



# **Sygate Personal Firewall Pro User Guide**

**Version 5.5**

## Copyright Information

Copyright© 2003 by Sygate Technologies, Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission of Sygate Technologies, Inc. Information in this document is subject to change without notice and does not constitute any commitment on the part of Sygate Technologies, Inc. Sygate Technologies, Inc. may own patents or pending patent applications, trademarks, copyrights, and other intellectual property rights covering the subject matter of this document. Furnishing of this documentation does not in any way grant you a license to any patents, trademarks, copyrights, or other intellectual property of Sygate Technologies, Inc.

Sygate, Sygate Secure Enterprise, and the Sygate 'S' Logo are registered trademarks or trademarks of Sygate Technologies, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other companies and product names referenced herein may be trademarks or registered trademarks of their respective holders.

*Documentation Version:*

*Online: SPFPro2519—HSPFPro55.7*

*Printed: PSPFPro55.7*

# Table of Contents

<b>Preface .....</b>	<b>ix</b>
Preface to Help for Sygate Personal Firewall Pro .....	ix
Getting Help.....	ix
What's in this Guide .....	x
What's New for the Firewall?.....	x
Related Documentation .....	xi
Intended Audience.....	xi
Technical Support .....	xi
Third-Party Product Support .....	xii
<b>Chapter 1. Receiving and Installing the Software.....</b>	<b>1</b>
Receiving the Software .....	1
Installing the Firewall Software.....	1
Registering Sygate Personal Firewall Pro.....	2
Uninstalling the Software.....	3
<b>Chapter 2. Test Your System's Vulnerability .....</b>	<b>5</b>
Using Sygate's Online Services.....	5
Performing a Quick Scan .....	6
Performing a Stealth Scan .....	6
Performing a Trojan Scan .....	6
Performing a TCP Scan.....	6
Performing a UDP Scan.....	6
Performing an ICMP Scan.....	7
<b>Chapter 3. Am I Under Attack?.....</b>	<b>9</b>
Help - The System Tray Icon is Flashing .....	9
<b>Chapter 4. The Software in Context.....</b>	<b>11</b>
Introduction .....	11
Some Options May Not Show .....	11
How Firewalls Work.....	12
What Does the Software Do? .....	12
Personal Firewall Defaults: an Introduction .....	12
<b>Chapter 5. Getting Around.....</b>	<b>13</b>
Starting and Using the Software.....	13
Password Protecting Your Security Settings .....	14
Setting a Password.....	14
Entering Your Password .....	14
Disabling Password Protection.....	15
Shortcut to the Software: the System Tray Icon.....	15
Alert Mode—Flashing System Tray Icon .....	16
Using the System Tray Icon .....	18
What the System Tray Icon Tells You .....	19
Using the Main Console.....	21
Menus and Toolbar .....	21

Toolbar Buttons.....	22
Traffic History Graphs .....	22
Broadcast Traffic.....	22
Running Applications Field.....	23
Message Console.....	24
Status Bar .....	24
Using the Menus and Toolbar.....	25
Toolbar Buttons.....	27
Understanding Pop-Up Messages.....	27
Why Did I Get a Pop-Up Message? .....	27
New Application Pop-up .....	27
Changed Application Pop-up .....	31
Trojan Horse Warning.....	32
Why Did I get a Security Notification? .....	33
Blocked Application Notification .....	33
Security Alert Notification.....	33
<b>Chapter 6. Setting Up Protection Based on Application .....</b>	<b>35</b>
How to Set Permissions by Application .....	35
Advanced Application Configuration.....	36
To Set Advanced Configuration .....	36
To Enable Scheduling.....	38
Reviewing and Changing the Permission Status of an Application.....	38
What is Access Status? .....	38
To Change the Status of an Application .....	40
<b>Chapter 7. Setting Up Protection by Configuration Changes .....</b>	<b>41</b>
How to Change Configuration Options .....	41
Review of General Configuration Options .....	42
System Tray Icon .....	42
Sygate Personal Firewall Service.....	43
Screensaver Mode.....	43
Hide Notification Messages .....	43
Password Protection.....	43
Sharing Files and Folders.....	44
Network Neighborhood Settings .....	44
Setting Detailed Security Options.....	45
Enable Intrusion Detection System.....	45
Enable anti-MAC spoofing .....	46
Enable port scan detection.....	47
Enable anti-IP spoofing.....	47
Enable driver-level protection .....	47
Enable OS fingerprint masquerading .....	47
Enable stealth mode browsing.....	47
NetBIOS protection.....	48
Enable DoS protection .....	48
Anti-Application Hijacking .....	48
Block Universal Plug and Play (UPnP) Traffic .....	48
Automatically block attacker's IP address for... second(s) .....	48

Block all traffic while the service is not loaded .....	48
Allow initial traffic.....	49
Enable DLL authentication.....	49
Automatically allow all known DLLs .....	49
Reset all fingerprints for all applications .....	49
Smart Traffic Handling .....	50
Enable smart DNS .....	50
Enable smart DHCP .....	50
Enable smart WINS .....	50
Setting Up Email Notification of Security Events .....	51
To Activate E-Mail Notification .....	51
Updating Your Security .....	52
Logging Security Events on Your System .....	53
To Set Log Size .....	53
To Set Log Days .....	53
To Clear the Log.....	54
To Enable the Security Log.....	54
To Enable the System Log .....	54
To Enable the Traffic Log .....	54
To Enable the Packet Log.....	54
<b>Chapter 8. Configuring Advanced Rules for Security .....</b>	<b>55</b>
Setting up Advanced Rules .....	55
Overview of Creating Advanced Rules.....	56
Advanced Rules: Provide a Name, Specify Allow or Block.....	57
Advanced Rules: Specify a Source .....	59
Advanced Rules: Specify Ports and Protocols .....	60
All Protocols .....	60
TCP 60	
UDP .....	61
ICMP.....	61
IP Type .....	61
Advanced Rules: Define a Schedule.....	62
Advanced Rules: Specifying Applications .....	63
<b>Appendix A. Monitoring Your System: Logs.....</b>	<b>65</b>
Understanding Logs.....	66
Exporting Logs.....	67
Viewing Logs .....	68
Viewing the Security Log .....	70
Viewing the Security Log.....	70
Icons for the Security Log.....	71
Personal Firewall Security Log Parameters and Description .....	71
Description and Data Fields for the Security Log .....	72
Back Tracing Hack Attempts for the Security Log .....	72
Filtering the Log Events by Severity in the Security Log .....	73
Filtering the Log Events by Date in the Security Log.....	73
Viewing the Traffic Log .....	75
Viewing the Traffic Log.....	75

Icons for the Traffic Log.....	76
Personal Firewall Traffic Log Parameters and Description .....	76
Description and Data Fields for the Traffic Log.....	78
Back Tracing Traffic Events for the Traffic Log.....	78
Viewing the Traffic Log Events by Date .....	78
Viewing the Packet Log.....	80
Viewing the Packet Log .....	80
Icons for the Packet Log .....	81
Firewall Packet Log Parameters and Description .....	81
Packet Decode and Packet Dump for the Packet Log .....	82
Back Tracing Packet Log Events .....	82
Viewing the Packet Log Events by Date.....	83
Viewing the System Log.....	84
Viewing the System Log .....	84
Icons for the System Log .....	84
Personal Firewall System Log Parameters and Description.....	84
Description and Data Fields for the System Log.....	85
Viewing the System Log Events by Date.....	85
Back Tracing Logged Events on the Personal Firewall.....	86
To Backtrace a Log Event.....	86
WhoIs.....	87
<b>Appendix B. More About Default Values .....</b>	<b>89</b>
Defaults: A Summary of Rules and Settings .....	89
Default Rules and Settings for the Personal Firewall.....	89
<b>Appendix C. Troubleshooting Sygate Personal Firewall Pro .....</b>	<b>91</b>
Firewall Configuration, Usage, and Software Expiration.....	92
Can I continue using the product after the end of the upgrade protection period? .....	92
Will the Firewall work on a computer that has multiple IP addresses assigned to a single NIC? .....	92
What should I do if I am having trouble with Network Shares?.....	92
Firewall Protection Against Attacks, Viruses, Trojans .....	94
Does the Firewall protect against viruses and Trojans?.....	94
After updating one of my applications, the Firewall shows a major attack. Do I have a Trojan? .....	94
Does the Firewall do Stateful Packet Inspection? .....	94
Firewall and Internet Connection Sharing, VPNs, and Networking.....	95
Is the Personal Firewall compatible with Microsoft's Internet Connection Sharing (ICS)? .....	95
How do I configure the Personal Firewall to work with ICS?.....	95
When the Test button is clicked, the Personal Firewall starts the Internet Connection Wizard. Why? .....	96
How do I set up the Personal Firewall to work with my CheckPoint VPN client software? .....	96
What should I do if experiencing a slow or non-existent connection after installing the Personal Firewall? .....	97

Should I Allow the win32 kernel core or ntkernel component?	
What about ICMP? .....	98
<b>Glossary .....</b>	<b>99</b>

## List of Tables

Table 1.	System Tray Icon colors .....	16
Table 2.	System Tray Icon .....	18
Table 3.	What the System Tray Icon Tells You.....	19
Table 4.	Running Applications Field.....	23
Table 5.	Firewall Menus .....	25
Table 6.	Pop-up: Remember My Answer? .....	30
Table 7.	Firewall Application Access Status.....	39
Table 8.	Personal Firewall Security Log Icons.....	71
Table 9.	Personal Firewall Security Log Parameters and Description.....	71
Table 10.	Viewing Personal Firewall Security Log Events by Date .....	73
Table 11.	Personal Firewall Traffic Log Icons .....	76
Table 12.	Personal Firewall Traffic Log Parameters and Description.....	76
Table 13.	Viewing Personal Firewall Traffic Log Events by Date .....	78
Table 14.	Personal Firewall Packet Log Icon .....	81
Table 15.	Personal Firewall Packet Log Parameters and Description .....	81
Table 16.	Viewing Personal Firewall Packet Log Events by Date .....	83
Table 17.	Icons for the Personal Firewall System Log.....	84
Table 18.	Personal Firewall System Log Parameters and Description .....	85
Table 19.	Viewing Personal Firewall System Log Events by Date.....	85



## Preface

This chapter introduces the Sygate Personal Firewall Pro. It provides:

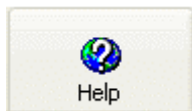
- “What’s New”
- “Related Documentation”
- “Intended Audience”
- “Technical Support”

## Preface to Help for Sygate Personal Firewall Pro

This manual aids you in the installation and use of the Sygate Personal Firewall Pro (the Personal Firewall).

### Getting Help

Select **Start | Programs | Sygate Personal Firewall | Sygate Personal Firewall Pro**. The Personal Firewall starts and displays the user interface. You can then choose **Help | Help topics...** from the menu bar, click the **Help** button, or press **F1**.



The online help system appears. It provides all the information needed to use the Personal Firewall.

All information in this help system is also available in the 5.5 *Sygate Personal Firewall Pro User Guide* in Adobe's PDF format for easy printing. You can download the *Sygate Personal Firewall Pro User Guide* from the Sygate Technologies web site at <http://smb.sygate.com>.

## What's in this Guide

This document, the *Sygate Personal Firewall Pro User Guide*, describes how to install and use the Firewall software.

For late-breaking news about known problems with this release, refer to the `Readme.txt` file that is included with this software.

## What's New for the Firewall?

This release of the Personal Firewall has a variety of new and enhanced features. Among them:

- **Provides Deep Packet Inspection**—The Personal Firewall provides further enhanced intrusion detection and prevention capabilities, including alerts when another user attempts to compromise your system. The end result is a system that analyzes network packets and compares them with known attacks and known behavioral patterns of attack, and then intelligently blocks the malicious attacks.
- **Denial of Service (DoS) Protection**—This enables the Personal Firewall to monitor and block incoming traffic with known Denial of Service (DoS) attack patterns. DoS attacks are characterized by an explicit attempt by an intruder to prevent legitimate users of a service from using that service by flooding a service with illegitimate traffic. This feature can be enabled or disabled.
- **Trojan Detection and Protection**—Trojan protection is enhanced to identify, block, and terminate the process of more types of Trojan attacks.
- **Universal Plug and Play (UPnP) Protection**—The Personal Firewall has a new option that protects computers from UPnP exploits. This feature can be enabled or disabled.
- **Log Dampener Feature**—The Personal Firewall adds new logging flexibility and performance enhancement features, including the option to selectively enable or disable the security logs, system logs, traffic logs, and full packet logs.
- **Smart WINS**—This feature allows Windows Internet Naming Service (WINS) requests only if they were requested. If the traffic was not requested, the WINS reply is blocked. The user can enable or disable this feature.
- **Active Response Protection**—Active response is a feature that automatically blocks all communication from a source host once an attack has been detected. For example, if the Personal Firewall detects a DoS attack originating from a certain IP address, the Personal Firewall will automatically block any and all traffic from that IP for the duration specified in the seconds field. The user can now stop a current active response session.
- **Anti-Application Hijacking Protection**—The Personal Firewall now protects against even more attacks, including such exploits such as “TooLeaky” and others.

- **Enhanced performance**—The Personal Firewall is now faster and takes fewer system resources.
- **Improved Logging Capabilities**—The Personal Firewall adds new logging flexibility, including the option to disable all logs.
- **Support for Windows Server 2003**—The Personal Firewall is now supported on Windows Server 2003 for Small to Medium Businesses. For server deployments greater than 500 seats and that need centralized management, Sygate Secure Enterprise is required.
- **Improved Microsoft System Installer Support**—The Personal Firewall is now packaged by default as a Microsoft System Installer (MSI) package to simplify deployment with Microsoft SMS and other software distribution tools.

## Related Documentation

This document describes how to use the Sygate Personal Firewall Pro, and includes the following documentation:

- **Online Help**—This help file provides the same information as the printed documentation, which is available in PDF format from the Sygate web site at <http://smb.sygate.com/support/> for easy printing.
- **Sygate Personal Firewall Pro User Guide** (this guide)—Describes how to use Sygate Personal Firewall Pro (PDF format).

## Intended Audience

This documentation has been written for end users of the Personal Firewall software.

This documentation assumes that the user is familiar with the basic functioning of Windows operating systems and standard Windows items, such as buttons, menus, toolbars, windows, etc. Further, this guide assumes that the user has an Internet connection, whether through a local area network, DSL connection, dial-up modem, wireless access point, or other connection method.

## Technical Support

Sygate Technologies provides a wide variety of service and support programs. Contact Sygate through its web site, by email, or by telephone.

**Sygate web site:**     <http://smb.sygate.com/support>

**Sygate Forums:**     <http://forums.sygate.com/vb>

**Email Support:**     [http://smb.sygate.com/support/forms/proreq\\_form.htm](http://smb.sygate.com/support/forms/proreq_form.htm)

**Priority** <http://smb.sygate.com/support/documents/pspf/priority.php>  
**Telephone**  
**Support (fee based)**

Sygate provides documentation support and accepts documentation feedback by email.

**Documentation feedback:** [documentation@sygate.com](mailto:documentation@sygate.com)

### **Third-Party Product Support**

If you obtained this product from a hardware or software company other than Sygate Technologies directly, your software license as well as all service and support should be obtained through that vendor. Check the addendum provided with the package for service and support information.

# Chapter 1. Receiving and Installing the Software

This chapter describes the various methods by which you may have received the Personal Firewall software, or which you may use to get another copy if your system administrator directs you to them. It also goes over the simple steps needed to install the software, if it has not already been installed. It concludes with instructions on how to uninstall the Personal Firewall.

## Receiving the Software

The Personal Firewall software can be distributed to you in a number of ways, one of which was used to get the software to your computer. You may need to take some action to go and get the software, or the software may already be installed.

- **Download from the Sygate site**—You connect to the Sygate Technologies Web site to download this tool, by going to [smb.sygate.com](http://smb.sygate.com). With this type of installation, you may be prompted for your agreement to the license agreement, location of the software on your hard drive, and so on, as described in “Installing the Software.”
- **Other Web download**—You receive an e-mail message or other pointer to a location on the Web or a server on your Extranet where a zipped file exists. Run that file, and it will unzip the Personal Firewall files and then run the `Setup.exe` program to install the Personal Firewall. With this type of installation, you may be prompted for your agreement to the license agreement, location of the software on your hard drive, and so on, as described in “Installing the Software.”

## Installing the Firewall Software

To install the software:

1. Run `Setup.exe`.  
The Personal Firewall Setup window appears.
2. Click **Next**.  
The License Agreement dialog box appears. Scroll through the agreement to make sure that you agree with its terms.

3. Click **I accept the license agreement** if you agree, then click **Next**.  
The Destination Folder dialog box appears.
4. Click **Next** to accept the default location for the Personal Firewall files or click **Browse** to select a different location.  
The Ready to Install the Application dialog box appears.
5. Click **Next**.  
If you are updating a previous installation, the Upgrade Installation dialog box appears.
6. If you want to keep the previous configuration, click **Yes**. Otherwise, click **No**.  
The Updating System window appears while the files are copied to your system, followed by the Finish window.
7. Click **Finish**.  
The Installer Information dialog box appears, telling you that you must restart your computer to begin using the Personal Firewall.
8. Click **Yes** to reboot your system and begin using the Personal Firewall, or click **No** if you plan to restart manually later.

## Registering Sygate Personal Firewall Pro

To register Sygate Personal Firewall Pro, select either one of the following options:

**Option 1.** Click **Register Later** and you will get a FREE, Fully Functional 30-Day trial period for Sygate Personal Firewall Pro to determine if this product meets your needs.

**Option 2.** If you have already purchased a license key from the Sygate Online Store and would like to register the software for your computer now, please fill out ALL fields given on the registration screen (use N/A for those that do not apply) and click **Register Now** (You must be connected to the Internet to complete the registration process).

**Note:**

All characters entered into “Serial Number” and “Registration Code” will be converted to uppercase automatically. The license key might contain look-alike characters such as the alphabet “I” in uppercase and the number “1”, or the alphabet “o” in uppercase and the number “0”)

**Option 3.** If you do not have a license and would like to purchase Sygate Personal Firewall Pro now, click **Buy Pro** and you will be taken to the Sygate Online Store where you can purchase and obtain a license key(s).

**Note:**

All characters entered into “Serial Number” and “Registration Code” will be converted to uppercase automatically.



The image shows a Windows-style dialog box titled "Registration for Sygate Personal Firewall Pro". The title bar is blue with a red close button. The main area has a light beige background. At the top, it says "Sygate Personal Firewall Pro" in red. Below that, it says "Thank you for installing Sygate Personal Firewall Pro." and "You have 18 day(s) remaining in your trial period. When this trial period expires, you will need to purchase a license key by clicking the 'Buy PRO' button below." There is a section titled "Registration Information" with a blue header. It says "In order to register your product successfully, all fields are required and you must be connected to the Internet." Below this are several input fields: "Name:", "Company:", "Position/Title:", "Phone Number:", "E-mail:", "Serial Number:" (with a hyphen separator), and "Registration Code:". At the bottom, there is a note: "Note: Your license key will be sent in the confirmation email after you make your purchase." and a link: "For support or to see our privacy policy, please visit [www.sygate.com](\"http://www.sygate.com\")." At the very bottom are three buttons: "Buy PRO", "Register Later", and "Register Now".

**Registration for Sygate Personal Firewall Pro**

**Sygate Personal Firewall Pro**

Thank you for installing Sygate Personal Firewall Pro.

You have 18 day(s) remaining in your trial period. When this trial period expires, you will need to purchase a license key by clicking the "Buy PRO" button below.

**Registration Information**

In order to register your product successfully, all fields are required and you must be connected to the Internet.

Name :

Company :

Position/Title :

Phone Number :

E-mail :

Serial Number :  --

Registration Code :

Note: Your license key will be sent in the confirmation email after you make your purchase.

For support or to see our privacy policy, please visit [www.sygate.com](http://www.sygate.com).

**Buy PRO** **Register Later** **Register Now**

## Uninstalling the Software

If you need to uninstall the Software:

1. Click the **Start Menu** on your task bar.
2. Click **Settings | Control Panel | Add/Remove Programs**.
3. Click **Sygate Personal Firewall Pro 5.5**.
4. Click **Remove**. Windows guides you through the process.

You can also remove Sygate Personal Firewall Pro from the **Start** menu:

1. Click the **Start Menu** on your task bar.
2. Click **Sygate Personal Firewall | UnInstall Sygate Personal Firewall Pro**





## Chapter 2. Test Your System's Vulnerability

This chapter describes ways to test the vulnerability of your system to outside threats. The test is available directly from Sygate via an online connection.

### Using Sygate's Online Services

Assessing your vulnerability to an attack is one of the most important steps that you can take to ensure that your system is protected from possible intruders. With what you learn from this battery of tests, you can more effectively set the various options on your Personal Firewall to protect your system from attack.

Click the **Security Test** button located on the main console of the Personal Firewall, or select **Test Your Firewall** from the **Tools** menu:



The Sygate Technologies Web page (<http://scan.sygate.com>) displays. If you then choose **Scan Now**, the Sygate Online Services scanner scans your computer and attempts to determine your IP address, operating system, Web browser, and other information about your system.

You can then choose one of the more focused scans. To find out more about each one, click the name of the scan.

- Quick Scan
- Stealth Scan
- Trojan Scan
- TCP Scan
- UDP Scan
- ICMP Scan

### **To scan your system:**

Click the name of the scan and then click **Scan Now**.

A brief document of frequently asked questions about Sygate Online Services is also available from the main scan page. Click **Scan FAQ** at the bottom left side of the screen.

## **Performing a Quick Scan**

Quick Scan is a brief, general scan that encompasses several scanning processes. It usually takes 20 seconds or less to accurately scan your computer's ports, protocols, services, and possible Trojans. The results are recorded in the Personal Firewall's Security log.

## **Performing a Stealth Scan**

The Stealth scan scans your computer using specialized stealthing techniques, which mimic portions of legitimate computer communication to detect the presence of a computer. The Stealth scan takes about 20 seconds to complete and is most likely not recorded in the Security log.

## **Performing a Trojan Scan**

The Trojan scan feature scans all of your computer's 65,535 ports for active Trojan horse programs that you or someone else may have inadvertently downloaded. The Trojan scan takes about 10 minutes to complete. A list of common Trojans is available on the Web site.

## **Performing a TCP Scan**

The TCP scan examines the 1,024 ports that are mainly reserved for TCP services, such as instant messaging services, to see if these ports are open to communication. Open ports can indicate a dangerous security hole that can be exploited by malicious hackers.

It scans ports on your computer that are connected to devices such as routers and proxies for users connecting to the Web site through such a device. The scan takes about 20 minutes to complete and is logged by the Personal Firewall as a scan event in the Security log.

## **Performing a UDP Scan**

The UDP scan uses various methods and protocols to probe for open ports utilizing UDP. The UDP scan will scan ports on your computer that are connected to devices such as routers and proxies for users connecting to the Web site through such a device. The scan takes about 10 minutes and should be logged in the Security log as a portscan from Sygate.

## **Performing an ICMP Scan**

When an ICMP scan has completed scanning a user's computer, it displays a page with the results of the scan. If a user is running the Personal Firewall, all scans are blocked.



## Chapter 3. Am I Under Attack?

### Help - The System Tray Icon is Flashing

If the system tray icon is flashing, the Personal Firewall is in Alert Mode because:



- An attack has been recorded on your computer in the Security Log.

OR

- You are missing a file or an application that is required by your System Administrator before you can log into the network. If a file or an application is missing, a message is probably displayed that lists the missing files or applications that you need to install before you can proceed.

To assess the status of the attack:

- Double-click the System Tray Icon

If the reason for the flashing is an attack, the Security Log is automatically displayed. Otherwise, the icon stops flashing.

The system tray icon can tell you many other things, as described here: “Shortcut to the Software: the System Tray Icon”



## Chapter 4. The Software in Context

This chapter introduces you to what the Personal Firewall is and how the Personal Firewall works, putting it into context. It includes:

- “Introduction”
- “Some Options May Not Show”
- “How Firewalls Work”
- “What Does the Do?”
- “Key Features”
- “Defaults: an Introduction”

### Introduction

The Personal Firewall is a security agent that is installed on workstations, servers, and laptops in the network enterprise and on home and small business systems. Once installed, it provides a complex and customizable firewall. In addition, it can also provide intrusion detection and prevention, such as detecting and identifying known Trojans, port scans, and other common attacks, and to selectively enable or block the use of various networking services, ports, and components. As you saw in the previous chapter, something that you may want to do immediately is to test your System’s vulnerability, using Sygate’s Web site to test it. For further information on this, see “Test Your System’s Vulnerability.”

