

McAfee Firewall

VERSION 4.0



COPYRIGHT

© 2002 Networks Associates Technology, Inc. and its Affiliated Companies. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

TRADEMARK ATTRIBUTIONS

ACTIVE SECURITY, ACTIVE SECURITY (IN KATAKANA), ACTIVEHELP, ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, BOMB SHELTER, CERTIFIED NETWORK EXPERT, CLEAN-UP, CLEANUP WIZARD, CNX, CNX CERTIFICATION CERTIFIED NETWORK EXPERT AND DESIGN, CYBERCOP, CYBERCOP (IN KATAKANA), CYBERMEDIA, CYBERMEDIA UNINSTALLER, DESIGN (STYLIZED N), DISK MINDER, DISTRIBUTED SNIFFER SYSTEM, DISTRIBUTED SNIFFER SYSTEM (IN KATAKANA), DR SOLOMON'S, DR SOLOMON'S LABEL, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (IN KATAKANA), EZ SETUP, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (IN KATAKANA), GUARD DOG, HELPDESK, HOMEGUARD, HUNTER, ISDN TEL/SCOPE, LANGURU, LANGURU (IN KATAKANA), M AND DESIGN, MAGIC SOLUTIONS, MAGIC SOLUTIONS (IN KATAKANA), MAGIC UNIVERSITY, MAGICSPY, MAGICTREE, MCAFEE, MCAFEE (IN KATAKANA), MCAFEE AND DESIGN, MULTIMEDIA CLOAKING, NET TOOLS, NET TOOLS (IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETSTALKER, NETWORK ASSOCIATES, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PC MEDIC 97, PCNOTARY, PGP, PGP (PRETTY GOOD PRIVACY), PRETTY GOOD PRIVACY, PRIMESUPPORT, RECOVERKEY, RECOVERKEY - INTERNATIONAL, REGISTRY WIZARD, REPORTMAGIC, RINGFENCE, ROUTER PM, SALESMAGIC, SECURECAST, SERVICE LEVEL MANAGER, SERVICEMAGIC, SMARTDESK, SNIFFER, SNIFFER (IN HANGUL), SNIFFMASTER, SNIFFMASTER (IN HANGUL), SNIFFMASTER (IN KATAKANA), SNIFFNET, STALKER, SUPPORTMAGIC, TIS, TMEG, TNV, TVD, TNS, TOTAL NETWORK SECURITY, TOTAL NETWORK VISIBILITY, TOTAL NETWORK VISIBILITY (IN KATAKANA), TOTAL SERVICE DESK, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, WEBSCAN, WEBSHIELD, WEBSHIELD (IN KATAKANA), WEBSNIFFER, WEBSTALKER, WEBWALL, WHO'S WATCHING YOUR NETWORK, WINGAUGE, YOUR E-BUSINESS DEFENDER, ZAC 2000, ZIP MANAGER are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners. © 2002 Networks Associates Technology, Inc. All Rights Reserved.

Contents

1	Welcome to McAfee Firewall 4.0	5
	What's new in this release?	5
	How McAfee Firewall works	7
	About this manual	7
	Frequently asked questions	8
2	Installing McAfee Firewall	11
	System requirements	11
	Installation steps	12
	Troubleshooting installation problems	14
	Removing or modifying your McAfee Firewall installation	16
	Important information about Windows XP migration	16
3	Getting Started with McAfee Firewall	17
	The Configuration Assistant	17
	The McAfee Firewall Home page	20
	The Title bar and Tool bar	20
	Status information	21
	The Task pane	22
	Other McAfee Firewall features	24
4	McAfee Firewall Configurations	27
	Overview	27
	Program configuration	27
	System configuration	31
5	McAfee Firewall's Intrusion Detection System	33
	About Intrusion Detection	33
	How to Configure the Intrusion Detection System	33
	Common attacks recognized by IDS	35

6	Updating McAfee Firewall	39
	About Instant Updater	39
	Instant Updater features	39
A	Product Support and Customer Service	41
	Contacting Customer Service and Technical Support	41
	About McAfee-at-home.com	41
	Emergency Support	41
	Index	45

Protect yourself while online with the advanced security of McAfee Firewall. Easy-to-use, yet highly configurable, McAfee Firewall secures your PC's connection to the Internet whether you connect via DSL, cable modem or dial-up. With intrusion detection, color coded security alerts, customizable audible alerts, detailed logging, and an application scan for Internet enabled applications, McAfee Firewall gives you the power you need to control the communications into and out of your PC, ensuring that your online experience is as safe as it is enjoyable.

McAfee Firewall:

- Controls file and print share access.
- Shows who is connecting to your computer if you allow sharing.
- Stops floods and other attack packets from being received by the Operating System.
- Blocks untrusted applications from communicating over the network.
- Provides detailed information about which sites you have contacted and the type of connection that was made.
- Can be set to block all traffic or traffic from a specific IP address immediately.

What's new in this release?

- **Firewall security check:** Examines your security settings for possible vulnerabilities.
- **Enhanced hacker tracing** with the addition of McAfee's Visual Trace technology.
- **Intrusion Detection System:** Detects common attack types and suspicious activity.
- **Home networking wizard:** Set up protection for personal computers sharing an Internet connection.
- **Wizard for creating custom rules:** Create custom configurations for specific programs.

- **Password protection:** Prevent others from tampering with your firewall settings using password protection.
- **Improved support for broadband connections.**
- **Usability enhancements:** McAfee Firewall 4.0 includes many user interface enhancements to make it easier than ever to secure your computer.

How McAfee Firewall works

McAfee Firewall is a simple-to-operate security tool that dynamically manages your computing security behind the scenes.

Setup

During the installation process, the Configuration Assistant prompts you with basic questions to set up McAfee Firewall to do specific tasks – according to your needs (e.g. allow sharing of files or not).

Operation

McAfee Firewall filters traffic at the devices that your system uses - network cards and modems. This means that it can reject inbound traffic before that traffic can reach vital functions in your computer and waste valuable system resources.

McAfee Firewall – the Gatekeeper

When McAfee Firewall is running, it monitors trusted and untrusted programs that communicate using the Internet. If a trusted application attempts to communicate, McAfee Firewall allows the program to function without restrictions. If an untrusted program attempts to communicate into or out of your computer, McAfee Firewall blocks the program's attempt to communicate via the Internet.

Configuration

Some network communications are needed to maintain network-based services. These are managed through user defined rules under the system settings of McAfee Firewall. The default system settings feature provides superior protection from hostile threats.

