



# Sunbelt **PersonalFirewall4**

## User Guide

Use of this software is subject to the End User License Agreement found in this User Guide (the License Agreement). By installing the software, you agree to accept the terms of the License Agreement. Copyright (c) 2007 Sunbelt Software. All rights reserved. All products mentioned are trademarks or registered trademarks of their respective companies. Information in this document is subject to change without notice. No part of this publication may be reproduced, photocopied, stored in a retrieval system, transmitted, or translated into any language without the prior written permission of Sunbelt Software, Inc.

# Contents

---

<b>Introduction</b> .....	<b>1-1</b>
Before You Start .....	1-2
Overview .....	1-2
Components .....	1-3
Functions and Features .....	1-4
System Requirements .....	1-4
Conflicting Software .....	1-5
Styles and References .....	1-5
<b>Installation</b> .....	<b>2-1</b>
Before You Install .....	2-2
Installation .....	2-2
Initial Settings .....	2-8
Upgrading to a New Version .....	2-8
Uninstalling the Personal Firewall .....	2-9
Updating the current version .....	2-10
<b>Purchasing and Product Registration</b> .....	<b>3-1</b>
Free Version vs. Full Version .....	3-2
Purchasing Sunbelt Personal Firewall .....	3-2
Product Registration .....	3-3
<b>Firewall Components and Basic Control Features</b> .....	<b>4-1</b>
Components .....	4-2
System Tray Icons .....	4-2
<b>Firewall Behavior and User Interaction</b> .....	<b>5-1</b>
Firewall Behavior .....	5-2
Connection Alert .....	5-3
Application Alert .....	5-6
Host Intrusion Alerts .....	5-8
Alerts For Connections with Rules .....	5-10
<b>Basic Firewall Configuration</b> .....	<b>6-1</b>
The Interface .....	6-2
Working with Network Connections .....	6-5
Working with Statistics .....	6-7
Setting Firewall Preferences .....	6-9
<b>Network Security</b> .....	<b>7-1</b>
What is Network Security? .....	7-2
Rules .....	7-2
How are Rules Applied? .....	7-2
Application Rules .....	7-3
Packet Filter Rules .....	7-7
Predefined Rules .....	7-20
Trusted Area .....	7-22
Advanced settings .....	7-23
Boot time Protection .....	7-24
Detecting New Network Interfaces .....	7-25
Checking Dialed Telephone Numbers .....	7-26
<b>Internal Firewall Rules</b> .....	<b>8-1</b>
Internal Network Traffic Rules .....	8-2
System Security Rules .....	8-4

AVG Component Rules .....	8-6
<b>Intrusion Detection .....</b>	<b>9-1</b>
Intrusions .....	9-2
Network Intrusion Prevention System (NIPS) .....	9-3
Host Intrusion and Prevention System (HIPS) .....	9-5
Application Behavior Blocking .....	9-9
<b>Web Content Filtering .....</b>	<b>10-1</b>
Ad Blocking, Privacy and Site Exception Parameters .....	10-2
Site Exceptions .....	10-5
<b>Logs &amp; Alerts .....</b>	<b>11-1</b>
Viewing Logs and Alerts .....	11-2
Context Menu .....	11-3
Log Options .....	11-4
Network Log .....	11-5
NIPS Log .....	11-6
HIPS Log .....	11-7
Behavior Log .....	11-8
Web Log .....	11-9
Debug, Error, Warning Logs .....	11-10
<b>Open-source libraries .....</b>	<b>12-1</b>
<b>Glossary .....</b>	<b>13-1</b>



## Introduction

---

Welcome to the Sunbelt Personal Firewall User Guide. This guide provides in-depth information and procedures that will not only help you to understand Sunbelt Personal Firewall, but also walk you through the steps needed to protect your computer or computer network.

Section	Page
Overview	1-2
Components	1-3
Functions and Features	1-4
System Requirements	1-4
Conflicting Software	1-5
Styles and References	1-5

## Before You Start

Anyone, from novices to advanced computer users, can use Sunbelt Personal Firewall (SKPF). However, novice computer users who do not have in-depth computer or networking knowledge, should install the Personal Firewall in *Simple* mode. Advanced computer users can install SKPF in *Advanced* mode. *To learn more about Simple vs. Advanced mode, see Initial Settings, page 2-8.*

## Overview

The Personal Firewall controls how computers share information through the Internet or a local network. It also protects computers from external or internal attacks by other computers. The Personal Firewall is especially useful for laptops since they are easier to compromise because of the increasing popularity of built-in wireless access.



**Note:** *Built-in Wireless access is when a computer has a device inside of it that allows you to connect to the internet from anywhere without needing to plug it into a connection.*

### What is a Firewall?

Basically, a firewall is a program that protects one computer from other computers. It examines information that tries to enter a computer from the outside (i.e. the internet), and determines if the information is safe or harmful.

### Our Solution

Potential intruders use various methods to determine if a computer is vulnerable to attacks. These methods vary from simply scanning the computer to far more sophisticated methods such as hacking. Sunbelt Personal Firewall uses a built-in intrusion prevention system that identifies and blocks both known and unknown attacks so you can breathe easy while surfing the web. It really is an essential element of Internet security.

### Glossary

This guide uses many technical terms. If specific terms or concepts are not clear, *refer the glossary on page 13-1*, for more information.

### Online Help

In addition to the user guide, we provide extensive online help from within the application. Press **F1** or the **Help** button at the bottom of any window while using the Personal Firewall console to open the online help.

## Components

Sunbelt Personal Firewall uses several components to protect your computer.

### Network Security

Network Security controls all communication inside your computer network and between your computer and the outside world. Network Security allows you to apply two types of rules:

- Application – permit or deny network application communication.
- Packet filter – permit or deny parts of messages.

The Personal Firewall includes set of predefined network security rules (i.e. for DNS, DHCP, etc.). These rules are separate from user-defined rules and can be enabled or disabled at any time. Whenever the Personal Firewall detects traffic that does not match the criteria for a rule, a dialog box opens asking the user to permit or deny the communication. An application or packet filter rule can also be created at that time.

### Behavior Blocking

The Behavior Blocking module controls applications that are running. It controls the following types of events:

- Running applications
- Replacing an application executable file
- Applications being run by other applications

In case of network traffic, you can define rules for individual applications. These rules permit or deny certain types of communications. Again, if a communication or event does not match the criteria for a rule, a dialog box opens and asks the user to permit or deny the communication.



**Note:** *Sunbelt Personal Firewall 4 controls all running applications, regardless if they participate communicate with the network or not. When a computer is infected, the firewall is more reliable than antivirus software. This is especially true if the virus is new and is not included in a particular virus database. Sunbelt Personal Firewall detects the attempt to replace the executable file and warns user.*

### Network Intrusion detection and Prevention (NIPS)

The Network Intrusion detection and Prevention System (NIPS) can identify, block and log known intrusion types. Sunbelt Personal Firewall uses a database of known intrusions that is updated regularly (The updated database is included with new versions of the firewall).

### Host Intrusion detection and Prevention (HIPS)

The Host Intrusion and Prevention System (HIPS) detects attempts to misuse applications that are running and attempt to execute malicious code.

### Web content filtering

Web content filtering enables the following features:

- blocks ads (according to URI/URL rules), scripts and other Web items
- blocks pop-up windows
- blocks scripts (JavaScript, VBScript)
- protects user computers from undesirable cookies and stops private information from being accessed through Web application forms.

You can define more specific settings for trusted servers and for cases when filtering might cause errors.

### Boot time protection

Boot time protection protects computers even when the firewall is not running (i.e. during a system reboot or when installing of a new version of the firewall).

## Functions and Features

Sunbelt Personal Firewall provides the following functions and features:

**Stop all traffic** – stops all traffic on the computer. This function can be helpful especially when undesirable or strange network activity is detected. Traffic can be restored after the appropriate security actions are taken.

**Logging** – Each firewall module creates an independent log that is stored in a text file. Logs can be viewed in a configuration dialog. Logs can also be stored on a Syslog server.

**Connections overview and statistics** – The overview provides information about established connections and ports opened by individual applications. Information on the current speed and size of transmitted data in both directions is also provided for active connections. The overview is automatically refreshed in predefined time intervals. Statistics show users the number of objects blocked by the Web content filter and the number of detected intrusions during specific time periods.

**Automatic update** – Regular checks are made for newer versions of the firewall. Whenever a new version is detected, users have the option of downloading and installing it. It is also possible to check for new versions manually.



**Warning:** *Sunbelt Personal Firewall 4 cannot be used on Windows NT Server, Windows 2000 Server and Windows Server 2003.*

## System Requirements

The following hardware and software is required to install Sunbelt Personal Firewall:

- Windows 2000 Professional, XP Home, XP Professional, and XP Media Center Edition operating systems
- CPU Intel Pentium or 100% compatible
- 64 MB RAM
- 10 MB of free disc space
- minimal screen resolution 800x600 pixels



**Note:** *Sunbelt Personal Firewall 4 does not run on Windows NT, Windows 2000 Server, Windows 2003 Server, 95, 98, ME, and 64 bit Versions of Windows.*



## Conflicting Software

Sunbelt Personal Firewall might conflict with applications that are based on identical or similar technologies. Sunbelt Software does not guarantee the Sunbelt Personal Firewall or your operating system will function correctly if the following types software applications are installed on the same operating system:

- **Personal firewalls** – Personal firewalls provide similar functions to Sunbelt Personal Firewall.
- **Network firewalls** – Network firewalls also protect computers. It is not necessary to use a personal firewall on a computer protected by a network firewall.






**Note:** *Sunbelt Personal Firewall can be combined with a router or a proxy server to create a basic network firewall. For more information on routers and proxy servers, go to the Glossary on page 13-1.*

As general rule, do not combine Sunbelt Personal Firewall with other firewalls.

## Styles and References

This guide uses the following styles and graphical references:

Style / Graphic	Used to:
ALL CAPS	indicate a keyboard button (Press ENTER).
<b>BOLD</b>	indicate a specific field, prompt, dialog, or Window (Type an IP address in the <b>Address</b> field).
<b><i>BOLD ITALIC</i></b>	indicate the action of clicking action buttons, Keys, links, menu bar items and menu selections ( <b><i>OK, Close, etc.</i></b> ).
<i>Italic</i>	emphasize program titles, window and web page names, key words, and “see” references. (Open the <i>Administrator Resource</i> web page).
<b>Word&gt;Strings</b>	indicate a series of menu selections (Click <b>View</b> on the main menu bar; then, select <b>Policy&gt;Default</b> ).
	caution users about a specific action.
	warn users of the consequences related to specific actions or about specific information they need to know before moving forward.
	alert users to a notation or tip relevant to the current topic.



## Installation

---

Now that Sunbelt Personal Firewall has been properly introduced, it is time to install it. This chapter covers the following topics:

Section	Page
Before You Install	2-2
Installation	2-2
Initial Settings	2-8
Upgrading to a New Version	2-8
Uninstalling the Personal Firewall	2-9
Updating the Current Version	2-10

## Before You Install

We have a few suggestions on how you can prepare your computer before installing the personal firewall:

- Uninstall other firewall programs and restart the computer. Removing other personal firewall programs is required before using Sunbelt Personal Firewall. To uninstall other firewall programs, see the user documentation for those programs.
- Close all other Windows programs, including programs displayed in the Windows system tray.



**Note:** If you have an older version of the personal firewall, remove it before installing the new version.

## Installation

Sunbelt Personal Firewall comes with a quick and easy-to-use InstallShield Wizard.

### To install Sunbelt Personal Firewall

- 1 Make a selection:

If...	...then...
Sunbelt Personal Firewall is being installed from a CD,	insert the CD in the disk drive. The installation should start automatically. If not, open <b>Windows Explorer</b> , navigate to the CD drive; then, double-click the <i>setup.exe</i> icon.
Sunbelt Personal Firewall is being installed from a download, open <b>Windows Explorer</b> , navigate to location where the <i>setup.exe</i> is saved,	double-click the icon to open the wizard.

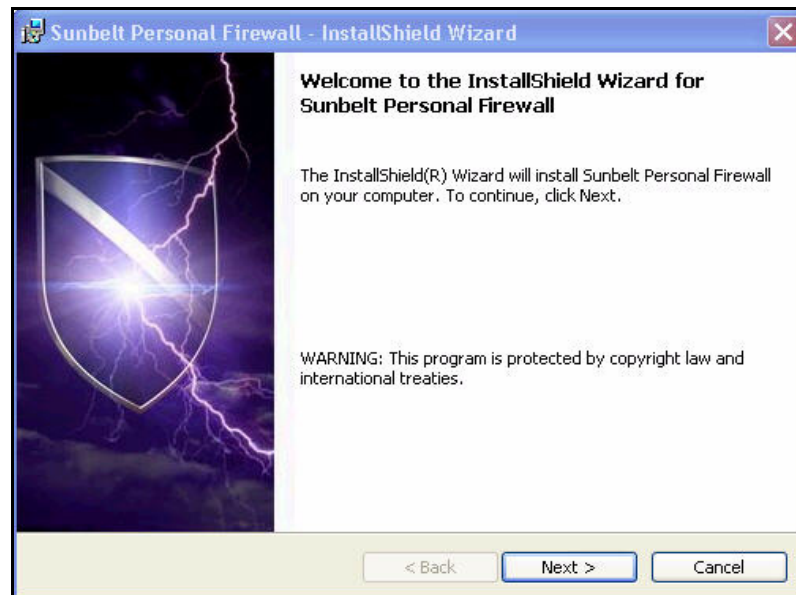


Figure 2-1 Installation Wizard: Welcome

- 2 Click **Next**. The **What's New** window opens. Scroll through the list to read about the changes between the last versions and the current one.

- 3 Click **Next**. The **License Agreement** window opens.



Figure 2-2 Installation Wizard: License Agreement

- 4 Make a selection:

To...	...select...
accept the license agreement,	<b>I accept the terms in the license agreement</b> ; then, click <b>Next</b> . The <b>Destination Folder</b> window opens. <i>Go to step 5.</i>
decline the license agreement,	<b>I do not accept the terms in the license agreement</b> ; then, click <b>Cancel</b> . The wizard closes.

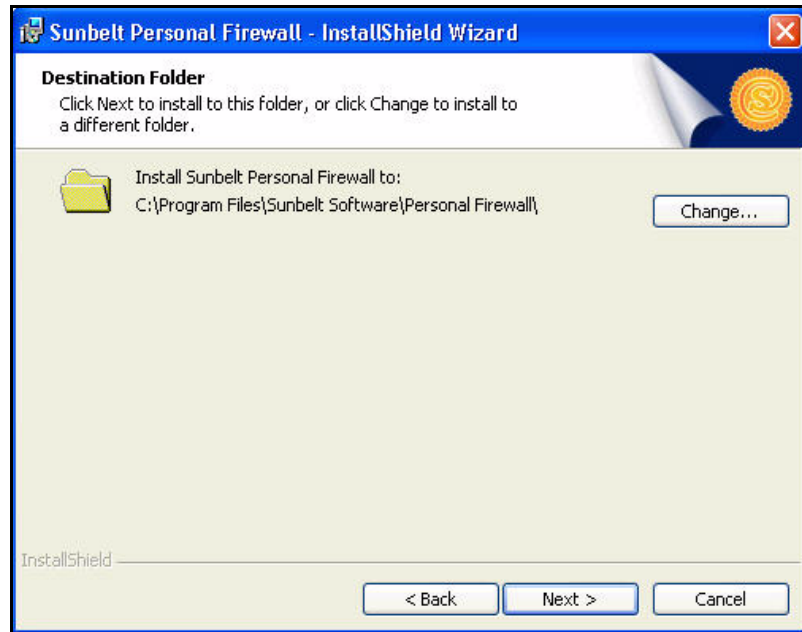


Figure 2-3 Installation Wizard: Installation Folder

5 Make a selection:

To...	...click...
accept the default folder (recommended),	<b>Next.</b> The <b>Initial firewall setting</b> window opens.
select a new folder in which to install the personal firewall,	<b>Change.</b> The <b>Change Folder</b> window opens. Select a new folder, click <b>OK</b> ; then, click <b>Next.</b> The <b>Initial firewall setting</b> window opens.  <b>Note:</b> We recommend that you keep the default selection.

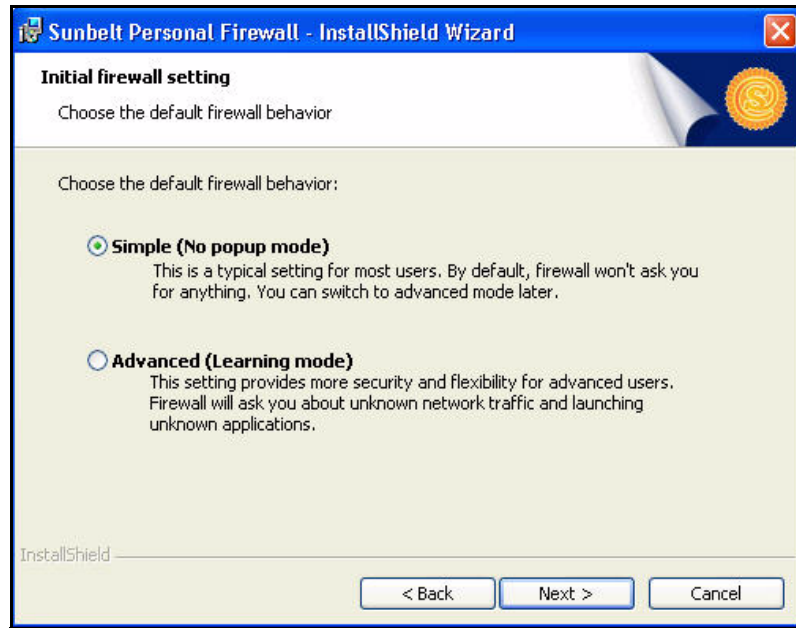


Figure 2-4 Installation Wizard: Initial Firewall Settings

6 Make a selection regarding the initial settings for the firewall:

To...	...select...
set the initial firewall settings to a basic mode where you are not required to supply detailed technical information,	<b>Simple.</b> Apply this setting if you have basic computer skills and/or are not familiar with technical concepts relating to networks and applications. See page 2-8 for more information.
set the initial firewall settings to advanced mode,	<b>Advanced.</b> This setting is for more advanced computer users who are familiar concepts like network traffic and blocking/allowing applications. See page 2-8 for more information.



**Note:** It is possible to switch to advanced mode later when you feel more comfortable with the program and/or gain more advanced knowledge of computer networking concepts.

7 **Next.** The **Ready to Install the Program** window opens.

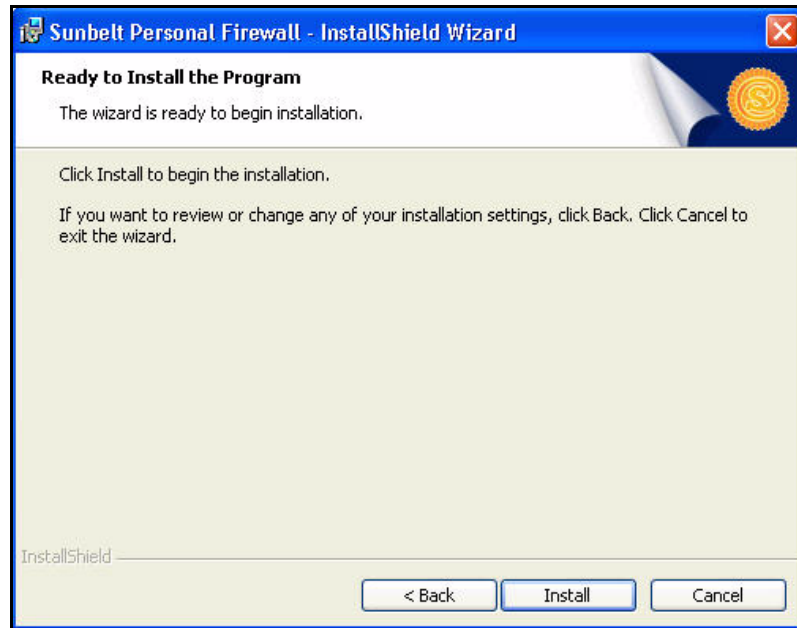


Figure 2-5 Installation Wizard: Ready to Install the Program

- 8 Click **Install** to install the personal firewall on your computer. The **InstallShield Wizard Completed** window opens after the installation is finished.

