McAfee Firewall

Getting Started

Version 2.10

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES, INC. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, McAfee hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

(i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the Documentation's proprietary notices.

c. **Volume Licenses.** If the Software is licensed with volume license terms specified in the applicable price list or product packaging for the Software, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume license authorizes. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Documentation's proprietary notices.

2. **Term.** This Agreement is effective for an unlimited duration unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. **Updates.** For the time period specified in the applicable price list or product packaging for the Software you are entitled to download revisions or updates to the Software when and as McAfee publishes them via its electronic bulletin board system, website or through other online services. For a period of ninety (90) days from the date of the original purchase of the Software, you are entitled to download one (1) revision or upgrade to the Software when and as McAfee publishes it via its electronic bulletin board system, website or through other online services. After the specified time period, you have no further rights to receive any revisions or upgrades without purchase of a new license or annual upgrade plan to the Software.

4. **Ownership Rights.** The Software is protected by United States copyright laws and international treaty provisions. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the applicable list price or product packaging for the Software. You may not transfer any of the rights granted to you under this Agreement. You may not reverse engineer, decompile, or disassemble the Software, except to the extent the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon, the Software in whole or in part. You may not copy the Software or Documentation except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by McAfee. McAfee reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

6. **Warranty and Disclaimer**

   a. **Limited Warranty.** McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be free from defects in materials and workmanship.

   b. **Customer Remedies.** McAfee's and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee's option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to McAfee at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent McAfee is subject to restrictions under United States export control laws and regulations.

   c. **Warranty Disclaimer.** Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MCAFEE DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, MCAFEE MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL MCAFEE OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL MCAFEE BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE MCAFEE CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF MCAFEE SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

8. **United States Government.** The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department's list of Specially Designated Nations or the United States Commerce Department's Table of Denial Orders. By downloading or using the Software you are agreeing to the foregoing and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

   IN ADDITION, YOU SHOULD BE AWARE OF THE FOLLOWING: EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE.

SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY PERSONAL OR BUSINESS USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION TO, OR IMPORTATION OF, ENCRYPTION BY: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE IT IS YOUR ULTIMATE RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS AND THAT MCAFEE HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). McAfee expressly disclaims any express or implied warranty of fitness for High Risk Activities.

11. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. This Agreement supersedes any other communications with respect to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee or a duly authorized representative of McAfee. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

12. **McAfee Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call (408) 988-3832, fax (408) 970-9727, or write: McAfee Software, 3965 Freedom Circle, Santa Clara, California 95054. http://www.mcafee.com.

    Statements made to you in the course of this sale are subject to the Year 2000 Information and Readiness Disclosure Act (Public Law 105-271). In the case of a dispute, this Act may reduce your legal rights regarding the use of any statements regarding Year 2000 readiness, unless otherwise specified in your contract or tariff.

Table of Contents

Chapter 1. Welcome to McAfee Firewall 11

About McAfee Firewall 11

How McAfee Firewall works 12

About McAfee Firewall documentation 12

McAfee Firewall online Help 13

Frequently Asked Questions 13

How will McAfee Firewall help me? 13

How is my PC at risk on the Internet? 14

What other protection do I need? 14

Are there any data packets that McAfee Firewall cannot stop? 15

What network devices does McAfee Firewall support? 15

What protocols can McAfee Firewall filter? 15

How can I still be harassed, even with McAfee Firewall? 16

Chapter 2. Installing McAfee Firewall 17

System requirements 17

About Winsock 2 17

Installing McAfee Firewall 17

Troubleshooting installation problems 18

Step 1: Clean up your hard drive 18

Step 2: Remove temporary files 19

Step 3: Close other software 19

Chapter 3. McAfee Firewall Configurations 21

Applications 21

Control applications 21

Default settings for applications 22

Systems 22

Control system 22

Default settings for System activity 24

Password Protection 25

Instructions for Administrators 25

Configuring Network, Display and Logging Controls 25
Configuring Applications 26
Configuring System Settings 27
Configuration after Adding/Removing Network Devices 28
Using Password Protection 28

Chapter 4. Glossary 31

Appendix A. Product Support 41
How to Contact McAfee 41
Customer service 41
Technical support 42
McAfee training 43

Index 45

Welcome to McAfee Firewall 1

About McAfee Firewall

McAfee Firewall is a personal firewall that lets you monitor, control and log your PC's network activity. It protects you from Internet hackers and keeps your PC private.

