for programs

Firewall allows you to block programs from accessing the Internet. Ensure that blocking a program will not interrupt with your network connection or another program that requires access to the Internet to function properly.

Block access for a program

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can block these permissions.

To block Internet access for a program:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program with **Full Access** or **Outbound-Only Access**.
4. Under **Action**, click **Block Access.**
5. Click **OK**.

Block access for a new program

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can add a new program and then block its access to the Internet.

To block Internet access for a new program:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. Under the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, click **Add Blocked Program**.
4. On the **Add Program** dialog browse for and select the program you want to add.
5. Click **Open**.
6. Click **OK**.

   The newly added program appears under **Program Permissions**.

Note: You can change the permissions of a newly added program as you would an existing program by selecting the program and then clicking **Grant Outbound-Only Access** or **Grant Full Access** under **Action**.

Block access from the Recent Events log

Many programs on your computer require inbound and outbound access to the Internet. However, you can also opt to block programs from accessing the Internet from the Recent Events log.

To block access for a program from the Recent Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under Recent Events, select the event description, and then click **Block Access**.
3. In the Program Permissions dialog, click **Yes** to confirm that you want to block the program.

Related topics

- View outbound events (page 54)

Removing access permissions for programs

Before removing a program permission for a program, ensure that its absence does not affect your computer's functionality or your network connection.

Remove a program permission

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can remove programs that have been automatically and manually added.

To remove a program permission for a new program:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program.
4. Under **Action**, click **Delete Program Permission**.
5. Click **OK**.

   The program is removed from the Program Permissions pane.

Note: Firewall prevents you from modifying some programs by dimming and disabling actions.

Learning about programs

If you are unsure which program permission to apply, you can get information about the program to help you decide on McAfee's HackerWatch Web site

Get program information

Many programs on your computer require inbound and outbound access to the Internet. Personal Firewall includes a list of programs that are automatically allowed full access, but you can modify these permissions.

Firewall can help you decide to grant or block Internet access for a program. Ensure that you are connected to the Internet so that your browser successfully launches McAfee's HackerWatch Web site, which provides up-to-date information about programs, Internet access requirements, and security threats.

To get program information:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Program Permissions**.
3. Under **Program Permissions**, select a program.
4. Under **Action**, click **Learn More**.

Get program information from the Outbound Events log

Personal Firewall allows you to get information about programs that appear in the Outbound Events log.

Before getting information about a program, ensure that you have an Internet connection and an Internet browser.

To get program information from the Outbound Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.
4. On the Outbound Events pane, select a source IP address, and then click **Learn more**.

   You can view information about the program on the HackerWatch Web site. HackerWatch provides up-to-date information about programs, Internet access requirements, and security threats.

Related topics

- View outbound events (page 54)

CHAPTER 4

Managing system services

To work properly, certain programs (including Web servers and file-sharing server programs) must accept unsolicited connections from other computers through designated system service ports. Typically, Firewall closes these system service ports because they represent the most likely source of insecurities in your system. To accept connections from remote computers, however, the system service ports must be open.

This list shows the standard ports for common services.

- File Transfer Protocol (FTP) Ports 20-21
- Mail Server (IMAP) Port 143
- Mail Server (POP3) Port 110
- Mail Server (SMTP) Port 25
- Microsoft Directory Server (MSFT DS) Port 445
- Microsoft SQL Server (MSFT SQL) Port 1433
- Remote Assistance / Terminal Server (RDP) Port 3389
- Remote Procedure Calls (RPC) Port 135
- Secure Web Server (HTTPS) Port 443
- Universal Plug and Play (UPNP) Port 5000
- Web Server (HTTP) Port 80
- Windows File Sharing (NETBIOS) Ports 137-139

In this chapter

Configuring system service ports

To allow remote access to a service on your computer you must specify the service and associated port to open. Only select a service and port if you are certain it must be open. Rarely is it necessary to open a port.

Allow access to an existing system service port

From the System Services pane, you can open or close an existing port to allow or deny remote access to a network service on your computer. An open system service port can make your computer vulnerable to Internet security threats; therefore only open a port, if necessary.

To allow access to a system service port:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **System Services**.
3. Under **Open System Service Port**, select a system service to open a port.
4. Click **OK**.

Block access to an existing system service port

From the System Services pane, you can open or close an existing port to allow or deny remote access to a network service on your computer. An open system service port can make your computer vulnerable to Internet security threats; therefore only open a port, if necessary.

