McAfee Firewall

VERSION 3.0

McAFEE
A Network Associates Business

McAfee Perpetual End User License Agreement - United States of America

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF SPECIFIED SOFTWARE (“SOFTWARE”) PRODUCED 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.

    a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all of the Software's proprietary notices unaltered and unobstructed.

    b. **Server-Mode Use.** You may use the Software on a Client Device as a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to, accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (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 unaltered and unobstructed.

    c. **Volume License Use.** If the Software is licensed with volume license terms specified in the applicable product invoicing 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 terms specify. 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 unaltered and unobstructed.

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 cease use of the Software and destroy all copies of the Software and the Documentation.

3. **Updates.** For the time period specified in the applicable product invoicing 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 of 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 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 sell, lease, license, rent, loan or otherwise transfer, with or without consideration, the Software. You shall not disclose the results of any benchmark test that you make of the Software to any third parties without McAfee' prior written consent. Customer agrees not to permit any third party (other than third parties under contract with Customer which contains nondisclosure obligations no less restrictive than those set forth herein) to use the Licensed Program in any form and shall use all reasonable efforts to ensure that no improper or unauthorized use of the Licensed Program is made. 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.

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.** You are advised that the Software is subject to the U.S. Export Administration Regulations. You shall not export, import or transfer Software contrary to U.S. or other applicable laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any third parties in doing so. You represent and agrees that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license. Additionally, you acknowledge that the Software is subject to export control regulations in the European Union and you hereby declare and agree that the Software will not be used for any other purpose than civil (non-military) purposes. The parties agree to cooperate with each other with respect to any application for any required licenses and approvals, however, you acknowledge it is your ultimate responsibility to comply with any and all export and import 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. McAfee reserves the right to periodically audit you to ensure that you are not using any Software in violation of this Agreement. During your standard business hours and upon prior written notice, McAfee may visit you and you will make available to McAfee or its representatives any records pertaining to the Software to McAfee. The cost of any requested audit will be solely borne by McAfee, unless such audit discloses an underpayment or amount due to McAfee in excess of five percent (5%) of the initial license fee for the Software or you are using the Software in an unauthorized manor, in which case you shall pay the cost of the audit. 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: Network Associates, Inc., McAfee Software Division, 3965 Freedom Circle, Santa Clara, California 95054. http://www.nai.com.

McAfee Perpetual End User License Agreement - Canada

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES INTERNATIONAL B.V. ("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 which you acknowledge you have received and read.

    a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all of the Software's proprietary notices unaltered and unobstructed.

    b. **Server-Mode Use.** You may use the Software on a Client Device as a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software which you acknowledge you have received and read. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to, accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (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 unaltered and unobstructed.

    c. **Volume License Use.** 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 unaltered and unobstructed.

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 cease use of the Software and destroy 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 of 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 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 sell, lease, license, rent, loan or otherwise transfer, with or without consideration, the Software. You shall not disclose the results of any benchmark test that you make of the Software to any third parties without McAfee's prior written consent. You agree not to permit any third party (other than third parties under contract with you which contract contains nondisclosure obligations no less restrictive than those set forth herein) to use the Software in any form and shall use all reasonable efforts to ensure that there is no improper or unauthorized use of 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. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be supplied by McAfee on request and on payment of such reasonable costs and expenses of McAfee in supplying that information. 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 or alter any proprietary notices or labels on the Software or Documentation. All rights not expressly set forth hereunder are reserved by McAfee.

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, REPRESENATIONS AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OR CONDITIONS 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, REPRESENTATION OR CONDITION 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.

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.** You have been advised that the Software is subject to the U.S. Export Administration Regulations and applicable local export control laws. You shall not export, import or transfer Products contrary to U.S. or other applicable local laws, whether directly or indirectly, and will not cause, approve or otherwise facilitate others such as agents or any third parties in doing so. If applicable to you, you represent and agree that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied your export privileges. You agree not to use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government and any other applicable local authority by regulation or specific license. Additionally, you acknowledge that the Software is subject to export control regulations in the European Union and you hereby declare and agree that the Software will not be used for any other purpose than civil (non-military) purposes. The parties agree to cooperate with each other with respect to any application for any required licenses and approvals, however, you acknowledge it is your ultimate responsibility to comply with any and all export and import 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 or condition of fitness for High Risk Activities.