The Personal Firewall is designed to protect your computer from intrusion and misuse, whether malicious or unintentional.

### Some Options May Not Show

This document, the *Sygate Personal Firewall Pro User Guide*, describes all options that the Personal Firewall supports, but describes some options that are only available with the Pro version of Sygate Personal Firewall. Options that are disabled may appear dimmed or may not appear at all on your computer. The following note appears next to those options:

➡ **Option Alert:** This option may appear dimmed or not at all. For further information, see “Some Options May Not Show.”

## How Firewalls Work

A firewall is hardware, software, or a combination of both that is used to prevent unauthorized Internet users from accessing a private network. All information entering or leaving the network must pass through the firewall, which examines the information packets and blocks those that do not meet the security criteria. Sygate Personal Firewall Pro starts with extensive firewall capabilities, and then enhances those capabilities with additional ones.

## What Does the Software Do?

The Personal Firewall protects an individual computer from network traffic that can cause harm to that computer. It does this in a variety of ways, which can be summarized into three categories of firewall rules:

1. **Allow:** The Personal Firewall *Allows* some traffic to flow. This is usually traffic that is known to be “safe”, usually because you have defined it, application by application, to be “safe.” Examples of traffic normally classified as safe include Outlook, Internet Explorer, Netscape Navigator, Outlook Express, and other common networking and communications software.
2. **Block:** The Personal Firewall *Blocks* some traffic. This is usually traffic that is known to be problematic or dangerous to your computer.
3. **Ask:** The Personal Firewall *Asks* whether incoming and outgoing traffic is allowed to access your computer or an organization’s network resources. When you run the Firewall, it initially asks you whether to permit your applications to access network resources. Optionally, it remembers your responses, so that you do not have to tell it again, for example, that you plan to use Internet Explorer or Netscape Navigator.

By using firewall rules, the Personal Firewall can systematically **Allow**, **Block**, or **Ask** about what action to take on incoming traffic from specific IP addresses and ports. The configuration of those rules with other security settings provides a security agent that protects your computer.

## Personal Firewall Defaults: an Introduction

The Personal Firewall comes with default security policy settings. As a security agent, those settings are designed to be relatively secure “out of the box.” However, the user can customize the default settings and default rules extensively.

For a more detailed summary, see, “Defaults: A Summary of Rules and Settings.”



## Chapter 5. Getting Around


This chapter presents an overview of the tools that you use in getting around in the Personal Firewall. It includes:

- “Starting and Using the “
- “Logging In and Logging Out”
- “Shortcut to the Software: the System Tray Icon”
- “Using the Main Console”

### Starting and Using the Software

The Personal Firewall is usually set to start automatically when you turn on your computer, protecting you immediately. If you want to make changes in the configuration of your Personal Firewall or if you want to review logs of potential attacks on your Personal Firewall, you bring up the application itself so that you can make changes.

You have two main ways of opening the Personal Firewall application:

- **System Tray Icon**—This way is easy to find: it is the icon that is on your system tray. Normally, it looks like this , an appearance that indicates that all is well, and that your system is transmitting traffic both to and from the network. To use the system tray icon, right click on it and make choices from there. For more information on how to use the system tray icon, see “Shortcut to the Personal Firewall: the System Tray Icon.”
- **The Main Console**—This is the control center for the Personal Firewall. From here, you have access to all of the settings and rules for the Personal Firewall. To bring up the main console, choose **Sygate Personal Firewall Pro** from the **Start** menu. The main console appears. For more information on the main console, see “Using the Main Console.”

## Password Protecting Your Security Settings

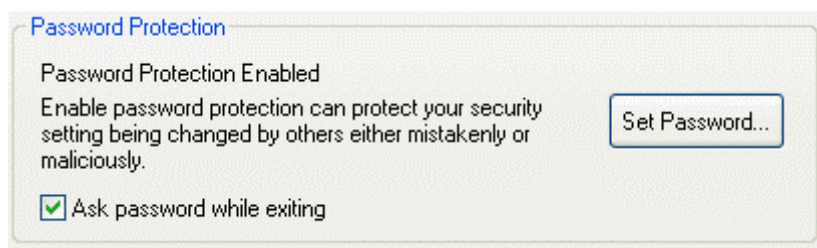
You can set your Personal Firewall to use a password prior to making any security changes, and to require a password before shutting down the Personal Firewall.

### Setting a Password

To set a password for the Personal Firewall, open the **Tools | Options | General** tab. Click the **Set Password...** button at the bottom right of the dialog box. The Password dialog box appears:

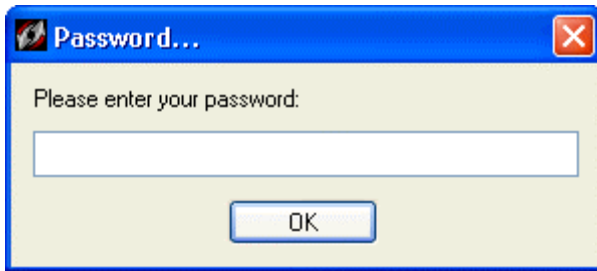


Enter your new password in the **New Password** field, and repeat it in the **Confirm New Password** field. Click **OK** to confirm, or click **Cancel** to discard your changes. From then on, this tab will show that password protection has been enabled:



### Entering Your Password

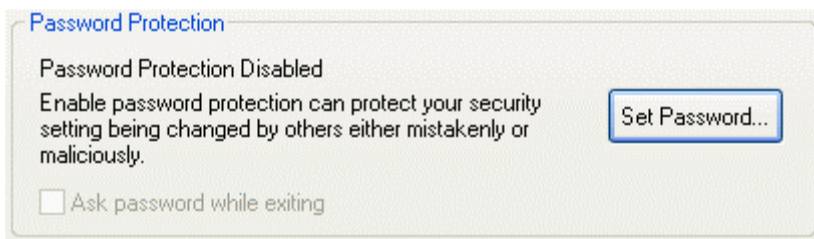
Once you have set a password, the Personal Firewall prompts you for that password whenever you double-click the System Tray icon to access your security settings. You can also choose to have the Personal Firewall prompt you for a password before exiting the Personal Firewall, by clicking **Ask password while exiting** in the **Password Protection** dialog box. The **Password...** dialog box that prompts you for your password is the same in either case:



Enter your password and click **OK** to access the Personal Firewall.

## Disabling Password Protection

You can choose to disable password protection by making no entry in the **New Password** field and confirming that in the **Confirm New Password** field. The tab will show that password protection has been disabled:



## Shortcut to the Software: the System Tray Icon



Once installed, the Personal Firewall displays a small icon in your system tray (located on the right end of your task bar), consisting of two arrows. The arrows represent system traffic: the upward-pointing arrow is outgoing traffic; the downward-pointing arrow is incoming traffic.

These arrows give you a real-time update of your computer's traffic flow. You might not see a constant icon appearance for more than a few seconds, especially if you frequently use the Internet or your network connection.

The colors of the arrows are always changing (as is the traffic flow on your computer). For most users, it should be sufficient to remember the following points about the colors of the icon:

**Table 1. System Tray Icon colors**

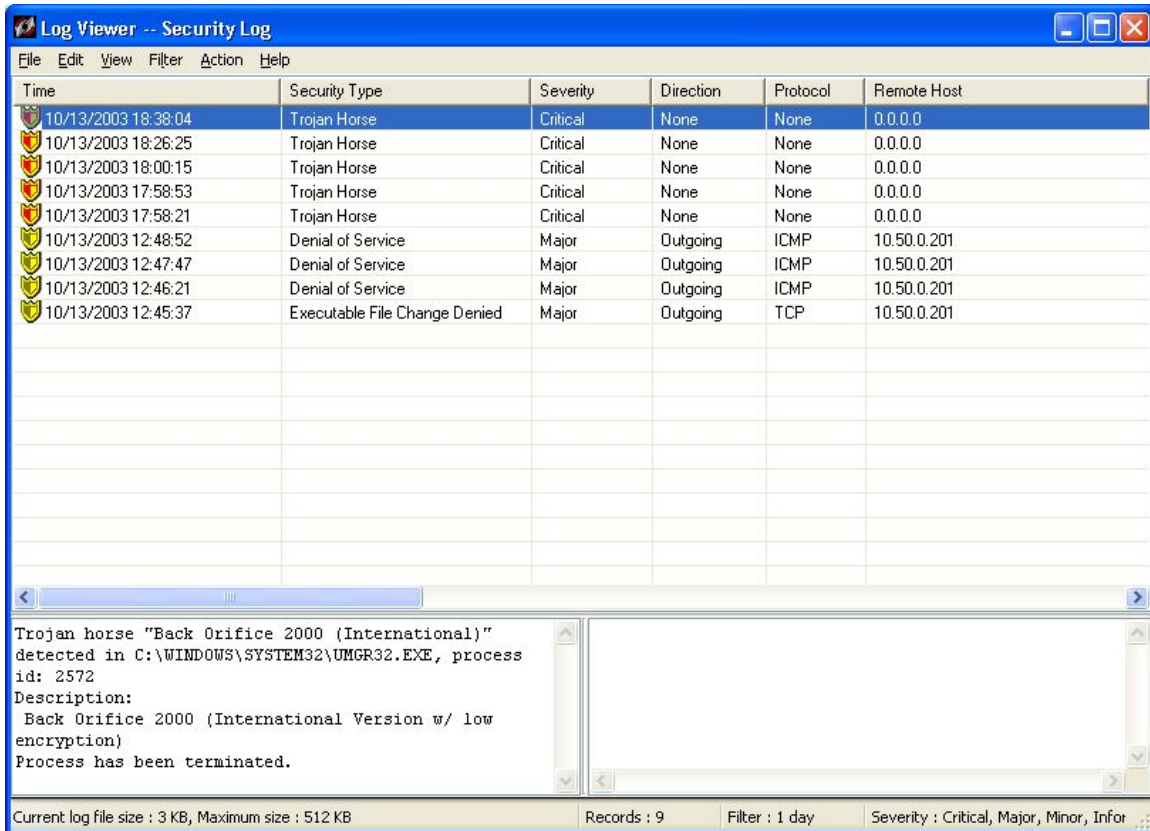
If the color of the arrow is...	...then...
<b>RED</b>	...traffic is being blocked by the Personal Firewall.
<b>BLUE</b>	...traffic is flowing uninterrupted by the Personal Firewall.
<b>GRAY</b>	...no traffic is flowing in that direction.

### Alert Mode—Flashing System Tray Icon

The System Tray Icon will sometimes flash on and off. This tells you that the Personal Firewall is in Alert Mode. Alert Mode occurs when the Personal Firewall records an attempted attack on your computer. To view the attack information, double-click on the icon. The Security Log will open, displaying new log entries.



The icon will stop flashing after you double-click it and view the Security Log. Note that opening the Security Log through the main console will not cause the System Tray Icon to stop flashing.



For information on reading a Security Log, start with the "Understanding Logs."

## Using the System Tray Icon

You can easily configure basic aspects of the Personal Firewall without even opening the main console. By right-clicking on the System Tray Icon, you can change your security level, view Help or log files, or even disable the Personal Firewall.

**Table 2. System Tray Icon**

Menu Option	What It will do for you...
<b>Sygate Personal Firewall</b>	Opens the Personal Firewall main console.
<b>Block All</b>	Blocks all network traffic.
<b>Normal</b>	Provides your pre-chosen list of security policies and applies them.
<b>Allow All</b>	Allows all network traffic. This setting should be used for troubleshooting only.
<b>Applications</b>	Opens the Applications List. For more on the Applications List, see “Setting Up Protection Based on Application.”
<b>Logs</b>	Opens the Firewall Logs. For more on Logs, start with “Monitoring Your System: Logs.”
<b>Options...</b>	Opens the Options dialog box, where you can make detailed choices about your security. For more information, see “Setting Up Protection by Configuration Changes.”
<b>Advanced Rules</b>	Opens the Advanced Rules dialog box, where you can write specific rules for <b>Allowing</b> or <b>Blocking</b> network access. For more information, see “Setting up Advanced Rules.”
<b>Hide System Tray Icon</b>	Removes the display of the System Tray icon for the Personal Firewall. The Personal Firewall is still running, but you no longer see the icon. To re-enable the icon, run the

**Table 2. System Tray Icon**


Menu Option	What It will do for you...
	Personal Firewall and choose the option to show it: From the Start menu, choose <b>Sygate Personal Firewall</b> . Then, from the <b>Tools</b> menu, toggle the <b>Hide System Tray Icon</b> to toggle the choice back on.
<b>Help Topics...</b>	Opens the online help system.
<b>About...</b>	Opens the About window, providing information on your installation of the Personal Firewall.
<b>Exit Sygate Personal Firewall</b>	Disables the Personal Firewall. ➡ <b>Option Alert:</b> This option may appear dimmed or not at all. For further information, see “Some Options May Not Show.”

You can roll your mouse over the System Tray Icon to see your current security level.

### ***What the System Tray Icon Tells You***

The table below illustrates the different appearances that the System Tray Icon may have, and what they mean.

**Table 3. What the System Tray Icon Tells You**

Icon	Meaning
	The Personal Firewall is in Alert Mode. This means that an attempted attack against your computer has been recorded in your Security Log. To make the icon stop flashing, double-click on the icon. The Security Log will open, displaying a new log entry.

**Table 3. What the System Tray Icon Tells You**

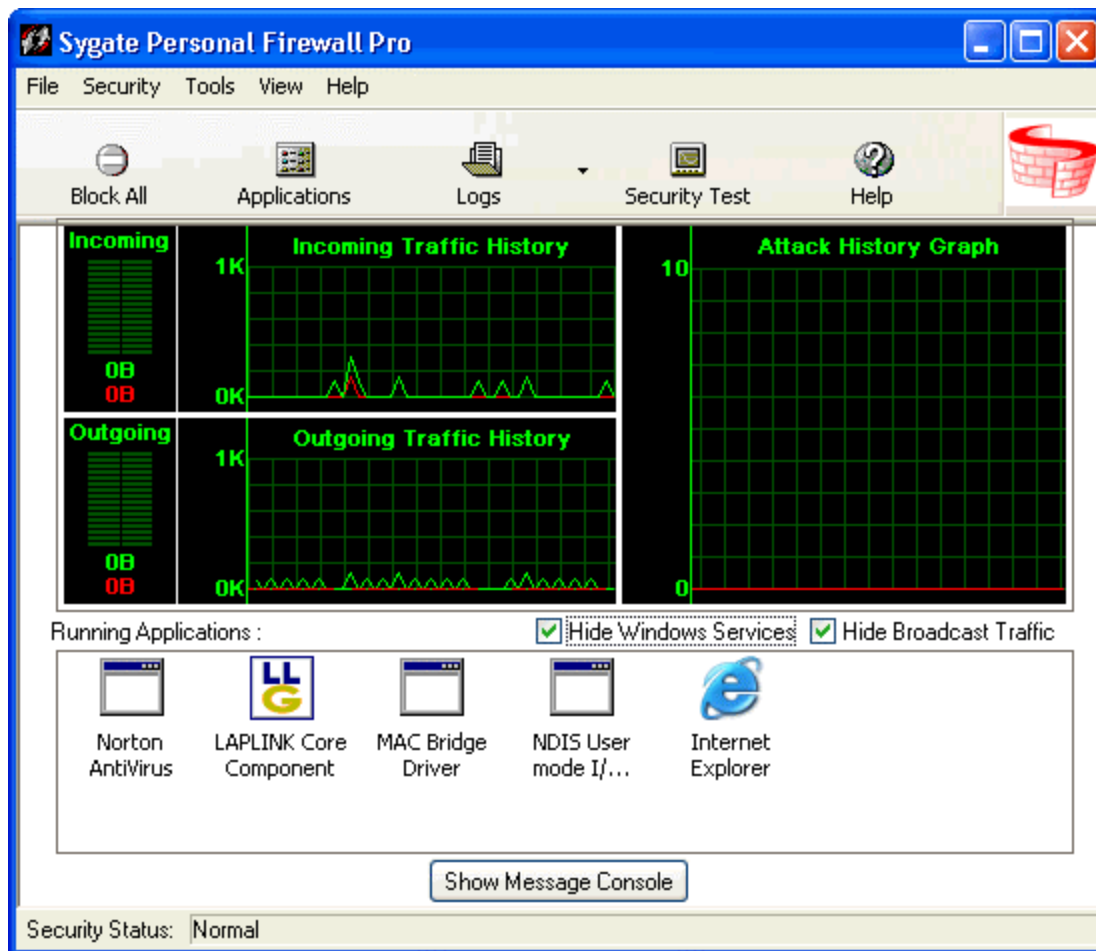
Icon	Meaning
	The Personal Firewall is in Allow All mode.
	The Personal Firewall is in Block All mode.
	Incoming traffic is flowing uninterrupted; there is no outgoing traffic.
	Both incoming and outgoing traffic are flowing uninterrupted.
	There is no incoming traffic; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; outgoing traffic is flowing uninterrupted.
	Incoming traffic is blocked; there is no outgoing traffic.
	Both incoming and outgoing traffic are blocked.
	There is no incoming traffic; outgoing traffic is blocked.
	Incoming traffic is flowing uninterrupted; outgoing traffic is blocked.
	No traffic is flowing in either direction.



## Using the Main Console

The Main Console for the Personal Firewall is available from your Start menu: click **Start | Programs | Sygate Personal Firewall Pro | Sygate Personal Firewall Pro**. The main console appears. You can also bring up the main console by clicking the System Tray Icon, as shown in the previous section.

The Personal Firewall interface is simple and intuitive. The main console (click to view image) provides real-time network traffic updates, online status, and links to logs, help files, and the Applications List.



The Personal Firewall interface is re-sizable, so you can view it as a full-screen or part-screen image.

## Menus and Toolbar

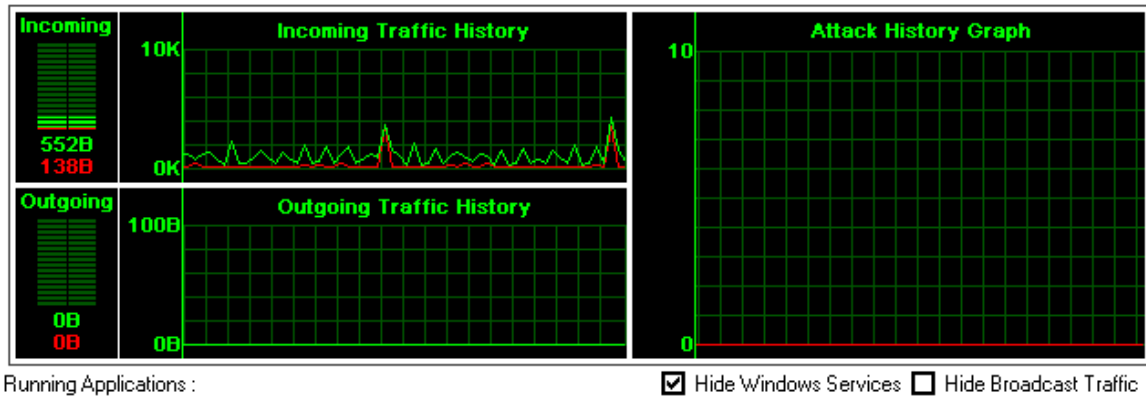
The top of the screen displays a standard menu.

## Toolbar Buttons

The buttons located below the menu items can be used to quickly access logs, view the Help file, or access the Applications List.

## Traffic History Graphs

One of most noticeable features of the Personal Firewall is the set of Traffic History graphs that are located below the toolbar on the main console.



The Traffic History graphs produce a real-time picture of the last two minutes of your traffic history. The graphs reload new information every second, providing instant data, as measured in bytes, about your incoming and outgoing network traffic.

The Traffic History graphs are broken into three sections. On the left side of the graphs section are the Incoming and Outgoing Traffic History graphs. These provide a visual assessment of the current traffic that is entering and leaving your computer through a network interface. This includes traffic that is allowed and traffic that is blocked. The green lines and bars indicate traffic that is allowed to pass through, and the red coloring indicates traffic that is being blocked by the Personal Firewall.

Additionally, the Attack History graph on the right side of the console provides information on attempted attacks against your machine.

### **Broadcast Traffic**

Broadcast traffic is network traffic that is sent to every computer in a particular subnet, and thus is not directed specifically to your computer. If you do not want to see this traffic, you can remove it from this graphical view by choosing to Hide Broadcast Traffic. You will then only see “unicast” traffic in this graph, which is traffic that directed specifically to your computer.

- Click **Hide Broadcast Traffic** below the Traffic History graphs to make this traffic no longer appear in the Traffic History graphs.

- Click **Hide Broadcast Traffic** to clear this setting, which causes broadcast traffic to appear.




## Running Applications Field

The Running Applications Field provides a list of all applications and system services that are currently running on your system. The display of application names can be changed through the View menu, or by right-clicking in the Running Applications field and selecting the desired view from the menu that appears.

You can also view the status of the applications. An application's "status" refers to the permissions that you allow it—whether it can access your Internet connection, if it can access that connection without asking you first, or if it is blocked from accessing the Internet or network altogether.

You can change the status of applications from the Running Applications field by right-clicking on an application's icon and selecting the desired status.

**Table 4. Running Applications Field**

Icon	Status	Description
	<b>Allow</b>	Icon appears normal, with no marks
	<b>Ask</b>	Icon appears with a small, yellow question mark
	<b>Block</b>	Icon appears with a red circle and cross-out mark

Additionally, application icons will display a small blue dot on lower left-hand or right-hand corner to indicate if it is receiving (left-hand) or sending (right-hand) traffic.

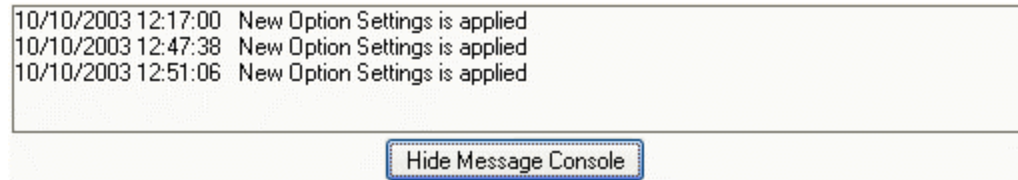


You can hide the display of system services by clicking **Hide Windows Services** above the Running Applications field. There are a number of services running at any given time, and since they are often crucial to the operation of your computer, you most likely want to allow them. You will see pop-ups that ask you if you want to allow these services to run. It is generally fine to allow them, and you can allow them permanently without worry. The Personal Firewall will block the services or applications if anything within the application's executable file changes. For instance, if you download a Trojan horse or an email virus that affects a service or application, the Personal Firewall will notice the difference and ask you if you want to allow it. If you have not made any changes to the service or application (such as

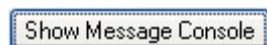
an upgrade), then you will want to block these applications from running and alert your system administrator. See “Understanding Pop-Up Messages” for details on pop-up messages.

## Message Console

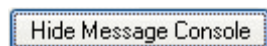
The Message Console of the Personal Firewall is located below the Running Applications field on the main console. It provides a real-time update of server-client communication, including profile downloads, Profile Serial Numbers, and server connection status.



The Message Console is, by default, hidden from view. To view the Message Console, click **Show Message Console** below the Running Applications field on the main console. The Message Console will appear.



To hide the Message Console from view, click **Hide Message Console**. The Message Console will collapse so that only the **Show Message Console** button is apparent.



## Status Bar

The Status Bar, located along the bottom of the Personal Firewall main console, provides the user with the current location profile information.



## Using the Menus and Toolbar

The top of the Personal Firewall screen displays a standard menu with the following options: **File**, **Security**, **Tools**, **View**, and **Help**.