To block access to a system service port:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. Under the Firewall pane, click **System Services**.
3. Under **Open System Service Port**, clear a system service to close a port.
4. Click **OK**.

Configure a new system service port

From the System Services pane, you can add a new system service port which, in turn, you can open or close to allow or deny remote access to a network service on your computer. An open system service port can make your computer vulnerable to Internet security threats, therefore only open a port when necessary.

To create and configure a new system service port:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **System Services**.
3. Click **Add**.
4. Under **Add Port Configuration**, specify the following:
   - Program name
   - Inbound TCP/IP ports
   - Outbound TCP/IP ports
   - Inbound UDP ports
   - Outbound UDP ports
5. Optionally describe the new configuration.
6. Click **OK**.

   The newly configured system service port appears under **Open System Service Port**.

Modify a system service port

An open and closed port allows and denies access to a network service on your computer. From the System Services pane, you can modify inbound and outbound information for an existing port. If port information is entered incorrectly, the system service fails.

To modify a system service port:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **System Services**.
3. Select a system service, and click **Edit**.
4. Under **Add Port Configuration**, specify the following:
   - Program name
   - Inbound TCP/IP ports
   - Outbound TCP/IP ports
   - Inbound UDP ports

- Outbound UDP ports

5 Optionally describe the modified configuration.

6 Click **OK**.

The modified configure system service port appears under **Open System Service**.

Remove a system service port

An open or closed port allows or denies access to a network service on your computer. From the System Services pane, you can remove an existing port and associated system service. After a port and system service is removed from the System Services pane, remote computers are no longer able to access the network service on your computer.

To remove a system service port:

1 On the Internet & Network Configuration pane, click **Advanced**.

2 On the Firewall pane, click **System Services**.

3 Select a system service, and then click **Remove**.

4 On the **System Services** dialog, click **Yes** to confirm that you want to delete the system service.

The system service port no longer appears in the System Services pane.

CHAPTER 5

Managing computer connections

You can configure Firewall to manage specific remote connections to your computer by creating rules, based on Internet Protocol addresses (IPs), that are associated with remote computers. Computers that are associated with trusted IP addresses can be trusted to connect to your computer and those IPs that are unknown, suspicious, or distrusted, can be banned from connecting to your computer.

When allowing a connection, ensure that the computer that you trust is safe. If a computer that you trust is infected through a worm or other mechanism, your computer can be vulnerable to infection. In addition, McAfee recommends that the computer(s) you trust are protected by a firewall and an up-to-date antivirus program also. Firewall does not log traffic or generate event alerts from IP addresses in the Trusted IP Addresses list.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

In this chapter

Trusting computer connections

You can add, edit, and remove trusted IP addresses in the Trusted and Banned IPs pane, under **Trusted IP Addresses**.

The **Trusted IP Addresses** list on the Trusted and Banned IPs pane lets you allow all traffic from a specific computer to reach your computer. Firewall does not log traffic or generate event alerts from IP addresses that appear in the **Trusted IP Addresses** list.

Firewall trusts any checked IP addresses on the list, and always allows traffic from a trusted IP through the firewall on any port. Firewall does not log any events from trusted IP addresses. Activity between the computer associated with a trusted IP address and your computer is not filtered or analyzed by Firewall.

When allowing a connection, ensure that the computer that you trust is safe. If a computer that you trust is infected through a worm or other mechanism, your computer can be vulnerable to infection. In addition, McAfee recommends that the computer(s) you trust are protected by a firewall and an up-to-date antivirus program also.

Add a trusted computer connection

You can use Firewall to add a trusted computer connection and its associated IP address.

The **Trusted IP Addresses** list on the Trusted and Banned IPs pane lets you allow all traffic from a specific computer to reach your computer. Firewall does not log traffic or generate event alerts from IP addresses that appear in the **Trusted IP Addresses** list.

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To add a trusted computer connection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Trusted IP Addresses**.
4. Click **Add**.
5. Under **Add Trusted IP Address Rule**, do one of the following:
   - Select a **Single IP Address**, and then enter the IP address.

- Select an **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** boxes.

6 Optionally select **Rule expires in**, and enter the number of days to enforce the rule.

7 Optionally, type a description for the rule.

8 Click **OK**.

9 In the Add Trusted IP Address Rule dialog, click **Yes** to confirm that you want to add the trusted computer connection.