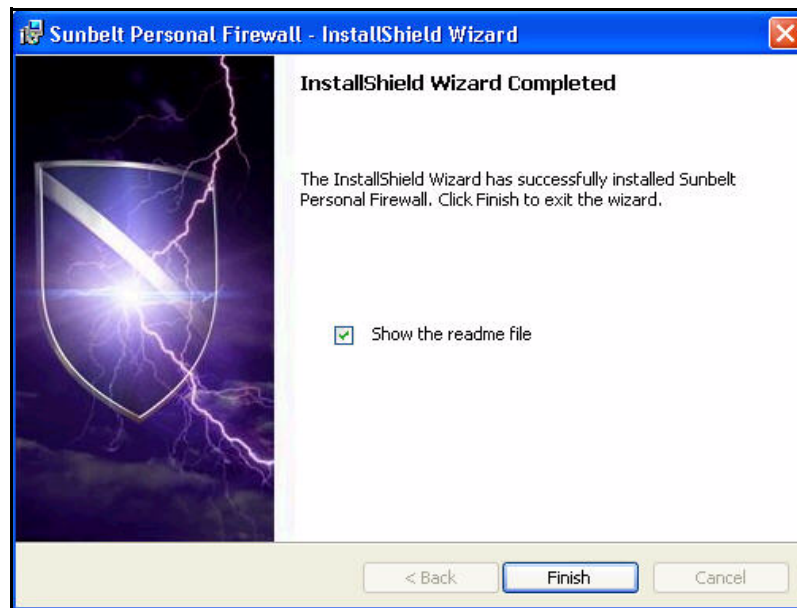


Figure 2-6 Installation Wizard: InstallShield Wizard Complete

- 9 Click **Finish**. A dialog box opens.

**10** Make a selection:

To...	...click...
restart the computer and finalize the installation,	<b>Yes.</b> Make sure work from any open applications is saved first; then, close all open windows.
close the dialog box without restarting your computer,	<b>No.</b> make sure to restart the computer later.



**Warning:** *If Sunbelt Personal Firewall will be used with the AVG antivirus, AVG must be installed before the Sunbelt Personal Firewall. If Sunbelt Personal Firewall detects the AVG antivirus when the firewall is started first time, corresponding rules are set for the antivirus.*



**Caution:** *The following information is for advanced users and should be taken into consideration:*

- *If you are using Windows XP Service Pack 2 or later, the installation program registers Sunbelt Personal Firewall in the Windows Security Center. During the installation, the firewall is registered as inactive.*
- *If the Windows firewall is running, Sunbelt Personal Firewall disables it on startup.*



## Initial Settings

During the installation (see page 2-5) users are required to select the firewall settings that will be applied after the installation is complete and the computer is restarted. The following selections are available:

- **Simple** — In simple mode, the firewall allows all outgoing communication (i.e. accessing the web) and blocks any incoming communication (i.e. web sites or hackers trying to access your computer). Network settings are automatically assigned to your computer and the system security feature is disabled. This means that you will not receive alerts that ask detailed questions that might require you to have more advanced computing and/or computer networking knowledge. Simple mode is set by default and it is recommended for those less knowledgeable about computer and computer networking.

If you have advanced knowledge of computers and/or computer networks, you can change the settings to a more advanced mode after the installation is complete.



**Note:** *The only exception to Simple mode is if you use a dial-up service (as opposed to cable or DSL) to access the internet. You will have to confirm the dial-up numbers you use to access the internet. Also, you are always asked to confirm a number if a new number is dialed or if a telephone number is changed.*

- **Advanced** — In Advanced mode, The firewall allows you to determine the levels of communication and system security. For example, the firewall you are alerted to take an action and whether or not a rule should be created for the action whenever an unknown communication is detected or an unknown application is started. You can create a specific firewall configuration for a host and a user.

If the Advanced mode is selected, Sunbelt Personal Firewall detects the active network interfaces. For each interface, users are asked whether or not the interface is connected to a trustworthy network. Advanced mode is recommended for experienced users and to those who want to apply custom settings. Advanced mode is not for beginners.

## Upgrading to a New Version

Upgrading to a new version of Sunbelt Personal Firewall is similar to the initial installation (as described in pages 2-2 to 2-7). it is not necessary to stop the application since it will be stopped and closed automatically by the installation program.



**Note:** *Sunbelt Personal Firewall includes a built-in automatic update verification system, see page 2-10.*

## Uninstalling the Personal Firewall

Uninstall Sunbelt Personal Firewall using the Add/Remove programs option in the Control Panel.

### To uninstall the personal firewall

- 1 Click **Start>Control Panel**. The **Control Panel** window opens.

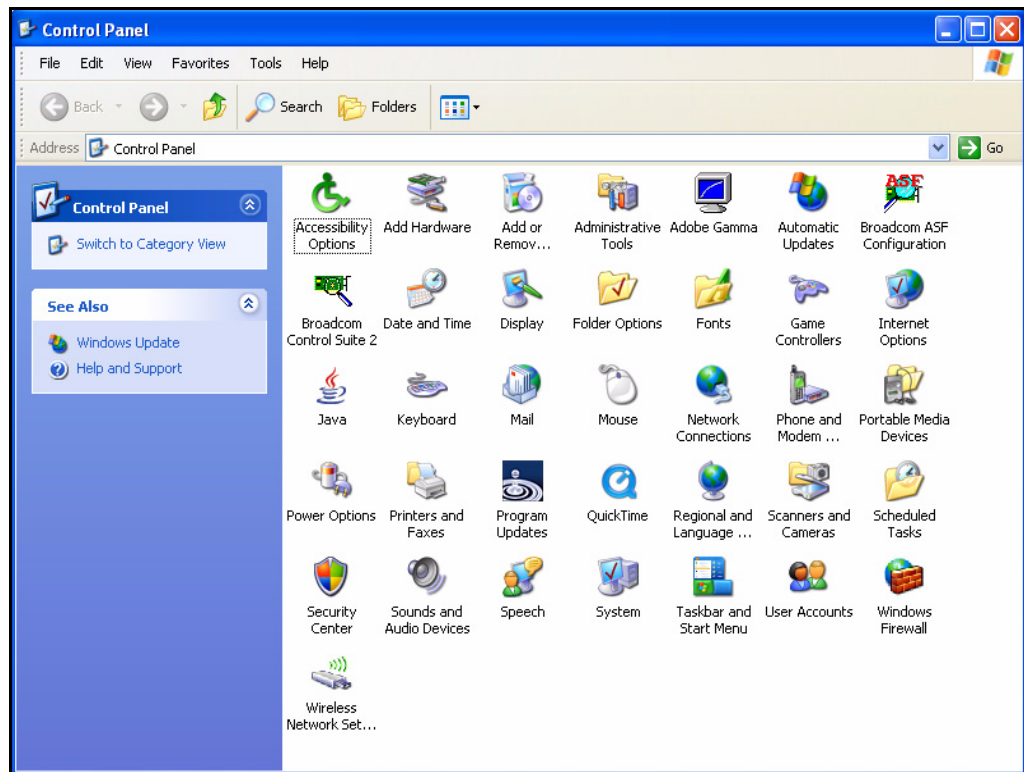


Figure 2-7 Control Panel

- 2 Double-click **Add or Remove Programs**. The **Add or Remove Programs** window opens.
- 3 Scroll down the list of programs; then, select **Sunbelt Personal Firewall**.
- 4 Click **Remove**. A dialog box opens. It asks you to confirm the decision to remove Sunbelt Personal Firewall.
  - Click **Yes** to uninstall the personal firewall.
  - Click **No** to cancel the uninstall process.

Files that were created after the installation (configuration files, logs, etc.) are not removed. After the personal firewall is uninstalled, these files can be either removed manually or kept for possible reinstallation.



**Note:** *If you are using Windows XP Service Pack 2 or later, the Sunbelt Personal Firewall registration in the Windows Security Center is deleted and the integrated Windows Firewall is enabled automatically after the uninstall.*

## Updating the current version

Sunbelt Personal Firewall automatically looks for new versions each time it starts. If a updated version is found, it can be downloaded. If the engine is not restarted; then, it will look for updates every 24 hours.

### To download an updated version of the personal firewall

- 1 Make a selection:

To...	...click...
automatically look for program updates,	<b>Overview</b> on the side menu, click the <b>Preferences</b> tab; then, select the <b>Automatically check for updates</b> box. Sunbelt Personal Firewall will look for updates each time your computer starts up. If updates are found, the <b>Update Wizard</b> opens.
manually check for updates,	<b>Overview</b> on the side menu, click the <b>Preferences</b> tab; then, click <b>Check now</b> . If updates are found, the <b>Update Wizard</b> opens.



**Note:** *If the latest version of Sunbelt Personal Firewall is installed, a dialog box opens stating that the latest version is installed.*

- 2 Click **Next** to download the new version and run the installation program. Sunbelt Personal Firewall always verifies the signature of a downloaded file. This feature ensures that the downloaded file is original and not infected by a virus, damaged, etc.



**Note:** *Stop the download or the installation process by clicking **Cancel**. If the process is canceled, the update is not offered again through the automatic update feature. However, it can be run manually.*

- 3 Restart the computer.



## Purchasing and Product Registration

---

Two editions of Sunbelt Personal Firewall are available: a full edition for which you pay to enable all of the features, and a limited edition that is free. This chapter covers the following topics:

Section	Page
Free Version vs. Full Version	3-2
Purchasing Sunbelt Personal Firewall	3-2
Product Registration	3-3

## Free Version vs. Full Version

Use the same installation procedure for the Free and Full versions of Sunbelt Personal Firewall. After a 30-day trial-period you must select one of the to use. The free version contains limited features, whereas all features are available with the full version.

### Free Version

The following limitations are applied to the Free Version:

- It is available for personal, noncommercial use only.
- Web content filtering, including its logs and statistics, is not available.
- Host Intrusion and Prevention System (HIPS) is not available.
- It cannot be used at Internet Gateways.
- Logs cannot be sent to a Syslog server.
- The configuration cannot be protected by a password and it is not possible to access and administer the firewall remotely.

### Full Version

The full version of the firewall is only available after purchasing a license number and registering the software. All features and components of the Firewall are available after registration.


### Technical Support

Only email technical support is provided for issues concerning Sunbelt Personal Firewall. Owners of multi-licences (licences for more than one user/computer) can contact our technical support by telephone. Go to <http://www.sunbelt-software.com> to find detailed contact information.

## Purchasing Sunbelt Personal Firewall

Purchase a licensed version of Sunbelt Firewall by following a few quick steps.

### To purchase a licensed version of Sunbelt Personal Firewall

- 1 Open a web browser. If the application is open, click **Overview**, the **License** tab; then click the <http://www.sunbelt-software.com/kerio.cfm> link in the **Homepage** field. The **Sunbelt Personal Firewall** page opens.
- 2 Click . The **Shopping Cart** page opens.
- 3 Make a selection:

To...	...click...
change the quantity of the order,	inside the field under the <b>Quantity</b> heading, type a new amount; then, click <b>Recalculate</b> . The amount under the <b>Price Total</b> heading is updated.
apply a coupon to your order,	inside the field under the <b>Got a Coupon</b> section, type the coupon number; then, click <b>Apply coupon</b> .
continue shopping without completing your order,	<b>Keep Shopping</b> . The <b>Webstore Products</b> page opens.



**Note:** Make sure to have a major credit card available (American Express, Visa, or MasterCard).

- 4 Click **Continue**. The **Login** page opens.

## 5 Make a selection:

To...	...click\type...
you have never used this online shop before and do not have an account,	<b>CREATE ACCOUNT.</b> Type the information required under steps 1, 2, and 3; then click <b>CONTINUE.</b> The <b>Checkout</b> window opens.
you are a returning customer,	your email address and password under returning Customer; then, click <b>LOGIN.</b> The <b>Checkout</b> window opens.

6 Click **Continue.** The first page of the **OnLineShop Secure Ordering Form** opens. .7 Type the credit card information under the Shopping cart section; then, click **PROCESS ORDER.** A confirmation window opens after the order is processed. The confirmation page contains the key needed to register Sunbelt Personal Firewall.

## 8 Make a selection:

If...	...click...
Sunbelt Personal Firewall is not installed on the user's computer,	the link under the license key on the confirmation page, download; then, install the application. <i>Go to page 2-1, to read how to install Sunbelt Personal Firewall.</i>
a trial version of Sunbelt Personal Firewall is on the users computer (and the OnLine Secure ordering form is being accessed through the application),	<b>Register</b> on the <b>License</b> tab. Go to Product Registration, page 3-3.

## Product Registration

Sunbelt Personal Firewall must be registered to enable all of the features contained within the full version.

### To register Sunbelt Personal Firewall from within the application

- 1 Click **Overview**, the **License** tab; then click **Register.** The **Registration Wizard** opens.
- 2 Type the license key in the **License number** field; then, click **Next.**
- 3 Type the relevant contact information in the required fields; then click **Next.**
- 4 Make a selection:

To...	...click...
add another subscription,	<b>Add;</b> type the number in the <b>Subscription</b> field in the <b>Subscription Editor</b> dialog box; then click <b>OK.</b>
continue without adding another subscription,	<b>Next.</b>

- 5 Click **Finish** to close the wizard. The License tab now contains detailed information on the current license.



**Note:** *The Personal Firewall GUI component is automatically restarted after the registration is complete. This enables all features that were not available in the trial version.*



**Note:** *The **Register** button in the Product section is disabled after the license key is registered.*

The License section provides information about the current license number, date of the license expiration and date of the last free update (subscription expiration date and time).

Make a selection:.

To...	...click...
register another subscription number,	<b>Add Subscription.</b> Go to step 4.
modify contact information,	<b>Modify data.</b> Go to step 3 on page 3-3.



## Firewall Components and Basic Control Features

---

Sunbelt Personal Firewall uses several components and system tray features. The Components section of this chapter is highly technical. We recommend that basic computer users should focus more on the System Tray Icons section. This chapter covers the following topics:

Section	Page
Components	4-2
System Tray Icons	4-2



## Components

Sunbelt Personal Firewall consists of eight key components:

- **Personal Firewall Engine** – this engine is the core part of the Sunbelt Personal Firewall. It runs as a service (Windows NT 4.0 or later) or in the background (Windows 98 and Me).
- **Low-level drivers** – these drivers are located at the core of an operating system during its startup. They are located between network interface drivers and the TCP/IP subsystem.
- **Network traffic low-level driver** – This driver detects and processes all incoming and outgoing IP traffic. It allows or blocks traffic in accordance with the firewall policy, and controls running applications and system processes.
- **Host intrusions low-level driver** – This low-level driver detects (and blocks — depending on settings in the user interface) Buffer overflow and Code injection intrusion types. The low-level drivers are stored in Windows system directory:
  - In Windows NT and 2000, the fwdrv.sys file is stored in C:\WINNT\system32\drivers.
  - In Windows XP, the fwdrv.sys and khips.sys files are stored in C:\WINDOWS\system32\drivers.
  - In Windows 98 and Windows Me, the fwdrv.vxd and khips.sys files are stored in the C:\WINDOWS\system directory.
- **Personal Firewall GUI** – The GUI (Graphical User Interface) starts automatically via the Personal Firewall Engine service. GUI is represented by a shield icon on the System Tray (see *graphic below*). Right-click the icon on the System Tray to open the configuration dialog or to select another option from the menu (stopping network traffic, disabling firewall, etc.). The Personal Firewall GUI is represented by the spf4gui.exe file found in the installation directory.
- **Crashdump sender** – This tool sends a crashdump file (assist.exe) to Sunbelt Software when the Firewall breaks down.
- **Libraries** – The components above use the following dynamic libraries (DLL):
  - kfe.dll — an interface of the low-level driver. This interface enables traffic between the driver and the Personal Firewall Engine.
  - gkh.dll — a module used for hot key control. This module disables the pop-up filter temporarily.
  - kwsapi.dll — the interface for the Windows Security Center (used for registration of the Sunbelt Personal Firewall and display of its status).
  - KTssleay32\_0.9.7.dll, libeay32\_0.9.7.dll — an OpenSSL library which provides encryption of configuration files and of communication between the Personal Firewall GUI and the Personal Firewall Engine.
  - KTiconv.dll — aniconv library which encodes and deciphers characters e.g. during Web content filtering, logging, etc.
  - KTzlib.dll — a zlib library which is used for crashdump packing.
- **Fast User Switching Support** – The Personal Firewall supports Fast User Switching in Windows XP. Multiple instances of the Firewall can be open at the same time. When this happens, the Personal Firewall Engine communicates with the instance that belongs to the active user. After the Personal Firewall Engine service starts, the first instance opens and runs under the account for which the Personal Firewall Engine service is running. After the user logs in, a new instance opens, and runs with the privileges of the user who is logged in. This instance is active until the user logs off or you switch users.

## System Tray Icons

A shield-shaped icon is displayed in the System Tray whenever the Personal Firewall is running. This component is started automatically by the Personal Firewall Engine. The icon also shows network activity of the computer on which the firewall is installed. Network traffic is represented by small colored bars at the bottom of the icon:

The green bar represents outgoing traffic, the red bar incoming traffic. Right-click the icon to open a menu providing more options.

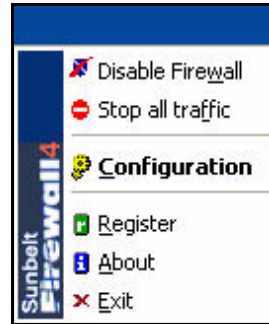


Figure 4-1 Context menu of systray icon Sunbelt Personal Firewall

Select an option for the system tray icon menu:

**Disable Firewall** – Select this option to disable all firewall activities (network communication filtering, monitoring of launched applications, intrusions detection and Web content filtering). Use this option to disable the firewall during activities such as system tests or debugging (i.e. network connection failures). We do not recommend disabling the firewall for long since your computer is not protected while it is disabled.

When the firewall is disabled, the menu selection switches to Enable Firewall. Use it to start the firewall.



**Note:** *In Windows XP Service Pack 2, the current status of the Sunbelt Personal Firewall is reported to the Windows Security Center.*

**Stop all traffic** – Select this option to block all network traffic. In cases where network traffic that should have been denied was permitted by mistake, use the Stop all traffic option to stop all active connections and to prohibit its recovery. If a traffic rule has been created (using the Create a rule for this communication option), it can be removed and the traffic can be enabled again.

When the firewall is disabled, the menu selection switches to Enable traffic. Use it to allow network traffic. Anytime the Personal Firewall Engine service is started, the Disable Firewall and Stop all traffic options are set to their default modes. For security reasons, it is not recommended that you leave the firewall disabled after the system starts up. Also, stopping all traffic might cause problems during user login.

**Configuration** – Select this option to open the configuration dialog box.

**About** – Select this option to open the **About Sunbelt Personal Firewall** window. This window provides general information about Sunbelt Personal Firewall and the versions of the individual components.

**Exit** – Select this option to stop the Personal Firewall Engine service and close the Personal Firewall (all open windows and application dialogs are closed and the icon on the Systray is hidden). Reactivated the Firewall by selecting **Start>All Programs>Sunbelt Software>Kerio Personal Firewall 4**.



## Firewall Behavior and User Interaction

---

Before learning how to configure Sunbelt Personal Firewall, it is important to understand how it behaves and interacts with users. This chapter covers the following topics:

Section	Page
Firewall Behavior	5-2
Connection Alert	5-3
Application Alert	5-6
Host Intrusion Alerts	5-8
Alerts for Connections with Rules	5-10

## Firewall Behavior

Information is transmitted through the Internet using TCP/IP protocols. TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language of the Internet. It can also be used as a communications protocol in a private network (i.e. inside a company or your home). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP protocols. Every computer to which you send or receive messages also has TCP/IP protocols.

### TCP/IP Layers

TCP/IP has two-layers. The higher layer, Transmission Control Protocol (TCP), divides a file into smaller chunks (packets) so the file easier to send. Each packet is numbered separately and includes the Internet address of the destination. The individual packets for a given file might travel by different routes through the Internet, however when they all arrive at their destination, they are reassembled into the original file (by the TCP layer at the destination). The lower layer, Internet Protocol (IP), manages the address part of each packet so that it arrives at the correct destination. If you are part of a computer network, each computer with access to the internet verifies the IP address in order to determine where to forward the message.

### Inspecting the Packets

Sunbelt Personal Firewall inspects each packet; then makes a decision based on the information acquired from the packets as well as the information from previous communications. A log is created to record the information about each approved connection. If a packet is not a threat, it is allowed into your computer. If it is a threat, it is filtered out. The firewall blocks all packets that have been filtered out. The process of inspecting the packets within the message is more efficient and more secure than basic packet filtering, which allows or blocks packets based on source and destination addresses, ports, or protocols, not necessarily their contents.

### Advanced (Learning Mode)

If **Advanced (learning mode)** was selected during the installation, Sunbelt Personal Firewall provides tutorial-style pop-ups to help you make better informed decisions about whether or not to allow a connection to the internet. You are also given the option of permanently permitting or denying a connection. If a connection is permitted or denied permanently, a corresponding rule is automatically created, and users are no longer prompted to permit or deny that particular connection.



**Note:** *The same method is used to verify running applications.*

The ability to modify rules gives users more control over network traffic to and from their computers. Only packets that meet certain criteria, or those that belong to approved connections are allowed through the firewall.

The dialog boxes that alert users about attempted connections are set to Always on Top. For example, if there more than one attempt to establish a connection to the internet is detected, they are put in a queue. Users must decide to allow or deny a connection in the dialog box that is on top before moving onto the next dialog box.