11. **Miscellaneous.** This Agreement is governed by the laws of the Netherlands. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Disputes with respect to this Agreement, as well as with respect to its conclusion and execution, will be submitted exclusively to the competent court in Amsterdam. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. McAfee reserves the right to periodically audit you to ensure that you are not using any Software in violation of this Agreement. During your standard business hours and upon prior written notice, McAfee may visit you and you will make available to McAfee or its representatives any records pertaining to the Software to McAfee. The cost of any requested audit will be solely borne by McAfee, unless such audit discloses an underpayment or amount due to McAfee in excess of five percent (5%) of the initial license fee for the Software or you are using the Software in an unauthorized manor, in which case you shall pay the cost of the audit. 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 have required that this Agreement and all documents relating thereto be drawn up in English. Les parties ont demandé que cette convention ainsi que tous les documents que s'y attachent soient rédigés en anglais.

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 +31 20 586 61 00 or write: McAfee, Gatwickstraat 25, 1043 GL Amsterdam, Netherlands. You will find our Internet web-site at http://www.nai.com.

Table of Contents

Welcome to McAfee Firewall 1

About McAfee Firewall

Protect yourself while online with the rock solid security of McAfee Firewall. Easy-to-use, yet highly configurable, McAfee Firewall secures your PCs connection to the Internet whether you connect via DSL, cable modem or dial-up. With its new advanced Intrusion Detection System, color coded security alerts, audible alerts, detailed logging and application scan for Internet capable applications with learning mode, McAfee Firewall gives you all the power you need to control the communications into and out of your PC ensuring that your online experience will be as safe as it is enjoyable.

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.
- 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.

New in this release

- **Intrusion Detection System** - Powerful, yet simple to configure, McAfee Firewall's Intrusion Detection System (IDS) detects common attack types and other suspicious activity. Users are able to easily block further communication from offenders.
- **System Application Scan** - McAfee Firewall can be set to scan a PC for programs that can communicate over the Internet and present a list of such programs to the user. Selecting the programs you want to allow from the onset, you can avoid being inundated by application alerts while online.
- **Color Coded Firewall Alerts** - Easily determine the severity of potential security threats with color coded onscreen alerts. You will quickly know the level of caution appropriate for each situation.

- **Customizable Audible Alerts** - Don't miss a security or privacy concern just because you happen not to be looking at your computer screen. You can also import their own sounds to be used as audible alerts.
- **Enhanced Graphical Display of Network Activity & Attacks** - McAfee Firewall now makes it easier than ever to determine what type of activity is taking place when you go online.
- **New OS Support** - McAfee Firewall supports Windows XP and Windows XP themes.

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 have possess advanced understanding of networking protocols.

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 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 a non-trusted application 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 4, “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 start McAfee Firewall help:

From the McAfee Firewall main window, click Help and select Contents and Index.
Result: Help for McAfee Firewall displays in an explorer-like view with the Contents tab selected for you.

- **Contents tab**

  1. Click the (**+**) next to each "chapter" (represented by a book) to display its "topics" or click the (**–**) next to a chapter to hide its topics.
  2. To view a particular topic, place your mouse pointer over the topic and click.

- **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.

- 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 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?

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.

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:

- Microsoft ® Windows ® XP Home Edition, Windows XP Professional, Windows 2000, Windows Me, Windows NT Workstation v4.0, Windows 98, or Windows 95B.
- Internet Explorer 4.01, Service Pack 2 or higher required for Windows 95 and Windows NT; IE 5.01 or later recommended.
- Personal computer with a Pentium 100 MHz or higher processor.
- 32 megabytes (MB) of RAM.
- 8 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 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.