About this manual

This manual provides the basic information you need to install, set up and get started with McAfee Firewall. More detailed information about how to perform tasks within McAfee Firewall is provided via online Help. You can get Help while working with the different windows and dialog boxes. You can also review the Readme.txt file which contains other general information, known issues, etc., about this product.

Frequently asked questions

The following are some frequently asked questions that you can briefly review:

How will McAfee Firewall help me?

McAfee Firewall protects your computer at the network level. It acts as a gatekeeper, checking every data packet going in or out of your PC. It allows only what you tell it to allow.

McAfee Firewall has been designed to be easy to use, while providing superior protection. Once you install and run it, it is configured to block known attacks and to ask you before allowing applications to communicate.

How is my PC at risk on the Internet?

When you connect to the Internet, you share a network with millions of people from around the world. While the Internet is a wonderful and amazing accomplishment, it brings with it all the problems of being accessible to complete strangers.

While communicating via the Internet, you should take safety precautions to protect your computing environment. If you use IRC (Internet Relay Chat) programs, be suspicious of files total strangers send you. Programs that give others remote access to your computer, such as Back Orifice (BO), are frequently disseminated in this manner. It is a good practice to scan files received using anti-virus programs such as McAfee VirusScan before you open or view files and their attachments.

When on the Internet, others can try to access your file shares. Therefore, you should check that they are only accessible to those you trust. Otherwise, untrusted parties can read and delete what is in your computer.

What other protection do I need?

McAfee Firewall provides network level protection. Other important types of protection are:

- Anti-virus programs for application-level protection.
- Logon screens and screen saver passwords to prevent unauthorized access.
- File encryption or encrypting file systems to keep information secret.
- Boot-time passwords to stop someone else from starting your PC.
- Physical access to the computer, e.g. stealing the hard drive.

A separate but also important issue is controlling access to information, misinformation and “filth” that is widely available on the Internet. You can use a number of content-filtering services or programs such as McAfee’s Internet Security that can filter the contents of data packets or restrict access to certain sites.

Are there any data packets that McAfee Firewall cannot stop?

Inbound Data: No. As long as McAfee Firewall supports a network device and is running, it is intercepting all incoming packets and will allow or block according to the way you have it configured. If you choose to block everything, it will.

Outbound Data: Yes and no. McAfee Firewall intercepts outbound data packets as they are passed to the network device driver. All popular applications communicate this way. A malicious program could communicate by other means, however.

What network devices does McAfee Firewall support?

McAfee Firewall supports Ethernet and Ethernet-like devices. This includes dial-up connections, most cable and ISDN modems and most Ethernet cards. It does not support Token Ring, FDDI, ATM, Frame Relay and other networks.

What protocols can McAfee Firewall filter?

McAfee Firewall can filter TCP/IP, UDP/IP, ICMP/IP and ARP. It intercepts all protocols, but others, such as IPX, must be either allowed or blocked - no filtering is done. The Internet uses the IP protocols. No others are sent. Also, IP networks are the most common.

How can I still be harassed, even with McAfee Firewall?

Many people use McAfee Firewall to block the “nukes” that cause their IRC connections to be broken. While McAfee Firewall blocks the nukes, there are other ways that attackers can still cause the connections to be broken:

- **Server-side nuking.** This is when the “nukes” are sent to the IRC server, not to your computer, telling the server that you can no longer be reached. To prevent this, the IRC server needs a firewall.
- **Flood blocking a TCP connection.** If a flood of packets is sent to you from a higher speed connection, McAfee Firewall can stop the packets, but the flood takes up all your bandwidth. Your system does not get a chance to send anything. Dial-up users are particularly vulnerable since they have the lowest speed connections.

TIP

To read additional frequently asked questions, refer to the Readme.txt file.

The setup program on your McAfee Firewall 4.0 installation CD lets you install the program easily on your computer. Installation should start automatically when you insert the CD into your computer's CD-ROM drive. The information in the following paragraphs will help you install and start using McAfee Firewall.

System requirements

To use McAfee Firewall you need:

- Microsoft Windows XP Home Edition, Windows XP Professional Edition, Windows 2000 Professional, Windows Me, Windows 98, or Windows 98 SE.
- Internet Explorer 4.01, Service Pack 2 or higher required; IE 5.01 or later recommended.
- Personal computer with a Pentium 100 MHz or higher processor.
- 32 megabytes (MB) of RAM.
- 30 MB of free hard disk space.
- CD ROM drive.
- Internet access required for various features.

About Winsock 2

McAfee Firewall uses an API (Application Programming Interface) that is not supported by versions of Winsock prior to v2.0. McAfee Firewall checks for the presence of Winsock 2 during the installation procedure and will inform you if the system does not have it. If you have the latest browser (e.g., Internet Explorer 6), this component is already built-in and you will not receive this prompt. Otherwise, you can get a free upgrade and is available from <http://www.microsoft.com> as well as other Web sites.

Installation steps

To avoid installation problems, close all open programs before you install McAfee Firewall, including programs that run in the background, such as screen savers or virus checkers.

After inserting the McAfee Firewall 4.0 installation CD into your computer's CD-ROM drive, an Autorun image should automatically display. To install McAfee Firewall software immediately, click Install McAfee Firewall, then skip to Step 5 to continue with Setup.

Use the steps below to install your software.

- 1** If your computer runs Windows 2000 Professional, or Windows XP, log on to your computer as a user with administrative rights. You must have administrative rights to install this software.
- 2** Insert the McAfee Firewall 4.0 CD in to your computer's CD-ROM drive. If the Installation Wizard does not automatically display, go to Step 3. Otherwise, skip to Step 4.
- 3** Use the following procedure if the Autorun installation menu does not display, or, if you obtained your software via download at a McAfee web site.
 - a** From the Windows Start menu, select Run. The Run dialog box displays.
 - b** Type <X>:\SETUP.EXE in the text box provided, then click OK.
- 4** Here, <X> represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted McAfee Firewall files. To search for the correct files on your hard disk or CD-ROM, click Browse.
 - a** Before proceeding with the installation, Setup first checks to see whether your computer has the Microsoft Windows Installer (MSI) utility running as part of your system software. If your computer runs Windows XP, the current version of MSI already exists on your system. If your computer runs an earlier Windows release, you may still have MSI in your computer if you previously installed other software that uses MSI. In either of these cases, Setup will display its first wizard panel immediately. Skip to Step 5 to continue.
 - b** If Setup does not find MSI or an earlier version of MSI is installed in your computer, it installs files necessary to continue the installation, then prompts you to restart your computer. Click Restart System. When your computer restarts, Setup will continue from where it left off.