## Connection Alert

The Connection Alert dialog box opens when Sunbelt Personal Firewall detects unknown internet traffic. You are prompted to allow or deny the connection to the Internet, and whether or not to create a corresponding rule.



**Note:** *The parameters in the Network Security section define how the Personal Firewall behaves when a network connection is detected. The Connection Alert dialog box opens if no corresponding rule is found.*



**Caution:** *If the Sunbelt Personal Firewall configuration is password-protected, a connection can still be allowed, however, a rule cannot be created for the connection (unless the password is specified).*



Figure 5-1 Connection alert (unknown traffic detection)



**Note:** *Communication is paused while the Connection Alert dialog is open.*

When an Alert dialog box opens, two sections stand out: the direction of the connection (incoming or outgoing), and the application and remote point trying to make the connection.

### Traffic direction and zone

A green stripe represents an outgoing connection (from a local computer to a general point on the internet or trusted IP address). A red stripe represents an incoming connection (from a general point on the internet or trusted IP address to a local computer). The remote location is shown in parentheses. Trusted area signifies group of trusted IP addresses, Internet signifies IP address that are not included in the Trusted area



### Local application and Remote point

Basic information about a connection is listed below the colored stripe:

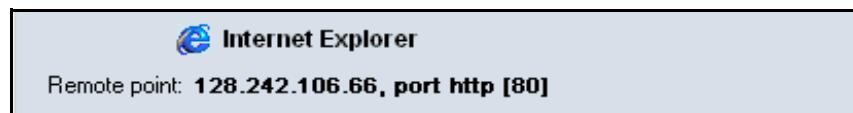


Figure 5-2 Connection alert — Local application and remote point

- The first line shows the application used by the local computer. If a description is not available, the name of a corresponding executable file is displayed. If an application has no icon, a default system icon is used.
- The second line shows the remote point DNS (Domain Name System - See Glossary, page 13-1.) name and its IP address (in brackets).



**Note:** DNS names are identified through DNS queries. If a corresponding DNS name is found, it substitutes the IP address.

- The remote point to which the connection is being made (in case of standard services), and the name of the service is displayed in addition to the port number.

Place the mouse pointer over the application name to see the path to the application executable file on your computer.



Figure 5-3 Connection alert — Full path to the application

### To take action based on an alert

- 1 Select the **Create a rule for this communication and don't ask me again** check box.



Figure 5-4 Connection alert — Actions

- 2 Make a selection:

To...	...click...
allow the communication,	<b>Permit.</b> The communication is allowed and the dialog box closes.
block the communication	<b>Deny.</b> The communication is blocked and the dialog box closes.
view more information about the communication,	<b>&lt;&lt;Details.</b> A Description box drops down. It provides more information about the connection and the application making the communication. Click this button again to hide the information.

- 3 To create an advanced filter rule, select the **Create an advanced filter rule** check box. Advanced filter rules are used to set more detailed parameters regarding incoming and outgoing communications.

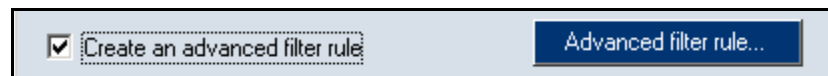


Figure 5-5 Connection alert — Create an advanced rule

- 4 To manage advanced packet filter rule definitions, click **Advanced filter rule...** The **Network Security - Advanced Packet Filter** window opens. Advanced rules can be added, edited, or removed anytime by opening the Personal Firewall application; then, clicking the **Applications** tab under the **Network Security** section.

## Application Alert

The application alert dialog boxes inform users that Sunbelt Personal Firewall detected an attempt to start an application, replace an application, or to run one application from another.



**Note:** Use the **System Security** section to define how the Personal Firewall behaves when applications are started. The Starting, Replacing, and Launching other application dialog boxes are opened if no corresponding rule is found.



**Warning:** If the Personal Firewall configuration is password-protected, the action is allowed only if a valid password is specified.

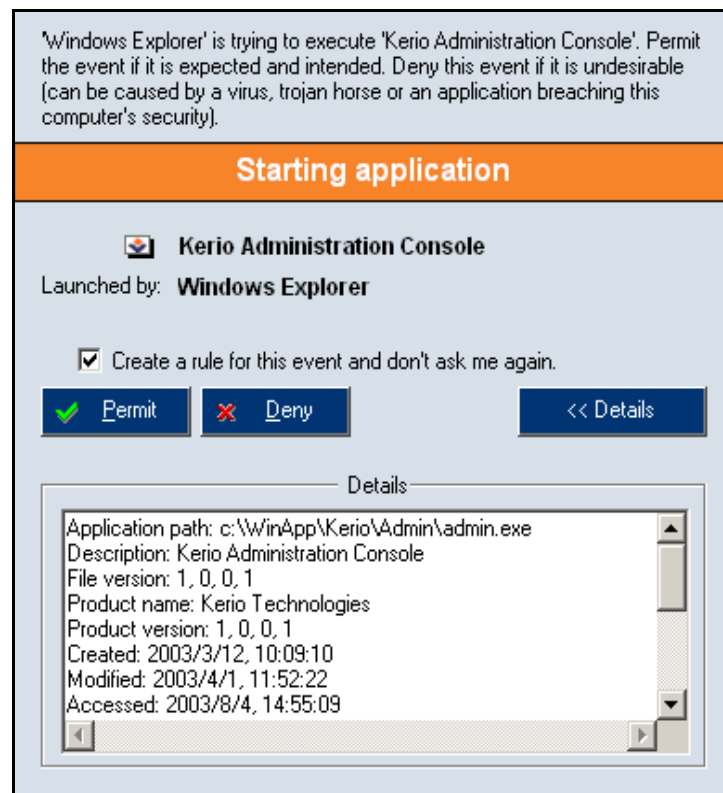


Figure 5-6 Starting/Replacing/Launching other application dialog



The Application alert dialog boxes provide the following information:

### Description

A brief description of a particular event and a general recommendation on the action that should be taken.

'Windows Explorer' is trying to execute 'Kerio Administration Console'. Permit the event if it is expected and intended. Deny this event if it is undesirable (can be caused by a virus, trojan horse or an application breaching this computer's security).

Figure 5-7 Starting/Replacing/Launching other application dialog — Event description



**Note:** If the description of the application (or the file name if there is no description available) is too long, it will be shortened to 32 characters, and three dots will be added at the end to show that the description is incomplete.

### Event Type

The orange strip contains Information on the type of event that was detected. Starting application signifies an attempt to launch an application, Replacing application signifies an attempt to replace an executable file for an application, and Application is launching other application signifies one application is attempting to launch another

Starting application

### Icon and application name

An icon and description of the application are provided below the orange bar. If no description is available, name of the executable file is displayed. If the application has no icon, the standard system icon for executable files will be used.

If the application was launched by another application, information on such application will be displayed below (Launched by).


 **Kerio Administration Console**  
Launched by: **Windows Explorer**

Figure 5-8 Starting/Replacing/Launching other application dialog — Icon and application name

Place the mouse pointer over the description on the application or over the description of the application by which it is launched to view a tool tip providing full path to the executable file of the corresponding application.


 **Kerio Administration Console**  
Launched by: **Windows Explorer** \\WinApp\Kerio\Admin\admin.exe

Figure 5-9 Starting/Replacing/Launching other application dialog — Full path to the application

To take action based on this alert, see *To take an action regarding an alert*, page 5-5.

## Host Intrusion Alerts

The Intrusion Attempt Blocked dialog box warns users that Sunbelt Personal Firewall detected a host intrusion attempt and blocked it.



**Note:** *The Intrusion Attempt Blocked alert is opens when there is no corresponding exception defined for the applications involved or if the Do not display warnings for this type of event is disabled.*

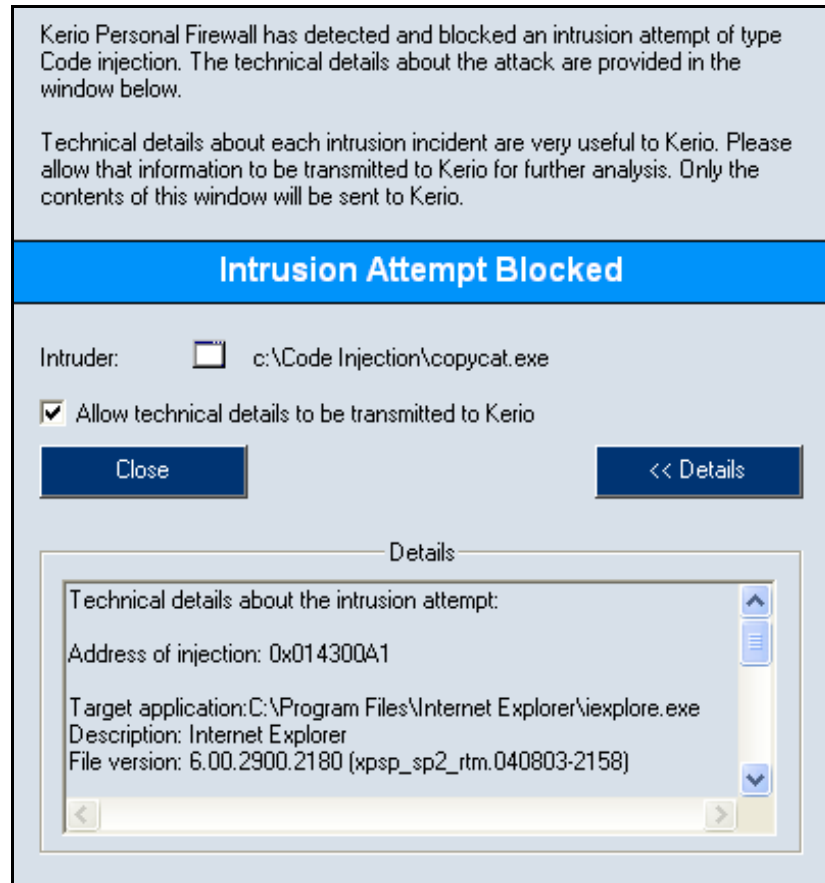


Figure 5-10 Host intrusion alert

### Description

A description of the attempted intrusion is provided at the top of the dialog box, including recommended response.

### Event type

The blue strip contains information on the type of event that was detected.



Figure 5-11 Intrusion Attempt dialog — Event

## The icon and application path

The paths to the target and injector applications as well as corresponding icons are listed directly below the event name. If the application does not use an icon, the standard system icon for executable files is used.



Figure 5-12 Code injection detected — Icons and intrusion description

In case of events that overflow the buffer, only the process where the intrusion was detected is provided (see below).

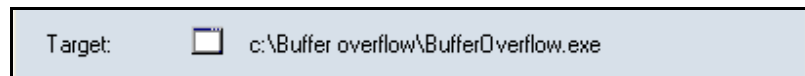


Figure 5-13 Buffer overflow detected — Icon and intrusion description

## To take action based on an intrusion alert

- 1 To Allow technical details to be transmitted to Sunbelt, select the **Create a rule for this communication and don't ask me again** check box.



Figure 5-14 Connection alert — Actions

- 2 Make a selection:

To...	...click...
close the dialog box,	<b>Close.</b> The the dialog box closes.
view more information about the communication,	<b>&lt;&lt;Details.</b> A Description box drops down. It provides more technical details about the intrusion. Click this button again to hide the information.

## Alerts For Connections with Rules

You can enable the Alert dialog box in rules or by running an application. This dialog box opens when a packet that is sent or received meets the conditions of a rule. A window opens in the right bottom corner of the screen. It provides basic details about the connection. If new events that meet the rule are detected while the dialog box is open, they are queued.



**Warning:** *If you close the Alert dialog box, all queued alerts are removed, regardless if they have been displayed or not.*

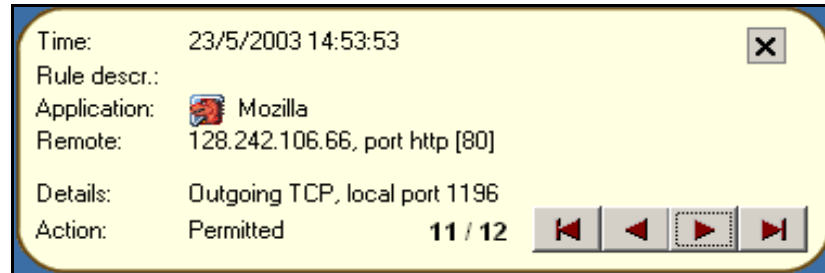


Figure 5-15 Network Connection Alert

The sample alert graphic above, provides the following information:

- **Time** – date and time the connection was initiated
- **Rule descr.** – description (name) of a the rule
- **Application** – icon and name of the application used for the communication. If the application does not have an icon, a default system icon is used. if the application does not have a name, the name of the corresponding executable file is listed.
- **Remote** – IP address and port number of the remote computer. If a name can be identified using DNS, the name is displayed instead of the IP address.
- **Details** – details about the connection: direction, protocol, and local port number
- **Action** – action that has been taken regarding the connection (Permitted or Denied)
- **Sequence number** – number of alerts in the queue and the order in which they arrived.
- **Navigation buttons** – click through the list of alerts in the queue.



## Basic Firewall Configuration

---

Now that we have discussed how the firewall behaves, it is time to learn more about the interface and how to configure basic parameters. This chapter covers the following topics:

Section	Page
The Interface	6-2
Working with Network Connections	6-5
Working with Statistics	6-7
Setting Firewall Preferences	6-9

## The Interface

Use the user interface to control how Sunbelt Personal Firewall protects your computer. There are two ways to open the user interface:

- Double-click the Sunbelt Personal Firewall icon in the System Tray
- Right-click on the icon and select Configuration from the menu.

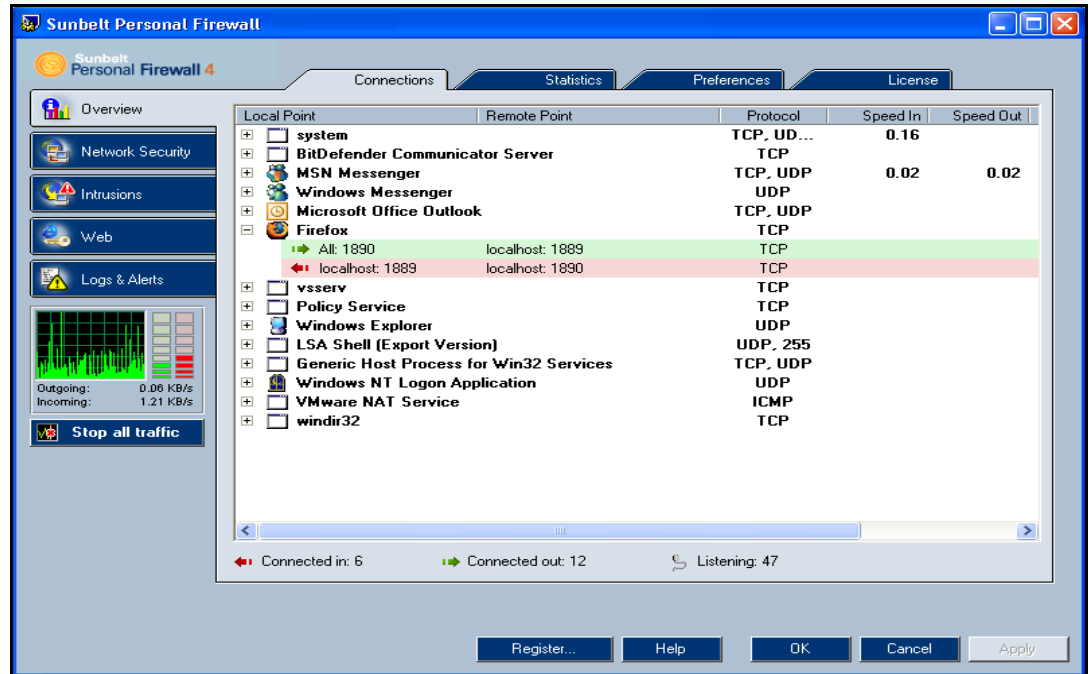


Figure 6-1 Sunbelt Personal Firewall Configuration Dialog

## Modules

The interface is divided into five modules, shown as side-tabs:

- **Overview** – list of active and open ports, statistic, user preferences.
- **Network Security** – rules for network communication of individual applications, packet filtering, trusted area definitions.
- **System Security** – rules for startup of individual applications
- **Intrusions** – configuration of parameters which will be used for detection of known intrusion types.
- **Web** — Web content rules (URL filter, pop-ups blocking, control over sent data)
- **Logs & Alerts** — logs viewing and settings



**Note:** The **Register** button is listed at the bottom with the **Help**, **OK**, **Cancel**, and **Apply** buttons only if you have not registered your version of Sunbelt Personal Firewall.

## Network Traffic Graph

A black and green chart on the left side of the window shows traffic for a particular network.

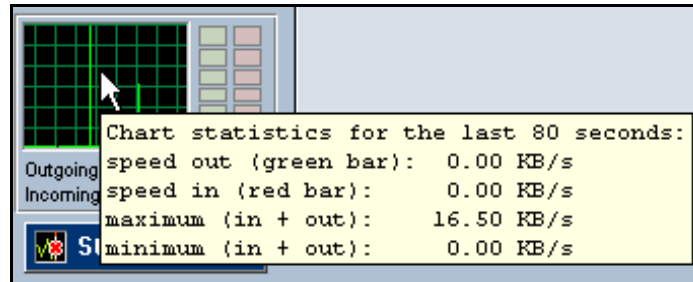


Figure 6-2 Traffic load of a particular network interface

The green bar next to the chart represents current speed of outgoing traffic. The red bar shows current speed of incoming traffic.

### To work with the network traffic graph

- 1 Click the chart to switch between the line graph and the bar graph visual.
- 2 Place the mouse pointer over the chart to see statistics relating to network traffic.
  - speed out (green bar) — current speed of outgoing traffic
  - speed in (red bar) — current speed of incoming communication
  - maximum (in+out) — the highest speed for incoming and outgoing traffic in the last 80 seconds
  - minimum (in+out) — the lowest speed for incoming and outgoing traffic in the last 80 seconds
- 3 To block all network traffic (all connections are stopped immediately), click **Stop all traffic**. This function is helpful when a communication that was supposed to be blocked was allowed by mistake. If you stop the traffic, the text on the button changes to **Enable traffic**.



Figure 6-3 Stop all traffic/Enable traffic



**Note:** Users can also right-click the Sunbelt Personal Firewall icon displayed in the System tray to access the Stop/Enable traffic option.

### Action Buttons

Buttons at the dialog bottom provide the following functions:

- **Help** – opens the online help for tab under a particular section
- **OK** – saves all changes and closes the window
- **Cancel** – closes the window without saving changes
- **Apply** – saves and applies all changes, but leaves the window open



**Note:** *Users can only make changes to one tab at a time. If a user clicks another tab or section, a dialog box opens. Click **Yes** to apply the changes or **No** to continue without saving.*



## Working with Network Connections

The Connections tab lists active connections and open ports used by individual applications. It also lists the applications that are actively involved in network communication and the applications that are waiting for connections.

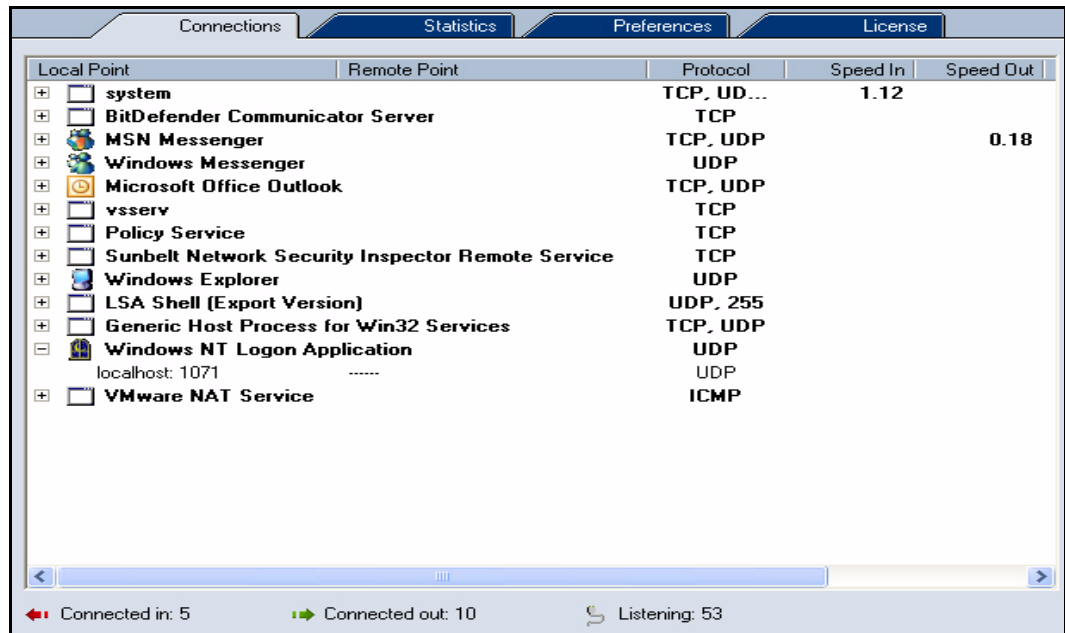


Figure 6-4 Connections Tab

The first line represents each application's icon and name (description) – if the application does not have an icon, the default system icon for executable files is used; if a description is not available, the name of the file without the extension is displayed. A port is considered open when it meets the following criteria:

- an outgoing connection is established (green background)
- an incoming connection is established (red background)
- an application is listening for connections — server mode (transparent background)

Click the [+] to expand a list of details relating to the connection. Click the [-] to hide open ports currently used by the application.