Installation steps

After inserting the McAfee Firewall 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 NT Workstation v4.0, Windows 2000 Professional, or Windows XP, log on to your system as a user with administrative rights. You must have administrative rights to install this software on your system.
2. Insert the McAfee Firewall CD in to your computer's CD-ROM drive. If the McAfee Firewall 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**.

    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**.
4. Before proceeding with the installation, Setup first checks to see whether your computer already the Microsoft Windows Installer (MSI) utility running as part of your system software.

    a. If your computer runs Windows XP, Windows Me, or Windows 2000, 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 McAfee Firewall 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 may 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.

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.

TIP: You are now ready to install your new software.

Working with Firewall 3

McAfee Firewall 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 in order to activate and use McAfee Firewall.

Please note, the Configuration Assistant cannot be started after clicking Finish. However, all preferences selected using the Configuration Assistant can be changed at any time. To change a setting, select Pick a task from the McAfee Firewall main window and follow the instructions displayed on the screen.

Network Control Settings

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

1. To set your Network Control settings, from the Firewall main window, select one of the following.

Internet Traffic Setting	Description
Block all	• 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.

Internet Traffic Setting	Description
Filter	• 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	• Configures McAfee Firewall to allow all Internet traffic into and out of your computer. All applications or programs in you computer will be allowed to access the Internet; applications 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 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**.

Allowed Applications Screen

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

TIP: Other programs can be "allowed" to access the Internet upon their first attempt to connect to the Internet.

---

2. Click **Finish**.

What's next?

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

- The Firewall service starts.
- The McAfee Firewall main window displays.
- You are now ready to start using McAfee Firewall!

Introduction to Firewall's new interface

Under the guidance of the Microsoft Corporation, McAfee introduces a new look to McAfee Firewall - the Inductive User Interface (IUI).

What is an Inductive User Interface?

An IUI is similar to common web-style design – each screen within the application focuses on a unique, clearly stated, fundamental purpose. An IUI also allows you to easily navigate from one screen to the next.

How will an IUI help me?

IUI simplifies using McAfee Firewall. On any screen within Firewall, you can easily determine how to complete a task or how to access another related or different task. You can easily navigate Firewall by selecting the **Back**, **Forward** and **Home** icons. These three icons are common to all Firewall screens.

How do I use the IUI?

First, start Firewall from the Windows Start menu.

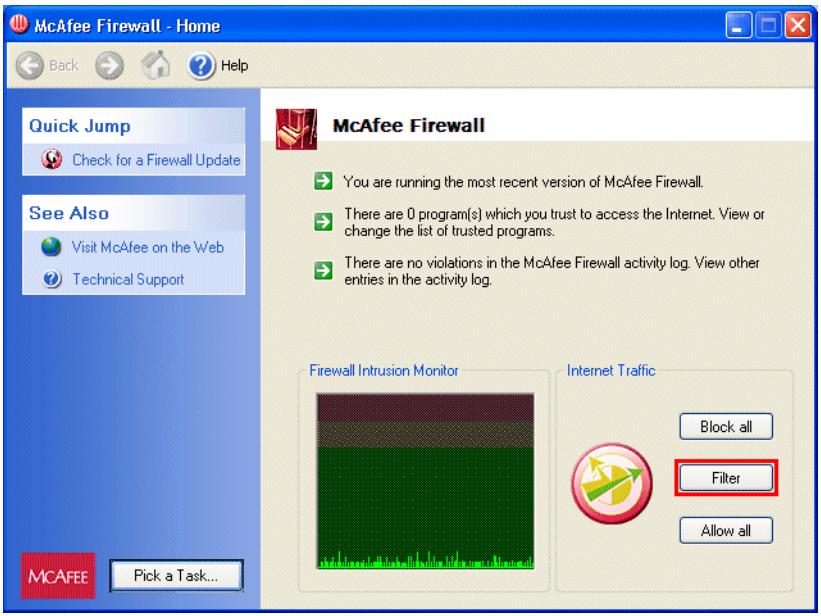

Figure 3-1. The Firewall Main Window

The Firewall main window is your central entry point to all Firewall tasks, features, and components. The main window displays three regions common to all Firewall screens.