**Table 5. Firewall Menus**

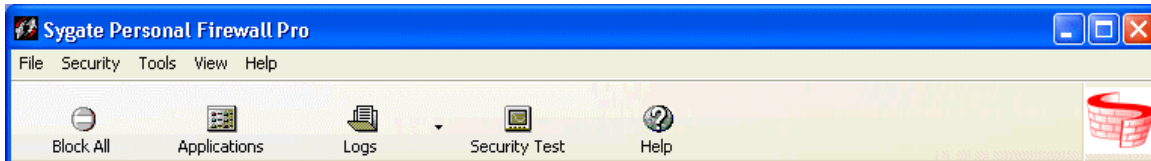
Menu	Menu choices
<b>File</b>	<ul style="list-style-type: none"> <li>• <b>Close</b>—Closes the Personal Firewall main console.</li> <li>• <b>Exit Personal Firewall</b>—Disables the Personal Firewall, effectively turning off security on your machine.</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>• <b>Block All</b>—Blocks all network traffic on your machine.</li> <li>• <b>Normal</b>—Blocks only selective traffic. This is the default configuration, and is a prudent choice.</li> <li>• <b>Allow All</b>—Permits all network traffic to flow on your machine. This is almost as non-secure as exiting the Personal Firewall, and is not recommended. It should be used for troubleshooting only.</li> </ul>
<b>Tools</b>	<ul style="list-style-type: none"> <li>• <b>Applications</b>—Opens the Applications List.</li> <li>• <b>Logs</b>—Opens the Logs.</li> <li>• <b>Options</b>—Opens the Options dialog box, which contains many security options, including email alerts, Network Neighborhood browsing rights, and log file configuration.</li> <li>• <b>Advanced Rules</b>—Opens the Advanced Rules dialog box, where you can set very specific rules for the implementation of security on your Personal Firewall.</li> <li>• <b>Update Signature</b>—Updates intrusion prevention signatures.</li> <li>• <b>Automatically Start Service</b>—This toggle setting sets whether the Personal Firewall will be launched automatically when your machine is booted.</li> <li>• <b>Hide System Tray Icon</b>—This toggle setting hides the System Tray Icon from view. If it is checked, the icon is hidden.</li> <li>• <b>Test Your Firewall</b>—Opens the Sygate Technologies scan site, allowing you to test the effectiveness of the Personal Firewall.</li> </ul>

**Table 5. Firewall Menus**

Menu	Menu choices
	<p>The View menu gives users the option to alter the display of software programs in the “Running Applications” field:</p> <p>These programs are applications that are currently accessing or attempting to access the network connection.</p> <ul style="list-style-type: none"> <li>• <b>Large Icons</b>—Displays 32x32 icons in the field. Each icon represents a software application or a system service.</li> <li>• <b>Small Icons</b>—Displays 16x16 icons.</li> </ul> <p>Both the large and small icon displays provide the full name of the application below the icon itself, and the icons are displayed in a “corkboard” fashion.</p>
<b>View</b>	<ul style="list-style-type: none"> <li>• <b>List</b>—Provides small icon representations, with the icons displayed in a standard list.</li> <li>• <b>Applications Details</b>—Provides not only a list of all running applications, but also useful information on the version number and location path of each application.</li> <li>• <b>Connection Details</b>—Provides further information on the type of connection being made by an each application accessing the network adapter, as well as the protocol, local and remote ports and IP addresses being used, the application path, and more.</li> <li>• <b>Hide Windows Services</b>—Toggles the display of Windows Services in the “Running Applications” field.</li> <li>• <b>Hide Broadcast Traffic</b>—Toggles the display of broadcast traffic in the “Running Applications” field.</li> </ul>
<b>Help</b>	<ul style="list-style-type: none"> <li>• <b>Managed Personal Firewall</b>—Links to the Sygate Technologies Web site to show the corporate version of the Firewall, Sygate Security Agent.</li> <li>• <b>Easy Internet Sharing</b>—Links to the Sygate Technologies Web site to show Sygate’s Home Networking product line</li> <li>• <b>Register...</b>—Brings up a registration screen so that you can register your copy of the Firewall</li> <li>• <b>Help Topics...</b>—Opens the Personal Firewall online help files.</li> <li>• <b>About</b>—Opens the About screen.</li> </ul>

## Toolbar Buttons

The buttons located below the menu provide shortcuts that can be used to quickly block all applications, change your application profiles, access the logs, test your Personal Firewall using the Sygate Technologies Web site, or view the Help file.



## Understanding Pop-Up Messages

This section goes over the range of Personal Firewall pop-up messages that may appear, including security notifications and warning messages, and describes how the Personal Firewall responds to potential problems.

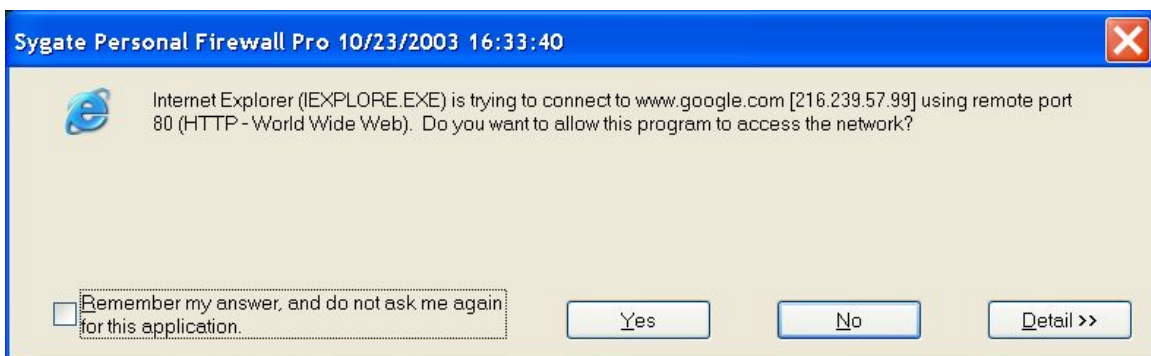
### Why Did I Get a Pop-Up Message?

An application-related pop-up message will occur for one of the following reasons:

1. An application that the Personal Firewall has never seen before, or that has been assigned the status of “Ask” is trying to access your network connection.
2. An application that normally accesses your network connection has changed, possibly because of a product upgrade.
3. Your computer has received a data packet that is not associated with any particular application.
4. The Personal Firewall has detected a Trojan horse on your computer.

### ***New Application Pop-up***

You may occasionally see the following pop-up message on your computer screen.



### ***What Does This Mean?***

The information on the pop-up tells you that Internet Explorer application is trying to access your network connection. Internet Explorer is trying to load [www.google.com](http://www.google.com), which has an IP address of 216.239.39.99. The server that powers that site is using server port 80.

This pop-up appeared because Internet Explorer has been opened, either directly by you, indirectly by you, or by another application.

You might have tried to open Internet Explorer. If so, either this is the first time that you have done so since you installed the Personal Firewall, or you have assigned Internet Explorer a status of “Ask”, meaning that every time Internet Explorer tries to access your network connection, the Personal Firewall will ask you to grant it access (for more information on status, see “Reviewing and Changing the Permission Status of an Application”).

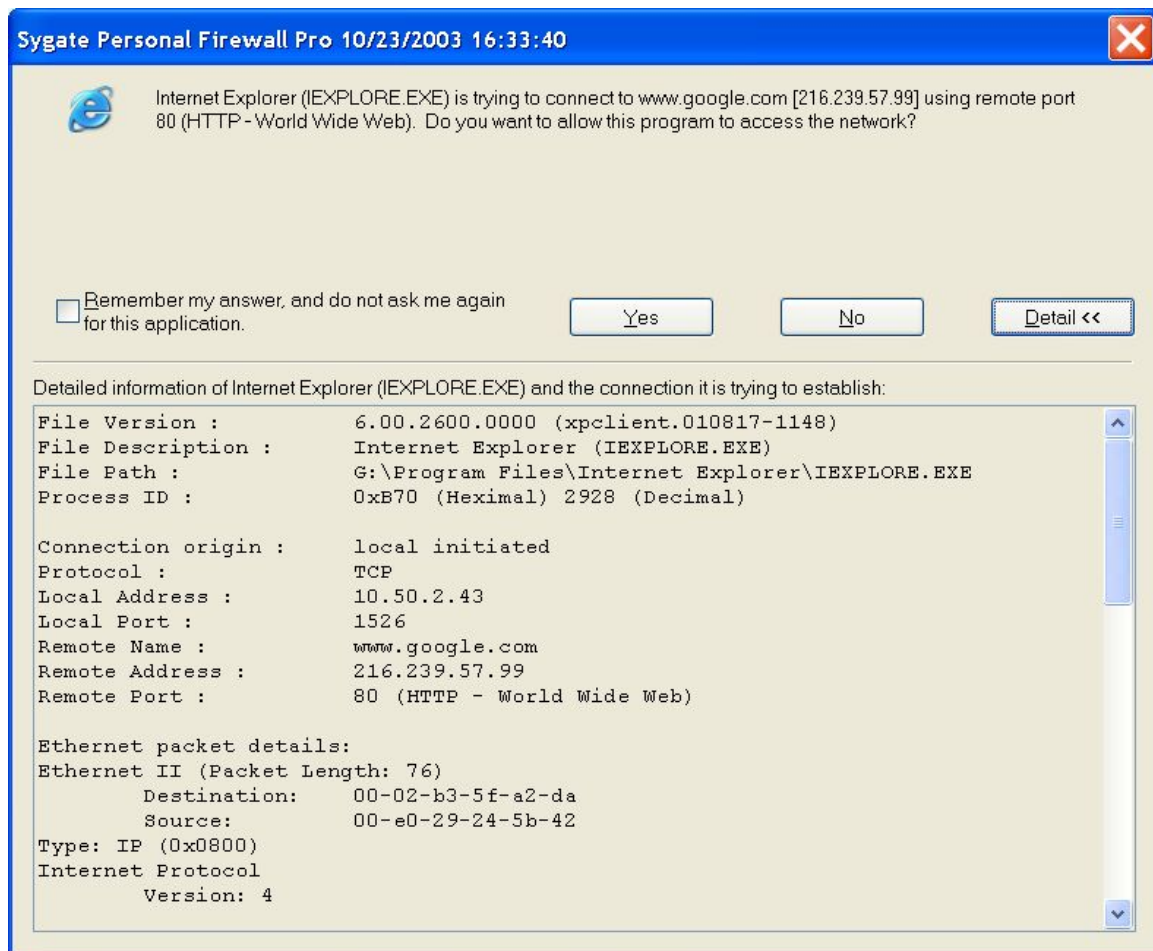
What if you did not directly try to open Internet Explorer? Perhaps you clicked on a link to a web site in an email. In such a case, it is probably safe to click **Yes** and allow Internet Explorer to access the network.

What if you didn’t open any program or click on any link, and a program suddenly tries to access your network connection? Again, there could be a number of different reasons. However, if you haven’t opened any programs that use the application listed on the pop-up message, or can’t see any reason why that application should try to access your network connection, it is always safest to click **No**. This might indicate the presence of a Trojan horse on your computer, something that needs to be checked immediately.



## Detail

Clicking the Detail button expands the pop-up box, providing further details on the connection the application is attempting to establish. Information such as the file name, version, and path are provided. Look at these items to make sure that they match the description of the application that you normally use. The details section should also indicate the location to which the file was attempting to connect: either local (meaning that it was trying to connect to your computer), or remote (meaning that the application was attempting to connect to an outside destination). Additionally, the local and remote port numbers and IP addresses should be provided, as shown in the following illustration:



## What Should I Do?

This kind of message is common when you first start using the Personal Firewall. In this particular example, Internet Explorer is trying to access the [www.google.com](http://www.google.com) web site at the remote port 80. Most servers use port 80 to send and receive information on the Internet, so this isn't anything unusual.

If you believe that you have triggered this application, it would be safe to click **Yes**. You have the option to tell the Personal Firewall to remember your answer in the future. If you click **Remember my answer, and do not ask me again for this application**, the Personal Firewall will remember your choice, and will act accordingly the next time this application tries to access your network connection.

If you have tried to open an application (such as a web browser) or a program that uses another application to access the Internet (such as a media streaming program) and you feel comfortable granting this application access to your network connection, then you can click **Yes**. The application will then be able to access your network. You can change the status of the application at any time, either in the Running Applications field or in the Applications List.

However, if a pop-up message is unexpected, and you can't see any reason why the listed application should try to access your network connection, click **No**, and click **Remember my answer....** This will assign the application the status of Block, so that it will be automatically blocked from your network connection any time it tries to gain access. You can change the status of the application at any time, either in the Running Applications field or in the Applications List.

You should also run a virus scan to make sure that you have not inadvertently downloaded a virus or a Trojan horse that could infect your computer files.

**Table 6. Pop-up: Remember My Answer?**

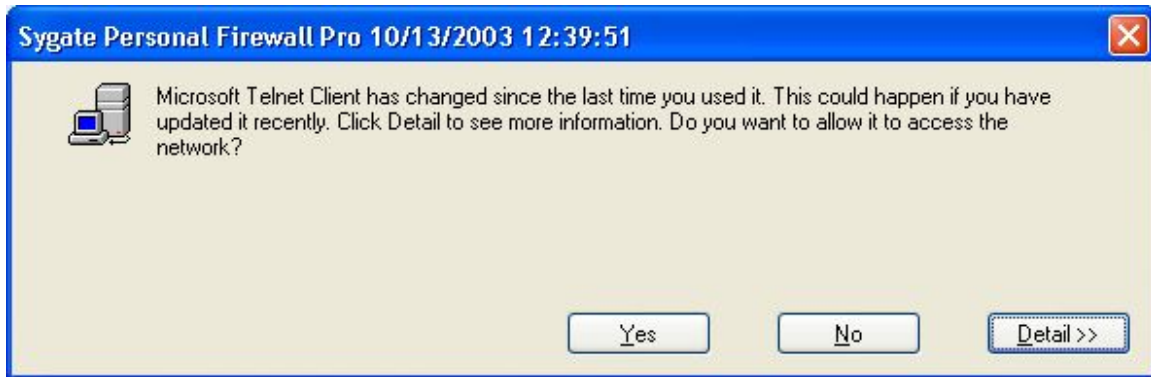
Click	Check "Remember my answer..." box?	Status Assigned
Yes	Yes	Allow
Yes	No	Ask
No	Yes	Block
No	No	Ask

### ***I Changed My Mind***

What if you change your mind about an application after you have allowed it or blocked it? Simply go to the main console of the Personal Firewall, right click on the application's icon in the Running Applications field, and click the desired status (**Allow**, **Ask**, or **Block**) from the menu that appears.

### ***Changed Application Pop-up***

Occasionally, you might see a pop-up such as the one pictured below.



### ***What Does This Mean?***

The application listed on the pop-up message is trying to access your network connection. Although the Personal Firewall recognizes the name of the application, something about the application has changed since the last time the Personal Firewall encountered it.

This could be because you have upgraded the product recently. The Personal Firewall uses an MD5 checksum to determine the legitimacy of an application. An upgraded version might not pass the checksum test, since a new build or new version of the application is likely to have a different checksum value.

On the other hand, if you have not recently upgraded the application, and see no reason why this message should appear, this could be an instance of a Trojan horse trying to access your network.

### ***Detail***

Clicking the Detail button expands the pop-up box, providing further details on the connection the application is attempting to establish. Information such as the file name, version, and path are provided. Look at these items to make sure that they match the description of the application that you normally use. The details section should also indicate the location to which the file was attempting to connect: either local (meaning that it was trying to connect to your computer), or remote (meaning that the application was attempting to connect to an outside destination). Additionally, the local and remote port numbers and IP addresses should be provided.

### ***What Should I Do?***

If you have recently upgraded the application mentioned on the pop-up message, it is probably safe to click **Yes** and allow the application network access. However, if you do not

think that you have recently upgraded the listed application, you should click **No** and run an antivirus software program or, if you are at work, contact your IT department.

### ***I Changed My Mind***

What if you change your mind about an application after you have allowed it or blocked it? Simply go to the main console of the Personal Firewall, right click on the application's icon in the Running Applications field, and click the desired status (**Allow**, **Ask**, or **Block**) from the menu that appears.

### ***Trojan Horse Warning***

Hopefully, you will never see a pop-up message like the following:



### ***What Does This Mean?***

This message indicates that the Personal Firewall has detected a known Trojan horse on your computer. It also explains that the Trojan horse has been blocked from accessing your network.

This means that a Trojan Horse is present on your system and has been activated. Either you tried to open the program identified as a Trojan horse, or it has been triggered by another program on your computer. It is possible that the Trojan was on your computer when you installed the Personal Firewall, or that you have recently downloaded it through a legitimate application, such as a web browser. The Trojan tried to access your network connection, and has been blocked by the Personal Firewall.

### ***What Should I Do?***

You should immediately notify your IT department. The Personal Firewall will block the Trojan from sending any information out of or into your computer, but it is still important to remove it from your system as soon as possible. The Personal Firewall will terminate the Trojan process automatically, but removal will require the assistance of your IT department.

## Why Did I get a Security Notification?

Security notifications are designed to let you know the status of your security. You will see a security notification for one of two reasons:

- **Blocked Application Notification:** An application that has been launched from your machine has been blocked in accordance with rules that you have set.
- **Security Alert Notification:** There has been an attack launched against your machine, and this notification will either simply inform you of the situation or provide instructions on how to deal with it.

### Blocked Application Notification

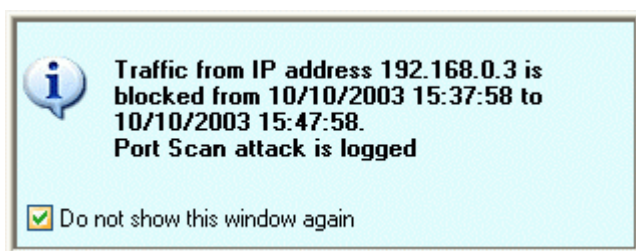
You may see notification messages above your system tray icon from time to time. They indicate that your system has blocked traffic that you have specified as not trusted. Please note that if you are operating under Block All mode, you will see these messages quite often. On the other hand, if you are operating in Allow All mode, you won't see any notifications at all.



If these notifications start annoying you, you can either click **Do not show this window again**, or you can disable these messages altogether in the **Options** window, under the **General** Tab.

### Security Alert Notification

You may see notification messages above your system tray icon from time to time. There are two types of notification messages. The notification pictured below indicates that the Personal Firewall has logged an attack.



If you do not want to see these notifications, you can either click **Do not show this window again**, or you can disable these messages altogether in the **Options** window, under the **General** Tab.

## Chapter 6. Setting Up Protection Based on Application

This chapter describes the various ways in which you can protect your system using the Personal Firewall, beginning with the individual applications that you have running on your system. You can set the permission status of an application, and you can change it later on. See below for setting an application's status, and see "Reviewing and Changing the Permission Status of an Application" for information on changing it later on.

### How to Set Permissions by Application

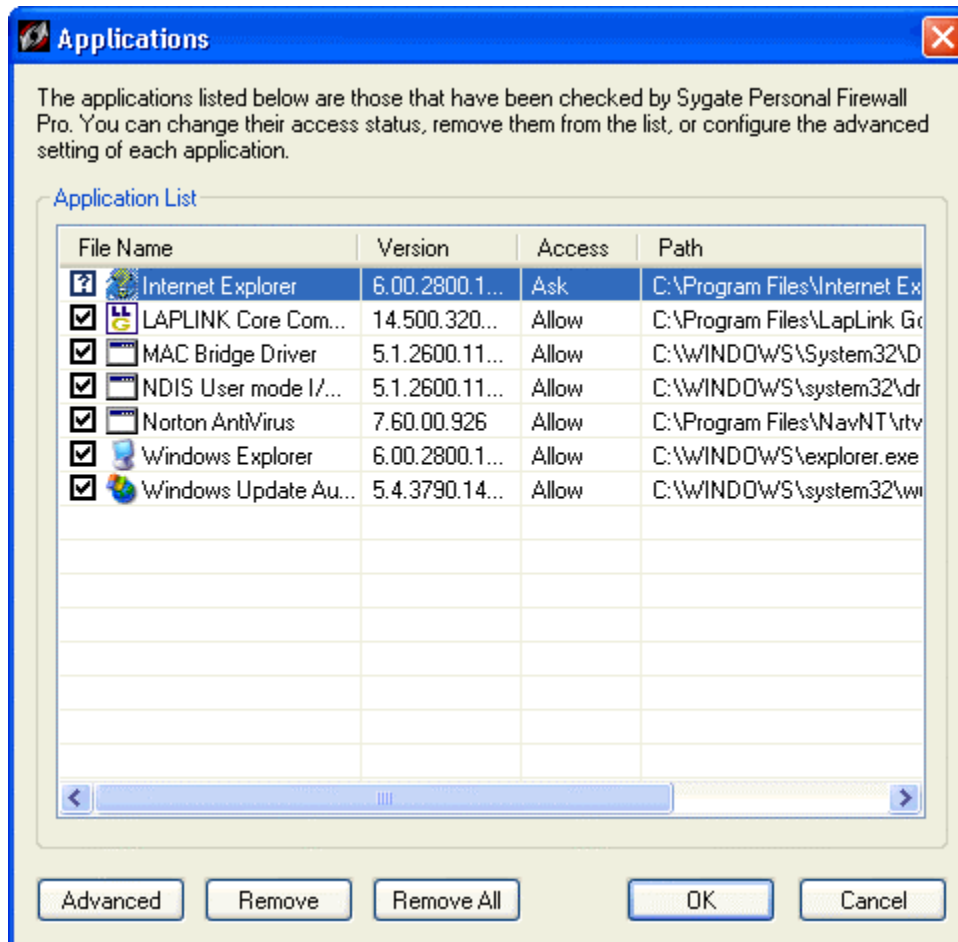
To set the permissions (**Allow** / **Block** / **Ask**) for your applications one by one, you approach through the Applications List. You can access the Applications List by clicking the **Applications** icon on the toolbar, or by selecting **Applications** under the **Tools** menu.

The Applications List shows all applications and services that have asked you for permission to access your network connection since the installation of the Personal Firewall. The application/service name, version, status, and path are provided in a simple screen.

Like the Running Applications field, you can change the display view for the applications and services shown in the Applications List. To change the view, right-click anywhere in the Applications List. Select **View** from the list of options, and then select the desired view. The different views are explained in the section covering the Main Console. For details, see "Using the Main Console for the Personal Firewall."

To select an application or service for configuration, click on any of its attributes as shown in the Applications List. The application or service name must be highlighted before you can change or configure its status. See "Setting up Advanced Rules" for information on security settings options.

The buttons at the bottom of the Applications List screen provide the option to remove selected or all applications from the list. Once an application/service is removed from the Applications List, its status is erased. When that application/service attempts to connect to the network again, you will be notified through a new application pop-up message (see “New Application Pop-up”), and be asked to assign a new status to the application/service.



## Advanced Application Configuration

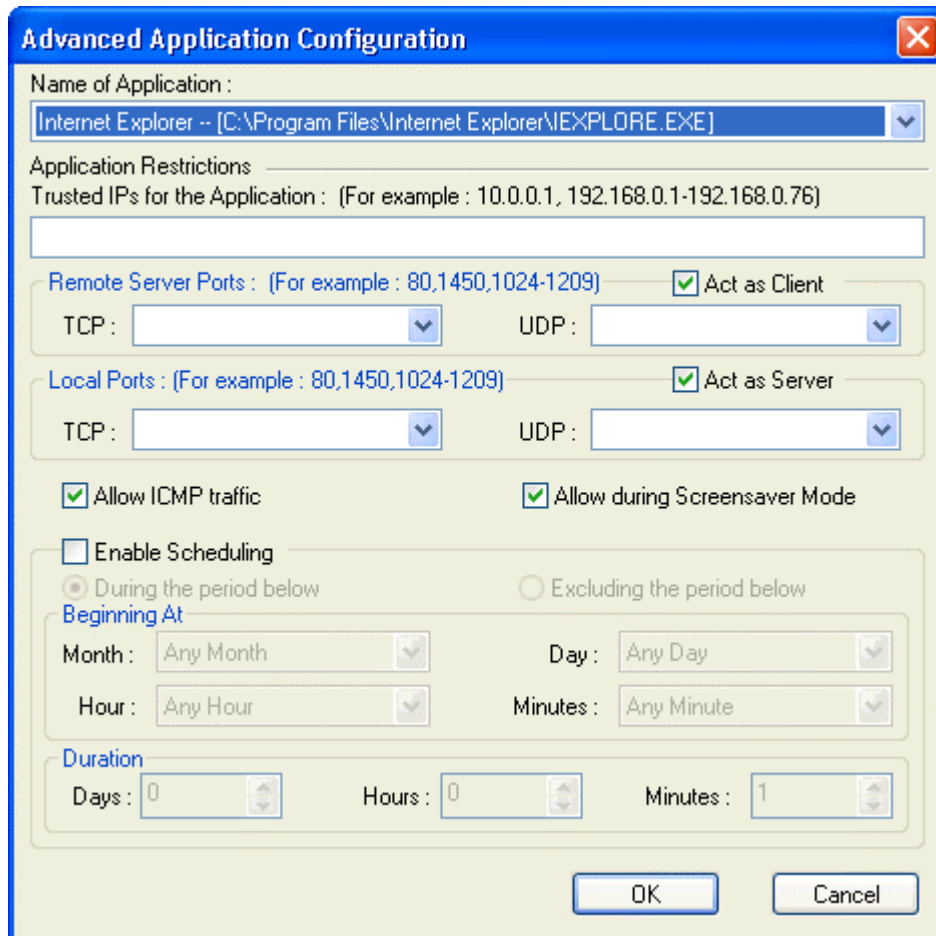
You can configure advanced security settings for each application on your application list by setting certain restrictions on which IP addresses and ports an application can utilize. Only users who have a firm grasp on computer ports and application protocols should use the advanced configuration options, lest unintended results occur.