McAfee Firewall:

- Stops fileshare and printshare access attempts.
- Shows who is connecting (i.e., 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.
- Detects hidden programs ("trojans") that can give remote access to your PC or reveal private information (e.g. online banking information).
- Provides detailed information about which sites you have contacted and the type of connection that was made
- Blocks all traffic while you are away, and your PC is connected 24 hours a day.

Figure 1-1. McAfee Firewall main window

How McAfee Firewall works

McAfee Firewall is a simple-to-operate security tool for the non-technical users. It dynamically manages your computing security behind the scenes, so that you do not even have to understand networking protocols. It is custom created at the moment it is needed, and only as needed, as you go on to do something else on your computer.

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 PC and before it can waste valuable system resources.

It monitors applications that are either trusted or not trusted. When trusted applications need to access a network, it manages everything in the computer to allow that application's traffic. When it detects non-trusted applications trying to access a network, it blocks all traffic to and from that application.

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

In addition, during the installation process, it will prompt you with some basic questions to set up McAfee Firewall to do specific tasks, according to your needs (e.g. allow sharing of files or not).

NOTE: For more information on how McAfee Firewall works, see Chapter 3, "McAfee Firewall Configurations."

About McAfee Firewall documentation

This Getting Started manual provides the basic information you need to install, setup and use McAfee Firewall. More detailed information on step-by-step instructions on how to perform a task within McAfee Firewall is provided via the Help files which you can access while working within the different windows and dialog boxes. You can also review the Readme.txt file which contain other general information (e.g., frequently asked questions) about the product.

McAfee Firewall online Help

To launch McAfee Firewall help:

In the McAfee Firewall main screen, click Help menu; then select Contents. The Help contents is displayed.

You can also search for a help topic via the Index or Find tabs.

- **Index tab**

1. In the text box, type the first few letters of the word or phrase you are looking for.
2. Locate what you are looking for; then double-click the topic or click the Display button.

- **Find tab**

  Clicking the Find tab enables you to launch a full text search. When you search for topics via the Find tab for the first time, a Find Setup Wizard is displayed. Follow the instructions on screen to setup the full text search option. After setup is complete:

1. In the text box, type the first few letters of the word or phrase you are looking for. You can also select matching words to narrow your search.
2. Once you have located what you are looking for in the display topic box, click the topic.

Frequently Asked Questions

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

NOTE: To read additional frequently asked questions, refer to the Readme.txt file of McAfee Firewall.

How will McAfee Firewall help me?

McAfee Firewall protects your PC 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 you with excellent 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 that is a truly wonderful and amazing accomplishment, it brings with it all the problems of being accessible to complete strangers.

When on the Internet, you need to lock down your PC. When you talk to strangers on IRC (Internet Relay Chat), be cautious of files they send you. This is one way the BO (Back Orifice) program spreads, giving people remote control of your PC. Check files you get for viruses.

When on the Internet, others can try to access your fileshares. You should check that they are not available, or else people can read and delete what is on your system.

The data you send can be seen by more people than just the intended receiver. Practically any system that is connected to any part of the network path used to relay your data packets can see what is sent. Also, it is hard to know with absolute certainty that you are talking to whom you think you are talking to.

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.
- Intrusion detection for an added level of network protection.
- 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 programs or services such as McAfee's Internet Guard Dog 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?

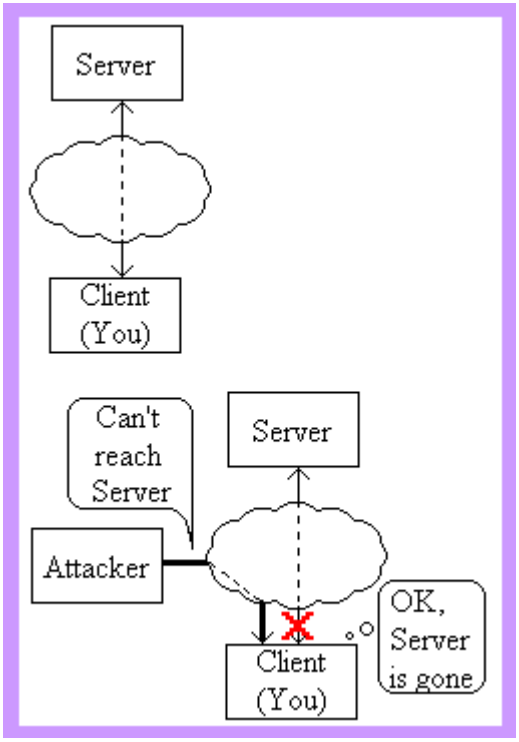
McAfee Firewall supports Ethernet and Ethernet-like devices on Microsoft Windows 95, 98 and NT 4.0 SP4 and SP5. This includes dial-up connections, most cable and ISDN modems and most Ethernet cards. It does not support Token Ring, FDDI, ATM, Frame Relay and other networks.