Pick a Task

Select **Pick a task** to access the primary task screen. From the primary task screen you can select one of the following tasks:

- **Manage the programs that you trust to access to the Internet.**
- **View your computer's current Internet activity**.
- **Configure advanced settings**.
- **Set alert preferences and sounds.**
- **Shutdown Firewall and exit**.

TIP: After picking a task, simply follow the on-line instructions to complete the task. If you would like to start a new task, select **Pick a task**.

Quick Jump

The **Quick Jump** section allows you access a function or program associated with McAfee Firewall (a function or program may include collection of tasks). For example, from the Quick Jump section you can:

- Click **Quick Jump** to show or hide the Quick Jump tasks.
- Select **Check for a Firewall Update** to start McAfee's Instant Updater. Instant Updater allows you to download updates to your product.

See Also

The **See Also** section displays links to external resources to help you use McAfee Firewall. From the See Also section you can:

- Click **See Also** to show or hide the See Also links.
- Select **Visit McAfee on the Web** to start your internet browser and go to www.McAfee-at-Home.com. Our McAfee-at-Home web site is a valuable resource for all of your McAfee product support needs.
- Select **Technical Support** to start your Internet browser and go to www.mcafeehelp.com. Here at www.mcafeehelp.com you will find solutions to all of your technical needs.

TIP: Click **X** in the upper right corner of any Firewall screen to close the Firewall main window.

Additional status information

Depending upon your configuration, the Firewall main window displays other helpful information such as:

- Details about your version of McAfee Firewall. If there is an update to your version of McAfee Firewall available for download, pick this task.
- The number of programs that you trust to access the Internet. To view or edit the list of trusted programs, pick this task.
- Firewall violation information. Pick this task to view your Firewall violation and activity logs.

McAfee Firewall Configurations 4

The configuration of McAfee Firewall is divided into two parts—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 part 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. Additionally, when undetected trojans on your system try to communicate out from your computer, McAfee Firewall will also prompt you whether you trust them or not, and the decision to stop trojans is easy and instantaneous.

Program configuration

Default settings

During your first attempt to start McAfee Firewall, the Firewall Configuration assistant prompts you to identify programs that you will automatically allow to communicate via the Internet. Based upon the options you selected, the "firewall" reacts accordingly. That is, to either block, allow, or filter a program's communication using the Internet.

Although the Firewall setup and installation wizard performs a thorough analysis of your computer's programs–an analysis to determine programs that use the Internet to communicate–it may not have been able to identify ***all*** of your computer's programs that communicate using the Internet. Or, perhaps, you install a program after installing McAfee Firewall that uses the Internet to communicate. In these scenarios, a Firewall Communication Alert message displays as an unrecognized program attempts to communicate.

The communication alert message asks you to select one of the following options:

- **No, never**: 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."
- **No, not this time**: The active attempt to communicate is blocked. The program is not added to the trusted programs list.
- **Yes, this time only**: The active attempt to communicate is allowed. The program is not added to the trusted programs list.
- **Yes, always:** Allows the program's current and all future attempts to communicate. The active program is added to the trusted programs list with an allowed state of "allowed."

If you allow or block an application 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.

Custom settings

McAfee Firewall monitors Internet traffic to see which applications 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 applications are automatically added to the "Trusted" list and will be allowed to communicate.

TIP: The Program Control window displays the current list of trusted programs and their current "allowed" state.

To view and configure the current list of trusted programs

1. From the McAfee Firewall main window select **Pick a task.**
2. From the primary task window, select **Manage the programs you trust to access the Internet**.
   Result: The Select a Program to Control window displays.
3. Select the program whose filtering settings you wish to configure (or click Browse to add a program to the list).

4. Select one of the following options:
   - Filter this programs's access to the Internet.
   - Allow this program to have full unfiltered access to the Internet.
   - Block this program from accessing the Internet.
   - Remove this program from the list.
5. Click **OK**.

Customized filtering rules

For all programs that you designate as "filter," McAfee Firewall provides you with the flexibility to create a set of custom filtering rules for the specific program. and can be created for any existing program that displays in the trusted programs list.