## To Set Advanced Configuration

1. Open the Applications List by clicking on the Applications icon on the Personal Firewall main console, or by right-clicking the System Tray Icon and selecting **Applications** from the list of choices.
2. Click the **Advanced** button at the bottom left corner of the Applications List screen.



3. The Advanced Application Configuration window opens.



4. Make sure that the correct application is selected in the Name of Application list box.
5. Decide if the application should be allowed network access during Screensaver Mode. Click **Allow during Screensaver Mode** to allow. Click to clear this choice, and thus to block the selected application during Screensaver Mode.
6. Enter trusted IPs or IP ranges in the Trusted IPs for the Application text box.

You must enter a valid IP address range. The following IP address ranges are not valid choices:

0.0.0.0  
255.255.255.255  
127.X.X.X

7. Enter the ports or ranges of ports that can be utilized for this application.

8. Click **OK** if you want the application restrictions to be in effect at all times. If you wish to set a time limit or schedule specific periods when the restrictions will be in effect, see “To Enable Scheduling” below.

## To Enable Scheduling

You can also set times for which the advanced configurations take effect. This scheduling lets you set up the application restrictions to be in effect either *during* a specific time period, or *excluding* a specific time period, using the list boxes on this screen.

1. Click **Enable Scheduling** below the Ports section on the Advanced Application Configuration screen.
2. Click either **During the period below** or **Excluding the period below**.
3. Select a Beginning Month, Day, Hour, and Minutes from the appropriate list boxes.
4. Enter a duration in units of Days, Hours, and/or Minutes.
5. Click **OK** to set scheduling restrictions.

## Reviewing and Changing the Permission Status of an Application

Depending on the type of control that the Personal Firewall is under, you may or may not be able to change an application’s access status.

- What is access status?
- How do I change an application’s access status?

### What is Access Status?

*Access Status* is a set of rules that governs how many rights an application has in terms of having access your network connection or modem. Depending on what status is assigned to an application (or service) and how much configuration you apply to it, an application can either gain access to your network any time, under certain conditions, with your permission, or be blocked from gaining access to the network altogether.

The Personal Firewall provides the following type of access status:

- Allow

An application with a status of Allow is permitted to have access to network connections. Under the Allow status, an application (or service) can be configured so that it can only access the network if using a certain port, or during certain hours.

- Ask

When a new application attempts to access your network connection while you are under the default security setting (Normal), the Personal Firewall displays a pop-up window to ask if you want to allow the application to have access to the network because the application has a default access status of Ask. If you have not allowed or blocked an application, the Personal Firewall prompts you every time it tries to gain access to the network or modem.

- Block

An application with a status of **Block** is denied access to the network.

You have several choices when the application pop-up message is displayed as shown in the following table.

**Table 7. Firewall Application Access Status**

If you click	If you check “Remember my answer...” box?	Your Personal Firewall will...
<b>Yes</b>	<b>Yes</b>	Allow the application.
<b>Yes</b>	<b>No</b>	Ask you if you want to allow the application.
<b>No</b>	<b>Yes</b>	Block the application.
<b>No</b>	<b>No</b>	Block the application this time, and in the future ask you if you want to allow the application.

If you select:

- **Yes** and tell the Personal Firewall to remember your answer, you are no longer prompted. This application is allowed to have access to the network until you change its access status. The application now has a status of **Allow**.
- **Yes** but do not elect to have the Personal Firewall remember your answer, then every time this application attempts to gain access to the network, you are asked each time whether or not the application is allowed or denied access. This application now has a status of **Ask**.
- **No** and tell the Personal Firewall to remember your answer, you are no longer prompted. This application is systematically denied access to the network unless you change its access status. This application now has a status of **Block**.

- **No** but do not elect to have the Personal Firewall remember your answer, then every time this application attempts to gain access to the network, you are asked each time whether or not the application is allowed or denied access. This application now has a status of **Ask**.

If you change your mind about the access status of an application, you can change its status from the Applications List.

### To Change the Status of an Application

1. Open the Applications List.
2. Click on the File Name of the appropriate application until the row is highlighted.
3. Right-click on the highlighted row.
4. Click the appropriate access status (**Allow**, **Ask**, or **Block**) from the list.
5. Click **OK** to close the Applications List.

## Chapter 7. Setting Up Protection by Configuration Changes

This chapter provides details how to protect your system by making changes in the Firewall's configuration options. This is where the most complex security policies can be crafted.

### How to Change Configuration Options

The **Options** selection of the **Tools** menu offers several settings for the Personal Firewall, including e-mail notification of attacks, screen saver mode, log file configuration, and Network Neighborhood options.

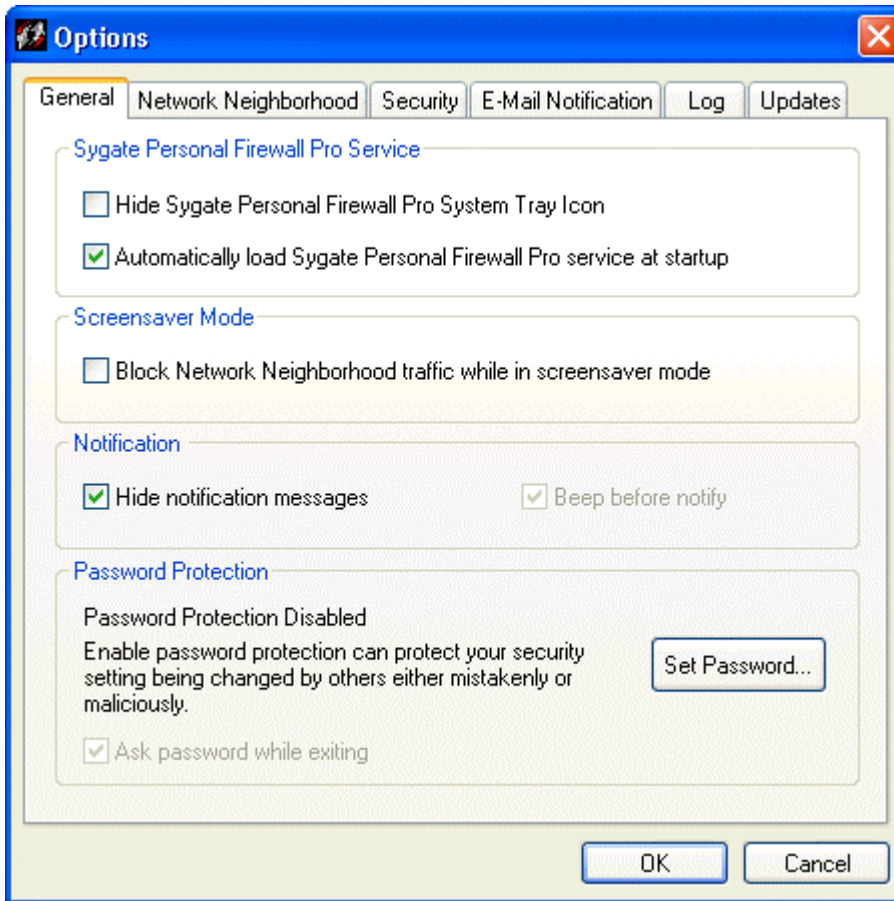
You can open the **Options...** window either from the **Tools** menu at the top of the main console, or by right-clicking the System Tray Icon and selecting **Options...** from the menu that appears. The **Options** window consists of the following tabs:

- **General** tab (see “Review of General Configuration Options”)
- **Network Neighborhood** tab (see “Sharing Files and Folders”)
- **Security** tab (see “Setting Detailed Security Options”)
- **E-Mail Notification** tab (see “Setting Up Email Notification of Security Events”)
- **Log** tab (see “Logging Security Events on Your System”)
- **Updates** tab (see “Updating Your Security”)

The **OK** and **Cancel** buttons are located at the bottom of every tab in the **Options** window. The **OK** button applies any changes that you have made in the **Options** window, and then closes the window. Clicking the **Cancel** button ignores any changes you may have made in the **Options** window, and closes the window while retaining the previous settings.

## Review of General Configuration Options

The broadest level of configuration options for protecting your Personal Firewall appears on the **General** tab. This tab provides access to options for the basic running of the Personal Firewall.



Two buttons appear at the bottom of the Options window, and can be accessed from each tab.

- Clicking the **OK** button applies any changes that you have made in the **Options** window, and then closes the window.
- Clicking the **Cancel** button ignores any changes you may have made in the **Options** window, and closes the window while retaining the previous settings.

### System Tray Icon

Checking this box will hide the System Tray Icon from view, or if it is hidden, will show the System Tray Icon. For details on the System Tray icon, see “Shortcut to the Software: the System Tray Icon.”

## **Sygate Personal Firewall Service**

Click this box to automatically launch the Personal Firewall at start-up.

## **Screensaver Mode**

Enabling the Screensaver Mode option automatically sets your security level to **Block All** when your computer's screensaver is activated. As soon as the computer is used again, the security level will return to the previously assigned level.

## **Hide Notification Messages**

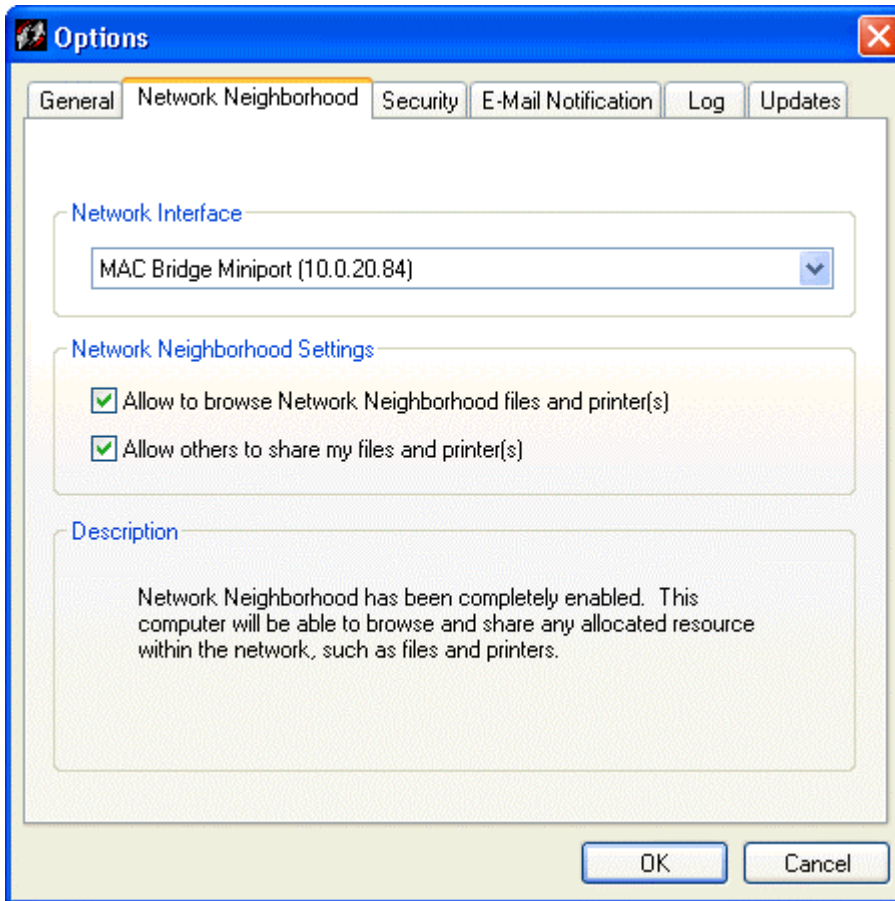
You can enable or disable the system tray notification messages by clicking [here](#). Additionally, you may select to allow audio announcement of the notification window.

## **Password Protection**

Enabling Password Protection will protect your settings from being changed by another user. Password Protection will prompt you to enter your password every time you access the Personal Firewall main console. For details, see "Password Protecting Your Security Settings"

## Sharing Files and Folders

The **Network Neighborhood** tab provides *multiple interface support* and network browsing rights configuration. The Network Neighborhood tab is made up of three sections: **Network Interface**, **Network Neighborhood Settings**, and **Description**.



The settings in the **Network Neighborhood** section apply to the network displayed in the **Network Interface** list box.

### Network Neighborhood Settings

1. Select the network from the **Network Interface** list box.
2. Decide if you wish to browse other computers on the network and if you wish to allow other users on the selected network to browse your computer. Under the **Network Neighborhood Settings** section, select the appropriate check boxes:
  - Select the **Allow to browse Network Neighborhood files and printer(s)** option to browse other files and printers on the selected network. This allows you to access other files on your network. If you disable this, you cannot copy files from network locations.

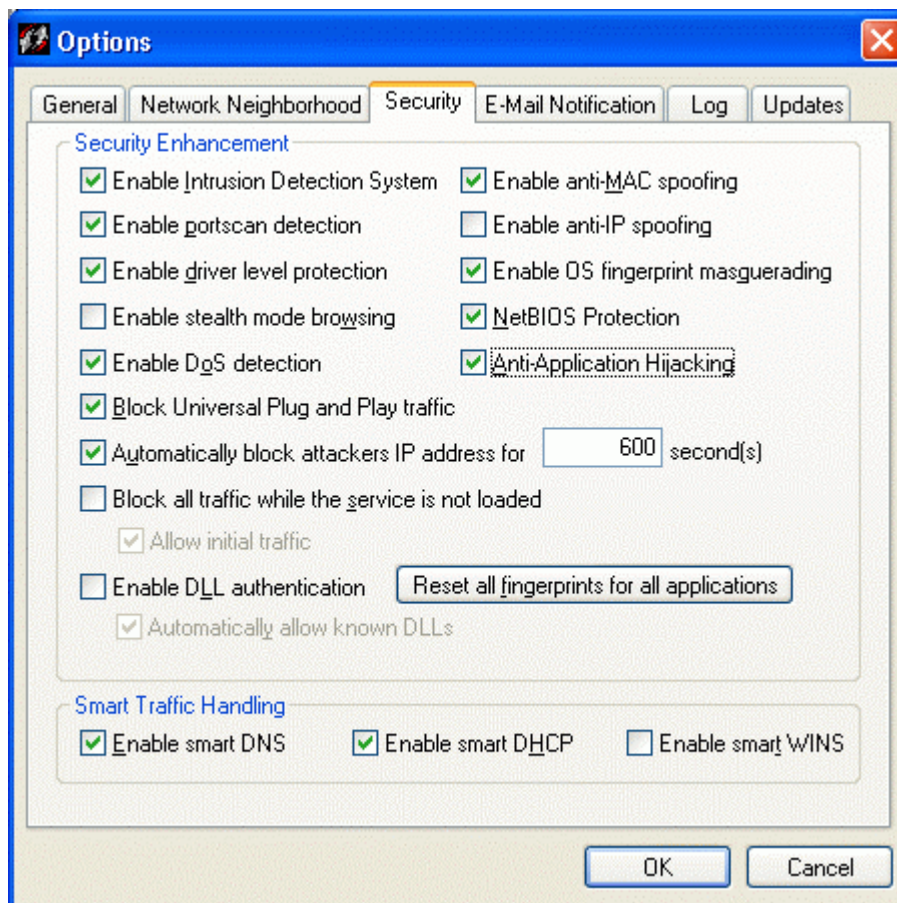


- Select the **Allow others to share my files and printer(s)** to allow other users of the selected network to browse your files and printer(s).

3. Click **OK**.

## Setting Detailed Security Options

The **Security** tab offers a way to enable and disable some of the more complex security options. As such, this tab provides both power and complexity. You should test settings made here before propagating them to other computers, to make certain that they work as you intend.



### Enable Intrusion Detection System

By default, this option is enabled in the Personal Firewall. This feature provides you with alerts when another user attempts to compromise your system. Intrusion detection on the Firewall actually enables a combination of both an intrusion detection system (IDS) and an intrusion prevention system (IPS). The end result is a system that analyzes network packets and compares them with both known attacks and known patterns of attack, and then blocks those attacks. One of the key capabilities of the Intrusion Prevention System is its capability to do deep packet Inspection. More details appear here.

## About Sygate's Intrusion Detection and Prevention System

Sygate's Intrusion Detection (SID) detects inappropriate and incorrect activity. It is a host-based Intrusion Detection system that operates on every computer on which the Firewall is installed. In addition, Sygate's Intrusion Detection works in conjunction with Sygate's Intrusion Prevention (SIP). As soon as a known attack is detected, it can be automatically blocked by one or several of Sygate's Intrusion Detection and Prevention systems, also commonly referred to as Intrusion Prevention Systems (IPS).

Sygate supports the following Intrusion Detection and Prevention systems:

**Port Scan Intrusion Detection and Prevention**—Sygate's Port Scan Intrusion Detection and Prevention system detects port scans. Although it can be a precursor to an intrusion attempt, it does not in itself allow access to a remote system. Whenever a port scan is detected, the port scan Intrusion Detection and Prevention system does not automatically block ports. Port Scan Detection is automatically enabled.

**Trojan Intrusion Detection and Prevention**—Sygate's Trojan Intrusion Detection and Prevention system automatically terminates known Trojan Horse programs before the Trojan Horse attempts to communicate.

**Signature-Based Intrusion Detection and Prevention**—Sygate's Signature-Based Intrusion Detection and Prevention system identifies known attacks by using a technique called pattern matching. For example, Sygate's pattern matching Intrusion Detection and Prevention system can watch web servers that can be programmed to look for the string `phf` in `GET /cgi-bin/phf?` as an indicator of a CGI program attack. Each packet is evaluated for a specific pattern, such as a string in a single packet. If a match occurs, the attack is blocked.

**Denial of Service Intrusion Detection and Prevention**—Sygate's Denial of Service (DoS) Intrusion Detection and Prevention system identifies attacks in which users or organizations are deprived of the services or a resource that they would normally expect to have available. It identifies known attacks based on multiple packets regardless of port number or type of Internet Protocol (IP), which is a limitation of signature-based Intrusion Detection and Prevention systems. Sygate's DoS Intrusion Detection and Prevention system is automatically enabled when you install the product.

## Enable anti-MAC spoofing

By default, this option is enabled on the Personal Firewall. Some hackers use MAC spoofing to attempt to hijack a communication session between two computers in order to hack one of the machines. MAC (media access control) addresses are hardware addresses that identify computers, servers, routers, etc. When Computer A wishes to communicate with Computer B, it may send an ARP (Address Resolution Protocol) packet to the computer.

The anti-MAC spoofing feature allows incoming and outgoing ARP traffic only if an ARP request was made to that specific host. It blocks all other unexpected ARP traffic and logs it in the security log.

### **Enable port scan detection**

By default, this option is enabled on the Personal Firewall. Port scanning is a popular method that hackers use to determine which of your computer's ports are open to communication. Ports are dynamically blocked by the Personal Firewall and are therefore protected from hacking attempts. This feature detects if someone is scanning your ports, and notifies you. If disabled, the Personal Firewall does not detect scans or notify you of them, but still protects your ports from hacking attempts.

### **Enable anti-IP spoofing**

By default, this option is disabled on the Personal Firewall. IP spoofing is a process used by hackers to hijack a communication session between two computers, which we will call Computers A and B. A hacker can send a data packet that causes Computer A to drop the communication. Then, pretending to be Computer A, the hacker can communicate with Computer B, thus hijacking a communication session and attempting to attack Computer B.

Anti-IP spoofing foils most IP spoofing attempts by randomizing the sequence numbers of each communication packet, preventing a hacker from anticipating a packet and intercepting it. It is recommended that you enable this option along with Enable OS fingerprint masquerading.

### **Enable driver-level protection**

By default, this option is already enabled on the Personal Firewall. This feature, when enabled, blocks protocol drivers from accessing the network unless the user gives permission. If a protocol driver attempts to access the network, you will see a pop-up message asking if you want to allow it.

### **Enable OS fingerprint masquerading**

By default, this option is enabled on the Personal Firewall. This option keeps programs from detecting the operating system of a computer running the Personal Firewall software. When OS Fingerprint Masquerading is enabled, the Personal Firewall modifies TCP/IP packets so it is not possible to determine its operating system. It is recommended that you enable this option along with **Enable anti-IP spoofing**.

### **Enable stealth mode browsing**

By default, this option is disabled on the Personal Firewall. *Stealth mode* is a term used to describe a computer that is hidden from web servers while on a network. A computer on the Internet, for instance, if in stealth mode, cannot be detected by port scans or communication attempts, such as **ping**.

## **NetBIOS protection**

By default, this option is enabled on the Personal Firewall. This option blocks all communication from computers located outside the Personal Firewall's local subnet range. NetBIOS traffic is blocked on UDP ports 88, 137, and 138 and TCP ports 135, 139, 445, and 1026. Be aware that this can cause a problem with Outlook if connecting to an Exchange server that is on a different subnet. If that occurs, you should create an advanced rule specifically allowing access to that server. For further information, see "Setting up Advanced Rules."

## **Enable DoS protection**

By default, this option is enabled on the Personal Firewall. This option causes the Personal Firewall to check incoming traffic for known Denial of Service (DoS) attack patterns. DoS attacks are characterized by an explicit attempt by an intruder to prevent legitimate users of a service from using that service.

## **Anti-Application Hijacking**

By default, this option is enabled on the Personal Firewall. This option causes the Personal Firewall to check for malicious applications that work by interjecting DLLs and Windows hooks into Windows applications, and to block those malicious applications when found.

## **Block Universal Plug and Play (UPnP) Traffic**

By default, this option is enabled in the Personal Firewall. This option causes the Personal Firewall to look for and block UPnP traffic to counter the vulnerabilities that are introduced by this operating system feature: The first vulnerability could enable an attacker to gain complete control over an affected system, while the second vulnerability could enable an attacker to either prevent an affected system from providing useful service or utilize multiple users' systems in a distributed denial of service attack against a single target. Users can disable this feature when using applications that require the UPnP protocol to operate.

## **Automatically block attacker's IP address for... second(s)**

By default, this option is enabled in the Personal Firewall. This feature blocks all communication from a source host once an attack has been detected. For instance, if the Firewall detects a DoS attack originating from a certain IP address, the Personal Firewall will block any and all traffic from that IP for the duration specified in the seconds field.

## **Block all traffic while the service is not loaded**

By default, this option is enabled in the Personal Firewall. This feature prevents any traffic from entering or leaving your computer during the seconds between the time that your machine turns on and the Personal Firewall is launched. This time frame is a small security hole that can allow unauthorized communication. Enabling this feature prevents possible Trojan horses or other unauthorized applications from communicating with other

computers. This also takes effect if the Personal Firewall crashes or if the Personal Firewall is shut down.

### ***Allow initial traffic***

By default, this option is enabled in the Personal Firewall. This option enables initial traffic, needed for basic network connectivity, to take place. This includes initial DHCP and netBIOS traffic so that the Personal Firewall can obtain an IP address, for example.

### **Enable DLL authentication**

By default, this option is disabled in the Personal Firewall. DLL stands for “dynamic link library”, which is list of functions or data used by Windows applications. Most, if not all, Windows applications use DLLs to run, and each application uses specific DLLs. Often, several applications will access the same DLL. However, some hackers try to disguise malicious code or applications as DLLs, and use them to hack computers. Most DLLs have a file extension of .dll, .exe, .drv, or .fon.

Enabling DLL authentication means that you allow the Personal Firewall to determine which DLLs are used by which trusted applications and to store that information. The Personal Firewall then blocks applications that are using DLLs that are not associated with a trusted application, or DLLs that are associated with a trusted application and that have changed. Note that this may take place if you download a patch to an application that modifies that application’s DLL, in which case you are prompted to approve or reject using this changed DLL.

Because this option can interfere with the functioning of Windows applications, it is recommended that only users who have a firm understanding of Windows and DLLs enable this feature.

### ***Automatically allow all known DLLs***

By default, this option is enabled in the Personal Firewall. This option will automatically *allow* DLL modules that are commonly loaded by the network application, without prompting the user. Disabling this feature will cause the engine to prompt for permission on all new DLLs that are loaded, and may cause very frequent prompting when using a complex network application, such as an Internet browser.

### **Reset all fingerprints for all applications**

By default, this option is enabled in the Personal Firewall. If you want to erase all application fingerprints, click this button. It clears the Personal Firewall’s memory of all application fingerprints. The result is that each time you use an application that uses the network, you are prompted through a pop-up message to **Allow** or **Block** that application’s activity.