- 5 Refer to steps displayed on the Installation Wizard to complete your installation.

TIP

If your computer does not have the required fonts to view the End User's License Agreement (EULA), then you can locate the appropriate EULA on your McAfee software installation CD. You must read and agree to the terms of the agreement to complete your installation.

NOTE

For all Windows 2000 Professional installations, McAfee Firewall requires a unique driver in order to function. During the installation process, you will be confronted with several warning messages notifying you that you are attempting to install an unsigned driver. Therefore, please click OK as often as necessary to install the driver and restart your computer if prompted to do so.

Troubleshooting installation problems

A failed installation can cause software problems that are difficult to track down. The major causes of installation failure are:

- Attempting to install while other software is running.
- Temporary files that conflict with the installation.
- Hard drive errors.

Follow the procedure outlined below to minimize the affect that these common conditions may have on your installation.

Step 1: Close other software

Disable all software running in the background:

- 1 Hold down the Ctrl and Alt keys on your keyboard, and then press the Delete key once. The Close Program dialog box appears.
- 2 Click End Task for every item on the list except Explorer.
- 3 Repeat steps 2 and 3 until you've closed everything except Explorer.
- 4 When you see only Explorer in the Close Program dialog box, click Cancel.

Step 2: Remove temporary files

Delete the contents of the Windows Temp folder:

- 1 Double-click the My Computer icon on your desktop. The My Computer window opens. Double-click the C: drive. You are now viewing the contents of your hard drive.
- 2 Double-click the Windows folder.
- 3 In the Windows folder, double-click the Temp folder.
- 4 In the menu, click Edit, then click Select All. All of the items in your Temp folder are highlighted.
- 5 Press the Delete key on your keyboard to delete the files. If Windows asks about deleting files, click Yes.
- 6 In the Windows taskbar, click Start, then click Shut Down.
- 7 Click Restart the computer, then click Yes in the Shut Down Windows dialog box to restart your PC.

Step 3: Clean your hard drive

Run the Windows hard drive utilities, ScanDisk and Disk Defragmenter to identify and fix any errors on your hard drive:

- 1 Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click ScanDisk.
- 2 In the ScanDisk window, select Standard and Automatically fix errors.
- 3 Click Advanced. In the Advanced Settings dialog box, make sure the following settings are selected:
 - ◆ Only if errors found
 - ◆ Replace log
 - ◆ Delete
 - ◆ Free
- 4 Ignore the other options, and click OK. Click Start. ScanDisk begins scanning your drive for errors. Depending on the size of your hard drive, ScanDisk may take several minutes to complete its job.
- 5 When ScanDisk is finished, close ScanDisk.
- 6 Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click Disk Defragmenter.
- 7 Click OK to start Disk Defragmenter. Depending on the speed of your computer and the size of your drive, this may take several minutes to complete.
- 8 Close Disk Defragmenter when it has finished defragmenting your disk.

Removing or modifying your McAfee Firewall installation

If your computer's operating system is...

- Windows 2000 Professional
- Windows XP Home Edition
- Windows XP Professional Edition

... you must log on to your computer using a profile with administrative rights.

Then do the following:

- 1 From the Windows Control Panel, start the Add/Remove applet.
- 2 Select McAfee Firewall and click:
 - ◆ **Remove** to remove McAfee Firewall from your computer.
 - ◆ **Change** to modify your McAfee Firewall installation.
- 3 Refer to steps displayed on the McAfee Firewall Installation Wizard to complete your changes.

Restart your computer as directed by setup.

Important information about Windows XP migration

Upgrading your computer's operating system from any version of Windows to Windows XP causes all McAfee products installed before migration to become disabled after migration to Windows XP.

You will be made aware of this situation as you make your first attempt to start a McAfee product (after migration) - you will be instructed to reinstall the product.

As such, you will need to uninstall all McAfee products and reinstall using your installation CD or the software obtained from McAfee via download.

After installing McAfee Firewall, you will need to configure your software for its first use. The Configuration Assistant guides you through this process.

The Configuration Assistant

Welcome Screen

The McAfee Firewall Configuration Assistant displays the first time you start McAfee Firewall. This wizard guides you through initial setup and activates McAfee Firewall on your computer. Select Back, Next, Cancel, and Finish to navigate the Configuration Assistant screens.

If you select Cancel on any Configuration Assistant screen, the activation and configuration process stops. **You must complete the Configuration Assistant on first use in order to activate and use McAfee Firewall.**

Network Control Settings

Network Control Settings identify how you want McAfee Firewall to respond when a program attempts to access the Internet; either into or out of your computer.

- 1 To set your Network Control settings, from the Welcome to McAfee Firewall screen, select one of the following.

Table 3-1. McAfee Firewall's Network Control Settings

Internet Traffic Setting	Description
Block all traffic	Configures McAfee Firewall to block all Internet traffic into and out of your computer. This is the most secure firewall setting; however, programs in your computer cannot access the Internet.

Table 3-1. McAfee Firewall's Network Control Settings

Internet Traffic Setting	Description
Filter all traffic	Gives you the opportunity to decide whether an application or program in your computer will be allowed to access the Internet. If an unrecognized program attempts to access your computer from the Internet, you will also be given an opportunity to allow or block its access your computer.
Allow all traffic	Configures McAfee Firewall to allow all Internet traffic into and out of your computer. All programs in your computer will be allowed to access the Internet; programs attempting to access your computer from the Internet will not be blocked. Allow all traffic disables all McAfee Firewall protection features and should only be used for diagnostic purposes.

- 2 Click Next.

Startup Options

This screen allows you to choose how you want McAfee Firewall to respond as you start your computer.

For your convenience, recommended Startup Load Options have been pre-selected for you.

- 1 Select **Load McAfee Firewall automatically at startup** if you want firewall protection as you start your computer. If you do not want McAfee Firewall to start as your computer starts, then clear this check box.
- 2 If you want to display a McAfee Firewall icon on your Windows desktop, then select **Place a McAfee Firewall icon on the desktop**. If you do not want an icon on your Windows desktop, then clear this check box.
- 3 Click Next.

Access to shares

If your computer is part of a workgroup, such as a home network, you can configure McAfee Firewall to allow access to your computer's network shares as well as allow your computer to access other computer's shares. A **share** is a resource such as a drive, directory, file, or printer available to a workgroup or home networked computers.