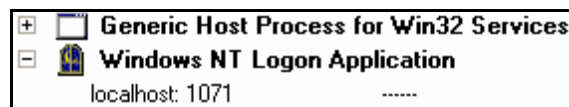


Figure 6-5 Connections - Expand List

### Connections Tab Column Headings

There are seven headings in the Connections tab:

- **Local Point** – Local IP address (or a corresponding DNS name) and port (or service name).
- **Remote Point** – IP address (or DNS name) and port number (or service name) of a particular remote point. The same information for the local IP address and port is provided (see above).
- **Protocol** – Protocol used (TCP, UDP, or both)
- **Speed In, Speed Out** – Current speed of incoming and outgoing data of the connection in kilobytes per second (KB/s).
- **Bytes In, Bytes Out** – Amount of incoming and outgoing data within the connection.

A key at the bottom of the tab shows the number of active connections and open ports.

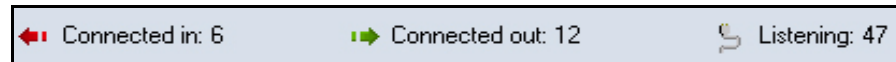


Figure 6-6 Connections - Incoming, Outgoing, Open Ports

### To manage options for connections

- 1 Click **Overview**; then click the **Connections** tab.
- 2 Right-click inside the main tab area to open the Connections submenu.

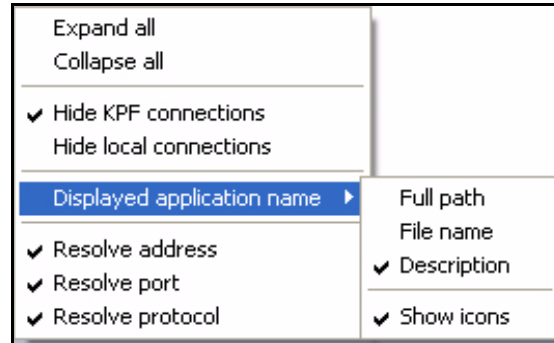


Figure 6-7 Connections - Tab Submenu

- 3 Make a selection:

To...	...select...
expand the details for all listed items relating to the connection,	<b>Expand all.</b> The details for each item are show in a sub-list.
contract the details for all listed items relating to the connection,	<b>Collapse all.</b> The sub-list of details for each item are contracted.
hide all information relating to the firewall connections,	<b>Hide KPF connections.</b>
hide all information relating to local connections,	<b>Hide local connections.</b>
determine how the name of the application is displayed,	<b>Full path, File name, Description</b> from the submenu next to <b>Displayed application name</b> .
The application icons next to the application path, file, or description,	<b>Show icons</b> from the submenu next to <b>Displayed application name</b> .
display address of the remote point,	<b>Resolve address.</b>
display the port connected to the remote point,	<b>Resolve port.</b>
display the protocol used to connect to the remote point,	<b>Resolve protocol.</b>

## Working with Statistics

The Statistics tab lists system statistics for intrusion detection and Web content filtering.

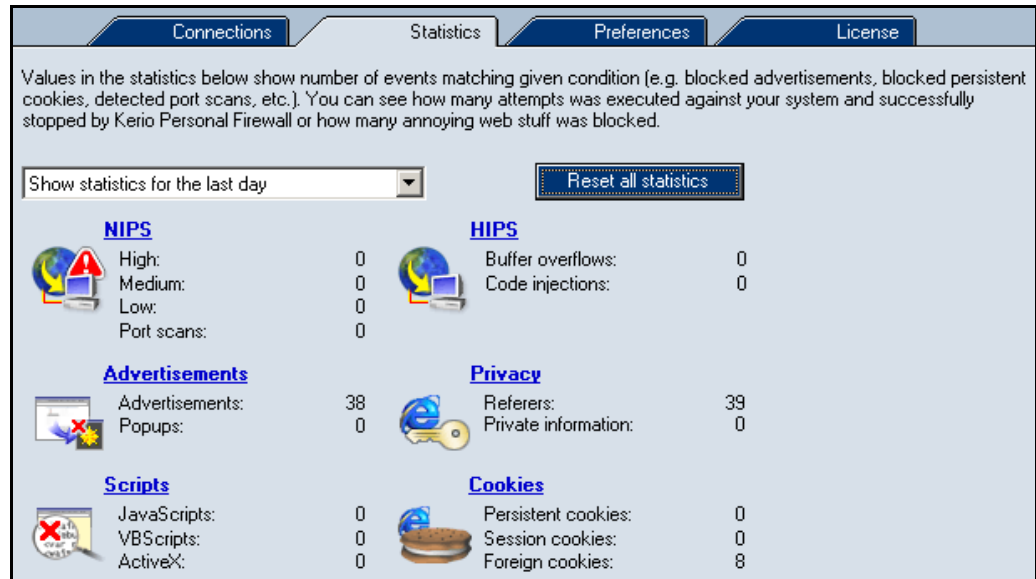


Figure 6-8 Statistics - Statistics on number of blocked intrusions and undesirable Web items

There are six statistical groups:

**NIPS** – Lists the number of detected intrusions:

- High priority — critical attacks
- Medium priority — medium level priority intrusions (e.g. service blocking)
- Low priority — low level priority intrusions (e.g. suspicious activities)
- Port scans — so called Port Scanning

**Advertisements** – Lists the number of blocked ads and web pages components:

- Advertisements — number of objects blocked by ad filtering rules
- Popups — number of blocked pop-up and pop-under windows

**Scripts** – Lists the number of detected scripts.

- JavaScripts — number of filtered JavaScript items
- VBScripts — number of filtered Visual Basic Script items
- ActiveX — number of filtered ActiveX components

**HIPS** – Number of detected attacks:

- Buffer overflow — number of buffer overflow attempts
- Code injection — number of code injection attempts

**Privacy** – Number of objects blocked by the Privacy function:

- Referers — number of Referer items filtered from the HTTP header
- Private information — number of blocked private items that were to be sent

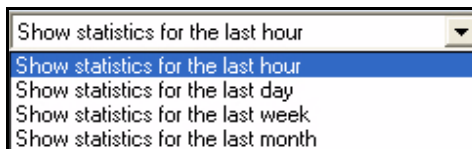
**Cookies** – Number of filtered cookies based on the following types:

- Persistent cookies — number of filtered cookies
- Session cookies — number of filtered temporary cookies
- Foreign cookies — number of filtered third party cookies

Click on the blue heading for a group to view the complete statistics for that heading in the **Logs & Alerts** section. See *Logs & Alerts, page 11-1, for more information.*

**To view statistics for a specific time frame**

- 1 Click **Overview**; then, click the **Statistics** tab.
- 2 Select a time frame from the drop-list.



*Figure 6-9 Statistics – Show Statistics... Drop-List*

- 3 To reset all monitored statistics, click **Reset all statistics**. A confirmation dialog box opens.
  - Click **Yes** to confirm the reset.
  - Click **No** to cancel the reset.

## Setting Firewall Preferences

Set user preferences and advanced firewall parameters in the Overview section on the Preferences tab.

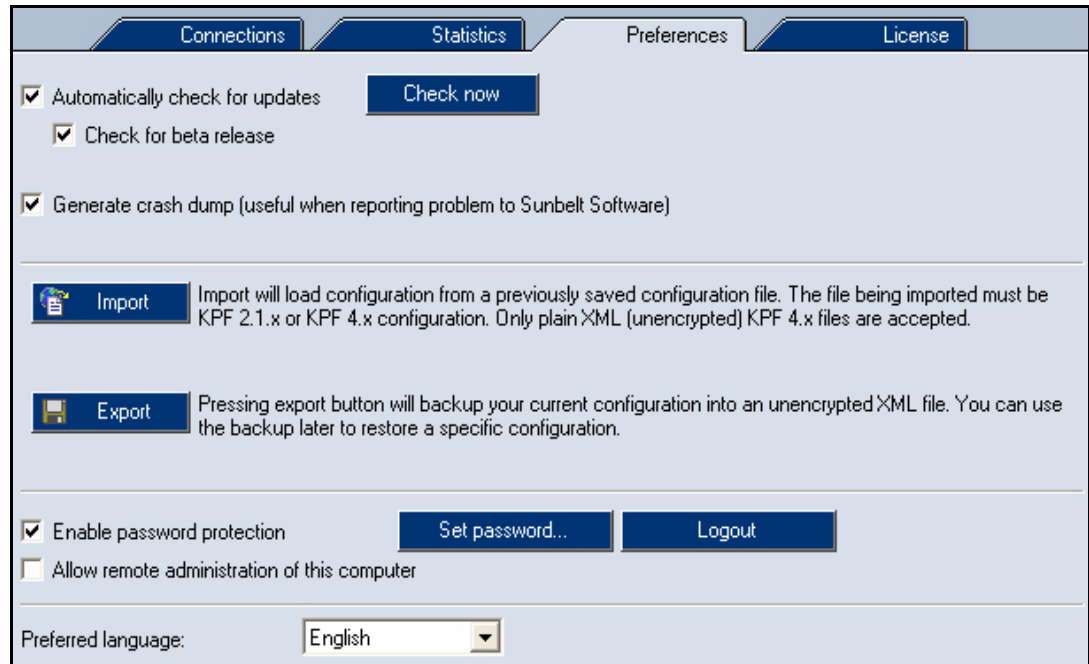


Figure 6-10 Overview - Preferences Tab

### To configure firewall preferences

- 1 Select **Overview**; then, click the **Preferences** tab.
- 2 Click **Check now** to see if there are any updates. This step is important if the user interface is being accessed for the first time. If a new version is found at the update server, users can download and install it. If the users already have the latest version, the following dialog box opens:

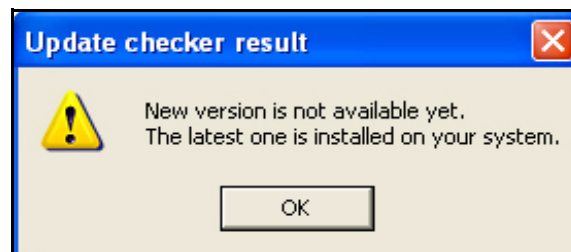


Figure 6-11 Check for new version — New version is not available

**3** Make a selection:

To...	...select...
set the firewall to automatically check for updates,	<b>Automatically check for updates.</b>
check for beta releases of new versions,	<b>Check for beta release.</b> Beta versions are versions of a program that are still being developed and tested. Therefore, they might operate smoothly and bugs may occur. Use the Select this option to participate in product testing.
generate a file that contains debugging information if the application crashes,	<b>Generate crash dump (useful when reporting problem to Sunbelt Software).</b> In the event of a crash, a file containing information relating to the crash is created, and the Assist utility is launched. This utility analyzes the crashdump file and decides whether it has anything in common with Sunbelt Personal Firewall. If the crash is related to the firewall, the Assist Utility provides Sunbelt Software with information relevant to the crash to we can provide an detailed analysis of the problem.



**Note:** Any received information will be used only for Sunbelt Personal Firewall debugging. It will not be used for another purpose nor it will be passed on to other parties.

## Configuration

Sunbelt Personal Firewall enables users to import and export application configurations to and from XML files. The option to import and export configuration files helps the firewall back-up, recover and restore important application parameters.

### To back up and restore application configuration files

- 1 Select **Overview**; then, click the **Preferences** tab.
- 2 Make a selection:

To...	...click...
open and restore configuration files,	<b>Import.</b> Select the file to import from the <b>Source file selection</b> window; then, click <b>Open</b> . A confirmation dialog box opens if the import was successful. Click <b>OK</b> .
backup the current configuration files,	<b>Export.</b> Select folder in which to store the file from the <b>KPF 4.x file selection</b> window; then, click <b>Save</b> . A confirmation dialog box opens if the import was successful. Click <b>OK</b> .



**Note:** *Encrypted configuration files cannot be imported.*

## Password Protection

It is possible to configure Sunbelt Personal Firewall so that it can be accessed only through password authentication (only authorized users are then allowed to modify settings). In such case, unauthorized users are allowed only to view the configuration; a password is required to make changes.

This action requires authentication. Please enter a valid password.

Password:

Figure 6-12 Password Protection

Users can set a system password from the Preferences tab. If password protection is enabled, a password is required to make any changes in the firewall configuration. We recommend that authorized users logout using the **Logout** button after making changes so unauthorized users cannot modify the configuration. It is also possible to log out from the menu accessed by right-clicking the icon in the System Tray.

### To set a password

- 1 Select **Overview**; then, click the **Preferences** tab.
- 2 Select the **Enable password protection** check box. The **KPF - change password** dialog box opens.
- 3 If a password was set previously, type it in the **Old password** field. If not, this field is grayed out.
- 4 Type the new password in the **New password** field; then, retype it in the **Retype password** field.
- 5 Click **OK** to set the password, or click **Cancel** to close the dialog box without setting a password. If the password was set successfully, a confirmation dialog box opens. Click **OK**.



**Note:** Only users with an authorized password can administer *Sunbelt Personal Firewall* from a remote location. If the *Enable password protection* option is disabled, remote administration cannot be enabled. The option is grayed out.

- 6 To allow this computer to be administered from a remote location, select the **Allow remote administration of this computer** check box.

### Remote Administration

Users can administer Sunbelt Personal Firewall from a remote location. All settings and functions can be accessed from a remote computer.

#### To access Sunbelt Personal Firewall from a remote computer

- 1 Select the **Overview** section; then click the **Preferences** tab.
- 2 Select the **Enable password protection** check box. The **Change Password** dialog box opens. Type the password information in the appropriate fields; then click **OK**.
- 3 Select the **Allow remote administration of this computer** check box.
- 4 Make a selection:

If...	...then...
Sunbelt Personal Firewall 4.x is installed on the remote computer,	select Remote Firewall Administration from the Sunbelt program group; then, run it.
Sunbelt Personal Firewall is not installed on the remote computer,	copy the kpf4gui.exe, KTLibeay32_0.9.7.dll, KTssleay32_0.9.7.dll and KTzlib.dll files from the local workstation (from the C:\Program Files\Sunbelt\Personal Firewall 4 directory) and run them on the remote workstation.  <b>Note:</b> If you intend to use a version of the interface in a language other than English, copy the trans subdirectory.



- 5 Type the appropriate information in the **Host** and **Password** fields.

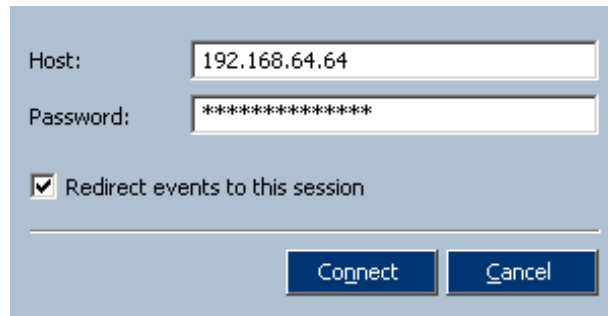


Figure 6-13 Access from a Remote workstation

- 6 To redirect alerts and notifications to the remote computer, select the **Redirect events to this session** check box. After a successful connection the host name or IP address is displayed in the header of the configuration window.
- 7 Click **Connect** to establish connection with the remote computer.



**Note:** Connection to a remote administration is allowed by the internal Sunbelt Personal Firewall policy. This means that it is not necessary to define special network security rules to enable remote administration.

After successfully connecting to the firewall, the Sunbelt Personal Firewall icon in the System tray has an R, symbolizing the remote connection. Right-click the icon to open a menu that provides the following functions:

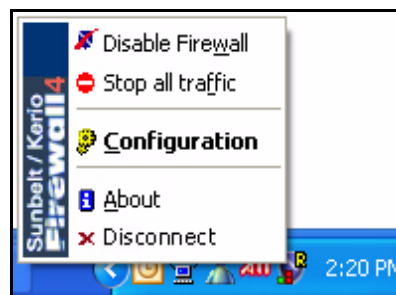


Figure 6-14 Remote administration — Context menu of the Systray icon

- **Disable firewall** – Select this options to deactivate the firewall (all security functions are disabled).
- **Stop All traffic** – Select this option to stop incoming and outgoing traffic.
- **Configuration** – Select this option to open the user interface and configure necessary settings.
- **About** – Select this option to view information about the individual versions of Sunbelt Personal Firewall components as well as license information.

- **Disconnect** – Select this option to disconnect from the remote Firewall and close the interface on the computer from which the remote access was granted.



**Note:** *The following functions are not available for remote connections:*

- *Stop all traffic (this function would block connection of the Personal Firewall Engine with the Personal Firewall GUI operating on the remote host)*
- *Logout (users must be authenticated to be allowed to administer the firewall remotely and they will be logged out automatically when disconnected from the Personal Firewall Engine)*
- *Exit (the Personal Firewall Engine service cannot be closed remotely; the Personal Firewall GUI running on the remote host can be closed using the Disconnect option).*

### Preferred language

Users can select preferred language for the Sunbelt Personal Firewall user interface.

#### To set a preferred language

- 1 Select **Overview**; then, click the **Preferences** tab.
- 2 Select a language from the **Preferred language** drop-list.
- 3 Click **OK** or **Apply**. Close the interface; then re-open it. Notice that the new language is used.

The Personal Firewall Engine detects which language versions are available; then, populates the **Preferred language** drop-list with the available versions.

Preferred language also affects the language in the help file. If a corresponding help file for the language is not found, Sunbelt Personal Firewall uses the English version of the help file.



## Network Security

---

Defining the network communication rules is one of the most important parts of the Sunbelt Personal Firewall configuration. This chapters covers the following topics:

Section	Page
What is Network Security?	7-2
Rules	7-2
How Are Rules Applied	7-2
Application Rules	7-3
Packet Filter Rules	7-7
Predefined Rules	7-20
Trusted Area	7-22
Advanced Settings	7-23
Boot Time Protection	7-24
Detecting New Network Interfaces	7-25
Checking Dialed Telephone Numbers	7-26

## What is Network Security?

The Network Security section controls all incoming and outgoing communication to and from your computer or computer network. Sunbelt Personal Firewall includes a set of predefined network security rules (i.e. for DNS, DHCP, etc.). These rules are separate from user-defined rules and can be enabled or disabled at any time.

## Rules

The following network communication rules are available:

- Applications – simple rules that define how the firewall behaves during network communications. Application rules are generated automatically. This process is based on the user responses to connection alerts regarding unknown network traffic.
- Advanced Packet Filter – detailed rules for network communications. Packet filter rule are defined manually in the Sunbelt Personal Firewall application or generated automatically based to user responses to connection alerts.
- Predefined – Sunbelt Personal Firewall includes set of predefined rules which are independent from individual applications. For these rules, only actions which will be taken can be set (allow or deny rule). Predefined rules can be either enabled or disabled (one option for all the rules).

## How are Rules Applied?

When a communication is detected, individual modules apply rules in a pre-defined order. If the communication meets the criteria for a rule, a corresponding action is taken. If one rule is applied to a communication, no more rules are applied. Rules for individual Sunbelt Personal Firewall modules are applied in the following order:

- 1 Intrusion detection system (IDS)
- 2 Network traffic Inspection (automatically lets in/out packets which belong to permitted connections),
- 3 Internal rules for *Sunbelt Personal Firewall* components — i.e. permission to access a web server in order to check and download new versions of the program
- 4 Advanced packet filter rules
- 5 Predefined network security rules
- 6 Application rules



**Note:** If individual firewall components are disabled, corresponding rules are not applied. Internal firewall rules cannot be switched off.

## Application Rules

View and modify Application rules on the Applications tab under the Network Security section.