## **Smart Traffic Handling**

### **Enable smart DNS**

By default, this option is enabled in the Personal Firewall. Smart DNS is a feature that blocks all DNS traffic, except for outgoing DNS requests and the corresponding reply. This means that if your computer sends out a DNS request, and another computer responds within five seconds, the communication will be allowed. All other DNS packets will be dropped.

If you disable this feature, please note that you will need to manually allow DNS name resolution by creating an advanced rule that allows UDP traffic for remote port 53.

### **Enable smart DHCP**

By default, this option is enabled in the Personal Firewall. Smart DHCP is a feature that allows only outgoing DHCP requests and incoming DHCP replies, and only for network cards that allow DHCP.

Should you choose to disable this feature, and need to use DHCP, you must create an advanced rule for UDP packets on remote ports 67 and 68.

### **Enable smart WINS**

By default, this option is disabled in the Personal Firewall. It allows Windows Internet Naming Service (WINS) requests only if they were solicited. If the traffic was not requested, the WINS reply is blocked.

## Setting Up Email Notification of Security Events

The **E-Mail Notification** tab provides you with the option to automatically notify a specified recipient via email of any attacks against your computer.

The screenshot shows the 'Options' dialog box with the 'E-Mail Notification' tab selected. The 'Notify Immediately' radio button is chosen. The 'From' field is 'psmith@yourcompany.com', 'To' is 'itsecurity@yourcompany.com', 'Cc' is 'psmith@yourcompany.com', and 'Subject' is 'Security alert'. The 'SMTP Server Address' is '10.0.3.12'. The 'My E-Mail Server Requires Authentication' checkbox is checked, with 'Authentication Server Address' as '10.0.3.20', 'User Name' as 'psmith', and 'Password' masked with dots. A 'Test E-Mail Notification' button is at the bottom left, and 'OK' and 'Cancel' buttons are at the bottom right.

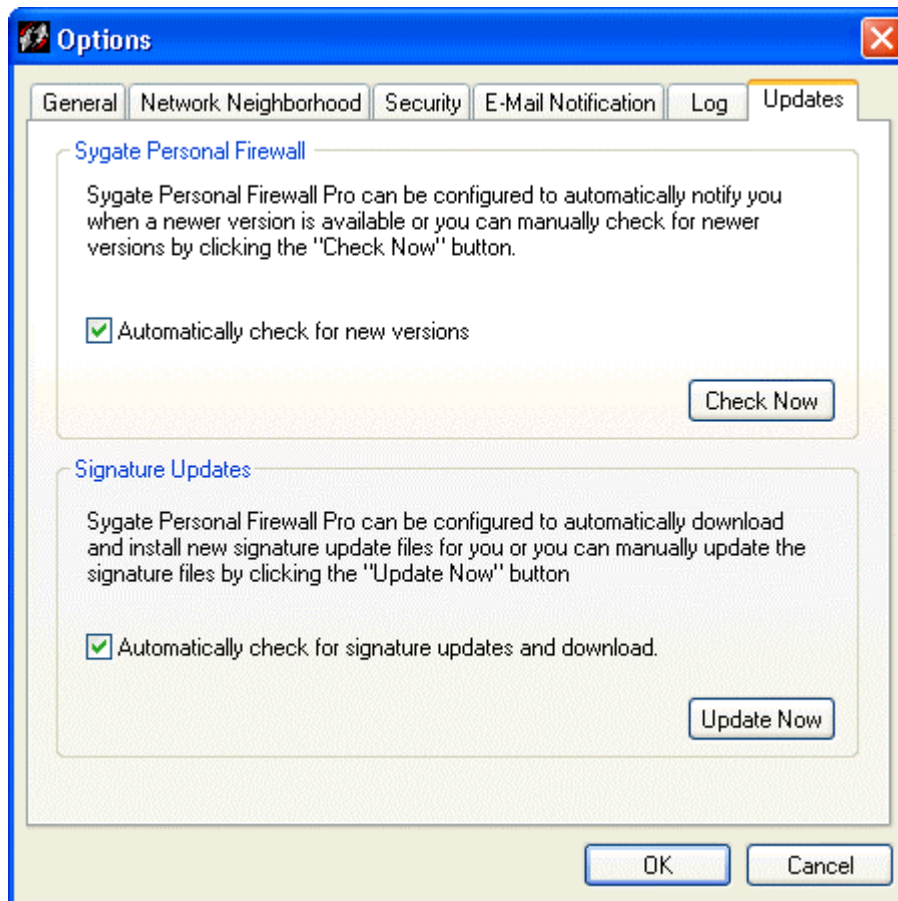
### To Activate E-Mail Notification

1. First, select the frequency of notification. You have three choices. Selecting **Do Not Notify** will disable the email notification option. Select **Notify Immediately** to have an email sent immediately following an attack on your computer. Alternately, you can select to have an email sent at regular intervals following an attack, by selecting the **After Every X Minute(s)** dial.
2. Enter an email address in the **From:** address field. This can be your personal email address or another email address.
3. Enter a recipient email address in the **To:** field. This can be an administrator's email address, or your email address, if you are accessing email remotely.
4. If you wish, you can send a courtesy copy of each email to a specified email address in the **Cc:** field.

5. Enter a subject in the **Subject** field.
6. Enter your SMTP Server Address.
7. If your email server requires authentication, click **My E-Mail Server Requires Authentication**. Enter the address of the authentication server in the **Authentication Server Address** field.
8. Enter your username and password for the authentication server in the appropriate fields.
9. Click **OK** to save changes.

## Updating Your Security

The **Updates** tab provides the capability of configuring your Firewall to check for:

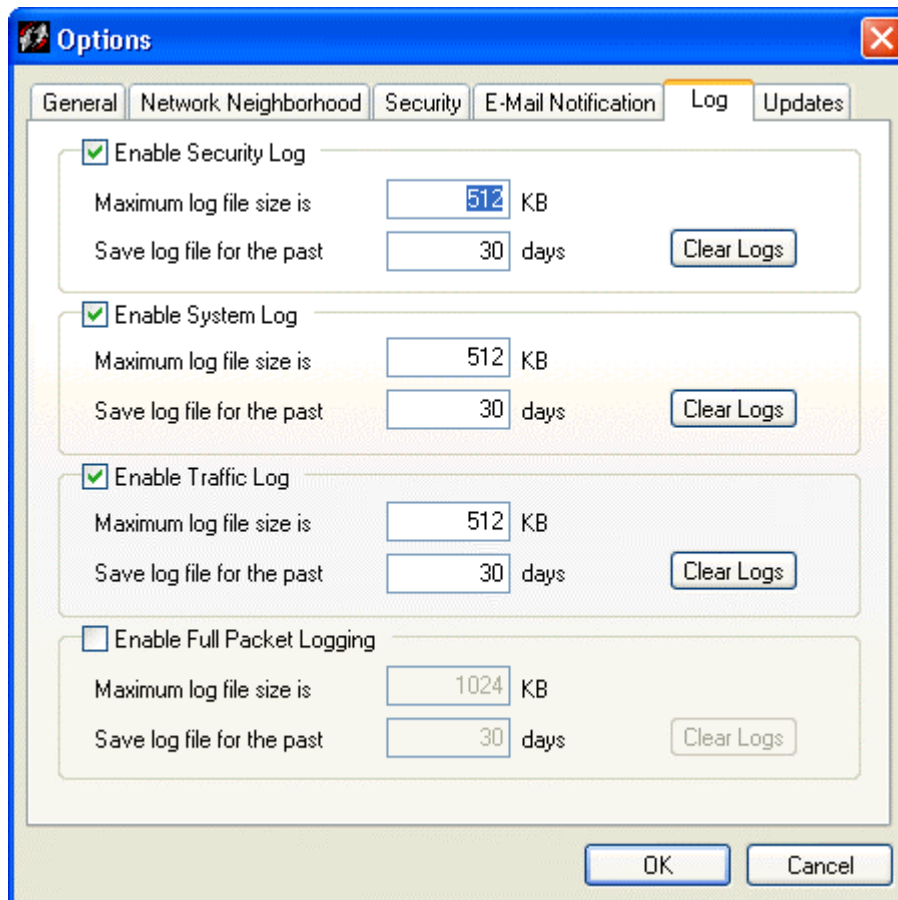


- **New versions**—Automatically check for, download, and install new versions of Sygate Personal Firewall Pro. Note that you can also do this manually: from the same screen, click **Check Now**.
- **Signature Updates**—Automatically check for, download, and install new Intrusion Detection signatures. Note that you can also do this manually: from the Main Menu, click **Tools | Update Signature**.



## Logging Security Events on Your System

The **Log File** tab provides a central location to manage the logs for the Personal Firewall. You can determine the standard log size for each log, as well as specify how many days of entries are recorded in each log. For more information on logs and how they work, see “Monitoring Your System: Logs.” You can also toggle whether or not logs are kept for each type of log.



### To Set Log Size

1. Click the appropriate **Maximum Log File Size** field and enter a size, in kilobytes, of the maximum size for the log file.
2. Click **OK**.

### To Set Log Days

1. Click the appropriate **Save Log File for the Past** field for the log you want to configure.
2. Enter a number of days.
3. Click **OK**.

## To Clear the Log

To clear a log from the **Log File** tab:

- Click **Clear Logs** for the log you want to clear.

## To Enable the Security Log

1. Click **Enable Security Log** to enable this choice.
2. Select a maximum file size (512 Kb is the default setting).
3. Enter a number of days for which the Personal Firewall should save the log file entries.
4. Click **OK**.

## To Enable the System Log

1. Click **Enable System Log** to enable this choice.
2. Select a maximum file size (512 Kb is the default setting).
3. Enter a number of days for which the Personal Firewall should save the log file entries.
4. Click **OK**.

## To Enable the Traffic Log

1. Click **Enable Traffic Log** to enable this choice.
2. Select a maximum file size (512 Kb is the default setting).
3. Enter a number of days for which the Personal Firewall should save the log file entries.
4. Click **OK**.

## To Enable the Packet Log

1. Click **Enable Full Packet Logging** to enable this choice.
2. Select a maximum file size (1024 Kb is the default setting).
3. Enter a number of days for which the Personal Firewall should save the log file entries.
4. Click **OK**.

## Chapter 8. Configuring Advanced Rules for Security

This chapter describes how to configure advanced security rules for the Personal Firewall. It goes through the various steps in creating an advanced rule that the Personal Firewall provides through its user interface, including:

- “Setting up Advanced Rules”
- “Overview of Creating Advanced Rules”
- “Advanced Rules: Provide a Name, Specify Allow or Block”
- “Advanced Rules: Specify a Source”
- “Advanced Rules: Specify Ports and Protocols”
- “Advanced Rules: Define a Schedule”
- “Advanced Rules: Specifying Applications”

### Setting up Advanced Rules

The Personal Firewall offers users the unique option to configure advanced rules that can override the rules automatically created by the firewall during normal user-firewall interaction. You may not realize it, but every time you allow or deny access to an application, you are creating a rule for that application. If you use Advanced Configuration to specify application access rights (such as scheduling and port rights), you are specifying parameters for the selected application, and thus creating an application rule. However, these rules are application-specific, so that if you create a schedule for an application, the schedule applies only to that application.

Advanced rules, on the other hand, are rules that you can create directly that affect all applications. If you create an advanced rule that blocks all traffic between 10 PM and 8 AM, the rule will override all other schedules and configurations that have been set for each application.

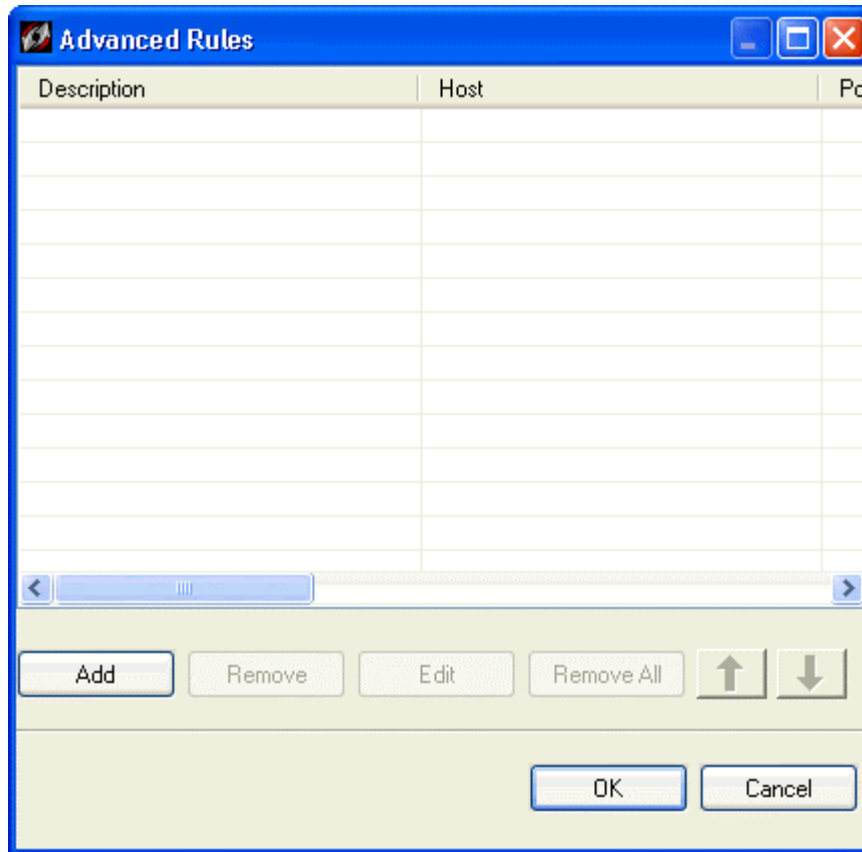
Rules in the Advanced Rules window will apply to all applications unless they are specifically tied to an individual application.

## Overview of Creating Advanced Rules

When you create an Advanced Rule, first decide what effect you want the rule to have.

Do you want to block all traffic when your screensaver is on? Would you like to allow all traffic from a particular source? Do you want to block UDP packets from a web site?

1. To begin, open the **Tools** menu at the top of the main console, and click **Advanced Rules**. The Advanced Rules dialog box will open, with an informational warning (click to view image) about their priority. Once you have created rules, they will appear in the main list.



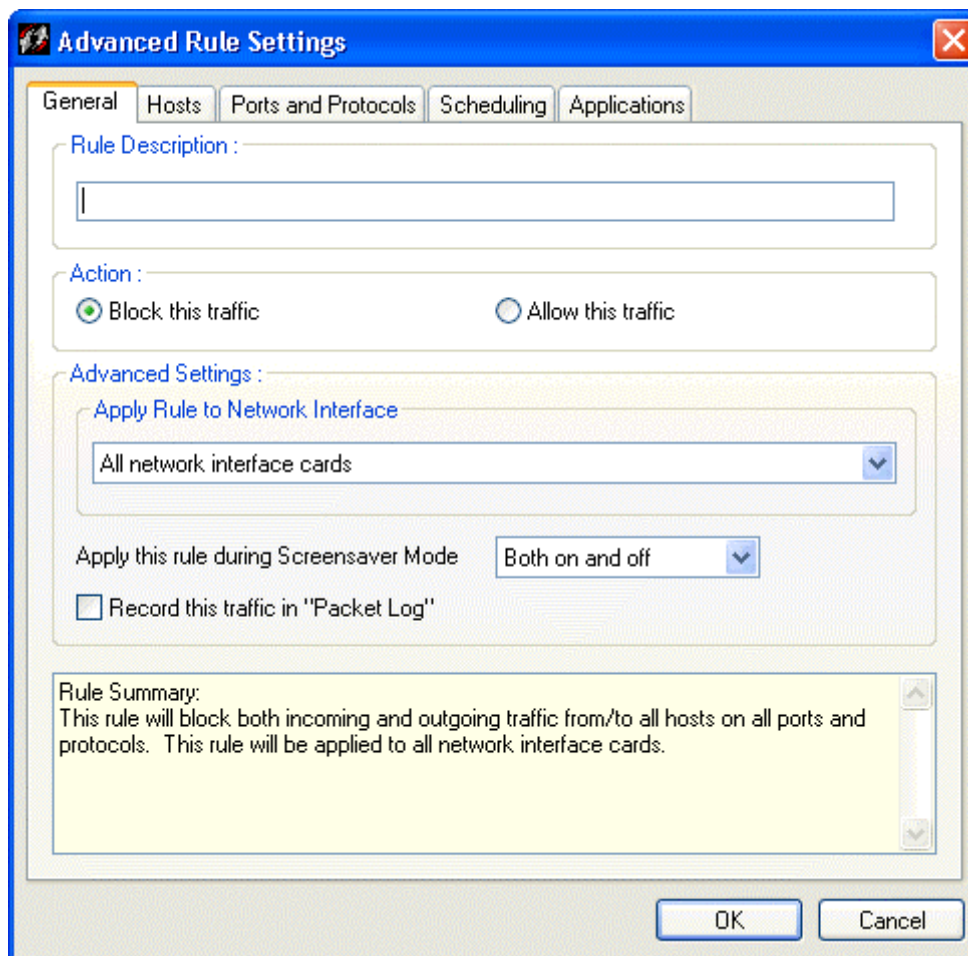
2. Click **Add**. The Advanced Rule Settings dialog box opens at the **General** tab.
3. Enter a descriptive name for your rule on this tab, and then specify the conditions for it on the other tabs.

To create a rule, you must first specify the kind of traffic, and the conditions that must exist for the rule to take effect. There are five different sections within the Advanced Rule Settings dialog box where you can specify the characteristics of the traffic: **General**, **Hosts**,

**Ports and Protocols, Scheduling, and Applications.** You can use as many sections as necessary to specify the conditions and characteristics (time of day, type of traffic, port number) that will cause the rule to take effect, as well as the effect the rule will have. The more information and characteristics that you enter in the Advanced Rule Settings dialog box, the more specific the rule will be. Note that each tab that contains specified information contributes to the functioning of a rule.

## Advanced Rules: Provide a Name, Specify Allow or Block

The **General** tab is used to provide a name for the rule you are creating, as well as the effect that the rule will have (allowing or blocking traffic).

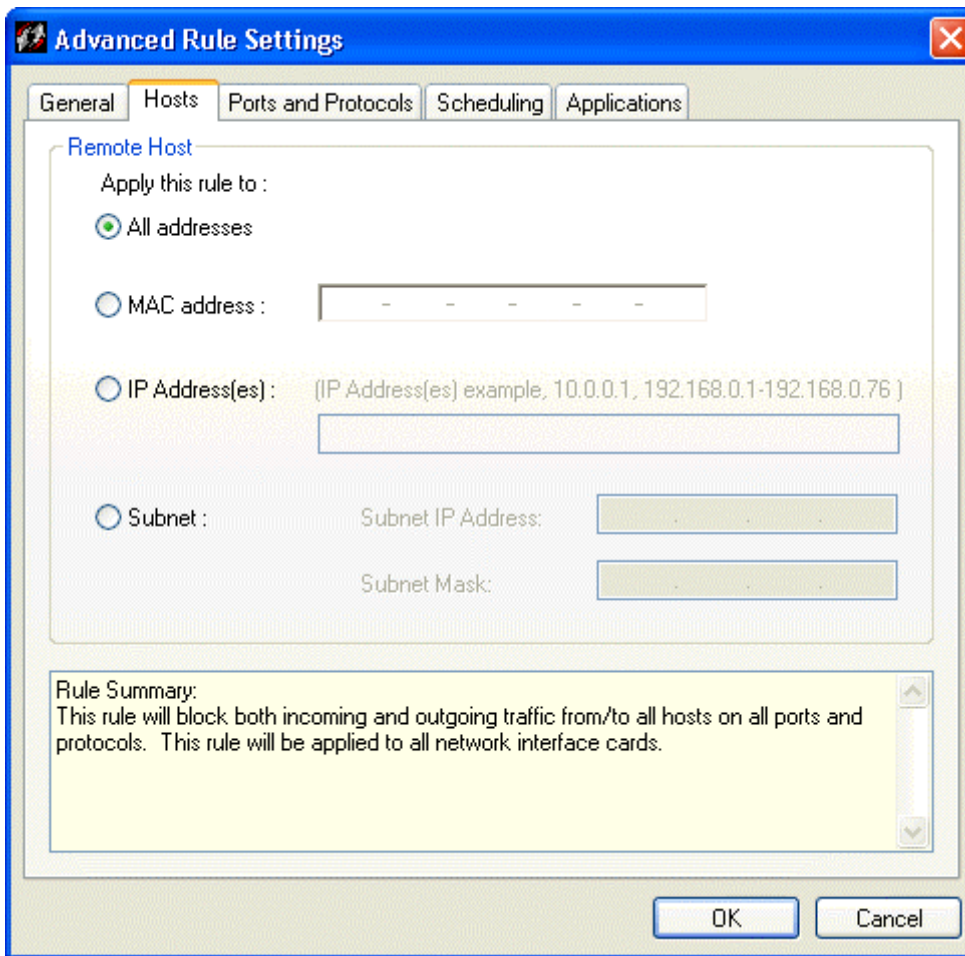


1. First, enter a rule description. This will also function as the name of the rule, and it should indicate qualities of the rule. For instance, “Rule1” may not be a very good name for a rule, but “Block After 10 PM” would be (assuming the rule had some sort of function that did block traffic after 10 PM).
2. Second, decide the main action of the rule - do you want to block traffic, or allow traffic?

3. Next, choose which network interface card this rule will apply to. If you have multiple network cards, select one from the list box, or select **All network interface cards** to apply the rule to every card.
4. Decide if this rule will be influenced by the activation of your computer's screensaver (if applicable).
  - **On**—The rule will be activated only when the screensaver is on. This is a great feature if you want to block all traffic and all ports while you computer is idle.
  - **Off**—This rule will be activated only if the screen saver is off and all other conditions are satisfied.
5. Both **On** and **Off**—This rule is unaffected by the screensaver.
6. Click **Record this traffic in "Packet Log"** if you want traffic affected by this rule to be entered in the Packet Log.
7. The Rule Summary field at the bottom of the General tab provides a summary of the rule's functionality. Click **OK** to set the rule, or click on another tab to further specify rule conditions and properties.

## Advanced Rules: Specify a Source

The **Hosts** tab is where you can specify the source (IP address, MAC address, or Subnet range) of traffic that you want to block or allow.



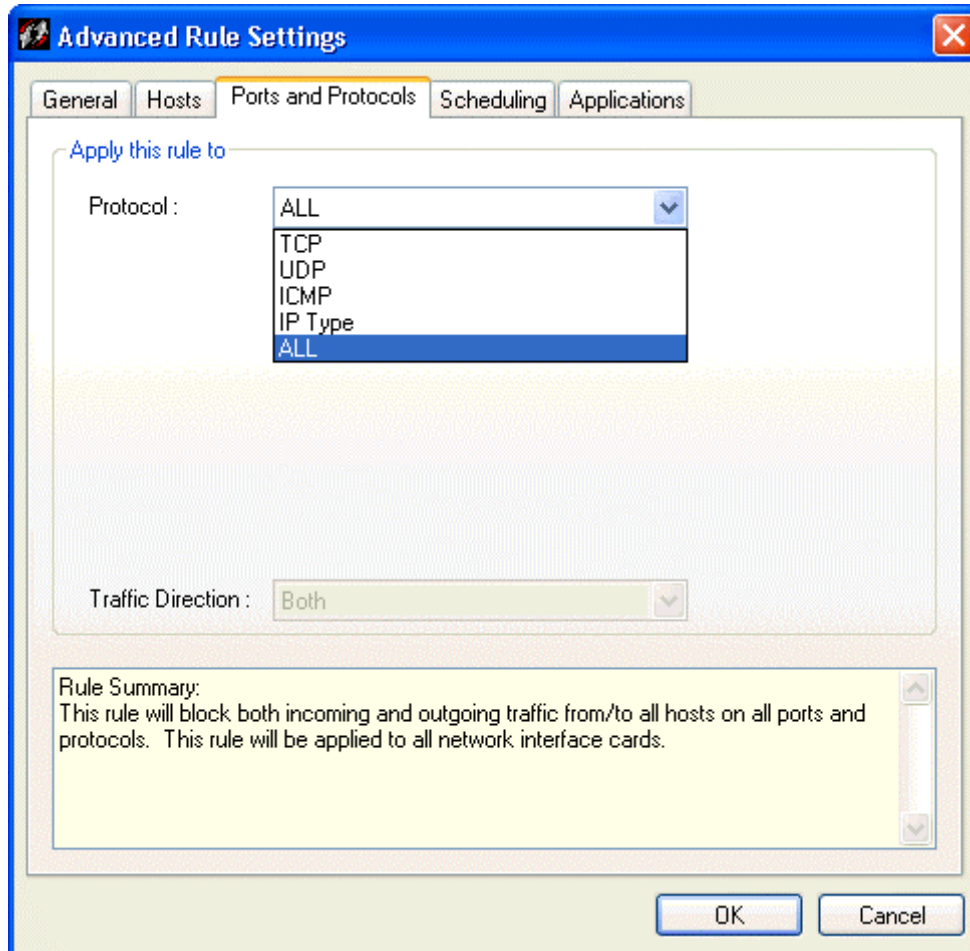
To block or allow traffic for a specified source:

1. Click the **Advanced Rules | Host** tab.
2. Select the way in which you want to identify the traffic source. Click **All Addresses** if you are planning on blocking traffic from all sources for this rule.
3. Click **MAC Address** and type the corresponding address or address range.
4. Click **IP Addresses** and type the corresponding address or address range.
5. Click **Subnet** and type the corresponding subnet IP address and Subnet mask.