- 1 **Access to other shares:** check the **Allow my computer to access other computer's shares** if you want to allow your computer to have access to the shared drives, directories, folders, and printers, etc. of other computers in your workgroup or home network.
- 2 **Access to my shares:** check the **Allow other computers to access my shares** check box to allow other computers in your workgroup or home network to have access to your shared drives, directories, folders, and printers, etc.
- 3 Click Next.

Allowed applications

During the configuration process, McAfee Firewall scanned your computer's hard disk to identify programs that use the Internet. For example, programs of this type would include Internet browsers, Internet e-mail programs, and ftp (file transfer protocol) clients. On this screen, you will identify programs that you will allow to access the Internet through McAfee Firewall.

To allow specific programs to access the Internet, do the following:

- 1 From the list of applications displayed on this, check the check box corresponding to each program you will allow access to the Internet.

Click **Search all drives** to search all of your computer's partitions, logical drives, and physical hard drives for programs that communicate using the Internet.

If you do not allow any or all of the programs displayed on this screen to communicate, you will be notified when each attempts to do so and decide whether to allow access to the Internet at that time.

- 2 Click **Finish**.

What's happens next?

After you complete the steps associated with setting up your initial configuration, the following events take place:

- 1 The firewall service starts.
- 2 The McAfee Firewall Home page displays.

You are now ready to start using McAfee Firewall!

TIP

Previous versions of McAfee Firewall did not allow you to run the Configuration Assistant more than once. However, McAfee Firewall 4.0 allows you to run the Configuration Assistant with an easily accessible link on the McAfee Firewall Home page.

The McAfee Firewall Home page



Figure 3-1. The McAfee Firewall Home page

The McAfee Firewall main window is your central entry point to all of McAfee Firewall's Tasks, Advanced Tasks, and shared features. The McAfee Firewall interface displays three regions common to all of McAfee Firewall's screens.

The Title bar and Tool bar

Title bar

The Home page displays most of your standard Windows elements; that which includes:

- The title bar displays the name of the program that is currently running.
- Close and minimize buttons. McAfee Firewall's interface is of fixed length and width. You cannot resize the interface.

Tool bar

The tool bar displays four browser-like buttons that are common to all screens.

- **Back.** Click Back to return to the last screen viewed.

- **Home.** Click Home to go to the McAfee Firewall Home page from any screen.
- **Next.** In conjunction with the Back button, use Next to go to any previously viewed screen during your current session.
- **Help.** Click Help to view its submenu. The Help submenu may include any of the following items.

Help submenu item	Select this item to...
Help on this page	♦ View online Help for the screen you are currently viewing.
Contents and index	♦ View online Help for McAfee Firewall.
Help on the Web	♦ Start your Internet browser and go directly to the McAfee Help Web site at McAfeeHelp.com.
McAfee at Home on the Web	♦ Start your Internet browser and go directly to McAfee-at-home.com.
About McAfee Firewall	♦ Version information about McAfee Firewall.

Status information

Depending upon your configuration, the McAfee Firewall Home page displays other helpful information such as:

- **Firewall Status: **Running** or **Stopped**.** Click the link below the status to start or stop McAfee Firewall.
- **Home page notification.** If there is an update to your version of McAfee Firewall available for download, select this task.
- **The number of programs currently communicating.** If you want to identify the program's communication, select this task to view your current activity.
- **Firewall warning information.** If there are any communication warnings, select this task to view the warning log.

Internet traffic settings

The Internet Traffic setting frame displays your current filtering setting. Here you determine if you want to **Block all**, **Allow all**, or **Filter** Internet Traffic. For more information about these settings, refer to [Table 3-1 on page 17](#).

To change an Internet traffic setting, simply click the desired setting. Changes are real-time and effective immediately.

McAfee Firewall status

This region of the Home page displays the current running state of McAfee Firewall. It is either running or not running.

If the McAfee Firewall status message is...	Then...
McAfee Firewall is Running	<ul style="list-style-type: none">Click Stop McAfee Firewall to disable firewall protection.
McAfee Firewall is Stopped	<ul style="list-style-type: none">Click Start McAfee Firewall to enable firewall protection.

Network Traffic monitor

The Network Traffic monitor displays a graphic representation of real-time network activity. The monitor is color-coded to help you identify normal network traffic, port scans, and worst of all, attacks.

- **Green zone:** Activity displayed in this zone is normal network activity. It is not uncommon to see activity in this zone reaching the yellow area.
- **Yellow zone:** This is the caution zone. You can view the Activity Log to analyze data for this traffic. Activity in the yellow zone could represent a port scan.
- **Red zone:** Red represents the worst level of network activity and usually represents an attack. You can view the details of the attack by accessing McAfee Firewall Activity Log. If this the attacker's IP address is available, you can attempt to trace the attacker using McAfee Firewall's Visual Trace component.

The Task pane

The Task pane displays links that allow you to start McAfee Firewall's **Tasks** and **Advanced Tasks**. Depending upon your configuration, the Task pane may or may not display a **McAfee** list. The McAfee list displays links that allow you start the Home page of any other current McAfee product installed in your computer.

About Tasks

Starting a task is as easy as clicking its link. The Task list allows you to start McAfee Firewall's major components. Although the tasks you can perform will vary based upon your computer's operating system and its configuration, primary tasks include:

- **Control Internet programs:** This task allows you to explicitly block or allow specific programs to access the Internet.

- **View network activity:** Select this task to view real-time network activity and view your current activity log.
- **Set alert preferences:** Choose how you want McAfee Firewall to notify you when a potential security breach occurs.
- **Set up Home Networking:** Helps make setting up protections for your PCs sharing an Internet connection a breeze.
- **Perform a security check:** This task allows you to start the McAfee Firewall Security Check process.
- **Set startup options:** Choose how you want McAfee Firewall to start.
- **Configuration Assistant:** This task starts the Configuration Assistant.

About Advanced Tasks

Similar to the primary Task list, the Advanced Task list may vary depending upon your version of Windows, its configuration, and other software that may be installed in your computer. McAfee Firewall's advanced tasks include:

- **Advanced options and logging:** Select this task to configure intrusion defense mechanisms, set up the automatic configuration of filtering rules, and identify the type of traffic you want to log.
- **Configure network adapters:** Choose this task to view your current network adapter and configure their communication settings.
- **Intrusion detection settings:** Select this task to configure how you want McAfee Firewall to respond when it detects an intrusion.
- **Block IP address:** If there is a specific IP address that you want to block from accessing your computer, or, if there is an IP address that is currently blocked that you want to allow, choose this task.
- **Set up password:** This task helps you to secure your McAfee Firewall settings with password security.
- **Other Tasks:** Select this task to navigate to a screen that allows you to start McAfee Firewall's shared features

About the McAfee list

The McAfee list displays links to start the Home page to any other supported McAfee product.