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?

Figure 1-2. Normal TCP Connection



Many people use McAfee Firewall (and PC FIREWALL) to block the "nukes" that cause their IRC connections to be broken (shown in Figure 1-1). 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 or ConSeal PC 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.

Installing McAfee Firewall 2

Most installation problems are a caused by having programs running while you try to install new software. Even if the installation appears normal, you won't be able to run the new program. 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.

System requirements

To use McAfee Firewall you need:

- IBM PC or compatible computer running Windows 95/98 or Windows NT.
- 5 megabytes (MB) minimum of RAM.
- 16 MB free hard disk space to install McAfee Firewall.
- Microsoft mouse or compatible pointing device.
- Access to the Internet, either a dial-up account with an Internet Service Provider (ISP) or a constant connection through a network.

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 5), 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.

NOTE: For more information on Winsock 2, refer to the Frequently Asked Question section of McAfee Firewall's Readme.txt file.

Installing McAfee Firewall

After closing all open programs, you are ready to install McAfee Firewall on your PC.

To install McAfee Firewall

1. Close all open programs.
2. Insert the McAfee Firewall CD in the CD-ROM drive.
3. In the McAfee Firewall Setup screen, click Install McAfee Firewall.

> **NOTE:** If the setup screen doesn't start automatically when you close your CD-ROM drive, click Start on the Windows taskbar, click Run, then type d:\setup. If D is not the drive letter of your CD-ROM drive, substitute the correct drive letter.

Troubleshooting installation problems

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

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

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

Step 1: Clean up your hard drive

Run the Windows 95 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.

> **NOTE:** These are the default settings.

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.

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: 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.

   You are now ready to install your new software.

McAfee Firewall Configurations 3

The configuration of McAfee Firewall is divided into two parts—application and system. Upon installation, a base set of rules for system services such as ICMP, DHCP and ARP is installed (these are considered default settings). The applications part is personalized. Whenever you run a new program that attempts to communicate over the Internet, McAfee Firewall will prompt you whether you trust the program or not.

For example, using the Netscape Web browser, enter a Web address or the Uniform Resource Locator in the location bar and then press ENTER. Netscape will attempt to connect to that URL over the Internet. The first time you do this, McAfee Firewall prompts if you "trust" Netscape. If you say "Yes", McAfee Firewall notes Netscape is allowed and whenever you use Netscape in the future, McAfee Firewall will allow Netscape traffic.

Behind the scenes, McAfee Firewall creates a rule allowing Netscape to communicate to the specific URL you have indicated and then deletes the rule once all traffic is received or once you exit Netscape. Additionally, when trojans on your system try to communicate out from your PC, McAfee Firewall will also prompt you whether you trust them or not, and the decision to stop trojans is easy and instantaneous.

Applications

Control applications

McAfee Firewall monitors network traffic to see which applications are communicating. Depending on your settings, it will allow or block an application's attempt to communicate.

To control which applications may communicate, click the Settings menu item and choose Applications.

If you choose to "Trust all applications" (putting a check mark in the box), then applications will be added to the "Trusted" list automatically and will be allowed to communicate.

If you do not choose to "Trust all applications", as shown in the figure above, then the first time you run an application and it tries to communicate, you will be prompted and asked if you want that application to communicate. You are only prompted once. Known applications are either allowed or blocked, depending on which list they have been put in.

Default settings for applications

When installed, the default setting is to prompt the user before allowing an application to communicate. The first time you run an application that uses the network, you will be prompted.

If you choose "Yes", the application will be allowed to communicate normally, as it would without McAfee Firewall running.

If you choose "No", the application will be blocked and will probably report an error message, such as "Network is unavailable".

If you allow an application the first time you are prompted, you may change this and block it at any time: just select the Settings / Applications menu item. There, you can move applications into either the "Trusted" list or the "Blocked" list.

When you exit McAfee Firewall, your settings are saved and will be the same the next time it is run.