The Rule Summary field at the bottom of the General tab provides a summary of the rule's functionality. Click **OK** to set the rule, or click on another tab to further specify rule conditions and properties.

## Advanced Rules: Specify Ports and Protocols

The **Ports and Protocols** tab provides an area to specify which ports and protocols, if any, should be affected by the traffic specified in the rule.



Select a protocol from the top list box.

### **All Protocols**

As indicated, the **ALL** selection will affect all protocols on all ports, for both incoming and outgoing traffic.

### **TCP**

If you select **TCP** from the Protocol list box, you will be given shown two more list boxes in which you can specify which ports (remote and/or local) should be affected by the rule. You can type the port numbers or select the port type from the list boxes for the both local and remote ports.



If you do not enter or select a port number, then all ports will be affected by the rule. If you enter a port number for the local port entry, but not for the remote port entry, then the local port you entered and ALL remote ports will be affected by the rule.

Then, select which traffic (**Incoming** or **Outgoing**) should be affected by the rule.

### **UDP**

If you select **UDP** from the list box, you will then see two port list boxes. You can type the port numbers or select the port type from the list boxes for both local and remote ports. If you do not enter or select a port number, then all ports will be affected by the rule. If you enter a port number for the local port entry, but not for the remote port entry, then the local port you entered and ALL remote ports will be affected by the rule.

Then, select which traffic (**Incoming** or **Outgoing**) should be affected by the rule.

### **ICMP**

If you select **ICMP** as the protocol for your rule, you will be shown a list of ICMP types. Select the types of ICMP that you wish allow or block by placing a check next to them. Then select the direction of traffic to be affected by the rule.

### **IP Type**

Should you select **IP Type** from the list of protocols, you will see a list of IP protocol types displayed on the lower half of the Ports and Protocols tab.

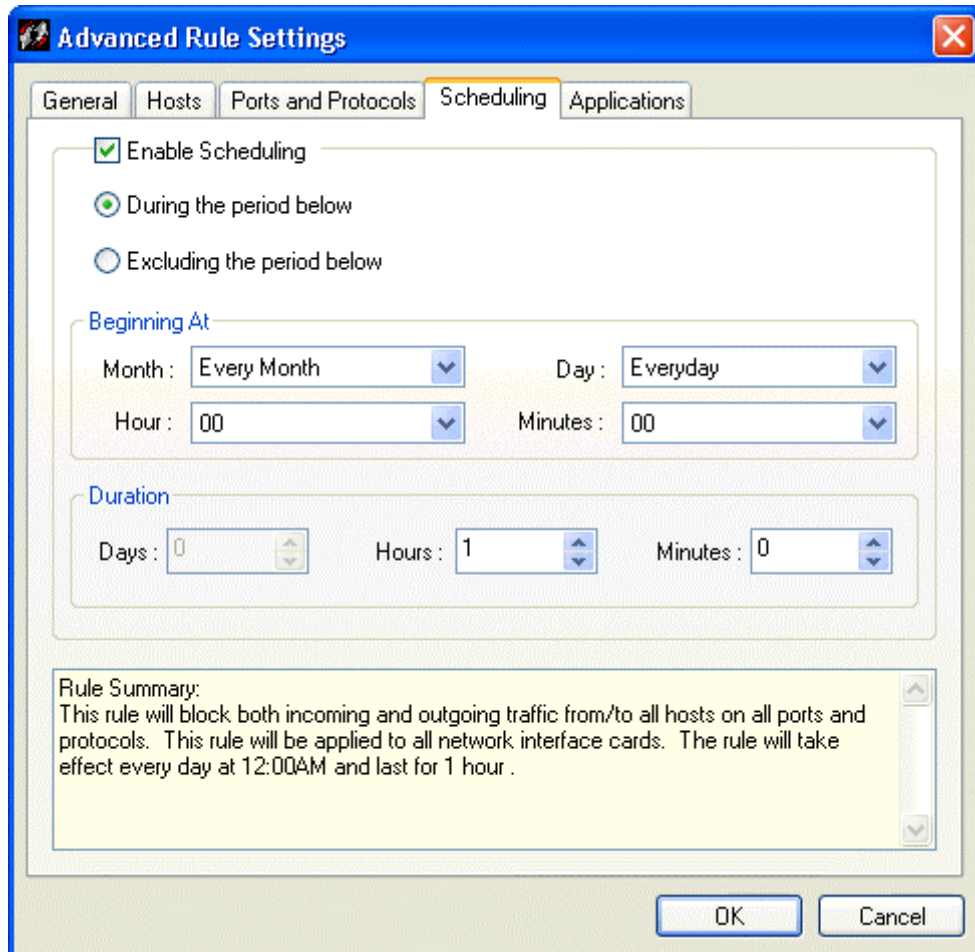
Then, select the traffic direction from the pull-down list.

Click **OK**. The Rule Summary at the bottom of the window provides a description of the rule and what traffic it will affect on your system.

## Advanced Rules: Define a Schedule

Scheduling is a good way to create a rule that you want to take effect only during (or excluding) certain time periods. For instance, if you want to block all traffic after 10 PM, then you can create a schedule that will permit the rule to do so.

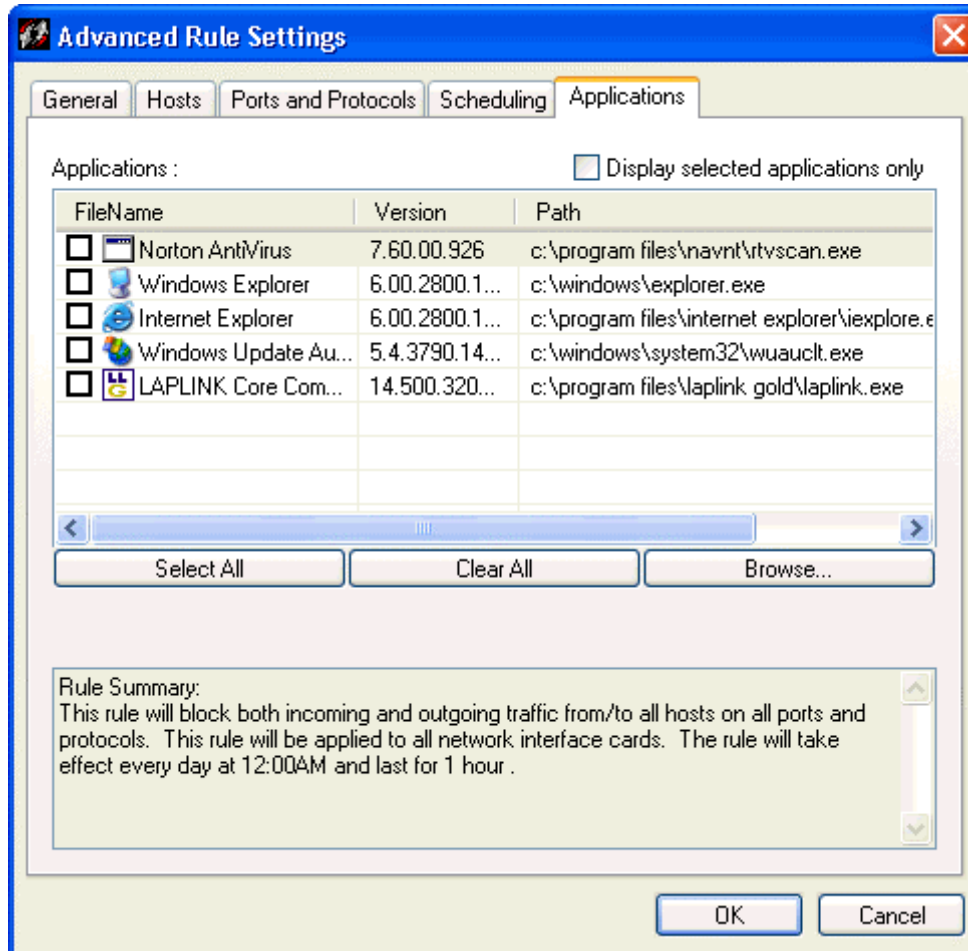
1. Open the **Scheduling** tab. Click **Enable Scheduling**.



2. Decide if you want the schedule to take place during a certain time period, or outside of a certain time period. Click either **During** or **Excluding**.
3. Select a month, day and beginning time from the list boxes, or leave the default settings, which will apply the rule schedule to all day, every day, all year.
4. If you have a beginning time, enter a duration for the rule's effect.
5. The Rule Summary field at the bottom of the General tab provides a summary of the rule's functionality. Click **OK** to set the rule, or click on another tab to further specify rule conditions and properties.

## Advanced Rules: Specifying Applications

You can specify applications that will be affected by advanced rules. The **Applications** tab provides a list of all applications that have accessed your network connection.



1. To select an application to be affected by this rule, click the box next to its name under the **FileName** column. You can select all applications in the table by clicking the **Select All** button. To browse for applications that are not displayed in the table, click **Browse...** and select the application from its directory.
2. You can choose to display only the applications that you have selected to be controlled by this rule by clicking **Display selected applications only**. The Rule Summary at the bottom of the window provides a description of the rule and what traffic it will affect on your system.



## Appendix A. Monitoring Your System: Logs

This appendix describes how you can monitor your system by using the logs that are present in the Personal Firewall. It begins with an overview of logs, describes how to export logs, and then describes each log, concluding with a section on back tracing logged events. The following topics are included:

- Understanding Logs
- Exporting Logs
- Viewing Logs
- Viewing the Security Log
- Viewing the Traffic Log
- Viewing the Packet Log
- Viewing the System Log
- Back Tracing Logged Events

## Understanding Logs

Personal Firewall logs are some of the key sources of information on how your Personal Firewall interacts with the network. With logs, you can tell when you have been blocked from the network, and to some extent why. You can also troubleshoot connectivity problems or possible network attacks.

In the Personal Firewall, a log is a record of information attempting to enter or exit your computer through your network connection. There are four separate logs that monitor different aspects of your network connection.

Logs are an important method for tracking your computer's activity and interaction with other computers and computer networks. They are particularly useful in detecting potentially threatening activity, such as port scanning, that is aimed at your computer.

To view the different logs available in the Personal Firewall, click on the **Logs** icon on the toolbar at the top of the main screen.

Click the **Logs** button to view the log that you most recently viewed



OR click the down arrow and select a log type

There are four different logs in the Personal Firewall:

- Security Log
- Traffic Log
- Packet Log
- System Log

Another important capability of the Personal Firewall is Back Tracing, which enables you to use ICMP to determine all the hops between your computer and an intruder on another computer.

## Exporting Logs

Logs can be exported and saved in different locations. You may want to do this to save space, but is it more likely that you do this to import them into a tool such as Microsoft Excel. Logs are an excellent tool for analyzing the traffic and the security incidents on your computer.

1. To export a log file, open the log in the **Log Viewer**.
2. Open the **File** menu, and select **Export...**
3. In the **Save As** window, select the location for the log file. We recommend giving it an appropriate name, incorporating the date, and type of log file (Security, Traffic, etc.).
4. Click **Save**.

## Viewing Logs

You can view the following types of logs for the Personal Firewall:

- **Security**—The Security log for the Personal Firewall records DoS attacks, port scans, executable file alterations, Trojan horse attacks, and host integrity.
- **Traffic**—The Traffic log for the Personal Firewall is a record of Personal Firewall network traffic.
- **Packet**—The Packet log for the Personal Firewall captures data packets for the Personal Firewall network traffic.
- **System**—The System log for the Personal Firewall only deals with the operation of the Personal Firewall.

To view logs on the Personal Firewall:

1. Click the **Logs** icon on the toolbar

OR

Click **Tools | Logs**

OR

Right-click the Tool Bar icon, and then click **Logs**

The most recently viewed log appears.

You can also click the down-arrow next to the **Logs** icon to choose a different log. The most recently viewed log appears by default, but you can choose any of the logs to view.

2. From the **View** list, select **Local View**, the default setting, or **Source View**. You can select how you view local and remote IP addresses or names. The following example is from the Security Log:
  - If you select **Local View** from the View list, then Remote Host, Remote MAC, Local Host, and Local MAC information appear. The Remote Host and Remote MAC always represent the IP address and MAC address of the attempted attacker whereas Local Host address and Local MAC always represent your IP address and your MAC address. Your system is always considered the Local system.
  - If you select **Source View** from the View list, then Remote Host, Remote MAC, Local Host and Local MAC information no longer appear. Instead, Source Host, Source MAC, Destination Host, and Destination MAC appear.



- If someone sends a message or attacks your system, then the originator's IP address and MAC address are listed in the Source Host and Source MAC columns whereas your IP number and your MAC address are listed in the Destination Host and Destination MAC because you are the recipient.
  - If you send a message or attack someone else's system, then your IP address and MAC address are listed in the Source Host and Source MAC columns whereas the recipient's IP number and MAC address are listed in the Destination Host and Destination MAC sections.
7. Click a different log name if you wish to view a different log.
  8. Click **Refresh** or press **F5** to update the log that you are viewing.

## Viewing the Security Log

The Security Log records potentially threatening activity directed towards your computer, such as port scanning, or denial of service attacks. The Security Log is probably the most important log file in the Personal Firewall.

### Viewing the Security Log

To view the Security Log on the Personal Firewall:

1. Click the down-arrow near the **Logs** icon on the toolbar, and then choose **Security Log...**

OR

Click **Tools | Logs | Security Log...**

OR

Right-click the Tool Bar icon, and then click **Logs | Security Log...**

You can also click the down-arrow next to the **Logs** icon to choose a different log. The most recently viewed log appears by default, but you can choose any of the logs to view.

2. From the **View** list, select **Local View**, the default setting, or **Source View**. You can select how you view local and remote IP addresses or names.
  - If you select **Local View** from the View list, then Remote Host, Remote MAC, Local Host, and Local MAC information appear. The Remote Host and Remote MAC always represent the IP address and MAC address of the attempted attacker whereas Local Host address and Local MAC always represent your IP address and your MAC address. Your system is always considered the Local system.
  - If you select **Source View** from the View list, then Remote Host, Remote MAC, Local Host and Local MAC information no longer appear. Instead, Source Host, Source MAC, Destination Host, and Destination MAC appear.
    - If someone sends a message or attacks your system, then the originator's IP address and MAC address are listed in the Source Host and Source MAC columns whereas your IP number and your MAC address are listed in the Destination Host and Destination MAC because you are the recipient.
    - If you send a message or attack someone else's system, then your IP address and MAC address are listed in the Source Host and Source MAC columns





whereas the recipient's IP number and MAC address are listed in the Destination Host and Destination MAC sections.

3. Click a different log name if you wish to view a different log.
4. Click **Refresh** or press **F5** to update the log that you are viewing.

### Icons for the Security Log

When you open a Security Log, icons are displayed at the left side of the first column. These are graphical representations of the kind of attack logged on each line, and they provide an easy way to scan the Security Log for possible system errors.

**Table 8. Personal Firewall Security Log Icons**

Icon	Description
	Severe attack
	Major attack
	Minor attack
	Information

### Personal Firewall Security Log Parameters and Description

The log is a data sheet, where each row represents a logged event, and the columns display information regarding the event. The columns are:

**Table 9. Personal Firewall Security Log Parameters and Description**

Name of Parameter	Description
Time	The exact date and time that the event was logged
Security Type	Type of Security Alert (for example: DoS attack, executable file, Ping of Death)
Severity	The severity of the attack (either Severe, Major, Minor, or Information)
Direction	Direction that the traffic was traveling in (incoming, outgoing, or unknown)—Most attacks are incoming, that is, they originate in another computer. Other attacks, like Trojan horses, are programs that have been downloaded to your computer and therefore are already present; they are considered outgoing. Still other attacks are unknown in direction; they include Active Response or application executable changed.
Protocol	Type of protocol—UDP, TCP, and ICMP
Remote Host	Name of the remote computer ( <i>only appears in Local View - this is the default</i> )
Remote MAC	MAC address of the remote computer ( <i>only appears in Local View - this is the default</i> )

**Table 9. Personal Firewall Security Log Parameters and Description**

<b>Name of Parameter</b>	<b>Description</b>
Local Host	IP address of the local computer <i>(only appears in Local View - this is the default)</i>
Local MAC	MAC address of the local computer <i>(only appears in Local View - this is the default)</i>
Source Host	Name of the source computer <i>(only appears in Source View)</i>
Source MAC	MAC address of the source computer <i>(only appears in Source View)</i>
Destination Host	IP address of the destination computer <i>(only appears in Source View)</i>
Destination MAC	MAC address of the destination computer <i>(only appears in Source View)</i>
Application Name	Name of the application associated with the attack
User Name	The User or Computer client that sent or received the traffic
Domain	Domain of the user
Location	The Location (Office, Home, VPN, etc.) that was in effect at the time of the attack
Occurrences	Number of occurrences of the attack method
Begin Time	The time the attack began
End Time	Time that the attack ended

## Description and Data Fields for the Security Log

Below the rows of logged events are the **Description** and **Data** fields. When you click on an event row, the entire row is highlighted. A description of the event, such as “Somebody is scanning your computer, with 13 attempts”, appears in the **Description** field.

## Back Tracing Hack Attempts for the Security Log

1. From the Traffic Log file, click on the event you want to back trace so that the entire row is highlighted.
2. Either right-click the row and select **Back Trace** from the pop-up window or click the **Action** menu and select **Back Trace**.

The Personal Firewall traces the event information. The **Back Trace Information** window is displayed with a trace route log.

3. To view detailed information on the original IP address, click the **Whois>>** button at the bottom of the **Back Trace** Information window. A drop panel appears, displaying detailed information about the owner of the IP Address from which the security event originated.
4. Click the **Whois<<** button again to hide the information.

For further information on Back Tracing, see “Back Tracing.”

## Filtering the Log Events by Severity in the Security Log

1. In the Security log, you can filter the events that you are viewing by the severity level of the attack.
2. In the **Log Viewer**, open the **Filter** menu.
3. Select **Severity**.

The **Severity** window appears.

4. Place check marks in each box next to the severity level(s) that you want to view. You have the following options:
  - ☐ Critical
  - ☐ Major
  - ☐ Minor
  - ☐ Information

You can view more than one type of event at once. The **Log Viewer** is automatically reloaded.

## Filtering the Log Events by Date in the Security Log

To filter the log events by date:

1. Click the **Filter** menu in the **Log Viewer** window.
2. Select which events you want to view from the list:

**Table 10. Viewing Personal Firewall Security Log Events by Date**

Events for...	Displays...
<b>1 Day Logs</b>	the events recorded on the current day
<b>2 Day Logs</b>	the events recorded over the past 2 days
<b>3 Day Logs</b>	the events recorded over the last 3 days, including the current day

**Table 10. Viewing Personal Firewall Security Log Events by Date**

<b>Events for...</b>	<b>Displays...</b>
<b>1 Week Logs</b>	the events recorded over the past 7 days
<b>2 Week Logs</b>	the events recorded over the past 14 days
<b>1 Month Logs</b>	the events recorded over the last 30 days
<b>Show All Logs</b>	all Security Log events

3. The log displays the requested events.

## Viewing the Traffic Log

Whenever your computer makes a connection through the network, this transaction is recorded in the Traffic Log.

### Viewing the Traffic Log

To view the Traffic Log on the Personal Firewall:

1. Click the down-arrow near the **Logs** icon on the toolbar, and then choose **Traffic Log...**

OR

Click **Tools | Logs | Traffic Log...**

OR

Right-click the Tool Bar icon, and then click **Logs | Traffic Log...**

You can also click the down-arrow next to the **Logs** icon to choose a different log. The most recently viewed log appears by default, but you can choose any of the logs to view.







2. From the **View** list, select **Local View**, the default setting, or **Source View**. You can select how you view local and remote IP addresses, MAC addresses, or ports/ICMP types.
  - If you select **Local View** from the View list, then Remote Host, Remote MAC, Remote Port/ICMP Type, and Local Host, Local MAC, Local Port/ICMP Type information appear. The Remote information always represents the attempted attacker whereas Local information always represents your local system. Your system is always considered the Local system.
  - If you select **Source View** from the View list, then Remote Host, Remote MAC, Remote Port/ICMP Type, and Local Host, Local MAC, Local Port/ICMP Type information no longer appear. Instead, Source Host, Source MAC, Source Port/ICMP Type, and Destination Host, Destination MAC, and Destination Port/ICMP Type appear.
    - If someone sends a message or attacks your system, then the originator's IP address, MAC address, and port/ICMP type are listed in the Source Host, Source MAC, and Source Port/ICMP columns whereas your IP number, MAC address, and your port are listed in the Destination Host, Destination MAC, and Destination Port/ICMP Code because you are the recipient.

- If you send a message or attack someone else's system, then your IP address, MAC address and port/ICMP code are listed in the Source Host, Source MAC, and Source Port/ICMP Code columns whereas the recipient's IP number, MAC address, and port/ICMP type are listed in the Destination Host, Destination MAC, and Destination Port/ICMP code sections.
3. Click a different log name if you wish to view a different log.
  4. Click **Refresh** or press **F5** to update the log that you are viewing.

## Icons for the Traffic Log

When you open a Traffic Log, icons are displayed at the left side of the first column. They are graphical representations of the kind of traffic logged on each line and provide an easy way to scan the Traffic Log. Traffic Log includes information about incoming and outgoing traffic.

**Table 11. Personal Firewall Traffic Log Icons**

Icon	Description
	Incoming traffic; passed through the Personal Firewall
	Incoming traffic; blocked by the Personal Firewall
	Outgoing traffic; passed through the Personal Firewall
	Outgoing traffic; blocked by the Personal Firewall
	Traffic direction unknown; passed through the Personal Firewall
	Traffic direction unknown; blocked by the Personal Firewall

## Personal Firewall Traffic Log Parameters and Description

Each row represents a logged event, and each column displays information about the event.

**Table 12. Personal Firewall Traffic Log Parameters and Description**

Name of Parameter	Description
Time	The exact date and time that the event was logged
Action	Action taken by the Personal Firewall: Blocked, Asked, or Allowed
Severity	The severity of the attack (either Severe, Major, Minor, or Information)
Direction	Direction that the traffic was traveling in (incoming or outgoing)
Protocol	Type of protocol - UDP, TCP, and ICMP
Remote Host	Name of the remote computer ( <i>only appears in Local View - this is the default</i> )
Remote MAC	MAC address of the remote computer ( <i>only appears in Local View - this is</i>



**Table 12. Personal Firewall Traffic Log Parameters and Description**

Name of Parameter	Description
	<i>the default)</i>
Remote Port/ICMP Type	Port and ICMP type on the remote computer <i>(only appears in Local View - this is the default)</i>
Local Host	IP address of the local computer <i>(only appears in Local View - this is the default)</i>
Local MAC	MAC address of the local computer <i>(only appears in Local View - this is the default)</i>
Local Port/ICMP Code	Port and ICMP code used on the Personal Firewall computer <i>(only appears in Local View - this is the default)</i>
Source Host	Name of the source computer <i>(only appears in Source View)</i>
Source MAC	MAC address of the source computer <i>(only appears in Source View)</i>
Source Port/ICMP Type	Port and ICMP type on the source computer <i>(only appears in Source View)</i>
Destination Host	IP address of the destination computer <i>(only appears in Source View)</i>
Destination MAC	MAC address of the destination computer <i>(only appears in Source View)</i>
Destination Port/ICMP Code	Port and ICMP code used on the destination computer <i>(only appears in Source View)</i>
Application Name	Name of the application associated with the attack
User	Login name of the user
Domain	Domain of the user
Location	The Location (Office, Home, VPN, etc.) that was in effect at the time of the attack
Occurrences	Number of occurrences of the attack method
Begin Time	The time the attack began
End Time	Time that the attack ended
Rule Name	The rule that determined the passing or blockage of this traffic

## Description and Data Fields for the Traffic Log

Below the rows of logged events are the **Description** and **Data** fields. When you click an event row, the entire row is highlighted. A description of the event is displayed in the **Description** field.