**Note:** *The following information is for cases when Sunbelt Personal Firewall is in Advanced mode. In the Simple mode, all outgoing traffic is allowed and all incoming communication is denied for any application (both for trusted zones and the Internet) and rules are not automatically created.*

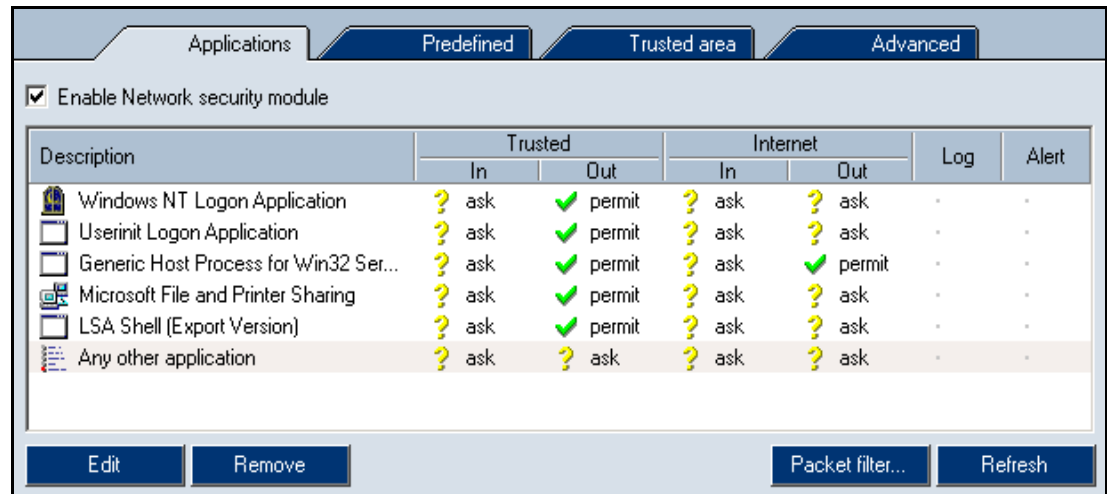


Figure 7-1 Network Security – Applications Tab

### Applications Tab Column Headings

There are five headings under the applications tab. They are described below.

**Description** – Lists the application icon and description. If there is no icon, a system icon is used. If a description is unavailable, the name of the executable file is listed.



**Note:** *Users cannot edit icons and descriptions of applications in Sunbelt Personal Firewall.*

**Trusted, Internet In/Out** – Lists the settings for how applications behave during a connection. Select one of the following actions for each zone and direction:

- *permit* – allows the connection
- *deny* – blocks the connection
- *ask* – asks the user to permit or deny the connection. Anytime a new connection is detected, an alert dialog box opens and ask the user to make a decision.



**Note:** *Rules can be edited in the Connection Alert dialog using the Create a rule for this communication option. If this option is selected, the default Ask action is switched to an action selected by the user.*

**Log** – Lists whether or not communication that meet the rule is logged into the Network log.

**Alert** – Lists whether or not an alert connection that meets the rule is detected.

Use the **Edit** button to edit a selected rule. Use the **Remove** button to remove a selected rule. Use the **Refresh** button to refresh the rule list.

## Defining Rules

Only one rule can be defined for each application. The order in which the rules are defined is not important.

### To configure basic application rules

- 1 Click **Network Security**; then click the **Applications** tab.
- 2 Make a selection:

To...	...select...
enable the Network Security Module,	Enable Network security module check box.
edit a rule,	a rule on the list; then click <b>Edit</b> . The <b>Connection settings for .exe</b> dialog box opens. See <i>To edit the settings for an application rule, page 7-5</i> .
remove a rule from the list,	a rule on the list; then, click <b>Remove</b> . A confirmation dialog box opens: <ul style="list-style-type: none"> <li>• Click <b>Yes</b> to remove the rule.</li> <li>• Click <b>No</b> to cancel the removal.</li> </ul>

- 3 Make a selection for new rules and refreshing the current list:

To...	...click...
add, edit, insert, or remove an advanced packet filter rules and/or IP group,	<b>Packet filter...</b> The <b>Network Security - Advanced Packet Filter</b> dialog box opens.
refresh the current list of rules,	<b>Refresh</b> .
Open the a help window relating to the current tab,	<b>Help</b> .
apply changes to the Applications tab, save them, and close the Sunbelt Personal Firewall configuration window,	<b>OK</b> .
cancel changes to the Applications tab without saving them, and close the Sunbelt Personal Firewall configuration window,	<b>Cancel</b> .
apply changes to the Applications tab and keep the Sunbelt Personal Firewall configuration window open,	<b>Apply</b> .

## Application Rule Settings

You can edit the settings attached to each application for which a rule is created. Use the settings to permit or deny connections to and from trusted areas and the internet. They also determine whether or not to record the details of each connection to a network log.

### To edit the settings for an application rule

- 1 Click **Network Security**; then, the **Applications** tab.
- 2 Select an application from the list; then, click **Edit**. The **Connection Settings** dialog box opens. The name of the application is displayed at the top of the box. The icon and full path to the application executable file is listed below the name.

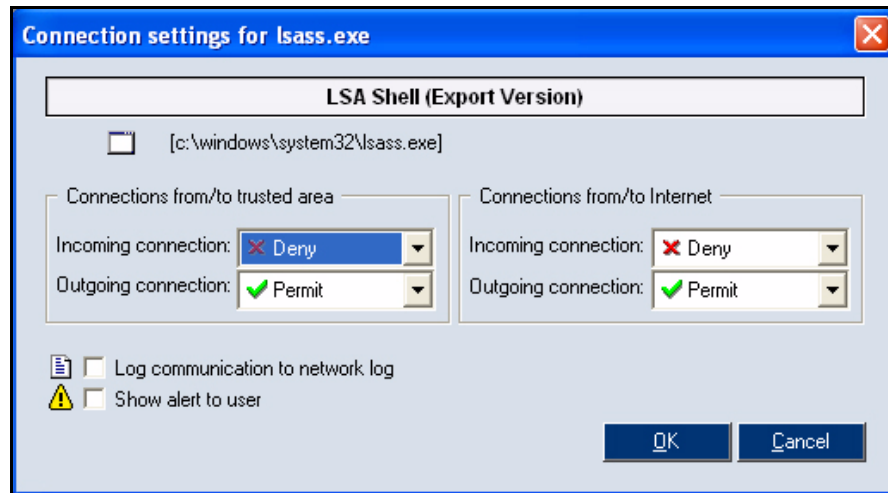


Figure 7-2 Edit Application Rule

- 3 Make a selection:

To...	...select...
set the permissions for connections from a trusted area,	Deny, Ask User, or Permit from the <b>Incoming connection</b> drop-list under the <b>Connections from/to trusted area</b> section.
set the permissions for connections to a trusted area,	Deny, Ask User, or Permit from the <b>Outgoing connection</b> drop-list under the <b>Connections from/to trusted area</b> section.
set the permissions for connections from the Internet,	Deny, Ask User, or Permit from the <b>Incoming connection</b> drop-list under the <b>Connections from/to Internet</b> section.
set the permissions for connections to the Internet,	Deny, Ask User, or Permit from the <b>Outgoing connection</b> drop-list under the <b>Connections from/to Internet</b> section.
log communications that meet this rule to the network log,	the <b>Log communication to network log</b> check box.
enable the Alert dialog box for connections meeting this rule,	the <b>Show alert to user</b> check box.

### Default Rule

The Another application rule (the default rule) is always located at the end of the list of application rules. This rule applies to network traffic that does not match any other rule. The default rule is highlighted in the rule list. It cannot be removed.



**Note:** You can set actions in the Any other application rule in order to switch between firewall modes:

- If at least one ask action is in the rule, the firewall works in the Advanced mode. Whenever unknown traffic is detected, you are asked to take an action; the traffic is handled according to your decision.
- If only the permit and/or deny actions are set for zones and directions, the firewall works in Simple mode. If unknown traffic is detected, a corresponding action is taken without asking the user.

The default rule is also used as a template for new rules that are automatically created after you click Permit or Deny on an Alert dialog box.

### Additional Application Options

You have several options available from within the Applications tab. Use the procedure below to manage those options

#### To manage individual application rules

- 1 Right-click an application to open a menu that lists additional options:

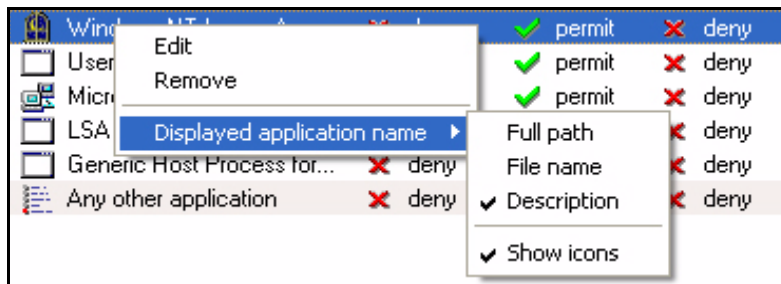


Figure 7-3 Rules for applications – Context menu

- 2 Make a selection:

To...	...select...
edit an rule,	<b>Edit.</b>
remove a rule,	<b>Remove.</b>
list an application by its path, name, or description,	<p><b>Displayed application name;</b> then, one of the following from the sub-menu:</p> <ul style="list-style-type: none"> <li>• Full path</li> <li>• File name</li> <li>• Description.</li> </ul> <p>Use the Show icon option to enable/disable application icons before the application name or description.</p>



- 3 Do one of the following to update the permissions under the Trusted or Internet columns:
  - left-click to switch between the Permit, Deny and Ask actions.
  - right-click to open a context menu and select an action.



Figure 7-4 Rules for applications – Actions

## Packet Filter Rules

Packet filter rules allow you to define advanced rules for specific network communication. You can define the local application and traffic direction, protocol, remote IP addresses, and remote and local ports.

### Filter Rules

Rules for packet filter can be defined as follows:

- **Manually** – Open the Advanced Packet Filter dialog where packet filter rules can be viewed, edited and removed (for details see below).
- **Automatically** – the Connection Alert dialog box pops-up when a connection does not meet a rule; if the Create an advanced filter rule option is selected, a packet filter rule is created instead of a standard rule.



**Note:** Packet filter rules do not distinguish between trusted area and the Internet (an IP address, subnet, IP group, etc. are always specified in the rule).

### To manually define packet filter rules

- 1 Click **Network Security**; then click the **Applications** tab.
- 2 Click **Packet Filter...** The **Network Security - Advanced Packet Filter** window opens.

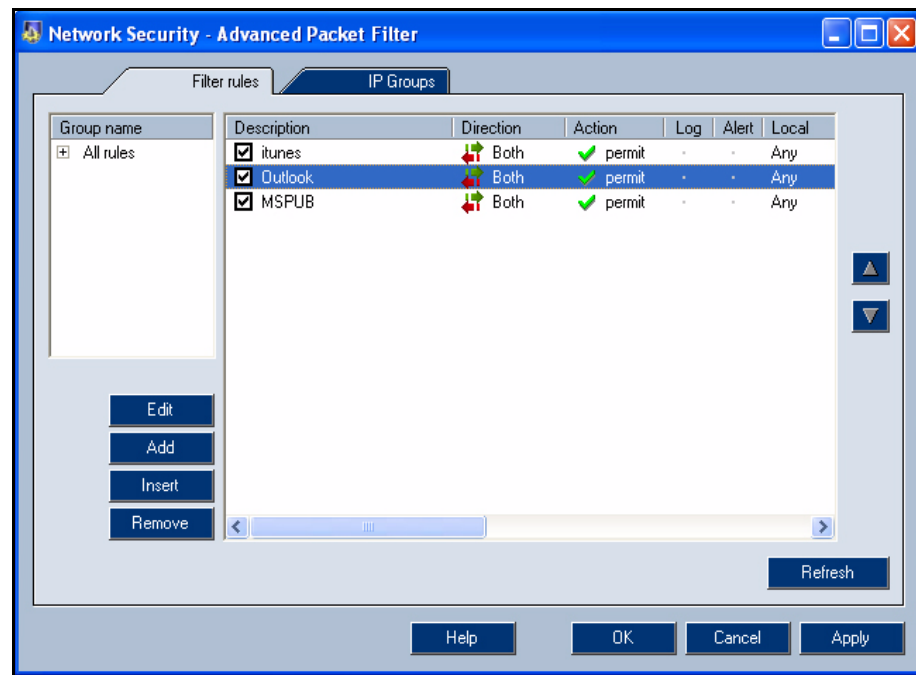


Figure 7-5 Advanced Packet Filter Rules – Filter Rules

The **Filter Rules** tab lists the rules for advanced packet filters. The rules are listed in the order in which they will be applied when a connection is detected. The first rule that the traffic meets is applied. The rules are applied from top to bottom.

Description	Direction	Action	Log	Alert	Local	Remote
<input checked="" type="checkbox"/> Internet Explorer	Outgoing	permit	-		Any	Address: gw, Port: 3128
<input checked="" type="checkbox"/> Internet Explorer	Outgoing	permit		-	Any	Port: http, Port: https
<input checked="" type="checkbox"/> Internet Explorer	Outgoing	permit	-	-	Any	Address: localhost
<input checked="" type="checkbox"/> SYSTEM	Outgoing	permit	-	-	Any	Group: kerio network, Port:

Figure 7-6 Packet Filter Rules

Packet filter rules can also be classified by groups. If a rule is in a group, it does not affect how rules are applied. Rules that are part of a group are for reference only. Rule groups are displayed on the left of the Filter Rules tab.

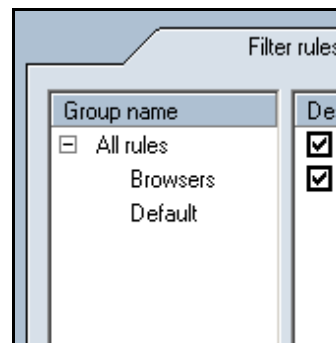


Figure 7-7 Rule groups of packet filter

### 3 Make a selection:

To...	...click...
edit an existing rule,	<b>Edit.</b> The <b>Filter rule</b> dialog box opens.
add a new rule,	<b>Add.</b> The <b>Filter rule</b> dialog box opens.
insert a rule above an item on the list, select a rule in the list; then,	<b>Insert.</b> The <b>Filter rule</b> dialog box opens.
remove a rule from the list,	<b>Remove.</b> The rule is deleted from the list.
refresh the current list of rules,	<b>Refresh.</b> The list of rules returns to its original state. For example, if you deleted a rule without clicking <b>Apply</b> , the rule is added back to the list.
move a rule down on the list,	
move a rule up on the list,	

Use the scroll bar to view more information about the rules.



**Note:** *If no rule is selected, only the Add button is available.*

*Hold down the Ctrl or the Shift key to select multiple rules. Groups of rules selected in this way can only be moved or deleted. Use the Edit button to edit the first selected rule (at the top). The Insert button inserts a new rule before the first rule of a particular group.*

- 4 Click on a group name to view the list of rules included in the group. The following two groups are predefined and they cannot be removed:
  - All rules (“parent group”) — includes all packet filter rules.
  - Default — includes all rules which have not been added into another group.



**Note:** *Groups of rules cannot be created nor removed explicitly. New groups can be created by entering a new group name during a rule definition. Groups are removed automatically when the last rule is removed.*

### Inside Packet Filter Rules

It is important to understand how individual parts of a rule and their items are related in order for you to correctly define the rules.

- As a whole, the rule is applied only to the network traffic that meets all of the conditions for the Protocol, Local and Remote settings.
- Inside the rule, the parameters and settings for protocols, IP addresses and ports they are applied individually. For example, the **Local** section lists two port ranges, 80-88 and 8000-8080. The rule is applied when a remote port contains one of these ranges.
- As far as the items listed in the Remote section, they have to meet the exact criteria. For example, the Remote entry is specified by the IP address 65.131.55.1 and port 80. This condition is met by traffic that includes a remote computer with the IP address 65.131.55.1 using port 80.

### Ensuring Proper Functionality

The Protocol, Local and Remote settings are closely related. Follow the suggestions below to ensure the rule functions properly:

- The port definition is helpful only for TCP and UDP protocols (ports are ignored by other protocols). If the rule is available for any protocol (the Protocol is not specified); then, the port numbers are not applicable since they are used only for traffic through TCP or UDP protocols.
- The application service is specified by port numbers and by protocols. In the packet filter rule dialog box, a service is represented by port only — the protocol must be entered manually.

For example, to create a rule for incoming HTTP connections (i.e. to enable access to a Web server on a computer that is protected by Sunbelt Personal Firewall), you must add a port in the **Local** section and select the HTTP service — this automatically sets the port value to 80. Next, go to the **Protocol** section to set the TCP protocol that is used by the HTTP service.

- The most common type of network traffic is the client to server communication. The server listens on a predefined port for an incoming connection. A client starts the connection by demanding a local port from the operating system that will be used for the connection. Unlike the server port, any port can be used temporarily for a client.

Example 1: To enable access to a Web server on a local computer with IP address 60.80.100.120, define the rule as follows:

- Protocol — [6] TCP (HTTP service uses the TCP protocol)
- Local — Port: [80] HTTP (Web server runs on a local computer)

- Remote — Address: 60.80.100.120. A client represented by a Web browser runs at a remote host. The port is unknown, that is why only the IP address is specified.

Example 2: To block connections to the Web server with IP address 90.80.70.60, define the rule as follows:

- Protocol — [6] TCP
- Local — This entry is left empty because the client port cannot be specified.
- Remote — Port: [80] HTTP, Address: 90.80.70.60

### Adding a Filter Rule

Several steps are required to add a filter rule. Make sure you have the correct protocol, port, and IP address information before creating the rule.

#### To add a rule

- 1 Click **Network Security**; then click the **Applications** tab.
- 2 Click **Packet Filter...**. The **Network Security - Advanced Packet Filter** window opens.
- 3 Click **Edit**. The **Filter rule** dialog box opens.

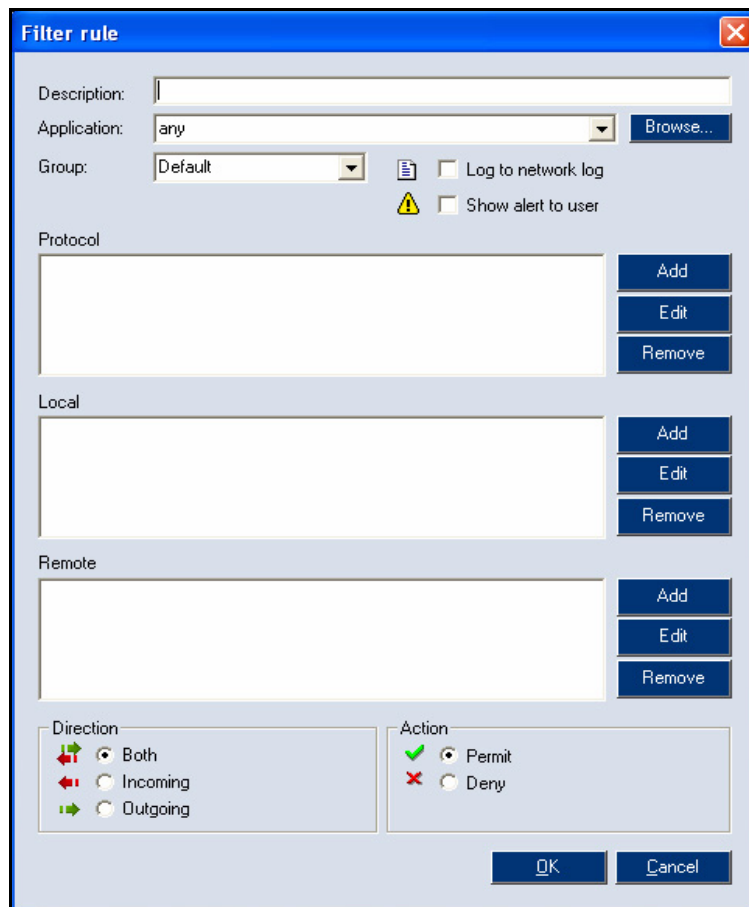


Figure 7-8 Filter Rule Dialog Box - Add a Rule

4 Make a selection regarding the description, application and groups:

Figure 7-9 Add Rule - Description, Application, Group

To...	...select...
add a description or name for the new rule,	the <b>Description</b> field; then type the description or name. We recommend typing a brief rule description (purpose, application name, etc.). This description is for reference only. The name of the local application is inserted for rule that are automatically generated.
add the location of the application to which the rule is applied,	the location from the <b>Application</b> drop-list, or click <b>Browse</b> , then select the application from the <b>Application selection</b> dialog box. You can also type the location manually. if you leave this field blank, a general rule will be created and applied to all applications.
assign the new rule to a group,	the group from the <b>Group</b> drop-list.
log communications that meet the criteria for rule in the network log,	the <b>Log to network log</b> check box.
enable an alert dialog box when network traffic meets the criteria for this rule,	the <b>Show alert to user</b> check box.

5 Make a selection regarding protocol parameters:

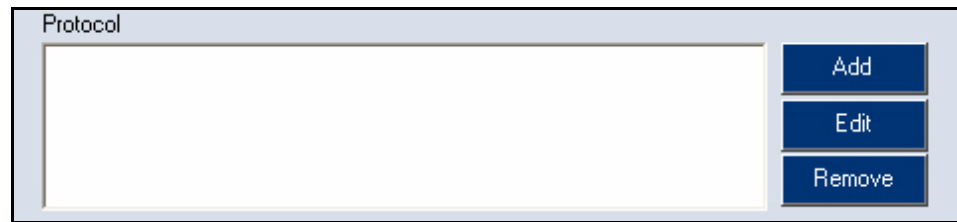


Figure 7-10 Add Rule - Protocol Settings

To...	...click/select...
add parameters for a protocol to which the rule will be applied,	<b>Add.</b> The <b>Filter rule - protocol</b> dialog box opens. See <i>To add filter rule protocol parameters, page 7-15.</i>
edit parameters for a protocol to which the rule will be applied,	<b>Edit.</b> The <b>Filter rule - protocol</b> dialog box opens.
delete protocol parameters,	<b>Remove.</b> The parameters are deleted from the list.