Systems

Control system

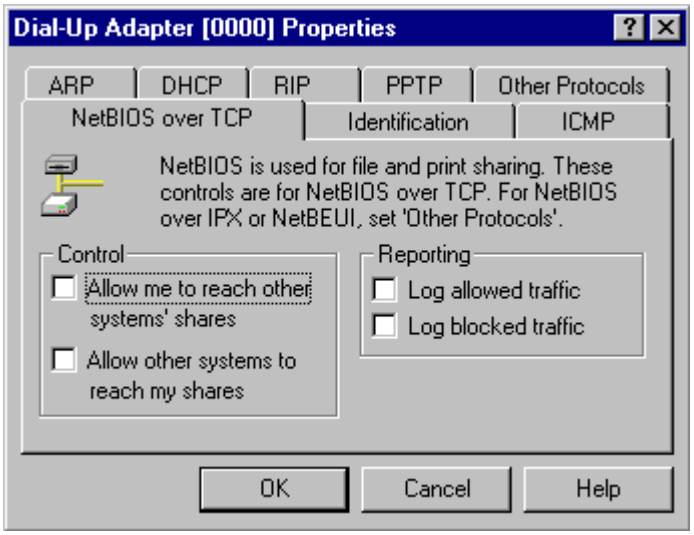
The operating system performs many types of network communication without reporting directly to the user. McAfee Firewall lets the user allow or block different system functions explicitly. Settings may be different for each network device, since a PC may, for example, be on an internal network as well as having a dial-up connection to the Internet.

To control System settings, click on the Settings menu item and choose System. Then choose the network device you want to configure.

Figure 3-1. System Settings

You can either double-click on the network device or click once and choose Properties.

Figure 3-2. Dial-Up Adapter [0000] Properties



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

NOTE: For more information, refer to the McAfee Firewall online Help.

Default settings for System activity

NetBIOS over TCP: Blocked

This will block all fileshare 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 filesharing may be allowed if "non-IP protocols" are allowed (see "Other Protocols" below).

Identification: Allowed

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).

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 (most often cable or ADSL modems and some internal networks, not for dial-up).

RIP: Blocked

Allow RIP if your adminstrator 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.

Password Protection

While McAfee Firewall is designed to protect a Windows computer from unwanted network communication, the security it provides can be undermined if the configuration can be altered. This is especially easy on Windows 95 and 98.

This problem is partially addressed by adding password protection to the configuration file. The protection is only partial because only the operating system can provide access control, such as is found in Linux and Unix.

When you use a password to protect your configuration:

- The settings cannot be changed while McAfee Firewall is running unless the correct password has been entered.
- The tampering of the configuration file will be detected the next time McAfee Firewall is run, if (and when) the password is entered
- If the password has not been entered, new networking applications will be blocked automatically.

Instructions for Administrators

Configuring Network, Display and Logging Controls

Network Control

This should usually be set to "Filter Traffic". If it is set to "Block Everything", the system will not be able to communicate over any network device. If it is set to "Allow Everything", nothing will be blocked. When it is set to "Filter Traffic", it controls network communications according to the Application and System settings.

Display Control

It is best to choose Summary mode when setting it up for other users. The information shown in Detail mode is intended for the Adminstrator and may reduce performance on high-speed networks.

Logging Control

It is important to log unknown traffic if you want to review the log files to look for intrusion attempts. This option should only be unselected if the computer is on a busy network and large amounts of (harmless) traffic fills the log file.

Configuring Applications

The following steps will help the Administrator set up the Applications portion of the configuration. While the configuration file (CPD.SFR) is not intended to be transferrable, the Applications settings can be successfully copied from one system to another. The System settings cannot.

1. Select the Settings menu item, and the Applications option on the popup menu.
2. Do not select "Trust all applications" unless you are very sure this is what you want. When selected, all applications are freely allowed to communicate and malicious "trojans" may go unnoticed.
3. Close the Application Settings dialog box, choosing "OK".
4. Add applications you want to communicate to the "Trusted Applications" list by running the application. You will be prompted to allow the application. Choose 'Yes'.
5. Once you have run the applications you want to communicate, review the Trusted and Blocked Applications lists by choosing Applications / Settings again, as in Step (1).
6. Select the application and click either Add, Remove, or Allow. Click the Trust all applications check box to allow all applications displayed in the list box.

Figure 3-3. Application Settings dialog box

7. Choose "OK" to close the dialog box.

8. Choose File / Save Settings if you want to write this new configuration to disk immediately. Note: the configuration is automatically written to disk when you exit McAfee Firewall.

Configuring System Settings

The following steps will help the Administrator set up the System portion of the configuration. While the configuration file (CPD.SFR) is not intended to be transferrable, the Applications settings can be successfully copied from one system to another. The System settings cannot. This is because different systems have different network devices and it is uncommon to find two that are the same.