## Back Tracing Traffic Events for the Traffic Log

1. From the Traffic Log file, click on the event you want to back trace so that the entire row is highlighted.
2. Either right-click the row and select **Back Trace** from the pop-up window or click the **Action** menu and select **Back Trace**.
3. The Personal Firewall traces the event information. The **Back Trace Information** window is displayed with a trace route log.
4. Click **Detail** at the bottom of the **Back Trace** Information window to view detailed information about the original IP address.  
A drop panel displays detailed information about the owner of the IP Address from which the traffic event originated.
5. Click **Detail** again to hide the information.

For further information on Back Tracing, see “Back Tracing.”

## Viewing the Traffic Log Events by Date

To filter the log events by date:

1. Click the **View** menu in the **Log Viewer** window.
2. Select which events you want to view from the list:

**Table 13. Viewing Personal Firewall Traffic Log Events by Date**

Events for...	Displays...
<b>1 Day Logs</b>	the events recorded on the current day
<b>2 Day Logs</b>	the events recorded over the past 2 days
<b>3 Day Logs</b>	the events recorded over the last 3 days, including the current day
<b>1 Week Logs</b>	the events recorded over the past 7 days

**Table 13. Viewing Personal Firewall Traffic Log Events by Date**

<b>Events for...</b>	<b>Displays...</b>
<b>2 Week Logs</b>	the events recorded over the past 14 days
<b>1 Month Logs</b>	the events recorded over the last 30 days
<b>Show All Logs</b>	all Traffic Log events

3. The log is automatically displays the requested events.

## Viewing the Packet Log

The Packet Log captures every packet of data that enters or leaves a port on your computer. The Packet Log is disabled by default in the Personal Firewall because of its potentially large size.

To enable the **Packet Log**, open the **Options** window by selecting **Options...** from the **Tools** menu. Click on the **Log** tab and click the check box next to the text **Enable Packet Log**. Then click **Apply**. If you do not have an **Options** window, the Packet Log is not available for your Personal Firewall.

## Viewing the Packet Log

To view the Packet Log on the Personal Firewall:

1. Click the down-arrow near the **Logs** icon on the toolbar, and then choose **Packet Log...**

OR

Click **Tools | Logs | Packet Log...**

OR

Right-click the Tool Bar icon, and then click **Logs | Packet Log...**

You can also click the down-arrow next to the **Logs** icon to choose a different log. The most recently viewed log appears by default, but you can choose any of the logs to view.


2. From the **View** list, select **Local View**, the default setting, or **Source View**. You can select how you view local and remote IP addresses or ports.
  - If you select **Local View** from the View list, then Remote Host, Remote Port, Local Host, and Local Port information appear. The Remote Host and Remote Port always represent the IP address and port of the attempted attacker whereas Local Host address and Local Port always represent your IP address and your port. Your system is always considered the Local system.
  - If you select **Source View** from the View list, then Remote Host, Remote Port, Local Host and Local Port information no longer appear. Instead, Source Host, Source Port, Destination Host, and Destination Port appear.
    - If someone sends a message or attacks your system, then the originator's IP address and port are listed in the Source Host and Source Port columns whereas your IP number and your port are listed in the Destination Host and Destination Port because you are the recipient.

- If you send a message or attack someone else's system, then your IP address and port are listed in the Source Host and Source Port columns whereas the recipient's IP number and port are listed in the Destination Host and Destination Port sections.
3. Click a different log name if you wish to view a different log.
  4. Click **Refresh** or press **F5** to update the log that you are viewing.

## Icons for the Packet Log

There is only one icon displayed in the Packet Log. It indicates the capturing of raw data packets.

**Table 14. Personal Firewall Packet Log Icon**

Icon	Description
	Full data packet captured

## Firewall Packet Log Parameters and Description

Each row represents a logged event, and the columns display information regarding the event. The columns are:

**Table 15. Personal Firewall Packet Log Parameters and Description**

Name of Parameter	Description
Time	The exact date and time that the packet was logged
Remote Host	Name of the remote computer ( <i>only appears in Local View - this is the default</i> )
Remote Port	Port on the remote host that sent/received the traffic ( <i>only appears in Local View - this is the default</i> )
Local Host	IP Address of the local computer ( <i>only appears in Local View - this is the default</i> )
Local Port	Port used on the Personal Firewall computer for this packet ( <i>only appears in Local View - this is the default</i> )
Source Host	Name of the source computer ( <i>only appears in Source View</i> )
Source Port	Port on the source host that sent/received the traffic ( <i>only appears in Source View</i> )
Destination Host	IP Address of the destination computer ( <i>only appears in Source View</i> )
Destination Port	Port used on the destination computer for this packet ( <i>only appears in Source View</i> )

**Table 15. Personal Firewall Packet Log Parameters and Description**

Name of Parameter	Description
Direction	Direction that the traffic was traveling in (incoming or outgoing)
Action	Action taken by the Personal Firewall: Blocked or Allowed
Application Name	Name of the application associated with the packet

## Packet Decode and Packet Dump for the Packet Log

Below the **Log Viewer** are two additional data fields that provide further detail regarding the selected event. In the Packet Log, these fields are labeled **Packet Decode**, which provides data on the type of packet logged, and **Packet Dump**, which records the actual data packet.

## Back Tracing Packet Log Events

1. From the Packet Log file, click on the event you want to back trace so that the entire row is highlighted.
2. Either right-click the row and select **Back Trace** from the pop-up window or click the **Action** menu and select **Back Trace**.
3. The Personal Firewall traces the event information. The **Back Trace Information** window is displayed with a trace route log.
4. Click **Detail** at the bottom of the **Back Trace** Information window to view detailed information about the original IP address.  
A drop panel displays detailed information about the owner of the IP Address from which the traffic event originated.
5. Click **Detail** again to hide the information.

For further information on Back Tracing, see “Back Tracing.”

## Viewing the Packet Log Events by Date

To filter the log events by date:

1. Click the **View** menu in the **Log Viewer** window.
2. Select which events you want to view from the list:

**Table 16. Viewing Personal Firewall Packet Log Events by Date**

Events for...	Displays...
<b>1 Day Logs</b>	the events recorded on the current day
<b>2 Day Logs</b>	the events recorded over the past 2 days
<b>3 Day Logs</b>	the events recorded over the last 3 days, including the current day
<b>1 Week Logs</b>	the events recorded over the past 7 days
<b>2 Week Logs</b>	the events recorded over the past 14 days
<b>1 Month Logs</b>	the events recorded over the last 30 days
<b>Show All Logs</b>	all Packet Log events

3. The log is automatically displays the requested events.

## Viewing the System Log

The System log records all operational changes, such as the starting and stopping of services, detection of network applications, software configuration modifications, and software execution errors. The System Log is especially useful for troubleshooting the Personal Firewall.

### Viewing the System Log

To view the System Log on the Personal Firewall:

- Click the down-arrow near the **Logs** icon on the toolbar, then choose **System Log...**

OR

Click **Tools | Logs | System Log...**

OR




Right-click the Tool Bar icon, and then click **Logs | System Log...**

You can also click the down-arrow next to the **Logs** icon to choose a different log. The most recently viewed log appears by default, but you can choose any of the logs to view.

### Icons for the System Log

When you open the System Log, icons are displayed at the left side of the first column. These are graphical representations of the kind of event logged on each line, and they provide an easy way to scan the System Log for possible system errors.

**Table 17. Icons for the Personal Firewall System Log**

Icon	Description
	Error
	Warning
	Information

### Personal Firewall System Log Parameters and Description

The Event Log is a data sheet, where each row represents a logged event, and the columns display information regarding the event. The columns are:



**Table 18. Personal Firewall System Log Parameters and Description**

Name of Parameter	Description
Time	The date and time that the event has been logged
Type	The type of event represents an Error, Warning, or Information. An Error log indicates a problem with the source; a Warning log indicates a potential problem; and an Information log provides information about an event involving the Personal Firewall.
ID	The ID assigned to the event by the Personal Firewall
Summary	Summary description of the event

### Description and Data Fields for the System Log

Below the rows of logged events are the **Description** and **Data** fields. When you click on an event row, the entire row is highlighted. A description of the event, such as “Install WsProcessSensor successful....”, appears in the **Description** field.

### Viewing the System Log Events by Date

1. To filter the log events by date, click the **View** menu in the **Log Viewer** window.
2. Select which events you would like to view from the list:

**Table 19. Viewing Personal Firewall System Log Events by Date**

Events for...	Displays...
<b>1 Day Logs</b>	the events recorded on the current day
<b>2 Day Logs</b>	the events recorded over the past 2 days
<b>3 Day Logs</b>	the events recorded over the last 3 days, including the current day
<b>1 Week Logs</b>	the events recorded over the past 7 days
<b>2 Week Logs</b>	the events recorded over the past 14 days
<b>1 Month Logs</b>	the events recorded over the last 30 days
<b>Show All Logs</b>	all System Log events

3. The log automatically displays the requested events.

## Back Tracing Logged Events on the Personal Firewall

Back tracing enables you to pinpoint the source of data from a logged event. Like retracing a criminal's path at a crime scene, back tracing shows the exact steps that incoming traffic has made before reaching your computer and being logged by the Personal Firewall.

The option to back trace a log event is available in both the Security and Traffic logs.

### To Backtrace a Log Event

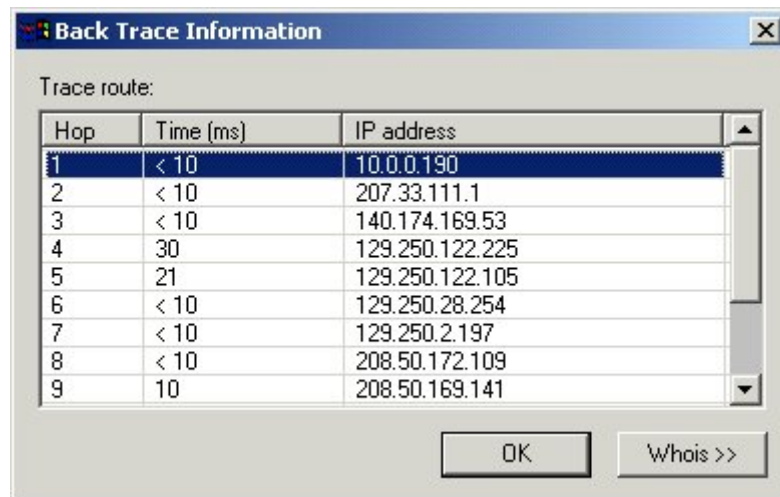
1. In an open log file, click on an event until it is highlighted.
2. Right-click on the highlighted event.

A pop-up window prompts you to **BackTrace**.

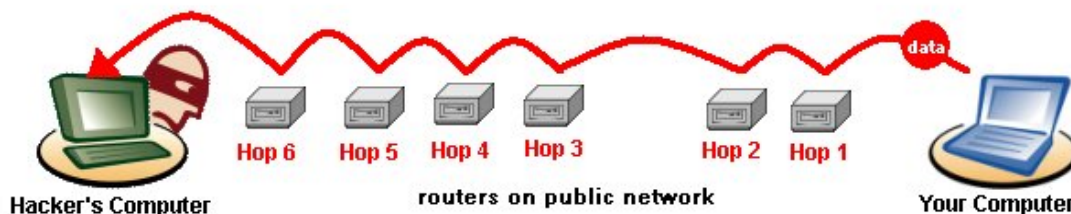
3. Click on the **BackTrace** option.

The Personal Firewall begins back tracing the event.

The **BackTrace Information** window is displayed. Information appears regarding the backtracing of the IP addresses that the log event data visited before arriving at your computer's front door.



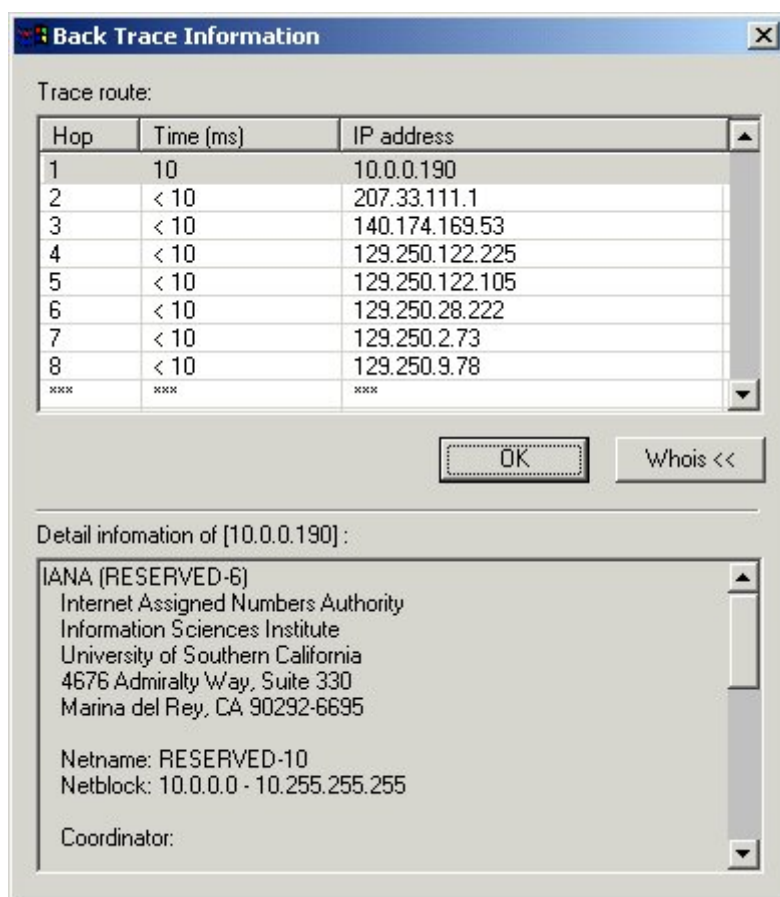
The **Trace Route** field provides details on each "hop" made by the data packet that was logged by the Personal Firewall. A "hop" is a transition point, usually a router, that a packet of information travels through at as it makes its way from one computer to another on a public network, such as the Internet.



Backtracing is the process of following a data packet backwards, discovering which routers the data took in order to reach your computer. In the case of a Security Log entry, you can trace a data packet used in an attack attempt. Each router that a data packet passes through has an IP address, which is provided in the **Trace Route** field.

## WhoIs

Clicking the **WhoIs** button prompts the Personal Firewall to pull up detailed information on each hop logged in the **Trace Route** field. The information is displayed in a drop-down Detail Information panel. Please note that the information displayed does not guarantee that you have discovered who the hacker actually is. The final hop's IP address lists the owner of the router that the hackers connected through, and not necessarily the hackers themselves.



You can cut and paste the information in the Detail information field by pressing **Control+C** to copy the information to the Windows clipboard, and then pasting it (**Control+V**) into an e-mail message to your system administrator, for example, asking about a particular site that connects to your computer.

Please note that the information provided in the **Detail Information** panel should be used responsibly. It is not advisable to contact persons listed in the **Detail Information** field unless you are experiencing a high number of security logs in which the attacks originate from one particular IP address.

## Appendix B. More About Default Values

This appendix provides a summary listing of the Personal Firewall default settings.

### Defaults: A Summary of Rules and Settings

This table provides a summary of rules and settings for the Personal Firewall.

#### Default Rules and Settings for the Personal Firewall

The following rules and settings apply:

- **VPNs enabled**—VPNs are enabled
- **IDS is enabled**—IDS is enabled immediately, and a new IDS library can be downloaded to the Personal Firewall by using the Update function
- **Ask before application use**—Ask for user permission before permitting an application to use the network and log that decision
- **Security: Normal**—The menu shows File, then Security, with the choices of Normal/Allow all/Block All. Normal is the default choice
- Popup messages enabled
- Allow ping reply
- Allow traceroute
- Browse Network Neighborhood enabled
- **Disable Network Neighborhood sharing**—Block access to any files on the end user's computer
- **Screensaver**—Ignore status
- **Windows Kernel**—Ask before permitting access
- **Block broadcast traffic**—Block all multicast and broadcast traffic and do not log it

- **Block all other traffic**—Block all remaining network traffic and log it. This is the final rule to be implemented and catches everything that has not otherwise been covered

## **Appendix C. Troubleshooting Sygate Personal Firewall Pro**

This section is designed to help you to understand some of the areas that are sometimes causes of confusion. It includes questions and answers on:

- “Firewall Configuration, Usage, and Software Expiration”
- “Firewall Protection Against Attacks, Viruses, Trojans”
- “Firewall and Internet Connection Sharing, VPNs, and Networking”

For the most up-to-date information, go to the Sygate Forums:  
<http://forums.sygate.com/vb/forumdisplay.php?s=&forumid=35>

## Firewall Configuration, Usage, and Software Expiration

The usual questions that come up in this area include:

### Can I continue using the product after the end of the upgrade protection period?

As with most software, the Personal Firewall will never stop functioning, once it has been registered. Purchasing the Upgrade Option gives you free updates and upgrades for a year, which includes updates to the Intrusion Detection signatures and upgrades to the Personal Firewall software.

### Will the Firewall work on a computer that has multiple IP addresses assigned to a single NIC?

The Personal Firewall cannot detect your network card if you are running Windows NT 4.0, Windows 2000, or Windows XP, AND if you have multiple IP addresses assigned to one of more of the network adapters. You will need to remove the other IP address if you want to run the Personal Firewall software.

### What should I do if I am having trouble with Network Shares?

In order to share files and printers, or to access mapped drives with the Personal Firewall, you must allow this feature for your inside NIC. To do this:

1. From the Main Menu, click **Tools | Options | Network Neighborhood**.
2. Enable both network settings for your inside NIC, by clicking **Allow to browse Network Neighborhood files and printer(s)**, and by clicking **Allow others to share my files and printer(s)**.
3. From the Main Menu, click **Tools | Options | Security**.
4. Be certain that **Enable driver level protection** and **NetBIOS Protection** are disabled. The default for these settings is *enabled*.
5. From the Main Menu, click **Tools | Applications**, or click the **Applications** button.
6. Set the following applications to **Allow** in the Running Applications list:
  - mpsrv
  - kernel
  - ntoskrnl
  - svchost
  - NetBeui

also, possibly set these applications to **Allow**:



- tcpsvcs
- nwlntpx.sys
- ndisui.sys
- ssdpsrv

## **Firewall Protection Against Attacks, Viruses, Trojans**

The usual questions that come up in this area include:

### **Does the Firewall protect against viruses and Trojans?**

The Personal Firewall does not check for viruses, but it works well with virus-scanning software. Programs that access the network are checked for Trojans. If one is found, the network access is blocked to that Trojan program, and the program is automatically terminated. The Personal Firewall specifies the location of the Trojans, but does not delete them from your computer.

### **After updating one of my applications, the Firewall shows a major attack. Do I have a Trojan?**

Upgrading any program will change the MD5 checksum, a value that the Personal Firewall uses to verify the integrity of each application on your computer. When the Personal Firewall sees that the executable for an application has been changed, it logs this in the Security Log with a severity of Major. If you have updated the software yourself, then there is probably no Trojan attached to it. However, if you have not updated the software and you receive this message, you should block the application and install a virus scanner using the latest signatures to remove this Trojan.

### **Does the Firewall do Stateful Packet Inspection?**

Yes, the Personal Firewall does Stateful Packet Inspection on every Remote TCP connection. The Personal Firewall also uses an algorithm to check Remote UDP and DHCP traffic to make sure that the communication is secure.

## Firewall and Internet Connection Sharing, VPNs, and Networking

The usual questions that come up in this area include:

### Is the Personal Firewall compatible with Microsoft's Internet Connection Sharing (ICS)?

Yes, it is.

### How do I configure the Personal Firewall to work with ICS?

To configure the Personal Firewall to work with ICS, all operating systems should be set as follows:

1. From the Main Menu, click **Tools | Applications**, or click the **Applications** button.
2. Set the following applications to **Allow** in the Running Applications list:
  - Kernel
  - LSA Shell
  - Generic Host Process
  - Application Layer Gateway Service (for Windows XP)
  - NCIS User mode I/O Driver

Based on the particular operating system in use, set the following applications to **Allow**:

- For Windows 98/ME:
  - ICSHAREP.VXD
  - ICSMGR.EXE
  - NDIS
  - NetBeui
  - IPX (if used)
  - Kernel
- For Windows 2000:
  - LSASS.EXE
  - TCP/IP
  - NDIS

- NetBeui
- IPX (if used)
- Kernel
- For Windows XP:
  - LSASS.EXE
  - ALG.EXE
  - NDIS
  - Kernel

### **When the Test button is clicked, the Personal Firewall starts the Internet Connection Wizard. Why?**

The Firewall service uses the Windows System Account for access. Because each user account in Windows can have different settings, sometimes the Windows System Account does not have the same Internet Explorer settings. In this case, you must manually set up the Internet Connection Wizard after clicking on one of the Firewall's built-in links.

### **How do I set up the Personal Firewall to work with my CheckPoint VPN client software?**

To allow CheckPoint's VPN client to work with the Personal Firewall, take the following steps, in order. Stop taking steps when the Firewall and VPN are both working:

1. Be sure that you have set the VPN client and all of its components to **Allow** under the Applications List.
2. Be sure that CheckPoint SecuRemote's firewall has not been enabled. If it has, you will need to take the following steps:
  - Uninstall both the Firewall and the CheckPoint VPN client
  - Reinstall the Firewall
  - Reinstall the CheckPoint VPN client software, specifying to install it *without* the CheckPoint firewall
3. Check your Traffic Logs to see if anything is being blocked when you try to use the VPN. If it is, create an Advanced Rule to allow those ports or applications.
4. Try creating an Advanced Rule to trust all traffic for the IP of your VPN server.
5. Try disabling driver level protection:
  - From the Main Menu, click **Tools | Options | Security**.

- Be certain that **Enable driver level protection** is disabled. The default for this setting is *enabled*.
6. Try disabling all security options:
- From the Main Menu, click **Tools | Options | Security**.
  - Click to clear all options.

### **What should I do if experiencing a slow or non-existent connection after installing the Personal Firewall?**

Here is the recommended procedure. Take the following steps, in order. Stop taking steps when your connection is working properly.

1. Be sure that you set your browser to **Allow** under the Applications List.
2. For DSL connections, be sure that you have set your NTS or PPPoE application to **Allow** under the Applications List.
3. Create Advanced Rules to **Allow** incoming and outgoing traffic to and from all hosts and applying to <all NICs>, as follows:
  - UDP remote and local ports 67 and 68 (one rule)
  - TCP remote and local ports 67 and 68 (one rule)
4. Create an Advanced Rule to trust the IP of your Internet Service Provider.
5. Try disabling NetBIOS protection:
  - From the Main Menu, click **Tools | Options | Security**.
  - Be certain that **NetBIOS Protection** is disabled. The default for this setting is *enabled*.
6. Try disabling driver level protection:
  - From the Main Menu, click **Tools | Options | Security**.
  - Be certain that **Enable driver level protection** is disabled. The default for this setting is *enabled*.
7. Try disabling all security options:
  - From the Main Menu, click **Tools | Options | Security**.
  - Click to clear all options.

## Should I Allow the win32 kernel core or ntkernel component? What about ICMP?

As a rule, if you are unsure about any application, you should not allow it to access the Internet. Only the applications that you specifically know about should be allowed. Under most circumstances, blocking the Windows kernel should not create a problem. However, some Internet Service Providers (ISPs) send you an ICMP message to verify that you are online. Blocking this message may cause them to turn off their interaction with your computer. If this happens, enable ICMP using the Advanced Rule editor:

1. From the Main Menu, click **Tools | Advanced Rules**. You may have to click **OK** on a warning message before entering the Editor.
2. Click **Add**. This will bring up a new rule template.
3. Give the rule a name, such as “Allow ICMP”, and then click **Allow this traffic**.
4. Click the **Ports and Protocols** tab, and select **ICMP** from the dialog box. You will get another list of options from which to choose.
5. Click **Echo Reply - 0** and **Echo Request - 8**.
6. Click **OK** to exit this rule.
7. Click **OK** to exit the Advanced Rule editor.

## Glossary

### A

**access point:** A network connection that allows a computer or user to connect to an enterprise network. Virtual Private Networks (VPNs), wireless communications, and Remote Access Service (RAS) dial-up connections are examples of access points. See also end point, wireless access point (wireless AP).