Other McAfee Firewall features

McAfee Firewall settings security check

Examines your firewall security settings, allowing you to rectify weaker settings before hackers get a chance to exploit them. The McAfee Firewall Settings Security Check flags and suggests changes to help you keep your system set to optimal security.

If Security Check detects an issue, click Fix and McAfee Firewall helps you analyze and correct potential problems.

Home networking wizard

Helps make setting up protections for your PCs sharing an Internet connection a breeze, providing helpful wizards to walk you through the process.

All networking media and hardware (such as cables and network adapters) must be installed in each computer in order for this wizard to locate your computers.

Password protection

Prevent others from tampering with your firewall settings by locking access to them with password security. Also helps keep your firewall protections secure by preventing the firewall from being shut down without your password.

About Visual Trace

Visual Trace is a multi-purpose Internet tool used for finding information and trouble-shooting connection problems.

At the simplest level Visual Trace shows you how packets (data) get from your computer to another computer on the Internet. You see all the nodes (equipment of various types on the Internet that is passing traffic) between your computer and the trace target.

There are many situations where you need this information. Visual Trace is a useful tool when troubleshooting connections or just verifying that everything is working OK. There is also a wealth of information presented by Visual Trace, including the domain owners, relative locations, and in many cases, the location of nodes.

Besides using Visual Trace to look for weak spots in a connection you can use it to:

- Discover whether you can't reach a site due to a failure at your Internet Service Provider (ISP) or further into the Internet

- Determine the point of a network failure that is preventing you from reaching a Web site.
- Determine the location of sites and their users, uncover the owners of a site, and help track down the origin of unwanted e-mail messages ('spam').
- Get detailed contact information on sites all over the world (where available).

How to start Visual Trace

You can start Visual Trace directly from the Windows start menu. You can also start Visual Trace from the McAfee Firewall Detail Activity screen, the Block IP dialog box, and if you are attacked, from the Windows system tray pop-up notification.

For more information about Visual Trace, please refer to online Help for Visual Trace.

Overview

The configuration of McAfee Firewall is divided into two classifications – application (program) and system. Upon installation, a base set of rules for system services such as ICMP, DHCP and ARP are installed (these are considered default settings).

On the other hand, the programs classification is personalized. Whenever you run a new program that attempts to communicate over the Internet, McAfee Firewall will prompt and ask you whether you want to trust the program or not.

For example, using Internet Explorer, enter an Internet address or URL (i.e: <http://www.mcafee-at-home.com>) in the address bar of your browser and press ENTER. Internet Explorer will attempt to connect to that URL over the Internet. The first time you do this, McAfee Firewall prompts if you “trust” Internet Explorer. If you say “Yes,” McAfee Firewall notes Internet Explorer is allowed and whenever you use Internet Explorer in the future, McAfee Firewall will allow its traffic.

As you allow programs to use the Internet, McAfee Firewall “learns” the rules you are creating for the program and saves them for future use. If a Trojan horse program attempts to communicate out from your computer, McAfee Firewall will also prompt you whether you trust them or not, and the decision to block the Trojan horse program from communicating is easy and instantaneous.

Program configuration

During your first attempt to start McAfee Firewall, the Configuration Assistant asked you to identify programs that you want to allow to communicate. At such time, McAfee Firewall created a default set of communication rules for the programs (applications); designated as **allowed** to communicate.

Based upon the type of program, for example, Internet browsers, e-mail, ftp, IRC, and file sharing programs, McAfee Firewall identifies the type of program and creates a default set of communication rules for each program in your computer. That is, to either block, allow, or filter a program’s communication attempts via the Internet.

Firewall Communication Alert Messages

A **McAfee Firewall Communication Alert** message displays if an unrecognized program attempts to communicate. There are several scenarios that could cause a program to be unrecognized.

- If you install a program that communicates via the Internet after installing McAfee Firewall, the program's first attempt to communicate will cause an alert message to display.
- Although the Configuration Assistant performs a thorough analysis of your computer's programs that use the Internet to communicate, it may not have been able to identify all of your computer's programs that use the Internet to communicate.

If an unrecognized program attempts to communicate, the resulting alert message generally asks you to select one of the following options:

- **No, deny at this time:** Blocks the program's current and all future attempts to communicate. The active program is added to the trusted list of programs with an allowed state of "blocked."
- **Yes, allow this time:** The active attempt to communicate is allowed. The program is not added to the trusted programs list.
- If you recognize the program and do not want to receive any future alerts for this program, check the **I recognize this program** check box.

TIP

If you allow or block a program the first time you are prompted, McAfee Firewall provides you with the flexibility to change this setting and block or allow it to communicate at any time in the future. As you exit McAfee Firewall, your settings are saved and will be the same the next time it is run.

Changing a program's allowed state

McAfee Firewall monitors Internet traffic to see which programs are communicating. Depending on your settings, it will allow, block, or filter a program's attempt to communicate.

If you choose to "Allow all" programs to communicate through your firewall, then all programs installed in your computer can communicate.

To view and configure the current list of trusted programs

- 1 From the Task list, select Control Internet programs.
- 2 Select the program whose filtering settings you wish to configure (or click Browse to add a program to the list).
- 3 Select one of the following options:

- ◆ Filter this program's access to the Internet.
 - ◆ Allow this program to have full unfiltered access to the Internet.
 - ◆ Block this program from accessing the Internet.
- 4 To add a program to the list, click Add and browse to select the program you want to add. To remove a program from the list, select the program you want to remove and click Remove.
 - 5 Click Apply.

How to customize filtering rules for a specific program

For all programs designated as “filter,” McAfee Firewall provides power users with the flexibility to create a set of custom filtering rules for each filtered program.

TIP

The **Customize** button becomes accessible if you select the **Filter this program's access to the Internet** option.

To create a custom filtering rule

- 1 From the Control Internet Programs screen, select the program for which you want to create a custom filtering rule.
- 2 Select the **Filter this program's access to the Internet** radio button.
- 3 Click **Customize**.

If the program currently maintains a default set of rules created by McAfee Firewall, then the **Customize filtering rules** dialog displays. If the program *does not* maintain a default set of rules, then the **What do you want this filtering rule to do?** dialog displays.

- 4 Refer to the instructions displayed on the Custom Filtering rules dialog boxes to complete your custom configuration.