6 Make a selection regarding local port settings:

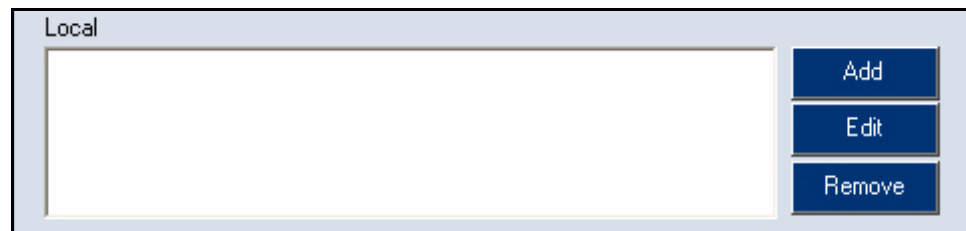


Figure 7-11 Add Rule - Local Settings

To...	...click/select...
add a single port or port range,	<b>Add.</b> Select Add port or Add port range from the drop-list. The <b>Filter rule - port</b> dialog box opens. See <i>To add local port settings, page 7-17.</i>
edit a single port or port range,	a port or port range; then click <b>Edit</b> . The <b>Filter rule - port</b> dialog box opens.
delete a single port or port range,	a port or port range; then, click <b>Remove</b> .

## 7 Make a selection regarding remote settings:

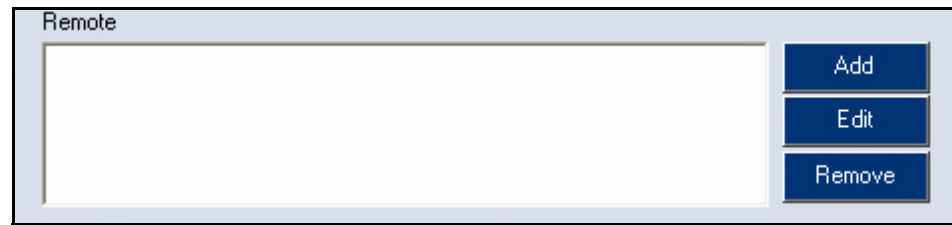


Figure 7-12 Add Rule - Remote Settings

To...	...click/select...
add a remote port, IP address, or IP group,	<p><b>Add</b>; then make a selection from the drop-list:</p> <ul style="list-style-type: none"> <li>• Add port</li> <li>• Add port range</li> <li>• Add address</li> <li>• Add address range</li> <li>• Add address / mask</li> <li>• Add IP group</li> </ul> <p>The <b>Filter rule - port</b> dialog box opens.</p>
edit a remote port, IP address, or IP group,	<p>a item from the list, click <b>Edit</b>; then make a selection from the drop-list:</p> <ul style="list-style-type: none"> <li>• Add port</li> <li>• Add port range</li> <li>• Add address</li> <li>• Add address range</li> <li>• Add address / mask</li> <li>• Add IP group</li> </ul> <p>The <b>Filter rule - port</b> dialog box opens.</p>
remove a remote port, IP address, or IP group,	<p>a item from the list; then, click <b>Remove</b>.</p>

- 8 Make a selection regarding the direction of the communication and an action to take when a network communication meets the rule:

The screenshot shows a configuration dialog with two sections: 'Direction' and 'Action'. In the 'Direction' section, there are three radio buttons: 'Both' (selected), 'Incoming', and 'Outgoing'. In the 'Action' section, there are two radio buttons: 'Permit' (selected) and 'Deny'.

Figure 7-13 - Network Communication Direction and Actions

To...	...select...
apply the rule to incoming and outgoing network connections,	<b>Both</b> under the <b>Direction</b> section. This is the default selection.
apply the rule only to incoming network connections,	<b>Incoming</b> under the <b>Direction</b> section.
apply the rule only to outgoing network connections,	<b>Outgoing</b> under the <b>Direction</b> section.
permit a network communication that meets the rule,	<b>Permit</b> under the <b>Action</b> section. This is the default selection.
deny a network communication that meets the rule,	<b>Deny</b> under the <b>Action</b> section.

- 9 Click **OK** to add the new rule.



## Protocol Parameters

Use the following procedure to set protocol parameters for the rule. Typically, a single protocol is used for traffic (i.e. TCP or UDP), however, some applications use multiple protocols concurrently (i.e. TCP and UDP using the same ports). If the Protocol is left empty, the rule is applied to any protocol. If an application uses TCP and UDP protocols at various ports, two different packet filter rules must be defined.

### To add filter rule - protocol parameters

- 1 Click **Network Security**; then click the **Applications** tab.
- 2 Click **Packet Filter...** The **Network Security - Advanced Packet Filter** window opens.
- 3 Click **Add**. The **Filter rule** dialog box opens.
- 4 Click **Add** under the **Protocol** section. The **Filter rule - protocol** dialog box opens.

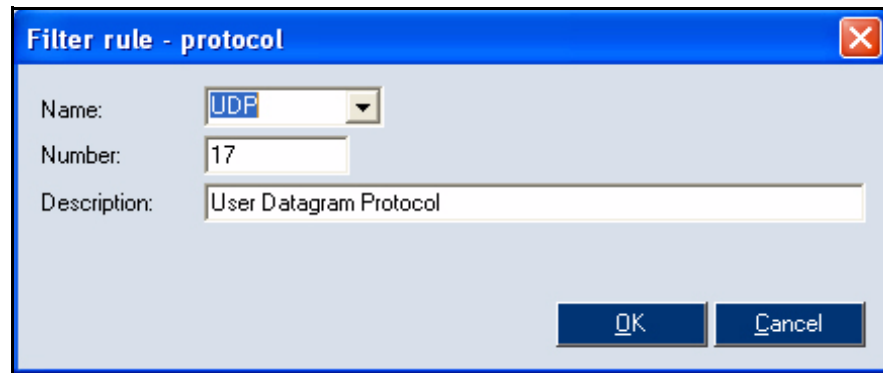


Figure 7-14 Add Rule - Protocol Filter

- 5 Select the type of protocol from the **Name** drop list. The number (specifying the protocol in the IP packet header) automatically populates the **Number** field, and a description for the rule populates the **Description** field. See the Glossary, page 13-1, for complete definitions.
  - TCP – Transmission Control Protocol
  - UDP – User Diagram Protocol
  - ICMP– Internet Control Message Protocol
  - IGMP – Internet Group Management Protocol
 If you select the ICMP protocol, the **Types** field appears below the **Description** field.



Figure 7-15 Add Rule - Protocol Filter - Types Field

To use more than the general ICMP protocol, click **Select** to open the **Filter Rule - protocol [ICMP types]** dialog box.

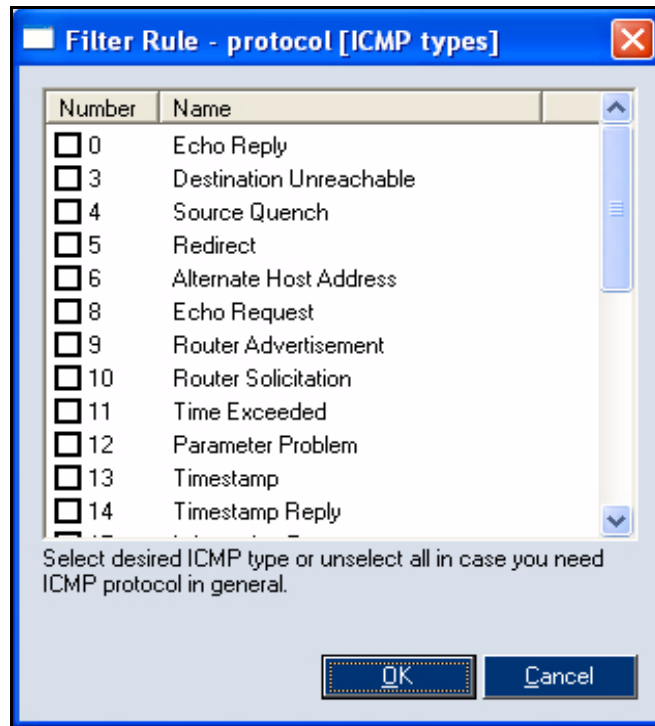


Figure 7-16 Add Rule - Protocol Filter - ICMP Types

Select the check box(es) next to the protocol types; then click **OK**. You return to the **Filter rule - protocol** dialog box. The numbers relating to the protocols, are listed in the **Types** field. If more than one protocol is selected, the numbers are separated by commas.

- 6 Click **OK** to add the Protocol.

**To add local port settings**

- 1 Click **Network Security**; then click the **Applications** tab.
- 2 Click **Packet Filter...** The **Network Security - Advanced Packet Filter** window opens.
- 3 Click **Add**. The **Filter rule** dialog box opens.
- 4 Click **Add** under the **Local** section; then select Add port or Add port range from the drop list. The **Filter rule - port** dialog box opens.

**To add remote port, IP address, or IP group settings**

- 1 Click **Network Security**; then click the **Applications** tab.
- 2 Click **Packet Filter...** The **Network Security - Advanced Packet Filter** window opens.
- 3 Click **Add**. The **Filter rule** dialog box opens.
- 4 Click **Add** under the **Remote** section; then make a selection from the drop-list:
  - Add port
  - Add port range
  - Add address
  - Add address range
  - Add address / mask
  - Add IP group
- 5 Type the required information; then click **OK**.

**To edit a rule**

- 1 Click **Network Security**; then click the **Applications** tab.
- 2 Click **Packet Filter...** The **Network Security - Advanced Packet Filter** window opens.
- 3 Click **Edit**. The **Filter rule** dialog box opens.
- 4 Edit the necessary parameters; then click **OK**.

## IP Groups

IP groups enable packet filter rules to be easily defined. Use the groups to specify the Remote entry in the dialog for packet filter rule definition. IP groups can be viewed and defined in the IP Group tab of the **Advanced Packet Filter** dialog box.

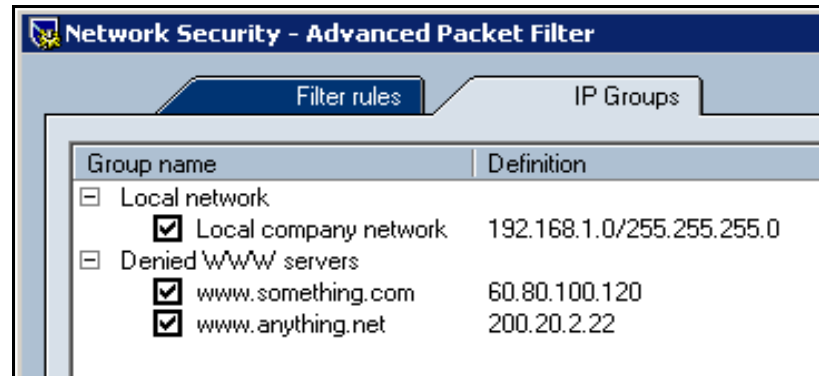


Figure 7-17 Packet filter — IP address groups

The tab contains two columns:

- Group name – name of an IP group. Use the “+” to expand a list of items included in a particular group.
- Definition – definitions of individual items of a particular group

Clear an item to temporarily disable a rule. This can be helpful for situations such as testing or debugging. It is not necessary to remove items, then define them again.

Click **Add** or **Edit** to open a dialog box to add or modify an IP group.

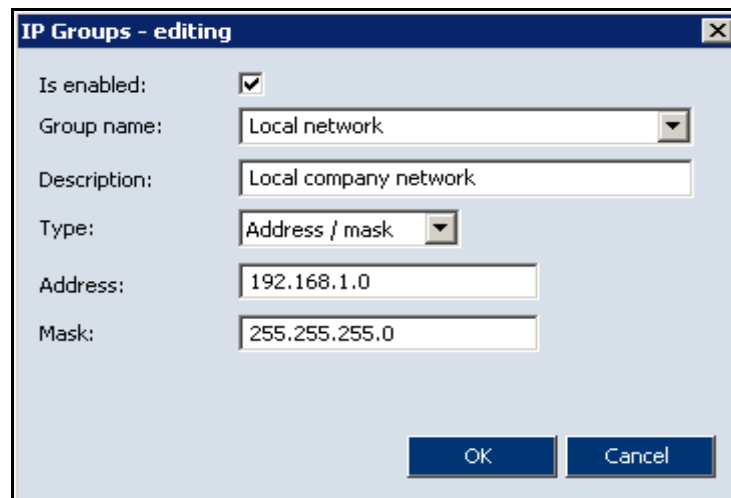


Figure 7-18 Packet filter — Addition of IP address group

### Is enabled

Select or clear this option to enable or disable the item. This option is identical to the matching field next to the item name in the IP Groups tab. If the Is enabled is cleared, the item is not active. This means that it is not included in the group.

**Group name**

Name of the group to which the item will be included. Specify the item using one of the following methods:

- select a name from the menu — the item will be added to this group
- enter a new group name — this group will be created automatically and the item will be added to the new group

**Type**

Type of the new item:

- Host — IP address of one computer
- Address range — define the First and Last address to specify IP range
- Address / mask — subnet defined by an IP address and mask
- Address group — another IP address group (IP addresses can be embedded into each other)

## Predefined Rules

Sunbelt Personal Firewall contains several predefined rules. These rules are independent from individual applications; they are applied globally. Decide whether individual predefined rules will be used or not.

### To manage predefined network security

- 1 Click **Network Security**; then the **Predefined** tab to view a list of the predefined rules for network traffic.

Description	Trusted	Internet
Internet Group Management Protocol	✗ deny	✗ deny
Ping and Tracert in	✓ permit	✗ deny
Ping and Tracert out	✓ permit	✓ permit
Other ICMP packets	✓ permit	✗ deny
Dynamic Host Configuration Protocol	✓ permit	✓ permit
Domain Name System	✓ permit	✓ permit
Virtual Private Network	✓ permit	✓ permit
Broadcasts	✓ permit	✓ permit

Figure 7-19 Network Security - Predefined rules

Predefined rules cannot be added or removed. However you can set actions relating to Trusted areas and the Internet for each rule.

- 2 To switch between permit and deny, click on the action (under Trusted or Internet) for the rule.



**Note:** The Ask action is not available for predefined rules.

- 3 To enable or disable (respectively) predefined rules for network communication, select or clear the Enable predefined network security option. If this option is not selected, predefined rules are ignored and Sunbelt Personal Firewall only uses application and advanced packet filter rules.
- 4 To restore actions for predefined rules to default values, click **Set to defaults**.

### Predefined Rules

Brief descriptions for the predefined network security rules are listed below.

#### Internet Group Management Protocol

The IGMP used to subscribe groups of multicast users. This protocol is disabled by default because can be misused easily. Do not to enable this protocol unless you run applications that use multicast technologies (typically for transmitting audio or video data through the Internet).

#### Ping and Tracert in, Ping and Tracert out

Programs Ping and Tracert (Traceroute) trace routes in a network to detect response of a remote computer. This is achieved through ICMP (Internet Control Message Protocol) messages.

First, a possible attacker tests if an elected IP address responds to control messages. Blocking these messages makes your computer invisible and reduces the chances of possible intrusions.

All incoming Ping and Tracert messages (from the Internet) are blocked by default. However, these messages are allowed from the trusted area (i.e. an administrator can test availability of a

computer by the Ping command). Outgoing Ping and Tracert messages are permitted for both areas. These methods are usually used to verify network connection functionality or availability of a remote computer.

### **Other ICMP packets**

Rules for other ICMP messages (i.e. redirections, destination is not available, etc.)

### **Dynamic Host Configuration Protocol**

DHCP is used for automatic definition of TCP/IP parameters (IP address, network mask, default gateway, etc.).



**Warning:** *DHCP* denial might cause that network connection of your computer will not work if TCP/IP parameters are defined through this protocol.

### **Domain Name System**

DNS is used to translate computer names to IP addresses. At least one connection to a DNS server must be permitted.

### **Virtual Private Network**

Virtual private network (VPN) is a secure connection between two local networks (or between a remote client and a local network) via the Internet using an encrypted channel. VPNs allow individuals and organizations to use the Internet as a secure means of communication. The VPN rule allows or denies a link to the local computer through the PPTP protocol.

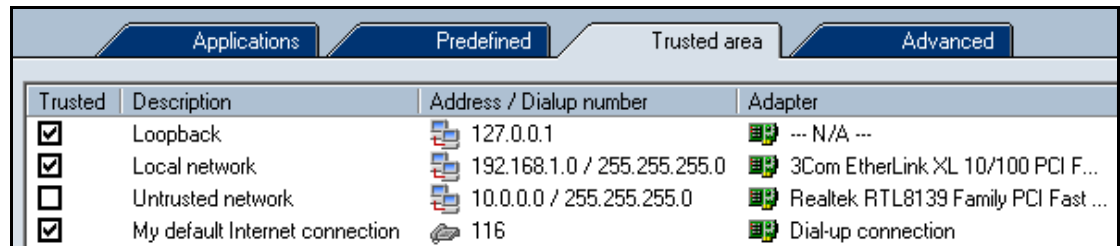
### **Broadcasts**

Rules for packets with general addresses. In the Internet, this rule is also applied on packets with multicast addresses.

## Trusted Area

Sunbelt Personal Firewall application rules uses two types of IP groups: trusted area and the Internet. Separate actions for incoming and outgoing traffic can be defined for each area. Trusted area is a user-defined IP group. Addresses that are not defined as trusted are automatically added to Internet zone.

Click **Network Security**; then, the **Trusted area** tab to define a trusted area.



Trusted	Description	Address / Dialup number	Adapter
<input checked="" type="checkbox"/>	Loopback	127.0.0.1	--- N/A ---
<input checked="" type="checkbox"/>	Local network	192.168.1.0 / 255.255.255.0	3Com EtherLink XL 10/100 PCI F...
<input type="checkbox"/>	Untrusted network	10.0.0.0 / 255.255.255.0	Realtek RTL8139 Family PCI Fast ...
<input checked="" type="checkbox"/>	My default Internet connection	116	Dial-up connection

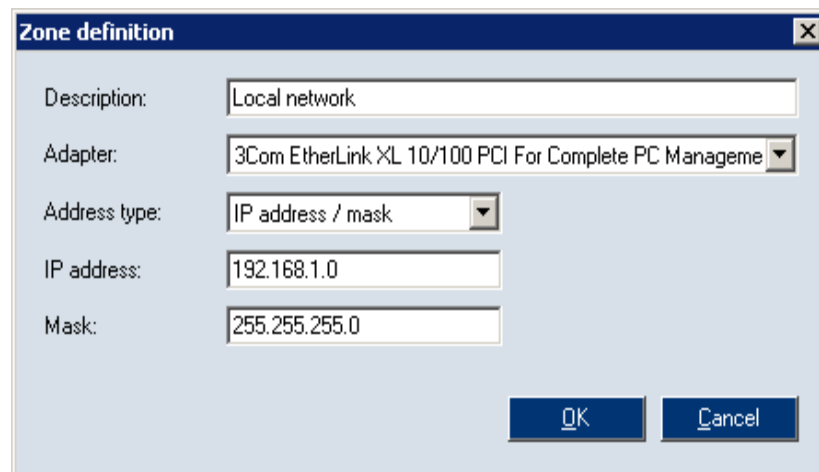
Figure 7-20 Network security / Trusted area section — Trusted area definition

Trusted areas can include any number of IP addresses, IP address ranges, subnets or networks connected to a particular interface. It is possible to specify an interface on which particular IP addresses are permitted for each item (protection from false IP addresses).

The Trusted area includes the predefined Loopback item. This item cannot be removed. It is a local loopback address and it is always considered trusted.

### To add/edit a trusted area

- 1 Click **Add** or **Edit**. The Zone definition dialog box opens.



**Zone definition**

Description: Local network

Adapter: 3Com EtherLink XL 10/100 PCI For Complete PC Manageme

Address type: IP address / mask

IP address: 192.168.1.0

Mask: 255.255.255.0

OK Cancel

Figure 7-21 Trustworthy zone definition

- 2 Type a description for the area in the **Description** field. This field is for reference only. It is recommended to provide description of the IP range, network, etc.
- 3 Select an adapter (interface) for which the IP addresses are used. This function protects users from false IP addresses — whenever a packet with a trusted address is received from an adapter that is not connected into the particular network, the packet is not trusted. Select *Any* if you do not want Sunbelt Personal Firewall to check adapters from which packets with a particular IP address were sent.



- 4 Select the type of item the address represents for the **Address type** drop-list.
  - Computer — a particular IP address of a computer (or a network device)
  - IP address / mask — subnet defined by IP address and mask of the network
  - IP address / range — IP range defined by first and last IP address
  - All addresses — any IP address

## Advanced settings

Use the Advanced tab to set more advanced network security parameters.