1. List all the network segments that are connected to computers that are to be configured.

   Include internal networks and any connection to an external network (e.g. the Internet) even if it is by modem. This is often a simple task, since most computers have just one or two network connections.

2. Decide what network traffic should be allowed on each network segment.

3. Select the Settings menu item, and the System option on the popup menu.

4. From the list of network devices, determine which device is connected to which network segment you listed in Step (1). If you have one modem but see two "Dial-Up Adapter" entries, one of them may be a Microsoft Virtual Private Network Adapter. Usually, the entry with the lower device number (e.g. [0000]) is the physical device and the other is the virtual device.

5. For each device:

   - Highlight the device in the list and select Properties.
   - According to the policies you defined in Step (2) above, allow or block the different types of network traffic.
   - Choose OK when done. Note: changes take effect for this device when you choose OK on the Properties page. Choosing Cancel on the System / Settings page does not cancel these changes. If in doubt, review the settings later to confirm.

6. Choose OK to close the System / Settings dialog box.

NOTE: You must check System Settings after adding or removing network devices.

Configuration after Adding/Removing Network Devices

The System Settings must be verified after changes are made to network devices. This is especially important if a network device is added or removed. If a device was removed, all settings may have to be re-entered, because they previous settings may now be associated with the wrong device. If a device is added, it will have to be configured for the first time.

1. Select the Settings menu item, and the System option on the popup menu.
2. For each network device:
   - Choose the device in the list and choose Properties.
   - Confirm that the settings shown are your choice. Makes changes where necessary.
   - Choose OK when done. Note: changes take effect for this device when you choose OK on the Properties page. Choosing Cancel on the System / Settings page does not cancel these changes. If in doubt, review the settings later to confirm.
3. Choose OK to close the System / Settings dialog box.

Using Password Protection

The following steps will help the Administrator protect the configuration. Without using password protection, the only way to make sure that setup has not been altered is to examine all settings. By using password protection, you will be notified if the setup file was altered.

1. Select the File menu item, and the "Password" option on the popup menu. This pops up another menu. Select "Set".
2. Enter a secret password in the two places shown and choose OK.
3. Write the password down and store it in a safe place. There is no mechanism for retrieving the password once it is lost.

The next time the program is run, it will prompt for the password to be entered. If it is not entered (you can simply hit the <Esc> key), the control functions are disabled (shown in gray) and the setup cannot be changed. Once the correct password is entered, the control functions may be used.

It is really important to choose a password that others will not guess. Choosing words, such as "open sesame" is a poor choice because there are password guessing programs that systematically try every word in the dictionary as well as common phrases, names, dates and other predicatable entries. It is better to choose several unrelated words, letters mixed with numbers, or completely random characters. The more, the better. There are password generation programs that can help you choose. They may help.

It is better to use a new password every time you make an important configuration change. Every file you create with a password is "valid" in that McAfee Firewall will see that it matches the password you used for it. Using a new password prevents someone from secretly replacing an older configuration file for a newer one.

Trojans such as BO and Netbus can log keyboard stokes. Therefore, they can log a password as you type it. While McAfee Firewall helps you detect trojans, you must be diligent in keeping them off your computer(s) before they compromise the security systems you put in place.

TIP: It is also good to have an anti-virus system such as McAfee VirusScan installed on your computer to ensure protection from Trojans and other known viruses.

Glossary 4

Address

A data field in a packet header that specifies either the sender or the intended receiver of the packet. Note that computers can often see data packets that are not intended for them.

Administrator

The person responsible for handling computer configurations as well as support.

Allow/Block (packets)

The action to take on a packet. Block means the packet is not sent/received. Allow means it is sent/received.

ARP

Address Resolution Protocol.

Authentication

The property of verifying that a person or system is who or what it claims to be. This can be achieved via Virtual Private Networks.

BO

Short for "Back Orifice", a trojan remote control program. This program is designed to illustrate the serious security breaches that are possible when using the Windows operating systems. It has been used to cause a lot of mischief and damage. BO's default setup is to listen on UDP port 31337.

BRKill

An attack program that exploits the security implementation weakness of Microsoft's TCP/IP. Starting with the IP address and a good guess of a TCP connection running (particularly on IRC or using PPTP), the attack finds the TCP packet sequence numbers and then attempts to close the connection by spoofing a "disconnect" packet.

Broadcast (networks)

A message addressed to all computers on a specified subnetwork.

Button

An item on a window that when pressed, causes an action to be performed. Usually by clicking the mouse button when the cursor is on it.

Connection

A method of data exchange that allows a reliable transfer of data between two computers.