Table 4-2. Customize Filtering Rules dialog buttons

Button	Description
Add	◆ Click Add to add a new rule and to display the What do you want this rule to do? dialog.
Remove	◆ Click Remove to remove a rule from the selected program. CAUTION: There is no “undo” feature.
Edit	◆ Click Edit to refine a filtering rule.

Table 4-2. Customize Filtering Rules dialog buttons

Button	Description
Restore	<ul style="list-style-type: none"> Click Restore to restore the default rules for the selected program. TIP: If you inadvertently Remove a filtering rule, click this button to restore the default rules for the selected program.
OK	<ul style="list-style-type: none"> Click OK to close the Customize Filtering Rules dialog and save your changes.
Cancel	<ul style="list-style-type: none"> Click Cancel to close the Customize Filtering Rules dialog without saving your changes.

Primary functions

From the list of primary functions displayed on the Customize Filtering Rules dialog, you can choose one of the following:

Table 4-3. Primary Functions

You can choose to...	by...
Allow communication...	<ul style="list-style-type: none"> protocol local port remote port
Block communication...	<ul style="list-style-type: none"> IP address domain name direction

Refining conditions

After you select the primary function for the rule, you can further refine the rule by checking the check boxes for any or all of the communication characteristics:

With...	Using...
<ul style="list-style-type: none"> direction domain names IP addresses 	<ul style="list-style-type: none"> protocols remote ports local ports

To customize the refinement condition, click [\[click here to select\]](#). Depending upon the communication characteristics selected, various dialog and text boxes display. For example, if the custom rule states “Block this program from communicating and the IP address is,” then an Add/Edit rule text displays allowing you to enter an IP address. Similarly, if you want to block a program from communicating by protocol, an Edit Protocols dialog displays.

To save your changes, click OK.

System configuration

Your computer’s operating system performs many types of network communication without reporting directly to you. McAfee Firewall lets you explicitly allow or block different system functions. Settings may be different for each network device, since a computer, for example, can be connected to an internal network as well as having a dial-up connection to the Internet.

Use the steps below to control your System settings.

- 1 From the Advanced Task list, select Configure network adapters.
- 2 From the Configure Network Adapter Settings screen, select the adapter you want to configure and click Adapter Settings to view or change the properties of this adapter.
Result: The Properties sheet for the selected network adapter displays.

You can then choose to allow or block NetBIOS over TCP, Identification, ICMP, ARP, DHCP, RIP, PPTP and other protocols (IP and non-IP).

Table 4-4. Default Settings for System Activity

System Activity Type	Description
NetBIOS over TCP: Blocked	This will block all file share activity over TCP as well as UDP broadcasts. Your system will not appear in anyone’s “Network Neighborhood” and theirs will not appear in yours. If your system is configured to support NetBIOS over other protocols, such as IPX or NetBEUI, then file sharing may be allowed if “non-IP protocols” are allowed (see “Other Protocols” below).
Identification: Blocked	This service is often required when getting email and is required by most IRC servers.
ICMP: Blocked	This protocol is often abused as a method of breaking people’s network connections (especially on IRC).

Table 4-4. Default Settings for System Activity

System Activity Type	Description
ARP: Allowed	ARP is a necessary Ethernet protocol and is not known to be a threat.
DHCP: Allowed if your system uses DHCP	The program looks in your system Registry to see if one of your network devices uses DHCP. If so, then DHCP is allowed for all devices. If not, then it is blocked for all devices. If you have more than one network device and one uses DHCP, you should check the DHCP setting for each device and allow only for the device that uses it (most often cable or ADSL modems and some internal networks, not for dial-up).
RIP: Blocked	Allow RIP if your administrator or ISP advises you to.
PPTP: Blocked	This should only be altered by the administrator.
Other Protocols: Blocked	If you are on an IPX network, you should allow "non-IP protocols". If you use PPTP, you should allow "other IP protocols". Ask your network administrator before making any change here.

About Intrusion Detection

Unlike other intrusion detection tools, McAfee Firewall's powerful Intrusion Detection System (IDS) is simple to configure and activate. Instead of requiring users to learn and understand a complex set of attacks to build their own defense lines against intrusions, McAfee Firewall's development team created a tool that, when activated with the click of a button, detects common attack types and suspicious activity.

Unprotected computers can be victimized. For example, attackers can use a TCP port scan to find out what services you are running on your machine. Once this is accomplished, they can try to connect to those services and attack your computer. If the attacker discovers that you are running a TELNET, ftp, or Web server, the attacker can try each of your computer's ports sequentially, from 1 to 65535, until an open port is found that they can connect to.

McAfee Firewall's IDS feature looks for specific traffic patterns used by attackers. McAfee Firewall checks each packet that your machine receives to detect suspicious or known attack traffic. For example, if McAfee Firewall sees ICMP packets, it analyzes those packets for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns. When McAfee Firewall matches packets with a known attack pattern, the software generates an event to warn you of a possible security breach.

When intrusion detection is on, traffic is checked by the intrusion detection system. When intrusion detection is active and McAfee Firewall detects an attack, you can block further communication from the suspected machine's IP address indefinitely or for a specific time period. When an attack is detected, McAfee Firewall alerts you with a Windows system tray notification.

NOTE

Because McAfee Firewall is analyzing packets and looking for patterns of packets that identify specific types of attacks, this feature may result in a very slight impact on your machine's performance.

How to Configure the Intrusion Detection System

Use the steps below to configure McAfee Firewall's intrusion detection system:

- 1 From the McAfee Firewall Home page, click Advanced Tasks.

- 2 From the Advanced Tasks list, select Intrusion detection settings.

Refer to the instructions displayed on the Configure Intrusion Detection Settings screen to complete this task.

Common attacks recognized by IDS

The following table lists attacks recognized by McAfee Firewall's IDS, a description of each attack, and the risk factor assigned to each attack.