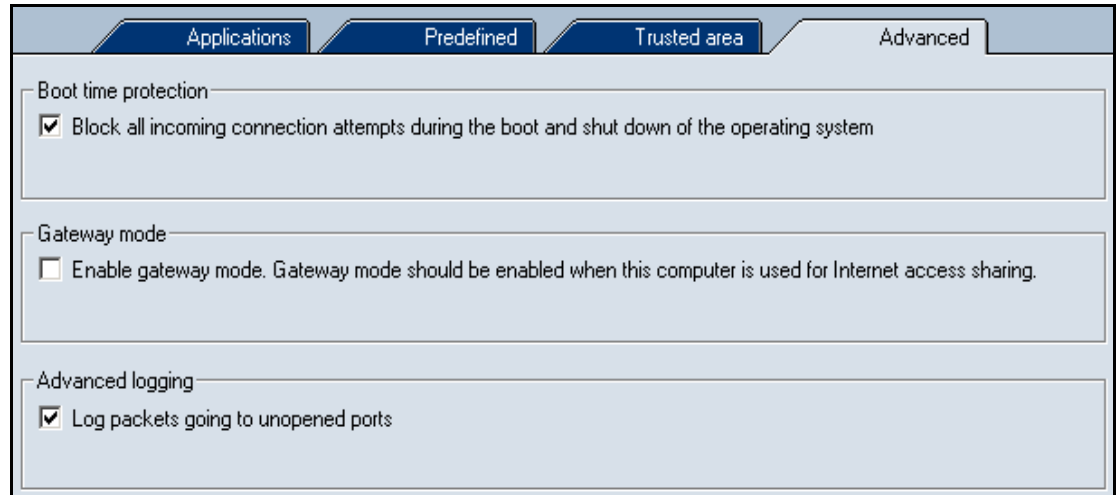


Figure 7-22 Network Security / Advanced section

### Boot time protection

Select or clear the Block all incoming connection attempts... option to enable/disable the computer during the time of booting. This option is enabled by the default. Disabling it is useful for testing and trouble-shooting (e.g. to solve problems with remote administration of the host protected by Sunbelt Personal Firewall). For security reasons, it is recommended that you do not disable this option unless necessary.

### Enable gateway mode

This option switches the firewall to a special mode – protection of the Internet gateway (the firewall will run on router or NAT router).

If this option is selected, Sunbelt Personal Firewall allows packets with destination ports from which no local application is running, or packets with destination IP addresses that are not local!

Use Advanced logging to log detected packets that include destination ports not belonging to any process in the local operating system. These packets are dropped automatically, however, they might point at an intrusion attempt (port scanning).



**Note:** *The gateway mode and the advanced logging cannot be combined. In the gateway mode, these packets are automatically let in (they are addressed to other hosts).*

## Boot time Protection

Sunbelt Personal Firewall's network traffic low-level driver protects computers even when the firewall is not running. This type of protection provides security for your computer at startup, during product updates, or when the Personal Firewall Engine service is not launched for any reason.

This function is enabled by default. It can be disabled or enabled in the firewall's GUI whenever necessary.

If Boot time protection is enabled, Sunbelt Personal Firewall's network traffic low-level driver behaves as follows:

- Only outgoing traffic is allowed and all incoming traffic is blocked upon startup. This implies that the server is always protected, however, its services are not available in this mode.
- If the Personal Firewall Engine does not start within in 5 minutes of the operating system startup, the driver is switched to the mode when it allows any traffic. This behavior ensures that communication with the server is not blocked in case the Personal Firewall Engine cannot be started for any reason.
- After the Personal Firewall Engine starts, the firewall permits and denies traffic in accordance with the defined network security rules.
- When the operating system is shut down (or being restarted), the firewall's driver blocks any incoming or outgoing traffic. This behavior ensures that the server is protected even when the Personal Firewall Engine service has stopped, but the network subsystem is not active.
- When the Sunbelt Personal Firewall service is stopped, the driver is switched to the mode where it permits all network traffic.

## Detecting New Network Interfaces

If the Advanced mode of the firewall is selected as default during the installation, the Sunbelt Personal Firewall automatically detects active network interfaces of the computer on which it is installed. After each new interface is detected, you are asked whether the interface is connected to a trustworthy network.

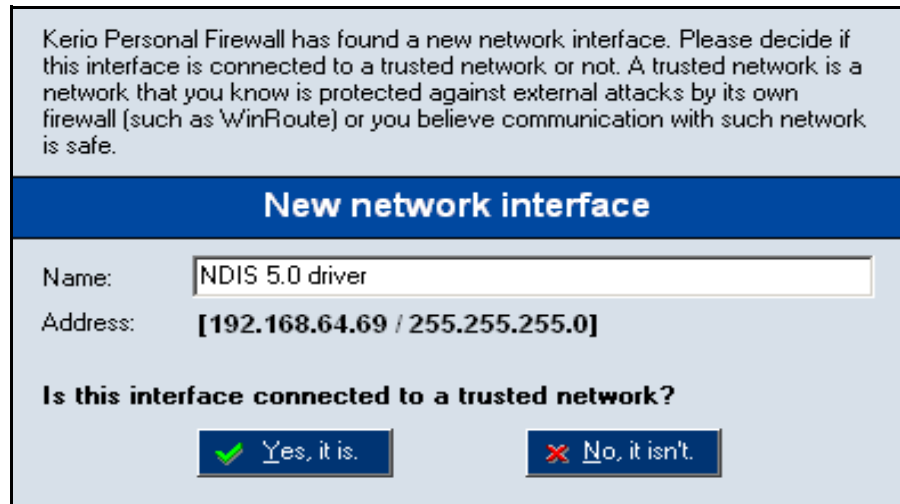


Figure 7-23 Detection of new network interfaces

The name in the Name field is name of a corresponding network adapter. Below it is the IP address of this adapter and the mask of the network to which it is connected. Name of the interface can be edited (it is recommended that you provide a short and apt description, e.g. Network card, Internet line, etc.). ID of the adapter detected at the corresponding controller is used as the name by default.

if you click **Yes, it is**, the subnet to which the interface is connected adds the IP address to the group of trustworthy IP addresses (Trusted area). If you click **No, it isn't**, it is considered as a part of the Internet.

- Anytime, group of trustworthy IP addresses can be edited. Whenever any other interface is added or enabled or an interface is connected to a new subnet, *Sunbelt Personal Firewall* detects it and the *New network interface* dialog is opened.
- As to dial-ups, the telephone number which is being dialed is displayed. User can enable or disable this connection.
- *Sunbelt Personal Firewall* finds out whether the telephone number has been changed since the dial-up was dialed the last time (this protects users from undesirable change of dial-up configuration).

## Checking Dialed Telephone Numbers

Sunbelt Personal Firewall can detect and block changes to dialed telephone numbers. This protects users from their dial-ups being redirected to high-price services. Connections can be redirected without informing the user (for example by an ActiveX object on a Web page). If a change is detected, Sunbelt Personal Firewall asks user to accept or reject the change. If the change is rejected, the line is hung-up immediately.

### How it works

As soon as an unknown connection is attempted, an alert asks the user whether or not the interface is connected to a trustworthy network (as in case of a new network adapter. The dial-up is considered as an interface in the Network security section.

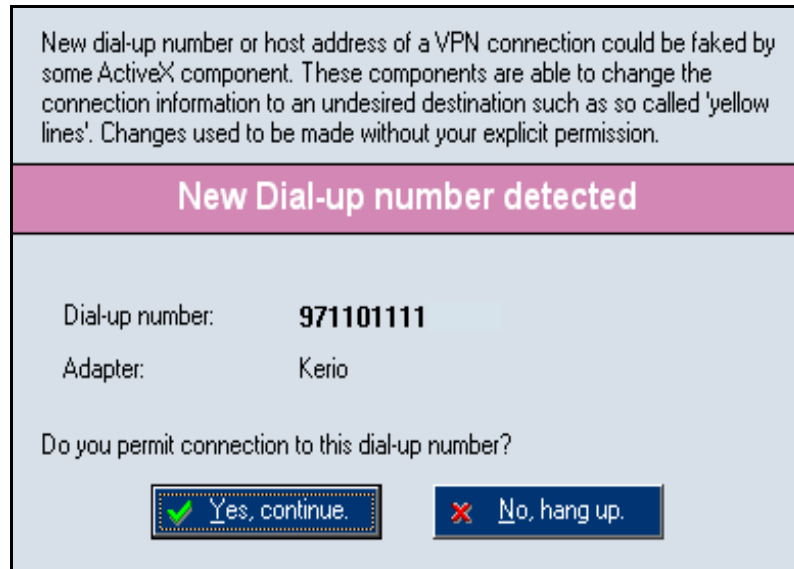


Figure 7-24 Detection of new dial-up number

If you click **Yes**, a dialog box opens. Set the interface parameters relating to the dial-up number.

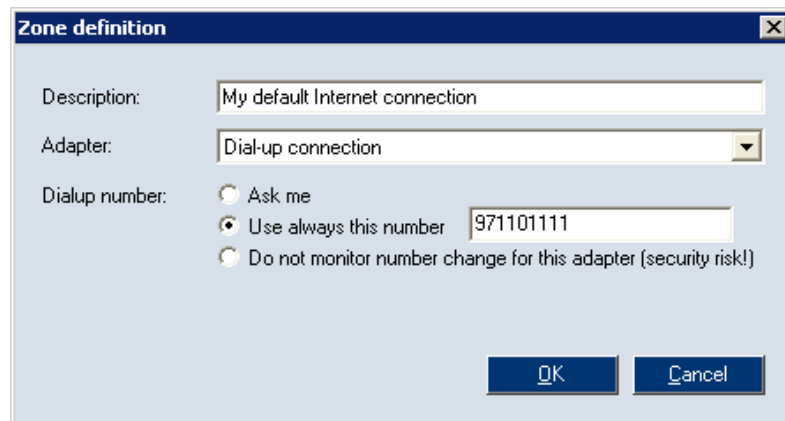


Figure 7-25 Checking of dialing telephone numbers settings

The following options are available for the Dialup number item:

- Ask — whenever a number is dialed, Sunbelt Personal Firewall asks you to accept or reject this number. If accepted, the firewall remembers the number. Otherwise, the line is hung-up immediately. If the new number is accepted, the Always use this number alternative is selected automatically and the number is saved.
- Always use this number — this option tell the firewall that the dial-up number is not to be changed. Whenever a change is detected, the New dial-up number dialog box opens and the user is asked to accept or reject the change.

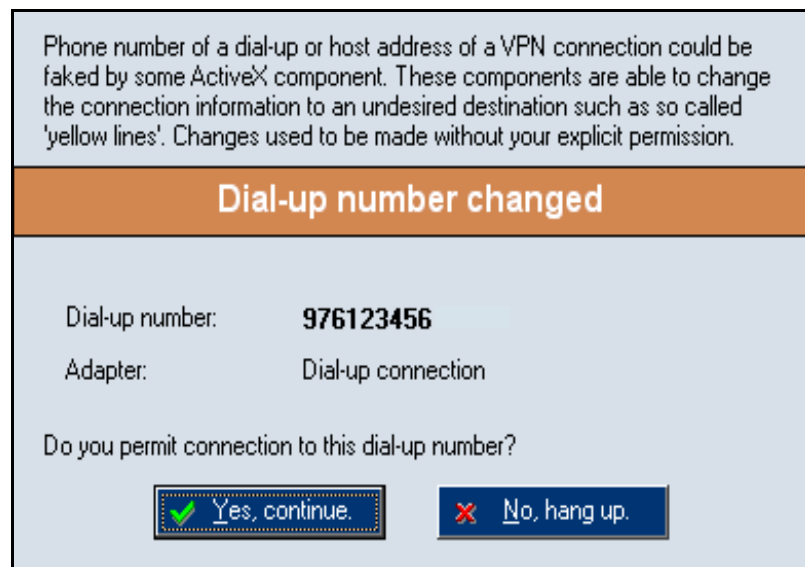


Figure 7-26 Dial-up number changed

The Dial-up number item provides the new telephone number (the number that is currently set for the dial-up connection).

Click Yes, continue so that Sunbelt Personal Firewall accepts the number, or No, to hang up to reject the change.

- Do not monitor number change — the firewall ignores changes to the dial-up number and always permits the line to be dialed. This option can be used in cases such as testing.



**Warning:** *This option is not secure (the firewall does not detect possible changes of the dial-up number) and it is not recommended to use it for the default dial-up connection!*



## Internal Firewall Rules

---

Sunbelt Personal Firewall includes predefined rules that allow network communication for specific cases (i.e. license registration, product update, etc.). These rules also allow some applications (system components) to startup. Internal firewall rules are applied prior to user-defined rules. Internal rules cannot be disabled nor modified. This chapter covers the following topics:

Section	Page
Internal Network Traffic Rules	8-2
System Security Rules	8-4
AVG Component Rules	8-6

## Internal Network Traffic Rules

Internal network traffic rules enable network traffic between individual firewall components during local or remote administration, Sunbelt Software registration, or check for new versions. Internal network traffic rules are not displayed in Personal Firewall user interface.

### Remote configuration

This rule allows a remote Personal Firewall GUI to connect to the Personal Firewall Engine. If remote administration is enabled, connections from any host are permitted. If not, only a connection from local host is enabled.

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Rem. adm. enabled	kpf4ss.exe	incoming	TCP+UDP	44334	any
Rem. adm. disabled	kpf4ss.exe	incoming	TCP+UDP	44334	localhost

### Communication between the Personal Firewall GUI and the Engine

This rule allows the Personal Firewall GUI to connect to the Personal Firewall Engine (connection to local administration).



**Note:** This rule allows only local connections (i.e. connections to the Personal Firewall Engine installed on the same computer). In case of remote administration, the Personal Firewall GUI is considered as a standard network application and network traffic policy is applied.

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Unconditional	kpf4gui.exe	outgoing	TCP+UDP	44334	any

### Communication from the Personal Firewall Engine to the GUI

This rule allows the Personal Firewall Engine to connect to the Personal Firewall GUI (displaying dialogs, notices, warning messages, etc.).

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Rem. adm. enabled	kpf4ss.exe	outgoing	TCP+UDP	any	any
Rem. adm. disabled	kpf4ss.exe	outgoing	TCP+UDP	any	localhost

### DNS Queries

This rule allows Sunbelt Personal Firewall components to send DNS queries to any DNS server. DNS queries are used to map host names that will be displayed in the Personal Firewall GUI, resolve destination IP addresses when accessing a remote administration, etc.

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Unconditional	kpf4ss.exe	both	UDP	53	any
Unconditional	kpf4gui.exe	both	UDP	53	any

### Sending Crashdump Files

If sending crashdump files is enabled, this rule allows the files to be sent to a corresponding server.

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Sending allowed	assist.exe	outgoing	TCP	any	crashes.sunbelt.com

### Logging of blocked pop-up and pop-under windows

If pop-up blocking is enabled, a special script, used for corresponding web pages, transmits Personal Firewall Engine information about blocked pages. Traffic is allowed through a TCP protocol, port (44501).

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Unconditional	any	outgoing	TCP	44501	localhost

### Update checker

This rule allows access to servers where new versions of Sunbelt Personal Firewall can be downloaded.



**Note:** The server is not specified since various servers can be used for this purpose.

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Proxy server	kpf4ss.exe	outgoing	TCP	proxy_port*	proxy_ip*
Direct access	kpf4ss.exe	outgoing	TCP	any	any

The Personal Firewall automatically resolves the connection between the IP address and the port proxy server.

### Product registration

This rule allows Sunbelt Personal Firewall license registration on a corresponding server.

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Proxy server	kpf4ss.exe	outgoing	TCP	prx_port*	prx_ip*
Direct access	kpf4ss.exe	outgoing	TCP	443	secure.sunbelt.com

The Personal Firewall automatically resolves the connection between the IP address and the port proxy server.



## Syslog

If logging to the Syslog server is enabled, this rule allows the Personal Firewall Engine to connect to the Syslog server.

Condition	Application	Direction	Protocol	Rem. port	Rem. address
Syslog enabled	kpf4ss.exe	outgoing	UDP	sslg_port*	sslg_ip*

IP address and port of the Syslog server specified in the Syslog section of the Settings tab.

## System Security Rules

The rules listed below allow various components of the operating system to startup. Internal system security rules are listed in this section. These rules cannot be removed, however, users can set actions for them (logging, notices, etc.).

Some of these internal rules are applied only in certain versions of Windows operating systems (some system components differ in individual versions).

### Rules for Operating System components

The following symbols are used in the description of system component rules to define file path:

- WIN\_DIR — the main directory of the Windows operating system (typically, C:\WINNT for Windows NT/2000, C:\WISK33lzNDOWS for other versions)
- SYS\_DIR — system directory of Windows (typically, C:\WINDOWS\SYSTEM for Windows 98/Me, C:\WINNT\SYSTEM32 for Windows NT/2000, and C:\WINDOWS\SYSTEM32 for Windows XP)

### Rules which are common to all versions of Windows

<i>Application</i>	<i>Description</i>	<i>Start</i>	<i>Modify</i>	<i>Launch another</i>
WIN_DIR\explorer.exe	Windows Explorer	Permit	Ask	Permit

### Special rules for Windows 98/ME operating systems

<i>Application</i>	<i>Description</i>	<i>Start</i>	<i>Modify</i>	<i>Launch another</i>
SYS_DIR\systray.exe	System Tray	Permit	Ask	Permit

### Special rules for Windows NT/2000/XP operating systems

<i>Application</i>	<i>Description</i>	<i>Start</i>	<i>Modify</i>	<i>Launch another</i>
SYS_DIR\services.exe	Services app.	Permit	Ask	Permit
SYS_DIR\winlogon.exe	Logon app.	Permit	Ask	Permit

### Special rules for Windows 2000/XP operating systems

<i>Application</i>	<i>Description</i>	<i>Start</i>	<i>Modify</i>	<i>Launch another</i>
SYS_DIR\svchost.exe	Generic Host Proc.	Permit	Ask	Permit

**Special rules for Windows XP operating system**

<i>Application</i>	<i>Description</i>	<i>Start</i>	<i>Modify</i>	<i>Launch another</i>
SYS_DIR\logonui.exe	Logon UI	Permit	Ask	Permit
SYS_DIR\csrss.exe	Client Server	Permit	Ask	Permit
SYS_DIR\smss.exe	Client Server	Permit	Ask	Permit
SYS_DIR\svchost.exe	Generic Host Proc.	Permit	Ask	Permit

**Rules for Sunbelt Personal Firewall components**

These rules enable individual Sunbelt Personal Firewall applications to run using special auxiliary programs. The following rules are common to all supported versions of Windows.

The KPF\_DIR expression represents a directory (path) where the Sunbelt Personal Firewall is installed (typically, C:\Program Files\Sunbelt\Personal Firewall 4).

<i>Application</i>	<i>Description</i>	<i>Start</i>	<i>Modify</i>	<i>Launch another</i>
KPF_DIR\kpf4gui.exe*	KPF GUI	Permit	Permit + log	Permit
KPF_DIR\kpf4ss.exe*	KPF Service	Permit	Permit + log	Permit
KPF_DIR\assist.exe*	Core dumper	Permit	Permit + log	Permit
KPF_DIR\cfgconv.exe*	Conf. conv.	Permit	Permit + log	Permit

## AVG Component Rules

If the AVG antivirus is detected when the Sunbelt Personal Firewall is started first time (immediately after the installation or after the `kpf.cfg` configuration file is removed), the following rules that allow network traffic for the antivirus components are automatically added to the Network security/ Applications section.



Description	Trusted		Internet		Log	Alert
	In	Out	In	Out		
 avgemc.exe	? ask	✓ permit	? ask	✓ permit	-	-
 avginet.exe	? ask	✓ permit	? ask	✓ permit	-	-

Figure 8-1 Network Security — Rules for AVG components

- The first rule allows the AVG E-mail Scanner component to communicate with mail servers. All data between the mail client and servers passes through E-mail Scanner.
- The second rule enables automatic updates of the AVG and virus database at corresponding servers.

User can change the rules for the AVG. If these rules are removed, Sunbelt Personal Firewall treats the AVG communication as an unknown communication.



**Warning:** *If you really use AVG, we recommend you not to remove these rules. The removal might block automatic update (the antivirus would not be able to detect new viruses), or problems with email might arise.*



## Intrusion Detection

---

Sunbelt Firewall uses three systems to prevent network intrusions and malware installation, as well as behavior monitoring. This chapter covers the following topics:

Section	Page
Intrusions	9-2
Network Intrusion Prevention System	9-3
Host Intrusion and Prevention System	9-5
Application Behavior Blocking	9-9

## Intrusions

Use the three systems in the **Intrusions** section protect your computer against harmful intrusions:

- **Network intrusion prevention system (NIPS)** — this system recognizes and blocks various types of network intrusions by blocking network connections that might be used to transfer dangerous data.
- **Host intrusion detection and prevention system (HIPS)** — this system recognizes and blocks malware used by intruders or viruses to run malicious codes.
- **Behavior Blocking** — this system monitors application behavior, such as an application being started by another process or modified application.