Cookies

A file placed on your hard drive by a Web site you visit. The original intent is for cookies to contain information about your preferences, so they can tailor the appearance according to your needs. This saves time when you visit the site the next time.

The security risk with cookies is that, since they are written directly to the hard drive, they can store something dangerous (e.g., virus) or private (e.g., password). There is also concern that one Web site can get a cookie created by another Web site. It appears that cookies cannot be used to get other data from a user's hard drive (e.g., applications used, database, address book, personal files, etc.). Cookies can also be used to track where a user has been within a Web site.

Netscape Navigator can be set to prompt you whether or not you want to accept a cookie. It is recommended that you do not accept cookies unless you have a reason for doing so.

datagram

A single, unsequenced packet. UDP is a datagram-based protocol.

Default

The configuration and behavior on installation, before any changes are made.

DHCP

Dynamic Host Configuration Protocol.

Dialog Box

A window used to help the user enter information.

DNS

Domain Name Service, a service for mapping computer names to its IP Address.

Email

Electronic mail, a method of sending messages to other people via computer networks.

Ephemeral (port)

Used temporarily, in the range 1024-5000. In McAfee Firewall, this range is called the "Temporary Range".

Ethernet

The most common type of local area network (LAN).

Fileshare

A file system resource that is available through a network connection.

System uses UDP broadcasts to announce its presence on a network and 'listens' to see who is out there. This is considered appropriate in a trusted office environment, but is completely inappropriate for an Internet connection.

Filter (firewalls)

A tool used to intercept / block all incoming and outgoing network traffic. McAfee Firewall filters traffic.

finger

A service that finds information about a user.

Firewall

A service that controls the transfer of data between computers. This includes the surrounding network. The firewall is responsible for filtering all packets and often provides proxy services to protect internal computers.McAfee Firewall is not a traditional firewall, but it does protect your PC in this fashion.

FTP

File Transfer Protocol, a high-level protocol for file transfer.

GRE

Generic Routing Encapsulation. The PPTP uses this protocol.

Hacker

There are many definitions. The one used here is a person who misuses computer resources, often finding or damaging information.

HTTP

Hypertext Transfer Protocol, a powerful tool used primarily for browsing the World Wide Web.

HTTPS

Secure HTTP. This is a variation of HTTP that uses encryption to add privacy.

ICMP

Internet Control Message Protocol, a maintenance protocol that handles error messages and helps network debugging. ICMP is carried in IP packets.

ICMP is easily abused and has become a serious annoyance to IRC chatgroup users. Because other users can find out information about you, such as your IP address, they can easily send false ICMP messages to your system, causing it to promptly drop your IRC connection.

ICQ

An Internet service that helps people find each other and share information. ICQ has been found to have security weaknesses.

Identification

A service that provides user information to be used on another system, so they can try to verify your identity. If you block it, other systems (such as email servers) may refuse you their services.

This service is also known as "ident" or "auth".

inbound packet

A packet arriving from a remote computer or network.

IP

The essential network protocol of the Internet. It supports TCP, UDP, ICMP and many others. McAfee Firewall filters TCP, UDP and ICMP, and System Settings allow you to allow or block the remaining protocols.

IPX

Network protocol, most commonly used by Novell. It supports SPX. Also, it can be tunneled over IP. McAfee Firewall can block IPX and other non-IP protocols.

IRC

Internet Relay Chat. A service that lets people on the Internet share a typed conversation. Whatever a person typed is sent to other people in the "chat group".

The risk here is that people might become hostile and try to "nuke" you or send you unpleasant email. Consider NetNanny to screen the messages that are sent in IRC.

ISDN

Integrated Services Digital Network

ISP

Internet Service Provider, the company that sells you access to the Internet.

Listening

TCP connections are made to a "listening" port that is ready to accept an incoming connection.

Local (address or port)

Refers to your machine, as opposed to a remote machine.

Log File

A record kept to track activity. The log file helps monitor what connections your computer has made and where unauthorized access (may have) originated.

Menu

A list of commands that are available. If a command is in gray, it is not available.

Message Box

A message window that appears briefly to provide information to the user.

Modem

A device that sends and receives data over a connection, most commonly over a telephone line, cable, ADSL or ISDN.

NetBEUI

NetBIOS Extended User Interface. A local-area protocol that operates underneath the NetBIOS interface. McAfee Firewall does not currently filter NetBEUI.To allow it, you must allow all non-IP protocols.

NetBIOS

A protocol that supports file and print sharing. This protocol can be carried over TCP and UDP or IPX or NetBEUI. You can select "allow me to reach other system's shares", or "allow others to reach my shares".