To create a custom filtering rule

1. From the **Select a program to control** window, select the program whose filtering rule you want to edit or customize.
2. Select the **Filter this program's access to the Internet** radio button.
3. Select **Customize the program's Internet filtering rules**.
   The Customize Filtering Rules window displays.

NOTE: The Customize the program's Internet filtering rules task displays if and only if the Filter this program's access to the Internet option is selected. For all other tasks, this task is hidden.

The Customize Filtering Rules window displays three fields (columns) for each custom rule. They are as follows:

- **Direction**: Type of Internet traffic–inbound or outbound.
- **Protocol**: Describes the type of communication protocol.
- **Port Range**: Describes the port number used by the corresponding communication protocol.

There are three tasks you can perform on the Customize Filtering Rules window. You can:

- **Change the selected filtering rule**.
  This task does not display if there are no existing custom rules.

- **Remove the selected filtering rule**.
  This task does not display if there are no existing custom rules.
- **Add a new filtering rule**.

4. Select **Add a new filtering rule**.
   The **Edit Rule** dialog box displays.
5. Click the radio button of the desired **Direction**.
6. Select a communication protocol from the **Protocol** drop-down pick list.
7. Enter a **Starting Port** number and an **Ending** Port number in their corresponding text boxes.
8. Click **OK** to add the new rule.

TIP: For more information about communication protocols, please refer to the Glossary section of this manual.

Additional information about filtering rule customization

- **To edit or change a filtering rule**, from the Customize Filtering Rules window, select the rule you want to change and click the **Change the filtering rule** task.
  Result: The Edit Rule dialog box displays. Refer to the steps described under "To create a custom filtering rule" on page 31 to complete the task.
- **To remove a filtering rule**, from the Customize Filtering Rules window, select the rule you want to remove and click the **Remove the selected filtering rule** task.

System configuration

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.

Use the steps below to control your System settings.

1. From the McAfee Firewall main window, select **Pick a Task**.
   The primary task window displays.
2. From the primary task window, select **Configure advanced settings**.
   The Configure Advanced Settings window displays.

3. Select **Configure network adapter settings.**

4. From the Configure Network Adapter Settings window, select the adapter you want to configure and click **View or change the properties of this adapter**.
   Result: The Properties sheet for the select 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).

NOTE: For more information, refer to online Help or to the Glossary in this Getting Started guide.

Please refer to Table 4-1 on page 34 for a detailed description of the default settings for system activity.

Table 4-1. Default Settings for System Activity

System Activity Type	Description
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 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.

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. From the **Configure Advanced Settings** window, select **Configure network adapter settings**.

2. For each network device:

   - Select the device in the list and click the **View or change the properties of this adapter** task.

- Confirm that the settings displayed are correct. Make changes where necessary.
- Click **OK** when you are finished.

NOTE: 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. Click **OK** to close the adapter's settings dialog box.

Intrusion Detection System – (IDS) 5

About Intrusion Detection

Firewall's Intrusion Detection System (IDS) is designed to help the same users that the Personal Firewall feature protects: small offices without a corporate firewall, corporate users working outside the corporate firewall, or home users. It defends isolated machines against many different kinds of attacks (i.e.: port scans and flood attacks).

All 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 machine. 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.

Unlike other intrusion detection tools, McAfee Firewall's powerful IDS feature 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, Firewall's development team created a tool that, when activated with the click of a button, detects all common attack types as well as suspicious activity.

McAfee Firewall's IDS feature looks for specific traffic patterns used by attackers. 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, all traffic is checked by the intrusion detection system. When intrusion detection is active and 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 can alert you with a Windows system tray notification.

NOTE: Because 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 feature:

1. Start McAfee Firewall from the Windows Start menu.
   The Firewall main window displays.

TIP: Another way to start McAfee Firewall is to right-click the McAfee Guardian icon displayed in the Windows system tray, point to McAfee Firewall and select Run Firewall.