Attack	Description	Risk Factor
1234	Also known as the Flushot attack, an attacker sends an oversize ping packet that networking software can not handle. Usually, computers hang or slow down. If a total lockup occurs, unsaved data may be lost.	Medium
Back Orifice	Back Orifice is a back door program for Windows 9x written by a group calling themselves the Cult of the Dead Cow. This back door allows remote access to the machine once installed, allowing the installer to run commands, get screen shots, modify the registry, and perform other operations. Client programs to access Back Orifice are available for Windows and UNIX.	High
Bonk	Designed to exploit an implementation error in the first Teardrop patch released by Microsoft, this attack is basically a Windows-specific variant of the original Teardrop attack.	High
Fraggle	This attack is a UDP variant of the Smurf attack. By sending a forged UDP packet to a particular port on a broadcast address, systems on the "amplifier" network will respond to the target machine with either a UDP response or an ICMP UNREACHABLE packet. This flood of incoming packets results in a denial of service attack against the target machine.	High
IP Spoofing	IP spoofing involves sending data with a falsified return IP address. There is nothing inherently dangerous about spoofing a source IP address, but this technique can be used in conjunction with others to carry out attacks TCP session hijacking, or to obscure the source of denial of service attacks (SYN flood, PING flood, etc.).	Medium
Jolt	A remote denial of service attack using specially crafted ICMP packet fragments. May cause slowdowns or crashes on target systems.	High
Jolt 2	A remote Denial of Service (DoS) attack similar to Jolt that uses specially crafted ICMP or UDP packet fragments. May cause slowdowns or crashes on target systems.	High
Land	This attack is performed by sending a TCP packet to a running service on the target host, with a source address of the same host. The TCP packet is a SYN packet, used to establish a new connection, and is sent from the same TCP source port as the destination port. When accepted by the target host, this packet causes a loop within the operating system, essentially locking up the system.	High
Nestea	This attack relies on an error in calculating sizes during packet fragment reassembly. In the reassembly routine of vulnerable systems, there was a failure to account for the length of the IP header field. By sending carefully crafted packets to a vulnerable system, it is possible to crash the target.	High

Attack	Description	Risk Factor
Newtear	A Denial of Service (DoS) attack that usually causes computers with a Windows NT-based operating system to crash. Although the attack is not usually harmful to the computer itself, data from running applications will most certainly be lost.	High
Oshare	A Denial of Service (DoS) attack caused by sending a unique packet structure to your computer. The results of these attacks can vary from a complete system crash, increased CPU load, or momentary delays, depending upon your computer's configuration. This will affect almost all versions of Windows 98 and NT-based systems with varying degrees based on the hardware involved.	High
Ping Flood	This attack involves sending very large numbers of ICMP ECHO (PING) requests to the host under attack. This attack is particularly effective when the attacker has a faster network connection than the victim.	High
Ping of Death	With this attack, a remote user can cause your system to reboot or panic by sending it an oversized PING packet. This is done by sending a fragmented packet larger than 65536 bytes in length, causing the remote system to incorrectly process the packet. The result is that the remote system will reboot or panic during processing.	High
Port Scanning	While not an attack in and of itself, a port scan often indicates that an attacker has begun looking at your system for potential weaknesses. A port scan consists of checking every TCP and/or UDP port to see what services (and hence, what vulnerabilities) might be present.	Low
Saihyousen	The Saihyousen attack may cause some firewalls to crash. It is caused by an attacker sending a stream of UDP packets.	High
Smurf	This attack is carried out by sending an ICMP ECHO REQUEST (PING) packet with a forged source address matching that of the target system. This packet is sent to "amplifier" networks — networks that allow sending packets to the broadcast address — so that every machine on the amplifier network will respond to what they think is a legitimate request from the target. As a result, the target system is flooded with ICMP ECHO REPLY messages, causing a denial of service attack.	High
SynDrop	Overlapping fragmented data sent by an attacker causes your computer to become unstable and or crash. Unsaved data could be lost.	High
Syn Flood	This attack can be used to completely disable your network services by flooding them with connection requests. This will fill the queue which maintains a list of unestablished incoming connections, forcing it to be unable to accept additional connections.	High
Teardrop	On vulnerable systems, it is possible to take advantage of a flaw in the way the TCP/IP stack handles fragmented packet reassembly to consume available memory resources. By sending a specially crafted IP datagram, this attack can cause many operating systems to hang or reboot.	High

Attack	Description	Risk Factor
UDP Flood	<p>A remote Denial of Service (DoS) attack designed to flood the target machine with more data than it can process, thereby preventing legitimate connections from being established.</p> <p>Machine is inaccessible via TCP/IP. Occurs when machine is put to sleep and then awakened.</p> <p>Make sure that "Load Only When Needed" is not checked in the TCP/IP control panel. Then TCP/IP is loaded all the time, allowing McAfee Firewall to function while the machine is asleep.</p>	High
Winnuke	<p>This attack is a Denial of Service (DoS) attack that completely disables networking on many Win95 and WinNT machines. Although Winnuke will not necessarily damage your computer, you may lose any unsaved data at the time of the attack. Restarting your computer should restore full operation.</p>	High

About Instant Updater

As technologies advance, we continually provide updates to McAfee software products. To ensure the highest level of protection, you should always obtain the latest version of your McAfee product.

Updating your software is simple using McAfee's Instant Updater. It is a seamless process and requires minimal interaction on your part.

Instant Updater is also the mechanism used to register your product with McAfee. In order to obtain product updates, you must register your product with McAfee.

Why Do You Need to Update?

- New features may be released for your McAfee product.
- Product fixes are periodically available.
- New product content is updated periodically.
- Updates to anti-virus signature files are frequently available.

How Does the Updating Process Work?

Instant Updater allows you to obtain and apply updates to your McAfee products while connected to the Internet. If an update exists, you will receive a notification. At that time, you can download and apply the updates to your products.

Instant Updater features

- **Auto Update is Instant Updater's default setting.**

Instant Updater silently checks for, and as appropriate, applies product updates while you are connected to the Internet.

Occasionally, Instant Updater may ask you to restart your computer to apply the updates. Auto Update checks for updates daily to ensure that your McAfee product, product content, and related elements such as the virus scan engine and DATs are current.

- **Auto Inquiry:** If Auto Inquiry is enabled, it allows you to receive notification of product updates while connected to the Internet. We do not recommend using Auto Inquiry if you have a slow internet connection
- **Manual Updating:** If you rarely connect to the Internet, you may prefer to use Manual Updating with your McAfee product. You can manually update while connected to the Internet. To do this, select the UPDATE function from within the individual product.

Manual Updating provides you with explicit control of the updating process.

Home page query

Related to Instant Updater is **Home page query**. This feature allows you to configure your McAfee product's home page to display a message when an update is available. After you install your McAfee software, Home page query "on" is the default setting.

Configuration

For additional information regarding auto inquiry and auto update settings, please refer to online Help.

Contacting Customer Service and Technical Support

For Product Support and Customer Service, please visit <http://www.mcafeehelp.co.uk>. Our support Web site offers 24-hour access to solutions to the most common support requests in our easy-to-use 3 step Answer Wizard. You may use our advanced options, which include a Keyword Search and our Help Tree, a tool designed for the more knowledgeable user in mind.