**Active Directory:** A Microsoft Windows directory service that maintains information about objects connected a network on a server called the Microsoft Windows 2000 Active Directory server. Active Directory makes it so network users can log on once to use resources (for which they have been granted access) anywhere on the network. See also directory server, LDAP.

**Active Response:** The ability to automatically block the IP address of a known intruder for a specific amount of time. The amount of time that the Sygate Personal Firewall blocks the IP address can be modified to any interval from 1 to 65,000 seconds.

**adapter:** See network adapter.

**Advanced Rule:** A rule that can be added on Sygate Personal Firewall to enforce a security policy. Advanced Rules can exhibit complex relationships between applications, IP addresses, and services. See also firewall rule, Simple Rule.

**Agent:** A computer running Sygate Security Agent software is also called an Agent computer. An Agent can be client controlled or server controlled. See also client, Client Control, Server Control, Sygate Security Agent, Sygate Personal Firewall.

**Anti-IP Spoofing:** An advanced setting that prevents an intruder from taking advantage of the ability to forge (or spoof) an individual's IP address. See also IP Spoofing.

**Anti-MAC Spoofing:** An advanced setting that prevents an intruder from taking advantage of the ability to forge (or spoof) the MAC address of an individual's computer. Anti-MAC Spoofing allows incoming and outgoing ARP traffic only if an ARP request was made to that specific host. It blocks all other unexpected ARP traffic and logs it in the security log. See also Smart ARP, MAC address, MAC Spoofing.

**antivirus:** Software and technology that is used to detect malicious computer applications, prevent them from infecting a system, and clean files or applications that are infected with computer viruses. Sygate software works together with, but does not include, antivirus software. See also virus.

**application authentication:** Authenticating an application that is running on the network by taking the entire binary of the application and doing an MD5 hash and comparing it with the application fingerprint stored on Sygate Personal Firewall. If the application was changed, it may not be authenticated depending on the rules the Firewall is using. See also application control, application fingerprint, DLL authentication, MD5 hash.

**application control:** Applications and what versions of the particular application can either be allowed or disallowed via security policies.

**application fingerprint:** A 128-bit number that is generated by performing an MD5 hash of an entire application packet. It is unique for each application. If the application is changed in any way, the application fingerprint changes.

**authorization:** The process of granting or denying access to a specific network resource or domain based on the user's identity.

## B

**backtrace:** A way of using ICMP to determine all the hops between your computer and an intruder on another computer. See also Internet Control Message Protocol (ICMP).

**broadcast:** Sending a packet to everybody on the network. See also multicast, unicast.

**buffer overflow:** Applications set aside areas of memory, or buffers, for use as storage, frequently setting aside a finite amount of memory for a buffer. A buffer overflow exists when an application attempts to store more data than can fit in a fixed-size buffer. Buffer overflow attacks occur when an intruder is able to send data in excess of a fixed-size application buffer and the application does not check to ensure this doesn't happen. By overflowing a buffer with executable code, an intruder can cause an application to perform unexpected and often malicious actions using the same privileges the application has been granted.



## C

**client:** A computer or program that uses shared resources from another computer, called a server.

**computers:** A personal computer, laptop, or workstation where users perform their work. In an enterprise environment, computers are connected together over a network.

## D

**Data Encryption Standard (DES):** An algorithm for protecting data using private encryption keys. DES-CBC is the Cipher Block Chaining (CBC) mode of DES, a stronger form of encryption, which applies an exclusive OR to each block of data with the previous block and then encrypts the data using the DES encryption key. 3DES or Triple DES is the strongest form of encryption where each data block is encrypted three times with different keys. See also encryption.

**demilitarized zone (DMZ):** A security measure used by a company that can host Internet services and has devices accessible to the Internet; the DMZ is an area between the Internet and the internal network that prevents unauthorized access to the internal corporate network using a firewall or gateway.

**Denial of Service (DoS):** A network-based attack that is characterized by an explicit attempt by an intruder to prevent legitimate users of a service from using that service. See also Denial of Service Checking.

**Denial of Service Checking:** An advanced setting that instructs the Sygate Personal Firewall to check for incoming traffic using known Denial of Service (DoS) techniques.

**DES:** See Data Encryption Standard (DES).

**destination IP address:** The IP address of the computer that is receiving packets of information.

**destination port:** The port of the computer that is receiving packets of information.

**DHCP:** See Dynamic Host Configuration Protocol (DHCP).

**directory server:** Software that manages users' accounts and network permissions. Active Directory is an example of a directory server accessed using Lightweight Directory Access Protocol (LDAP). See also Active Directory, Lightweight Directory Access Protocol (LDAP).

**DLL:** Dynamic link library, a list of functions or data used by Windows applications. Most DLLs have a file extension of .dll, .ocx, .exe, .drv, or .fon.

**DLL authentication:** The ability to validate shared or application-specific dynamic link libraries (DLLs) and ensure the integrity of applications. The Sygate Personal Firewall can be instructed to allow or block known DLLs. An added level of protection can also be enabled to block DLLs from being dynamically allowed when an application is executed. See also application authentication, application fingerprint, DLL, DLL fingerprint.

**DLL fingerprint:** A 128-bit number that is generated by performing an MD5 hash of an entire DLL packet. It is unique for each DLL. The MD5 hash or fingerprint of each DLL is stored on the Sygate Personal Firewall. If the DLL is changed in any way, the DLL fingerprint changes. See also DLL, DLL authentication, MD5 hash.

**domain:** A group of computers that are part of a network and share a common directory database. Each domain has a unique name and is organized in levels that are administered as a unit using common rules.

**domain name:** The name by which a group of computers is known to the network. Most organizations have a unique name on the Internet that allows individuals, groups, and other organizations to communicate with them. See also domain.

**DoS attack:** See Denial of Service (DoS).

**driver-level protection:** A Sygate software feature that blocks protocol drivers from gaining access to the network unless a user gives permission. If a protocol driver attempts to gain access to the network through a client running the Sygate Personal Firewall, depending on the rule set, the protocol driver is allowed, blocked, or a pop-up message displays. See also protocol driver blocking.

**Dynamic Host Configuration Protocol (DHCP):** A TCP/IP protocol that provides dynamic configuration of host IP addresses and enables individual computers on an IP network to extract configuration parameters from a DHCP server. DHCP lets a system administrator supervise and distribute IP addresses from a central point in the network.

## E

**encryption:** The use of an algorithm to convert typically sensitive data into a form that is unreadable except by authorized users. See also Communications Channel Encryption.

**endpoint:** Any network device that connects to the enterprise network and runs network-based applications. Network devices can include laptops, desktop computers, servers, and PDAs. See also access point.

## F

**filtering logs:** Viewing selected information from logged information. For example, a filter can be set up so that you can view only blocked traffic, critical information, or logged events occurring during the past day. See also logs.

**firewall:** Hardware, software, or a combination of both that is used to prevent unauthorized Internet users from accessing a private network. All information entering or leaving the network must pass through the firewall, which examines the information packets and blocks those which do not meet the security criteria. The Sygate Personal Firewall Allows, Blocks, or Asks whether incoming traffic is allowed to access an organization's network or resources. By using firewall rules, the Firewall can systematically allow, block, and ask incoming traffic from specific IP addresses and ports. See also firewall rule.

**firewall rule:** A stipulation that helps to determine whether or not a computer can gain access to a network. For example, a firewall rule may state "Port 80 is allowed."

**Fragmented Packets:** A packet that is broken into smaller pieces to send the packet more efficiently through an organization's network or Internet. When Allow Fragmented Packets is enabled, the Firewall automatically allows the fragmented packets. See also packet.

## H

**hijack:** A type of attack where an intruder takes control of an existing communication session between a server and a legitimate user who has connected and authenticated with the server. The intruder can monitor the session passively recording the transfer of sensitive information such as passwords and code. Another type of hijacking involves an active attack done by forcing the user offline (with a Denial of Service attack) and taking over the session. The intruder begins acting like the user, executing commands, and sending information to the server.

**Host Integrity:** The ability to define, enforce, and restore the security of clients in order to secure enterprise networks and data. Host Integrity rules can be set up to verify that clients attempting network access are running antivirus software, patches, and hot fixes and other application criteria. This is a feature of Sygate Secure Enterprise. See also Sygate Enforcer.

**Host Integrity Remediation:** A feature that allows an automatic system update, if needed. Working together with the Sygate Enforcer, Host Integrity rules can be set up to verify that clients attempting access are running antivirus software, patches, and hot fixes, as well as checking specified registry key values, then update the client's system and files automatically if they are out of date. Formerly called Host Integrity Restoration. This is a feature of Sygate Secure Enterprise.

**Host Integrity Restoration:** See Host Integrity Remediation.

## I

**ICMP:** See Internet Control Message Protocol (ICMP).

**icon:** A small visual image displayed on a computer screen to represent an application, a command, an object, or to indicate status. Icons shown on screens in Sygate software are also used to display status. For example, in the Sygate Personal Firewall interface, blinking blue lights indicate incoming and outgoing traffic.

**IDS:** See Intrusion Detection System (IDS).

**inbound traffic:** Traffic that was initiated from a remote computer. See also outbound traffic.

**Internet Control Message Protocol (ICMP):** An Internet protocol (defined in RFC 792) that is primarily for reporting errors in TCP/IP messages and exchanging limited status and control information.

**Internet Information Services (IIS):** Web services software from Microsoft that is the Hypertext Transport Protocol (HTTP) server for the Microsoft Windows platform.

**Intrusion Detection System (IDS):** A device or software that detects and notifies a user or enterprise of unauthorized or anomalous access to a network or computer system. Sygate's IDS operates on every machine in an enterprise on which the Sygate Personal Firewall is installed by analyzing network packets targeted at the network node and comparing them with signature database entries. An IDS helps identify attacks and probes by monitoring traffic for attack signatures that represent hostile activity. See also Intrusion Prevention System (IPS).

**Intrusion Prevention System (IPS):** A device or software used to prevent intruders from accessing systems from malicious or suspicious activity. This is contrast to an Intrusion Detection System (IDS), which merely detects and notifies. Sygate Personal Firewall is both an IDS and an IPS product since the Firewall includes both an IDS and firewall functionality making it capable of not only detecting but also blocking an attack. See also Intrusion Detection System (IDS).

**IP address:** A 32-bit address used to identify a node on a network. Each node on the network must be assigned a unique address in dotted decimal notation, such as 125.132.42.7. See also local IP address, remote IP address.

**IP fragmentation:** A packet that has been split into two or more packets. The Sygate Personal Firewall supports IP fragmentation, the ability to receive or send incomplete packets over the network. See also packets, Fragmented Packets.

**IP spoofing:** IP spoofing is a process where an intruder uses an IP address of another computer to acquire information or gain access. Because the intruder appears to be someone else, if a reply is sent, it goes to the spoofed address, not the intruder's address. See also Anti-IP Spoofing.

**IPS:** See Intrusion Prevention System (IPS).

## L

**LDAP:** See Lightweight Directory Access Protocol (LDAP).

**library:** See signature library, System Library, custom library.

**Lightweight Directory Access Protocol (LDAP):** A standard directory access protocol for searching and updating information directories containing, for example, email addresses, phone numbers, and computer names and addresses. LDAP is the primary protocol used to access directory servers such as Active Directory. See also Active Directory, directory server.

**local IP address:** From the perspective of the Firewall, the IP address of the computer the user is working on. See also IP address.

**local port:** From the perspective of the Sygate Personal Firewall, the port on the computer being used for this connection. See also port.

**Log Dampener:** An option that causes the Sygate Personal Firewall to log only one event if multiple similar events happen in a relatively short time frame. This protects the Firewall from being inundated by hundreds or thousands of events happening at the same time in a DoS attack. For example, if a thousand packets are received in one second, the Firewall logs that the event happened a thousand times. See also logs.

**logs:** Files that store information generated by an application, service, or operating system. The information is used to track the operations performed.

**lsass.exe:** A Local Security Authority Service Executable and Server DLL on the Windows operating system. It is a Windows security mechanism used to verify user logins.

## M

**MAC address:** A vendor hardware address that identifies computers, servers, routers, or other network devices. See also Anti-MAC Spoofing.

**MAC Spoofing:** Intruders use a technique called MAC (media access control) spoofing to hack into a victim's computer by using the MAC address of another computer to send an ARP (Address Resolution Protocol) response packet to the victim even though the victim did not send an ARP request. The victim host renews the internal ARP table using the malicious ARP response packet. See also Anti-MAC Spoofing.

**mapisp32.exe:** Microsoft Windows Messaging Subsystem Spooler, allows mail applications to use a standard Messaging Application Program Interface (MAPI) to access messages, addresses, and transport services.

**MD5 hash:** A one-way function that produces a unique 128-bit value. MD5 hashing transforms information and produces a value that it cannot be changed back into its original form. This method is used for encrypted authentication (for example, verifying passwords or authenticating applications).

**mstask.exe:** The Task Scheduler engine used by the Windows operating system.

**multicast:** Sending a message simultaneously to more than one destination on a network. See also broadcast, unicast.

## N

**NetBIOS protection:** A feature on the Sygate Personal Firewall that blocks all communication from computers located outside the client's local subnet range. NetBIOS traffic is blocked on UDP ports 88, 137, and 138 and TCP ports 135, 139, 445, and 1026. See also subnet.

**network adapter:** A device that connects a computer to a network.

**network interface card (NIC):** A device that is installed in a computer that provides the ability to communicate with other connected devices on the network.

**ntoskrnl.exe:** NT Kernel & System, a standard Windows service that initializes the kernel and drivers needed during a session.

## O

**OS Fingerprint Masquerading:** A feature that keeps programs from detecting the operating system of a computer running the Sygate Personal Firewall software. When OS Fingerprint Masquerading is enabled, the Firewall modifies TCP/IP packets so it is not possible to determine its operating system.

**outbound traffic:** Traffic that was initiated from the local computer. See also inbound traffic.

## P

**packet:** A unit of data sent over a network. It is accompanied by a packet header that includes information, such as the message length, priority, checksum, and the source and destination address. When packets are sent over a network protected by Sygate Personal Firewall, each packet is evaluated for specific patterns that indicate known attacks. If a match occurs, the attack is blocked. See also Fragmented Packets.

**policy:** See security policy.

**port:** A connection on a computer where devices that pass data to and from the computer are physically connected. Ports are numbered from 0 to 65535. Ports 0 to 1024 are reserved for use by certain privileged services. See also Authentication port, local port, remote port, source port.

**port scan:** A method that hackers use to determine which of your computer's ports are open to communication. It is done by sending messages to computer ports to locate points of vulnerability. Although it can be a precursor to an intrusion attempt, port scanning does not in itself provide access to a remote system. See also Portscan Checking.

**Portscan Checking:** An option on the Sygate Personal Firewall that monitors all incoming packets that are blocked by any security rule. If several different packets were blocked on different ports in a short period of time, a security log entry is generated. Portscan Checking does not block any packets. A security policy needs to be created to block traffic in the event that a port scan occurs.

**priority:** The order in which rules take effect. Rules with a higher priority (0 being highest, 15 being lowest) take effect before rules with lower priority. Advanced Rules, by default, have a priority of 5.

**protocol driver blocking:** A security measure that blocks malicious applications from using their own protocol driver to exit the network surreptitiously.

## R

**registration code:** An alphanumeric value that must be specified during the installation of the Sygate Personal Firewall Pro.

**remote IP address:** The IP address of the computer to which information is being transmitted.

**remote port:** A port on another computer attempting to transmit information over a network connection.

**restoration:** See Host Integrity remediation.

**rule:** See Advanced Rule, firewall rule, Simple Rule.

**Running Applications list:** Located below the traffic flow graphs; a list of all applications and services that are currently accessing (or attempting to access) a Firewall's network connection. The status of the applications is also displayed.

## S

**Schedule:** An Advanced Rule that allows for triggering an event at certain times of the day.

**security alerts:** A sound or notification indicating that the Sygate Personal Firewall has detected an attack against the client computer.

**server:** A computer on a network that manages network resources for one or more clients.

**service:** A network port, a UDP port, an IP protocol type, or an ICMP type.

**services.exe:** Services and Controller application, a standard controller that manages many Windows services.

**severity:** A mechanism for Sygate Personal Firewall logging system that indicates how critical an event is. Severity ranges from 0 to 15, where 0 is the most critical and 15 is least critical.

**signature:** A rule that defines how to identify an intrusion. Sygate's Intrusion Detection System identifies known attacks by pattern-matching against rules or 'signatures' stored in the System Library or a custom library. See also signature library, System Library.

**signature library:** A set of IDS signatures. Sygate provides a library of known signatures in the System Library, which can be kept up-to-date by downloading the latest version from the Sygate Technologies web site to your Sygate Personal Firewall Pro. See also System Library.

**Smart ARP:** An advanced security setting for Sygate Personal Firewall that allows Address Resolution Protocol (ARP) requests only if the machine that sent the incoming packet is recognized within the enterprise's network address space. If the incoming network request is not recognized from being with the enterprise's network address space, the request is blocked.

**Smart DHCP:** Allows a DHCP client to receive an IP address from a DHCP server while protecting against DHCP attacks from the network. Sygate Personal Firewall software allows an incoming DHCP response for five seconds if that system is awaiting a response from a DHCP request. If no DHCP request was made by the Firewall system, Smart DHCP does not allow the packet. Note that Smart DHCP does not block any packets; blocking is done by the normal security rule set. See also Dynamic Host Configuration Protocol (DHCP).



**Smart DNS:** Allows a Domain Name Server (DNS) client to resolve a domain name from a DNS server while providing protection against DNS attacks from the network. This option blocks all Domain Name Server (DNS) traffic, except outgoing DNS requests and the corresponding reply. If the client computer sends out a DNS request and another computer responds within five seconds, the communication is allowed. All other DNS packets are dropped. Smart DNS does not block any packets; blocking is done by the normal security rule set.

**Smart WINS:** Allows Windows Internet Naming Service (WINS) requests only if they were solicited. If the traffic was not requested, the WINS reply is blocked.

**sniffing:** The process of actively capturing datagram and packet information from a selected network. Sniffing acquires all network traffic regardless of where the packets are addressed.

**source IP address:** The IP address from which the traffic originated. See also IP address.

**source port:** The port number on which the traffic originated. See also port.

**spoofing:** A technique used by an intruder to gain unauthorized network access to a computer system or network by forging known network credentials. IP spoofing is a common method for intruders to gain unauthorized network access to a computer systems or network.

**Stealth Mode Browsing:** An option that detects all HTTP traffic on port 80 from a web browser and removes information such as the browser name and version, the operating system, and the reference web page. It will stop web sites from knowing which operating system and browser you are using. Stealth Mode Browsing may cause some web sites not to function properly, because it removes the browser signature, called the HTTP\_USER\_AGENT, from the HTTP request header and replaces it with a generic signature.

**subnet:** Portions of a TCP/IP network used to increase the bandwidth on the network by subdividing the network into portions or segments. All IP addresses within a subnet use the same first three sets of numbers (such as 192.168.1 in 192.168.1.180 and 192.168.1.170) indicating they are on the same network. A subnet is See also subnet mask.

**subnet mask:** A value that allows a network to be subdivided and provides for more complex address assignments. The subnet mask format is nnn.nnn.nnn.nnn (such as 255.255.255.0).

**svchost.exe:** Generic Host Process for Win32 Services, a generic host process for services that are run from dynamic link libraries (DLLs). It checks the services portion of the registry to create a list of services it needs to load. Multiple instances of Svchost.exe may be running at the same time.

**Sygate Endpoint Enforcement:** The ability of the Sygate Security Agent to execute Host Integrity rules independent of the Sygate Enforcer. The Agent can take an action if the Host Integrity rules fail, block access to the enterprise network by switching to a quarantine location, and then initiate the appropriate restorative action.

**Sygate Enforcer:** A software component that allows only remote and wireless clients running the Sygate Security Agent and complying with Host Integrity rules to gain access to the enterprise network. Sygate Enforcers can secure various places on the network to protect entry through a VPN server, wireless LAN, and to safeguard servers. When a client attempts to access the enterprise network, the Enforcer requests the unique ID assigned to the Agent to verify that it is a legitimate client. The policy of the particular client is verified and Host Integrity rules are checked before allowing access to the network. If a client does not satisfy the Enforcer's qualifications and a rule fails, the Enforcer can monitor and log certain events, block certain users if the Host Integrity rules fail, display a popup message, or quarantine the computer in a restricted area until the software is updated.

**Sygate Management Server:** A centralized point of control over all Sygate Security Agents that enables network administrators to define and distribute security policies, collect logs, and maintain the integrity of the corporate network. Also referred to as the Management Server in Sygate documentation. See also Sygate Security Agent.

**Sygate Personal Firewall:** A host-based firewall whereby the users define their own security policies, including many of the capabilities of Sygate Security Agent, but without the enterprise management features. See also Sygate Security Agent.

**Sygate Secure Enterprise:** A software suite that includes the Sygate Management Server, one or more Sygate Security Agents, the Sygate Event Logger, and optionally, one or more Sygate Enforcers. It protects wireless, VPN and wireless connected laptops, workstations, and servers with firewall, intrusion detection, and policy enforcement. See also Sygate Security Agent, Sygate Enforcer, Sygate Event Logger, Sygate Management Server.

**Sygate Security Agent:** Software component that enforces rule-based security on devices, whether remote or behind a corporate firewall, using security policies defined on the Sygate Management Server. Also referred to as the Agent in Sygate documentation. The Agent must be installed on every device before it can connect to the enterprise network. The Agent can detect, identify, and block known Trojans and Denial of Service attacks, and also protects against new or unknown attacks by blocking applications and traffic that violates a defined set of security policies. Port scans are also detected and logged to alert users and system administrators of potential attacks, while maintaining system security.

**synchronization:** Refers to automatically keeping directory servers up to date with the user database including synchronizing between LDAP, Active Directory, and NT Domain. System administrators can specify how often to synchronize the user database with the directory server. See also Active Directory, Lightweight Directory Access Protocol (LDAP).

**System Library:** A Sygate library containing preconfigured IDS signatures to help detect and prevent known attacks. See also custom library, signature library.

**system tray:** The lower right section of the taskbar on the Windows desktop, which is used to display a clock and icons representing certain programs such as volume control, network connection status, and antivirus software. The Sygate Personal Firewall icon can be displayed here.

## T

**Transmission Control Protocol/Internet Protocol (TCP/IP):** Internet protocols that every Internet user and every Internet server uses to communicate and transfer data over networks. TCP packages the data into packets that get sent over the Internet and are reassembled at their destination. IP handles the addressing and routing of each data packet so it is sent to the correct destination.

**trigger:** An event that causes a rule to take effect. When creating rules, you can assign specific triggers, which cause Firewalls to react in a specific way, and actions, which specify what to do when the trigger takes place. For example, you can block all traffic originating from a certain IP address or block traffic during certain hours of the day. Triggers can be linked to specific applications, hosts, schedules, and services.

**Trojan, Trojan horse:** An application that carries out an unauthorized function covertly while running an authorized application. It is designed to do something other than what it claims to, and frequently is destructive in its actions. The Sygate Personal Firewall automatically detects and terminates known Trojan horse applications before the Trojan horse attempts to communicate.

**trusted application:** An application that is allowed to run on a Sygate Personal Firewall. See also application authentication, Application Learning.

## U

**UDP:** See User Datagram Protocol (UDP).

**unicast:** Sending a message to one specific computer. See also broadcast, multicast.

**User Datagram Protocol (UDP):** A communications protocol for the Internet network layer, transport layer, and session layer that uses the Internet Protocol (IP) when sending a datagram message from one computer to another. UDP does not guarantee reliable communication or provide validated sequencing of the packets.

## V

**virtual private network (VPN):** A secure network connection that interconnects different corporate network sites, allows remote users to connect to the enterprise network, and allows controlled access to different corporate networks. Although a VPN provides a secure tunnel for network traffic, it leaves the connection points open to attack.

**virus:** A program that is designed to spread from computer to computer on its own, potentially damaging the system software by corrupting or erasing data, using available memory, or by annoying the user by altering data. A virus is designed to replicate. Generally, it is spread by infecting other files.

**vulnerability scan:** An attempt to use security attacks to detect security weaknesses in a computer. The Sygate Personal Firewall includes a Test button that assesses an Firewall's vulnerability to attack. It requires a public IP address. See also port scan.

## W

**wireless access point (wireless AP):** A network connection that allows a computer or user to connect to an enterprise network without the use of a hardwired connection to the network. See also access point, end point.

**worm:** A type of computer virus that can replicate itself over a computer network and perform destructive tasks such as using up computer memory resources. Worms do not infect other files as viruses typically do, but instead worms make copies of themselves over and over depleting system resources (hard drive space) or depleting bandwidth (by spreading over shared network resources). See also virus.