The newly added IP address appears under **Trusted IP Addresses**.

Add a trusted computer from the Inbound Events log

You can add a trusted computer connection and its associated IP address from the Inbound Events log.

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To add a trusted computer connection from the Inbound Events log:

1 Ensure the Advanced menu is enabled. On the Common Tasks pane, click **Reports & Logs**.

2 Under **Recent Events**, click **View Log**.

3 Click **Internet & Network**, and then **Inbound Events**.

4 On the Inbound Events pane, select a source IP address, and then click **Trust this address**.

5 In the Add Trusted IP Address Rule dialog, click **Yes** to confirm that you want to trust the IP address.

The newly added IP address appears under **Trusted IP Addresses**.

Related topics

- Event Logging (page 52)

Edit a trusted computer connection

You can use Firewall to edit a trusted computer connection and its associated IP address.

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To edit a trusted computer connection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Trusted IP Addresses**.
4. Select an IP address, and then click **Edit**.
5. Under **Add Trusted IP Address Rule**, do one of the following:
   - Select a **Single IP Address**, and then enter the IP address.
   - Select an **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** boxes.
6. Optionally, check **Rule expires in**, and enter the number of days to enforce the rule.
7. Optionally, type a description for the rule.
8. Click **OK**.

   The modified IP address appears under **Trusted IP Addresses**.

Remove a trusted computer connection

You can use Firewall to remove a trusted computer connection and its associated IP address.

Computers associated with trusted IP addresses can always connect to your computer. Before adding, editing, or removing a trusted IP address, ensure it is one with which it is safe to communicate or remove.

To remove a trusted computer connection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Trusted IP Addresses**.
4. Select an IP address, and then click **Remove**.
5. In the **Trusted and Banned IPs** dialog, click **Yes** to confirm that you want to remove the trusted IP address under **Trusted IP Addresses**.

Banning computer connections

You can add, edit, and remove trusted IP addresses in the Trusted and Banned IPs pane, under **Banned IP Addresses**.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

Add a banned computer connection

You can use Firewall to add a banned computer connection and its associated IP address.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

To add a banned computer connection:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Banned IP Addresses**.
4. Click **Add**.
5. Under Add Banned IP Address Rule, do one of the following:
   - Select a **Single IP Address**, and then enter the IP address.
   - Select an **IP Address Range**, and then enter the starting and ending IP addresses in the **From IP Address** and **To IP Address** fields.

6 Optionally, check **Rule expires in**, and enter the number of days to enforce the rule.

7 Optionally, type a description of the rule.

8 Click **OK**.

9 On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm that you want to add the banned computer connection.

The newly added IP address appears under **Banned IP Addresses**.

Edit a banned computer connection

You can use Firewall to edit a banned computer connection and its associated IP address.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

To edit a banned computer connection:

1 From the Internet & Network Configuration pane, click **Advanced**.

2 On the Firewall pane, click **Trusted and Banned IPs**.

3 On the Trusted and Banned IPs pane, select **Banned IP Addresses**.

4 Select an IP address, and then click **Edit**.

5 Under **Add Trusted IP Address Rule**, do one of the following:

- Select a **Single IP Address**, and then type the IP address.
- Select an **IP Address Range**, then type the starting and ending IP addresses in the **From IP Address** and **To IP Address** fields.

6 Optionally, check **Rule expires in**, and type the number of days to enforce the rule.

7 Optionally, type a description of the rule.

Click **OK**. The modified IP address appears under **Banned IP Addresses**.

Remove a banned computer connection

You can use Firewall to remove a banned computer connection and its associated IP address.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

To remove a banned computer connection:

1. From the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Trusted and Banned IPs**.
3. On the Trusted and Banned IPs pane, select **Banned IP Addresses**.
4. Select an IP address, and click **Remove**.
5. On the **Trusted and Banned IPs** dialog, click **Yes** to confirm that you want to remove the IP address from **Banned IP Addresses**.

Ban a computer from the Inbound Events log

You can ban a computer connection and its associated IP address from the Inbound Events log.

IP addresses which appear in the Inbound Events log are blocked. Therefore, banning an address adds no additional protection unless your computer use ports that are deliberately opened or unless your computer includes a program that has been granted access to the Internet.