If you cannot find a solution to your problem, you may also access our FREE Chat Now! and E-mail Express! options. Chat and E-mail enables you to quickly reach our qualified support engineers and customer service agents, through the Internet, at no cost. Phone support information can also be obtained from our self-help web site at: <http://www.mcafeehelp.co.uk>.

About McAfee-at-home.com

McAfee is famous for its dedication to customer satisfaction. We continue this tradition by making our site on the World Wide Web a valuable resource for answers to your questions about McAfee Consumer Products. We encourage you to visit us at <http://www.mcafee-at-home.com> and make this your first stop for all of your product needs.

Emergency Support

If you installed a McAfee retail product into your computer and a computer-related emergency arises that prevents you from connecting to the Internet, you may call the telephone number displayed below to obtain a technical support callback.

Emergencies consist of the following:

- Your computer cannot connect to the Internet.
- Your computer was attacked by a virus and it cannot connect to the Internet.
- Your computer freezes after installing a McAfee product.

- You would like to speak with a customer service agent to purchase a McAfee product, rather than make a purchase at our eStore.

For a technical support callback, please be sure to leave your complete name and telephone number; and our expert technical support representatives and customer service agents will return your call as soon as possible.

When we call you, please have the following information readily available:

- The version number of your McAfee software. You can locate this information by selecting Help > About.
- The Windows operating system and version number
- Amount of memory (RAM)
- Model name of hard disk (internal/external)
- Extra card, boards, or hardware
- A complete description of the problem, for example, the EXACT error message as it appears on screen, what actions did you perform before you received the error message, is the error persistent, can you duplicate the problem.

Contact addresses:

Network Associates International B.V.
P.O. Box 58326
1040 HH Amsterdam
The Netherlands

Customer Service
McAfee Consumer Products
Apollo Contact Centre
Units 2-6, Boucher Business Centre
Apollo road, Belfast BT12 6 HP
UK

Emergency Telephone Numbers:

Country:	Telephone Number:
Austria	017 908 75 810
Belgium	02 27 50 703
Denmark	03 5258 321
Finland	09 229 06 000
France	01 70 20 0 008
Germany	06 966 404 330
Ireland/Eire	01 601 55 80
Italy	02 45 28 15 10
Luxembourg	040 666 15670
Netherlands	020 504 0586
Norway	02 3050420
Portugal	00 31 20 586 6430 (English spoken)
Spain	901-120 175 (* toll share)
Sweden	08 57 92 9004
Switzerland	022 310 1033
United Kingdom	020 794 901 07

Index

Numerics

1234 Attack, [35](#)

A

About

Advanced tasks, [23](#)

McAfee list, [23](#)

Tasks, [22](#)

Advanced Tasks, [23](#)

Advanced options and logging, [23](#)

Block IP address, [23](#)

Configure network adapters, [23](#)

Intrusion detection settings, [23](#)

Set up password, [23](#)

Alert Messages, [28](#)

B

Back orifice, [35](#)

Bonk, [35](#)

Browser requirements, [11](#)

C

Common Attacks

1234, [35](#)

Back orifice, [35](#)

Bonk, [35](#)

Flushot, [35](#)

Fraggle, [35](#)

IP spoofing, [35](#)

Jolt, [35](#)

Jolt 2, [35](#)

Land, [35](#)

Nestea, [35](#)

Newtear, [36](#)

Oshare, [36](#)

Ping Flood, [36](#)

Ping of Death, [36](#)

Port Scanning, [36](#)

Saihyousen, [36](#)

Smurf, [36](#)

Syn Flood, [36](#)

SynDrop, [36](#)

Teardrop, [36](#)

UDP Flood, [37](#)

Winnuke, [37](#)

Configuration Assistant, [7, 17](#)

Access to shares, [18](#)

Allowed applications, [19](#)

Network control settings, [17](#)

Startup options, [18](#)

Copyright Information, [ii](#)

Custom filtering rules, [29](#)

D

DATs, [39](#)

Default Settings for System Activity, [31](#)

Default system activity settings

ARP, [32](#)

DHCP, [32](#)

ICMP, [31](#)

Identification, [31](#)

NetBIOS over TCP, [31](#)

PPTP, [32](#)

RIP, [32](#)

F

FAQ, [8](#)

Filtering protocols, [9](#)

Firewall Communication Alert Messages, [28](#)

Flood blocking a TCP connection, [9](#)

Flushot, [35](#)

Fraggle, [35](#)

Frequently asked questions, [8](#)

H

Hard disk requirements, 11

I

Instant Updater

 About, 39

 Auto Inquiry, 40

 Auto Update, 39

 Configuration, 40

 Home page query, 40

 Manual Update, 40

Internet traffic settings, 21

Intrusion Detection

 About, 33

 How to Configure, 33

IP Spoofing, 35

J

Jolt, 35

Jolt 2, 35

L

Land, 35

M

McAfee list, 23

N

Nestea, 35

Network Control Settings

 Allow all, 18

 Block all, 17

 Filter, 18

Network devices support

 Ethernet cards, 9

Network Traffic monitor, 22

Newtear, 36

O

Operating system requirements, 11

Oshare, 36

P

Ping flood, 36

Ping of death, 36

Port scanning, 36

R

RAM requirements, 11

Readme, 7

S

Saihyousen, 36

Screen layout

 Internet traffic settings, 21

 The Task pane, 22

 Title bar, 20

 Tool bar, 20

Server-side nuking, 9

Smurf, 36

Syn flood, 36

synDrop, 36

System settings, 31

T

Tasks, 22

 Configuration Assistant, 23

 Control Internet programs, 22

 Other Tasks, 23

 Perform a security check, 23

 Set alert preferences, 23

 Set startup options, 23

 Set up Home Networking, 23

 View network activity, 23

Teardrop, 36

The Task pane, 22

Title bar, 20

Token Ring, 9

Tool bar, 20

Troubleshooting

 Installation problems, 14

 Windows XP migration, 16

U

UDP flood, [37](#)
Uninstalling, [16](#)

V

VirusScan scan engine, [39](#)

W

Windows XP migration, [16](#)
Winnuke, [37](#)
Winsock 2, [11](#)

For more information on products,
worldwide services, and support,
contact your authorized McAfee sales
representative or visit us at:

www.mcafeehelp.co.uk

Customer Service
McAfee Consumer Products
Apollo Contact Centre
Units 2-6, Boucher Business Centre
Apollo road, Belfast BT12 6 HP
UK

www.mcafee-at-home.com



NA-593-0010-UK-1