NetBus

A program designed perform installation without the user knowing about it and allow remote control of the system, including keyboard logging and file access. NetBus uses TCP ports 12345 and 12346 by default.

Netware-IP

A Netware protocol sent using the IP protocol.

Network

A channel used to support communication between computers, e.g. Ethernet or Internet.

Network Device

A hardware computer component that connects your computer to a network, such as Ethernet or Internet.

News (NNTP)

A service available through most ISPs where thousands of newsgroups discuss specific topics, and users may post relevant articles. Remember that anything you post will be archived permanently and can be retrieved at such website as www.deja.com. Also, if you post using your real email address, you WILL receive an unending stream of "spam" (junk email).

ntp

Network Time Protocol, a service that supplies the time.

Operating System

The low-level program that supports the running of all other programs on a computer. OS/2, Linux and Windows are operating systems.

outbound packet

A packet leaving your computer or network to a remote destination.

Packet

A block of data sent over a communication medium, such as the Internet.

Packet Filter

A function of a firewall that checks inbound and outbound packet, and allows or blocks them, depending on predefined rules.

Password

A secret character sequence used for authentication.

Passwords can be stolen by trojans such as BO and NetBus. For better security, consider token-based authentication or one-time passwords.

Phone Book

A set of dial-up services available on your system (look on your system for Dial-Up Networking).

ping

An ICMP-based service used to verify the availability of computers on a network.

POP2

Post Office Protocol, version 2. Used to transfer email.

POP3

Post Office Protocol, version 3. Used to transfer email.

Port

A number used by protocols such as TCP and UDP to identify a communication instance.

PPP

Point-to-Point Protocol, a low-level protocol used to transport higher-level protocols such as IP.

PPPoE

PPP over Ethernet

PPTP

Point-to-Point Tunneling Protocol

Printshare

A printer resource available through a network connection.

Protocol

A standardized method of communication, e.g. IP.

RARP

Reverse Address Resolution Protocol, an Ethernet protocol used to resolve IP addresses.

RAS

Remote Access Service, a service that supports dial-up connections.

Remote (address or port)

Refers to another machine you might communicate with, as opposed to your (local) machine.

RIP

Routing Information Protocol, a UDP-based protocol used to send routing information to systems on a network.

Service

An application or function often considered part of the operating system.

SLIP

Serial Line Internet Protocol, a predecessor to PPP.

SMTP

Simple Mail Transfer Protocol, a popular email protocol.

SNMP

Simple Network Management Protocol. A protocol used to manage networks and routing.

SPX

Sequenced Packet Exchange, a connection-based IPX protocol

TCP

A connection-based Internet Protocol carried in IP packets. Examples of TCP-based applications and services are FTP, web browsing, email, and IRC.

Telnet

A TCP-based service that supports remote logins (usually to UNIX systems). With telnet, you are sending your username and password over a network and they may be stolen by someone and used to break in. Consider a VPN for privacy.

tftp

Trivial file transfer protocol, a UDP-based file transfer protocol. tftp is a security risk because it involves no interaction with the user - it can occur without you knowing about it.

Toggle

A setting that switches between two positions or values.

trojan

A program or piece of executable code that is transmitted without the user's knowledge, often allowing outsiders to break into or control the system

Tunnel

Encapsulates one protocol or data stream within another. A Virtual Private Network (VPN) tunnels data by encrypting it and then encapsulating it within a protocol such as TCP (better) or UDP (worse).

UDP

A connectionless (datagram) Internet Protocol carried in IP packets. Examples of services and applications that use UDP are ICQ, DNS, NetBIOS (for broadcasts etc.) and RIP.

Virus (software)

A piece of code that works without the knowledge of the recipient. It is transmitted inside other software, can duplicate itself, spread and damage your data and / or system.

VPN

Virtual Private Network. A secure private connection, usually through an untrusted network. You can link the LAN's of two offices through the Internet using a VPN, and systems in either office can access those in the other, as if they were on the same LAN. The route through the Internet is invisible. Hackers or snoopers on the Internet just see encrypted traffic and cannot get your private information.

Another configuration of a VPN is "client/server", where computers, such as laptop PCs connect to a VPN server which gives access to a protected network. Home or mobile workers can connect to the office and have the same secure link and can access office systems.

WINS

Windows Internet Name Service, a protocol similar to DNS.

Winsock

A part of the Microsoft Windows operating systems that handles most network connections and some ICMP. It does not handle file or print shares.