Add an IP address to your **Banned IP Addresses** 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 address from accessing open ports.

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 ban a trusted computer connection from the Inbound Events log:

1. Ensure the Advanced menu is enabled. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Click **Internet & Network**, and then **Inbound Events**.
4. In the Inbound Events pane, select a source IP address, and then click **Ban this address**.
5. On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm that you want to ban the IP address.

   The newly added IP address appears under **Banned IP Addresses**.

Related topics

- Event Logging (page 52)

Ban a computer from the Intrusion Detection Events log

You can ban a computer connection and its associated IP address from the Intrusion Detection Events log.

Computers that are associated with unknown, suspicious, or distrusted IP addresses can be banned from connecting to your computer.

Since Firewall blocks all unwanted traffic, it is normally not necessary to ban an IP address. You should ban an IP address only when you are certain an Internet connection poses a specific threat. Ensure that you do not block important IP addresses, such as your DNS or DHCP server, or other ISP-related servers. Depending on your security settings, Firewall can alert you when it detects an event from a banned computer.

To ban a computer connection from the Intrusion Detection Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Click **Internet & Network**, and then click **Intrusion Detection Events**.
4. In the Intrusion Detection Events pane, select a source IP address, and then click **Ban this address**.
5. On the **Add Banned IP Address Rule** dialog, click **Yes** to confirm that you want to ban the IP address.

   The newly added IP address appears under **Banned IP Addresses**.

Related topics

- Event Logging (page 52)

CHAPTER 6

Logging, monitoring, and analysis

Firewall provides extensive and easy-to-read logging, monitoring, and analysis for Internet events and traffic. Understanding Internet traffic and events helps you manage your Internet connections.

In this chapter

Event Logging

Firewall allows you to specify whether you want to enable or disable logging and, when enabled, which event types to log. Event logging allows you to view recent inbound and outbound events. You can also view intrusion detected events.

Configure event log settings

To track firewall events and activity, you can specify and configure the types of events to view.

To configure event logging:

1. On the Internet & Network Configuration pane, click **Advanced**.
2. On the Firewall pane, click **Event Log Settings**.
3. On the Event Log Settings pane, do one of the following:
   - Select **Log the event** to enable event logging.
   - Select **Do not log the event** to disable event logging.
4. Under **Event Log Settings**, specify which events types to log. Event types include the following:
   - ICMP Pings
   - Traffic from Banned IP Addresses
   - Events on System Service Ports
   - Events on Unknown Ports
   - Intrusion Detection (IDS) events
5. To prevent logging on specific ports, select **Do not log events on the following port(s)**, and then enter single port numbers separated by commas, or port ranges with dashes. For example, `137-139, 445, 400-5000`.
6. Click **OK**.

View recent events

If logging is enabled, you can view recent events. The Recent Events pane shows the date and description of the event. The Recent Events pane only displays activity for programs that have been explicitly blocked from accessing the Internet.

To view Firewall's recent events:

- On the **Advanced Menu**, under the Common Tasks pane, click **Reports & Logs** or **View Recent Events**. Alternatively, click **View Recent Events** under the Common Tasks pane from the Basic Menu.

View inbound events

If logging is enabled, you can view and sort inbound events.

The Inbound Events log includes the following logging categories:

- Date and time
- Source IP address
- Host name
- Information and event type

To view your firewall's inbound events:

1. Ensure the Advanced menu is enabled. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Click **Internet & Network**, and then **Inbound Events**.

Note: You can trust, ban, and trace an IP address from the Inbound Event log.

Related topics

- Add a trusted computer from the Inbound Events log (page 43)
- Ban a computer from the Inbound Events log (page 49)
- Trace a computer from the Inbound Events log (page 57)

View outbound events

If logging is enabled, you can view outbound events. Outbound Events include the name of the program attempting outbound access, the date and time of the event, and the location of the program on your computer.

To view your firewall's outbound events:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Select **Internet & Network**, and then **Outbound Events**.

Note: You can grant full and outbound-only access for a program from the Outbound Events log. You can also locate additional information about the program.

Related topics

- Grant full access from the Outbound Events log (page 28)
- Grant outbound-only access from the Outbound Events log (page 30)
- Get program information from the Outbound Events log (page 35)

View intrusion detection events

If logging is enabled, you can view inbound events. Intrusion Detection events display the date and time, the source IP, and the host name of the event. The log also describes the type of event.