2. On the McAfee Firewall main window, select **Pick a task**.
3. Select **Advanced Firewall settings**.
4. To activate McAfee Firewall's intrusion detection system, check the **Activate Intrusion Detection** check box. Conversely, to deactivate the Intrusion detection system, clear the check mark from the **Activate Intrusion Detection** check box.
5. To block traffic from an attacker's IP address, check **Automatically block attackers.**
6. You can control how long McAfee Firewall blocks traffic from the attacker's IP address:
   - To block traffic until you remove the host, click **until removed**.
   - To block traffic from the attacker's IP address for a specific number of minutes, click **For,** and enter the **number of minutes.**
7. To play a sound when attacked, click **Play sound when attacked** and select a sound from the menu.
8. To display a Windows system tray notification, as an attack occurs, click **Show tray notification** when attached.
9. Click **OK.**

Update your McAfee Product 6

Introduction to 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.

IMPORTANT: 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

- **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.

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

- **Auto-Inquiry**: Auto-inquiry enabled allows you to receive notification of product updates while connected to the Internet. The default setting for Instant Update is Auto-Inquiry enabled. If you do not connect to the Internet on a regular basis, you may want to disable Auto-Inquiry and use the manual update feature.

TIP: We do not recommend Auto-Inquiry enabled if you have slow internet connection.

- **Auto-Update**: If you do not want to be bothered with notification messages regarding updates, you can enable Auto-Update. Auto-Update enabled allows you to download and apply product updates without notification messages. Updates are "silently" downloaded and applied to your McAfee product.

Configuration

For additional information regarding auto-inquiry and auto-update settings, please refer to on-line help.

Product Support A

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

- Version number of your McAfee software

> **TIP:** From the McAfee Firewall main window select Help > About to find this information.

- Windows operating system version number
- Amount of memory (RAM)
- Complete description of the problem
- EXACT error message as on screen
- What steps were performed prior to receiving error message?
- Is the error persistent; can you duplicate the problem
- Model name of hard disk (internal / external)
- Extra cards, boards, or hardware

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:

Network Associates
13465 Midway Road
Dallas, TX 75244
U.S.A.

> **NOTE:** (972) 308-9960 is telephone call to the United States of America.

www.McAfee-at-Home.com

McAfee is famous for its dedication to customer satisfaction. We have continued 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 support needs.

NOTE: For a status on an existing order, you may send an e-mail message to *salesordersupport@nai.com*.

Technical Support

For agent assisted support, please visit *http://www.mcafeehelp.com*. 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. Additionally, you may use our advanced options, which include a Keyword Search and our Help Tree, which have been designed with the more knowledgeable user in mind. If a solution to your problem cannot be found, you may also access our 24-hour FREE Chat Now! and Email Express! options. Chat and E-mail will enable you to quickly reach our qualified support engineers, through the internet, at no cost. Phone support information can also be obtained from our self-help web site at: *http://www.mcafeehelp.com*.

Support Forums and Telephone Contact

If you do not find what you need, try one of our automated services at the following locations.

World Wide Web	*www.mcafee-at-home.com*
E-commerce	*http://estore.nai.com*
Support web site	*http://www.mcafeehelp.com*
Download web site	*http://www.mcafee-at-home.com/download/default.asp*
CompuServe	*GO MCAFEE*
America Online	*keyword MCAFEE*
Microsoft Network	*mcafee*

Common Attacks Recognized by Intrusion Detection

B

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

Attack	Description	Risk Factor
Back Orifice	Back Orifice is a backdoor program for Windows 9x written by a group calling themselves the Cult of the Dead Cow. This backdoor 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
Jolt2	A remote denial of service 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

Attack	Description	Risk Factor
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
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
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
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
UDP Flood	A remote denial of service attack designed to flood the target machine with more data than it can process, thereby preventing legitimate connections from being established.	High
Machine is inaccessible via TCP/IP.	Occurs when machine is put to sleep and then awakened. 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 Firewall to function while the machine is asleep.	

Glossary

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.

Index

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

Network Associates
13465 Midway Road
Dallas, TX 75244

www.mcafee-at-home.com

NAI-516-0010-3