Product Support A

BEFORE YOU CONTACT McAfee Software for technical support, locate yourself near the computer with McAfee Firewall installed and verify the information listed below:

- Have you sent in your product registration card?
- Version of McAfee Firewall
- Customer number if registered
- Model name of hard disk (internal or external)
- Version of system software
- Amount of memory (RAM)
- Extra cards, boards or monitors
- Name and version of conflicting software
- EXACT error message as on screen
- What steps were performed prior to receiving error message?
- A complete description of problem

How to Contact McAfee

Customer service

To order products or obtain product information, contact the McAfee Customer Service department at (972) 308-9960 or write to the following address:

McAfee Software
3965 Freedom Circle
Santa Clara, CA 95054
U.S.A.

You can also order products online at http://store.mcafee.com

If you need further assistance or have specific questions about our products, send your questions via email to the appropriate address below:

- For general questions about ordering software: mcafeestore@beyond.com
- For help in downloading software: mcafeedownloadhelp@beyond.com
- For a status on an existing order: mcafeeorderstatus@beyond.com

To inquire about a promotion: mcafeepromotions@beyond.com

Technical support

Support via the web

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web (http://www.mcafee.com) a valuable resource for answers to technical support issues.

We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

Take advantage of the McAfee Product KnowledgeCenter—your free online product support center - 24 hours a day, 7 days a week (http://support.mcafee.com/tech_supp/pkc.asp).

Support forums and telephone contact

If you do not find what you need or do not have web access, try one of our automated services.

Table A-1.

World Wide Web	www.mcafee.com
CompuServe	GO MCAFEE
America Online	keyword MCAFEE
Microsoft Network	mcafee

If the automated services do not have the answers you need, please contact McAfee at the following numbers Monday through Friday between 9:00 AM and 6:00 PM Pacific time for 30-day free support, and 24 hours a day - 7 days a week for Per Minute or Per Incident support.

Table A-1.

30-Day Free Telephone Support	972-308-9960
Per Minute Telephone Support	1-900-225-5624
Per Incident Telephone Support ($35)	1-800-950-1165

McAfee training

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

Disclaimer: Time and telephone numbers are subject to change without prior notice.

Index

A

About McAfee Firewall 11
Address 31
Administrator 31
Allow / Block (packets) 31
ARP 24, 31
Authentication 31

B

BO 31
BRKill 31
Broadcast (networks) 31
Button 32

C

Configuration after Adding / Removing Network Devices 28
Configurations 21
Configuring Applications 26
Configuring Network, Display and Logging Controls 25
Configuring System Settings 27
Connection 32
Control applications 21
Control system 22
Cookies 32

D

datagram 32
Default 32
Default settings for applications 22
DHCP 24, 32
Dialog Box 32
Dial-Up Adapter 23
DNS 32

E

Email 33
Ephemeral (port) 33
Ethernet 33

F

Fileshare 33
Filter (firewalls) 33
finger 33
Firewall 33
Flood blocking a TCP connection 16
FTP 33

G

GRE 33

H

Hacker 33
How is my PC at risk on the Internet? 14
How McAfee Firewall works 12
HTTP 33
HTTPS 34

I

ICMP 24, 34
ICQ 34
Identification 34
Inbound Data 15
inbound packet 34
Installing McAfee Firewall 17
Instructions for Administrators 25

IP 34
IPX 34
IPX network 24
ISDN 35
ISP 35

L

Listening 35
Local (address or port) 35
Log File 35

M

McAfee Firewall filter 15
Menu 35
Message Box 35
Modem 35

N

NetBEUI 35
NetBIOS 35
NetBIOS over TCP 24
NetBus 36
Netware-IP 36
Network 36
Network Device 36
News (NNTP) 36
Normal TCP Connection 16
ntp 36

O

Operating System 36
Outbound Data 15
outbound packet 36

P

Packet 36
Packet Filter 36
Password 37
Password Protection 25
Phone Book 37
ping 37
POP2 37
POP3 37
PPP 37
PPPoE 37
PPTP 24, 37
Printshare 37
Protocol 37
protocols 15

R

RARP 38
RAS 38
Remote (address or port) 38
RIP 24, 38

S

Server-side nuking 16
Service 38
SLIP 38
SMTP 38
SNMP 38
SPX 38
System activity 24
System requirements 17

T

TCP 38
Telnet 38
tftp 39
Toggle 39
trojan 39
Tunnel 39

U

UDP 39
Using Password Protection 28

V

Virus (software) 39
VPN 39

W

WINS 40
Winsock 40
Winsock 2 17