To view your intrusion detection events:

1. Under the Common Tasks pane, click **Reports & Logs**.
2. Under Recent Events, click **View Log**.
3. Click **Internet & Network**, and then click **Intrusion Detection Events**.

Note: You can ban and trace an IP address from the Intrusion Detection Events log.

Related topics

- Ban a computer from the Intrusion Detection Events log (page 50)
- Trace a computer from the Intrusion Detection Events log (page 58)

Working with Statistics

Firewall leverages McAfee's HackerWatch security Web site to provide you with statistics about global Internet security events and port activity.

View global security event statistics

HackerWatch tracks worldwide Internet security events, which you can view from SecurityCenter. Information tracked lists incidents reported to HackerWatch in the last 24 hours, 7 days, and 30 days.

To view global security statistics:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **HackerWatch**.
3. View security event statistics under **Event Tracking**.

View global Internet port activity

HackerWatch tracks worldwide Internet security events, which you can view from SecurityCenter. Information displayed includes the top event ports reported to HackerWatch during the past seven days. Typically, HTTP, TCP, and UDP port information is displayed.

To view worldwide port activity:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **HackerWatch**.
3. View the top event port events under **Recent Port Activity**.

Tracing Internet traffic

Firewall offers a number of options for tracing Internet traffic. These options let you geographically trace a network computer, obtain domain and network information, and trace computers from the Inbound Events and Intrusion Detection Events logs.

Geographically trace a network computer

You can use Visual Tracer to geographically locate a computer that is connecting or attempting to connect to your computer, using its name or IP address. You can also access network and registration information using Visual Tracer. Running Visual Tracer displays a world map which displays the most probable route of data taken from the source computer to yours.

To geographically locate a computer:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Visual Tracer**.
3. Type the computer's IP address, and click **Trace**.
4. Under **Visual Tracer**, select **Map View**.

Note: You cannot trace looped, private, or invalid IP address events.

Obtain computer registration information

You can obtain a computer's registration information from SecurityCenter using Visual Trace. Information includes the domain name, the registrant's name and address, and the administrative contact.

To obtain a computer's domain information:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Visual Tracer**.
3. Type the computer's IP address, and then click **Trace**.
4. Under **Visual Tracer**, select **Registrant View**.

Obtain computer network information

You can obtain a computer's network information from SecurityCenter using Visual Trace. Network information includes details about the network on which the domain resides.

To obtain a computer's network information:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Visual Tracer**.
3. Type the computer's IP address, and then click **Trace**.
4. Under **Visual Tracer**, select **Network View**.

Trace a computer from the Inbound Events log

From the Inbound Events pane, you can trace an IP address that appears in the Inbound Events log.

To trace a computer's IP address from the Inbound Events log:

1. Ensure the Advanced menu is enabled. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Click **Internet & Network**, and then **Inbound Events**.
4. On the Inbound Events pane, select a source IP address, and then click **Trace this address**.
5. On the Visual Tracer pane, click one of the following:
   - **Map View**: Geographically locate a computer using the selected IP address.
   - **Registrant View**: Locate domain information using the selected IP address.
   - **Network View**: Locate network information using the selected IP address.
6. Click **Done**.

Related topics

- Tracing Internet traffic (page 56)
- View inbound events (page 53)

Trace a computer from the Intrusion Detection Events log

From the Intrusion Detection Events pane, you can trace an IP address that appears in the Intrusion Detection Events log.

To trace a computer's IP address from the Intrusion Detection Events log:

1. On the Common Tasks pane, click **Reports & Logs**.
2. Under **Recent Events**, click **View Log**.
3. Click **Internet & Network**, and then click **Intrusion Detection Events**. In the Intrusion Detection Events pane, select a source IP address, and then click **Trace this address**.
4. On the Visual Tracer pane, click one of the following:
   - **Map View**: Geographically locate a computer using the selected IP address.
   - **Registrant View**: Locate domain information using the selected IP address.
   - **Network View**: Locate network information using the selected IP address.
5. Click **Done**.

Related topics

- Tracing Internet traffic (page 56)
- Logging, monitoring, and analysis (page 51)

Trace a monitored IP address

You can trace a monitored IP address to obtain a geographical view which shows the most probable route of data taken from the source computer to yours. In addition, you can obtain registration and network information about the IP address.

To monitor program bandwidth use:

1. Ensure that the Advanced Menu is enabled and click **Tools**.
2. On the Tools pane, click **Traffic Monitor**.
3. Under **Traffic Monitor**, click **Active Programs**.
4. Select a program and then the IP address that appears below the program name.
5. Under **Program Activity**, click **Trace This IP**.
6. Under **Visual Tracer**, you can view a map which shows the most probable route of data taken from the source computer to yours. In addition, you can obtain registration and network information about the IP address.

Note: To view the most up-to-date statistics, click **Refresh** under **Visual Tracer**.

Related topics

- Monitoring Internet traffic (page 60)

Monitoring Internet traffic

Firewall provides a number of methods to monitor your Internet traffic, including the following:

- **Traffic Analysis graph**: Displays recent inbound and outbound Internet traffic.
- **Traffic Usage graph**: Displays the percentage of bandwidth used by the most active programs during the past 24 hour period.
- **Active Programs**: Displays those programs that currently use the most network connections on your computer and the IP addresses the programs access.

About the Traffic Analysis graph

The Traffic Analysis graph is a numerical and graphical representation of inbound and outbound Internet traffic. In addition, the Traffic Monitor displays programs using the greatest number of network connections on your computer and the IP addresses that the programs access.

From the Traffic Analysis pane, you can view recent inbound and outbound Internet traffic, current, average, and maximum transfer rates. You can also view traffic volume, including the amount of traffic since you started Firewall, and the total traffic for the current and previous months.

The Traffic Analysis pane displays real-time Internet activity on your computer, including the volume and rate of recent inbound and outbound Internet traffic on your computer, connection speed, and total bytes transferred across the Internet.

The solid green line represents the current rate of transfer for incoming traffic. The dotted green line represents the average rate of transfer for incoming traffic. If the current rate of transfer and the average rate of transfer are the same, the dotted line does not appear on the graph. The solid line represents both the average and current rates of transfer.

The solid red line represents the current rate of transfer for outgoing traffic. The red dotted line represents the average rate of transfer for outgoing traffic. If the current rate of transfer and the average rate of transfer are the same, the dotted line does not appear on the graph. The solid line represents both the average and current rates of transfer.

Related topics

- Analyze inbound and outbound traffic (page 61)

Analyze inbound and outbound traffic

The Traffic Analysis graph is a numerical and graphical representation of inbound and outbound Internet traffic. In addition, the Traffic Monitor displays programs using the greatest number of network connections on your computer and the IP addresses that the programs access.

To analyze inbound and outbound traffic:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Traffic Monitor**.
3. Under **Traffic Monitor**, click **Traffic Analysis**.

Tip: To view the most up-to-date statistics, click **Refresh** under **Traffic Analysis**.

Related topics

- About the Traffic Analysis graph (page 60)

Monitor program bandwidth

You can view the pie chart, which displays the approximate percentage of bandwidth used by the most active programs on your computer during the past twenty-four hour period. The pie chart provides visual representation of the relative amounts of bandwidth used by the programs.

To monitor program bandwidth use:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Traffic Monitor**.
3. Under **Traffic Monitor**, click **Traffic Usage**.

Tip: To view the most up-to-date statistics, click **Refresh** under **Traffic Usage**.

Monitor program activity

You can view inbound and outbound program activity, which displays remote computer connections and ports.

To monitor program bandwidth use:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **Traffic Monitor**.
3. Under **Traffic Monitor**, click **Active Programs**.
4. You can view the following information:
   - Program Activity graph: Select a program to display a graph of its activity.
   - Listening connection: Select a Listening item under the program name.
   - Computer connection: Select an IP address under the program name, system process, or service.

Note: To view the most up-to-date statistics, click **Refresh** under **Active Programs**.

CHAPTER 7

Learning about Internet security

Firewall leverages McAfee's security Web site, HackerWatch, to provide up-to-date information about programs and global Internet activity. HackerWatch also provides an HTML tutorial about Firewall.

In this chapter

Launch the HackerWatch tutorial

To learn about Firewall, you can access the HackerWatch tutorial from SecurityCenter.

To launch the HackerWatch tutorial:

1. Ensure that the Advanced Menu is enabled, and then click **Tools**.
2. On the Tools pane, click **HackerWatch**.
3. Under **HackerWatch Resources**, click **View Tutorial**.

Index