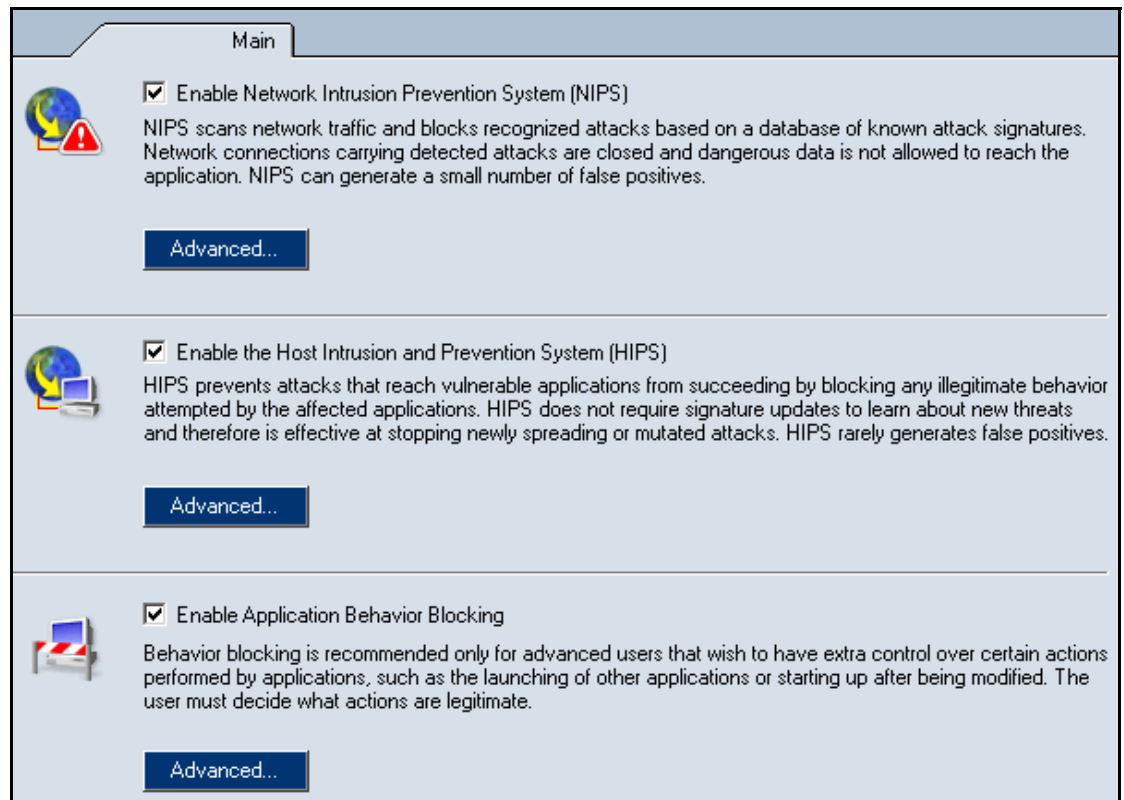


Figure 9-1 Intrusions - Main

## Network Intrusion Prevention System (NIPS)

Sunbelt Personal Firewall detects and blocks many types of network intrusions. It uses an internal intrusion database that is automatically updated each time a new version of the firewall is installed or updated. This is one reason you should update Sunbelt Personal Firewall after receiving an alert that an update is available.

The Sunbelt Personal Firewall uses the Network Intrusion Detection and Prevention System (NIPS) to scan network traffic and block attacks based on a database of known attack signatures.



**Note:** NIPS rules are stored in the `config\IDSRules` subdirectory of the installation directory (`C:\Program Files\Sunbelt\Personal Firewall 4\config\IDSRules` by default).

### NIPS Parameters

NIPS parameters enable you to set specific actions for high, medium, and low priority intrusions, as well as whether or not the intrusions will be recorded in the NIPS log.

#### To enable NIPS and set NIPS parameters

- 1 Click **Intrusions**. The **Main** tab opens. See *Figure 9-1 Intrusions* on page 9-2.
- 2 Select the **Enable Network Intrusion Prevention System (NIPS)** check box.
- 3 Click **Advanced**. The **Intrusion Prevention System Settings** dialog box opens.

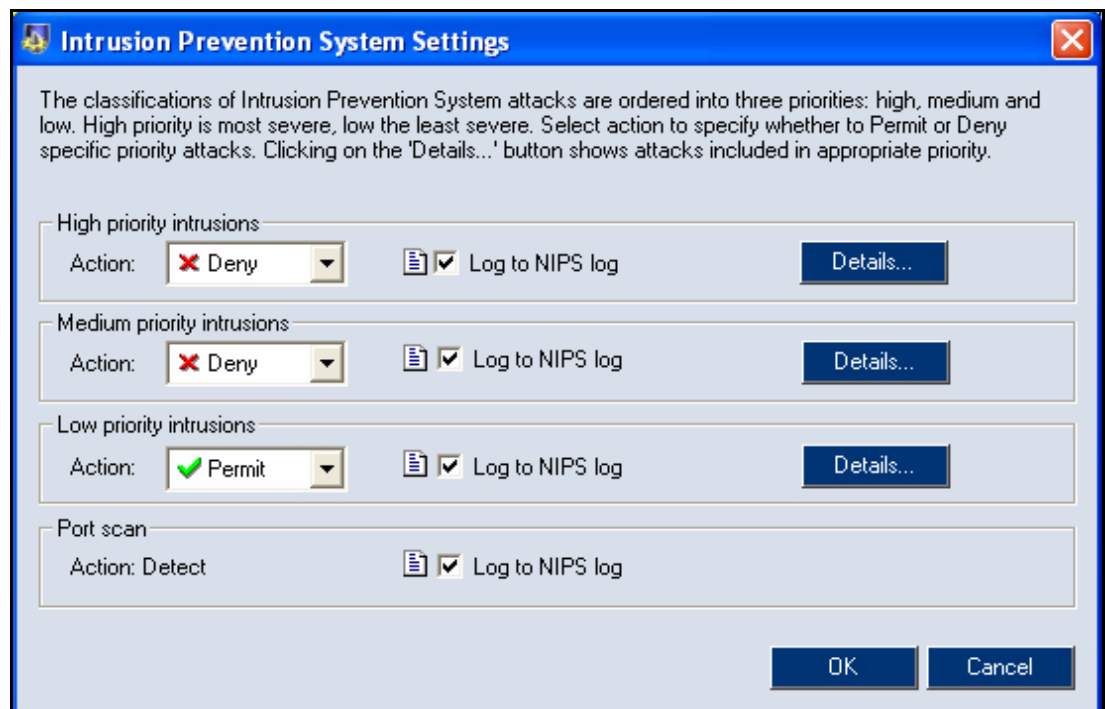


Figure 9-2 Intrusions — NIPS Settings

## 4 Make a selection:

To...	...select...
set an action for critical intrusions that could seriously damage your computer,	<i>Permit</i> or <i>Deny</i> from the <b>Action</b> drop-list under <b>High Priority Intrusions</b> . We recommend setting the action to <i>Deny</i> .
set an action for medium intrusions like blocked services or connections,	<i>Permit</i> or <i>Deny</i> from the <b>Action</b> drop-list under <b>Medium Priority Intrusions</b> . We recommend setting the action to <i>Deny</i> .
set an action for low-level intrusions like errors, invalid formats, etc.,	<i>Permit</i> or <i>Deny</i> from the <b>Action</b> drop-list under <b>Low Priority Intrusions</b> . We recommend setting the action to <i>permit</i> . You do not want to block necessary services.
record high, medium, and low priorities to the NIPS log,	the <b>Log to NIPS log</b> check box under the <b>High, Medium, and Low priority Intrusion</b> sections.
record the results of port scans to the NIPS log,	the <b>Log to NIPS log</b> check box under the <b>Port scan</b> section. Port Scans are attacks that detect open ports on a particular computer. Attack to open ports cannot be blocked, they can only be detected. Closed ports are blocked automatically.

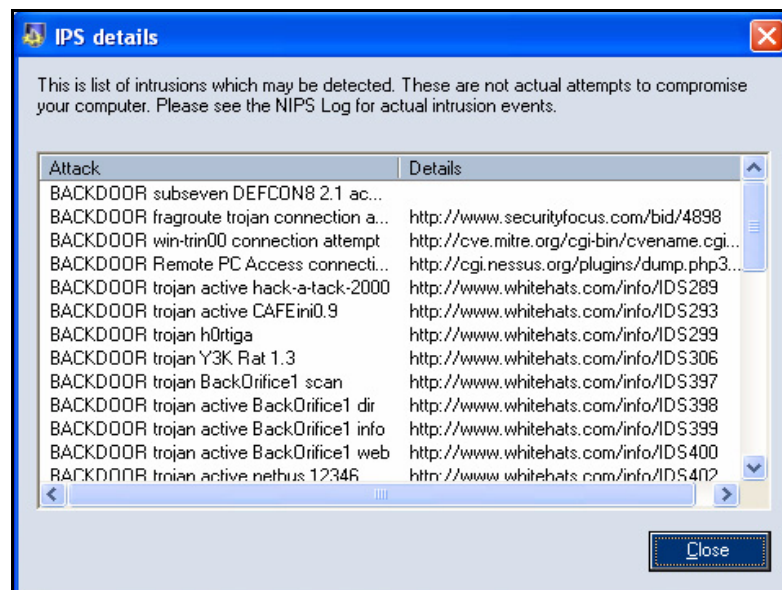
5 Click **Details...** The **IPS details** dialog box opens. It lists the possible intrusions. Click **Close** to return to the **Intrusion Prevention System Settings** dialog box.

Figure 9-3 Intrusions - Details

The IPS Details dialog box lists describes the type of attack and where you can find more information.

6 Click **OK** to save the parameters and return to the **Main** tab.

## Host Intrusion and Prevention System (HIPS)

Host Intrusion Prevention System (HIPS) targets applications or viruses trying to harm your computer. Disabling harmful applications helps protect you from security leaks in applications running on the server.

### Buffer Overflow

A buffer is an area on your computer reserved for temporarily storing information while it is waiting to be transferred between locations (either on your computer or between your computer and another device).

### Buffer Overflow

Buffer overflow is when a process attempts to store more data in a buffer than there is memory allocated for it. The extra data overwrites adjacent memory locations. Buffer overflows can cause processes to crash or produce incorrect results. They can be triggered by applications or viruses designed to execute malicious code or to make the program operate in an unintended way.

### Code Injection

Code injection is a technique used to insert malicious code into a running computer process. This can be done either locally or remotely through the web. Locally means that an application writes malicious code into another application's address space; when run, it appears as if the host application is responsible. The malicious code is executed using a trustworthy process.

### HIPS configuration

HIPS parameters enable you to limit and control the size of buffers and prevent code injection.

#### To enable HIPS and set HIPS parameters

- 1 Click **Intrusions**. The **Main** tab opens. See *Figure 9-1 Intrusions on page 9-2*.
- 2 Select the **Enable Host Intrusion Prevention System (HIPS)** check box.
- 3 Click **Advanced**. The **Host Intrusion Prevention System - Advanced Settings** dialog box opens.

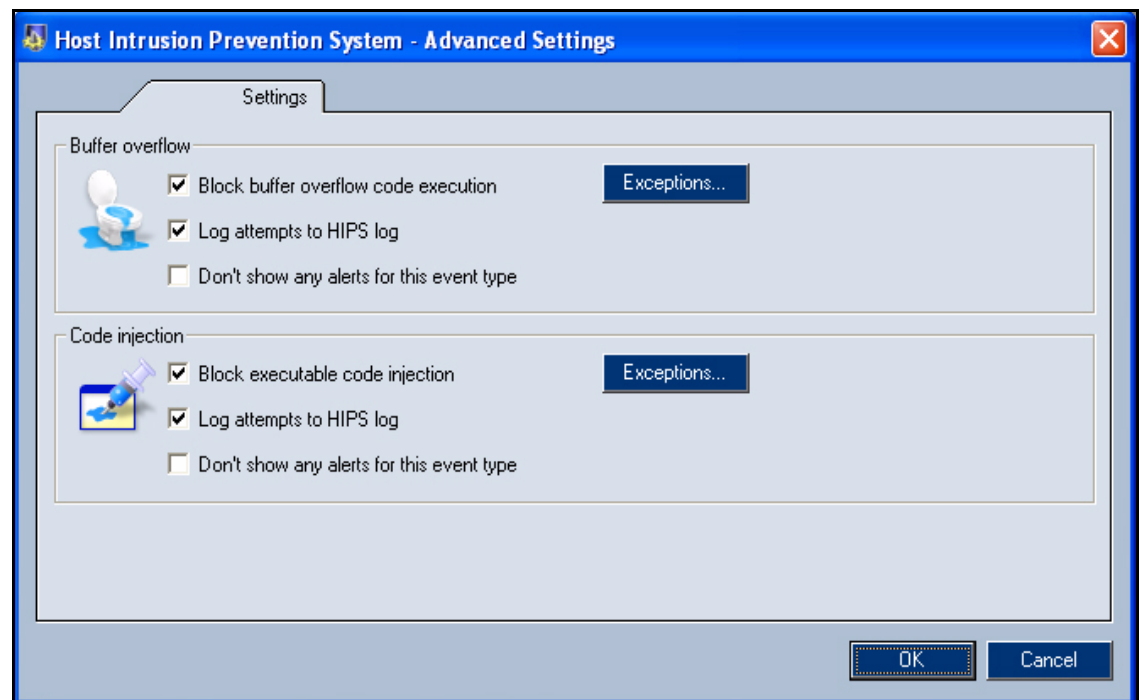


Figure 9-4 Intrusions – Host Intrusion Prevention System - Advanced Settings



4 Make a selection under **Buffer overflow**:

To...	...select the...
a disable codes from executing in case of buffer overflow,	<b>Block buffer overflow code execution</b> check box.
log code executions attempted during buffer overflow to the HIPS log,	<b>Log attempts to HIPS log</b> check box.
disable alert windows that would notify you if a code attempts to execute during buffer overflow,	<b>Don't show any alerts for this event type</b> check box.

5 To specify an executable to which a buffer overflow alert will not apply, click **Exceptions...** The **Buffer Overflow Exceptions** dialog box opens. See to add an exception to buffer overflow parameters, page 9-7.

6 Make a selection under **Code injection**:

To...	...select the...
block malicious code form being injected into running processes,	<b>Block executable code injection</b> check box.
log code injection attempts to the HIPS log,	<b>Log attempts to HIPS log</b> check box.
disable alert windows that would notify you if a code attempts inject itself into a running process,	<b>Don't show any alerts for this event type</b> check box.

7 To specify an executable to which a code injection alert will not apply, click **Exceptions....** The **Code Injection Exceptions** dialog box opens. See to add an exception to code injection parameters, page 9-8.

Code injection technology is used by various legitimate applications — these applications will not function correctly. Sunbelt Personal Firewall allows to define exceptions, i.e. list of applications which can use this technology. Exception for an application can be defined in the Code injection exceptions dialog (opened by the Exceptions option) where a relevant executable file can be browsed.

8 Click **OK** to save the parameters and return to the **Main** tab.

### To add an exception to buffer overflow parameters

- 1 Open the **Host Intrusion Prevention System - Advanced Settings** dialog box; then click **Exceptions...** under the *Buffer overflow* section. The **Buffer Overflow Exceptions** dialog box opens.

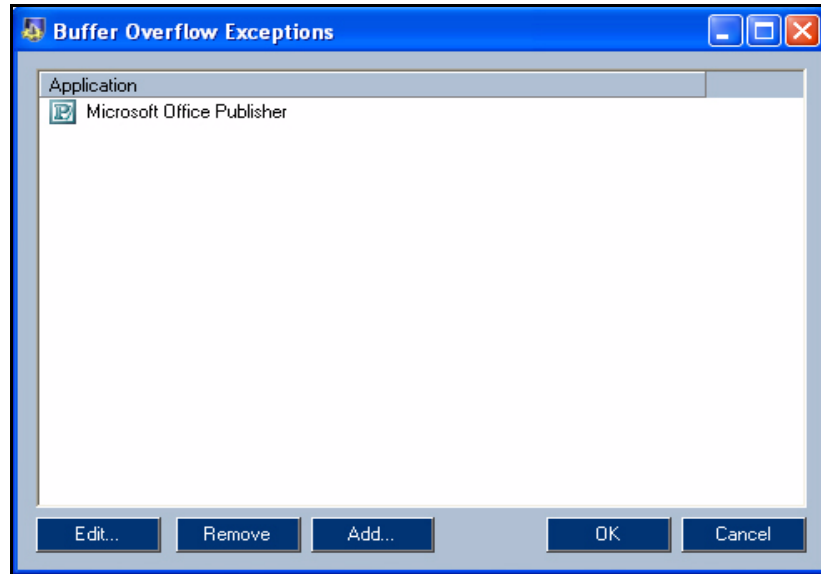


Figure 9-5 Intrusions - Buffer Overflow Exceptions

- 2 Make a selection:

To...	...click...
edit an existing item,	<b>Edit...</b> after selecting an item from the list. The <b>Edit Buffer Overflow Exception</b> dialog box opens. Click <b>Browse...</b> to search for then select an item; then click <b>OK</b> .
remove an existing item,	<b>Remove</b> . The item is removed from the list.
add a new item,	<b>Add...</b> The <b>Edit Buffer Overflow Exception</b> dialog box opens. Click <b>Browse...</b> to search for then select an item; then click <b>OK</b> .

- 3 Click **OK**. You return to the **Host Intrusion Prevention System - Advanced Settings** dialog box.

### To add an exception to code injection parameters

- 1 Open the **Host Intrusion Prevention System - Advanced Settings** dialog box; then click **Exceptions...** under the **Code injection** section. The **Code Injection Exceptions** dialog box opens.

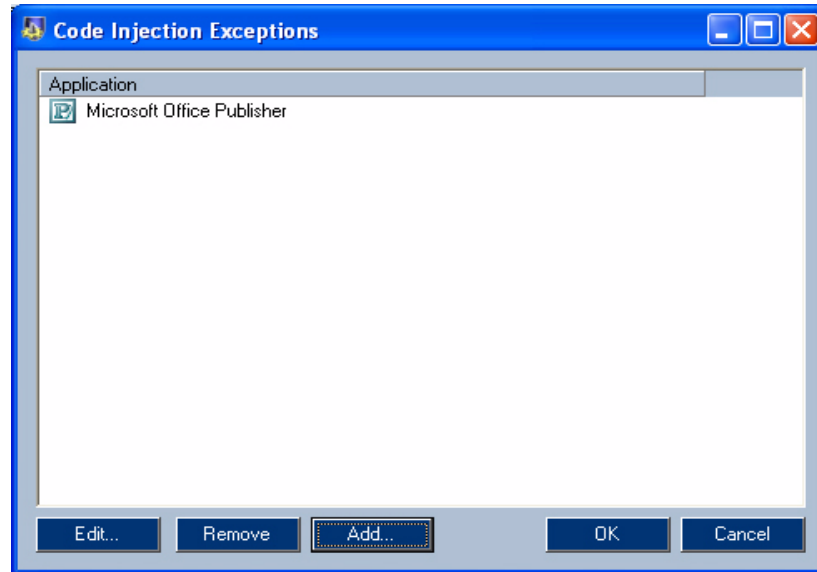


Figure 9-6 Intrusions - Code Injection Exceptions

- 2 Make a selection:

To...	...click...
edit an existing item,	<b>Edit...</b> after selecting an item from the list. The <b>Edit Code Injection Exception</b> dialog box opens. Click <b>Browse...</b> to search for then select an item; then click <b>OK</b> .
remove an existing item,	<b>Remove</b> . The item is removed from the list.
add a new item,	<b>Add...</b> The <b>Edit Code Injection Exception</b> dialog box opens. Click <b>Browse...</b> to search for then select an item; then click <b>OK</b> .

- 3 Click **OK**. You return to the **Host Intrusion Prevention System - Advanced Settings** dialog box.

## Application Behavior Blocking

Sunbelt Personal Firewall controls all applications used in the operating system, regardless of whether or not they use network communication. This control enables it to immediately detect when an application is infected by a new virus or attacked by malware. This differs from anti-virus (AV) software in that AV software usually takes some time to detect a virus; then, it must find an appropriate virus database.

### Application behavior Blocking Configuration

Use Application Behavior Blocking to set behavior blocking parameters that enable you to control applications on your computer.

#### To enable application behavior blocking and set blocking parameters

- 1 Click **Intrusions**. The **Main** tab opens. See *Figure 9-1 Intrusions on page 9-2*.
- 2 Select the **Enable Application Behavior Blocking** check box.
- 3 Click **Advanced**. The **Application Behavior Blocking** dialog box opens.

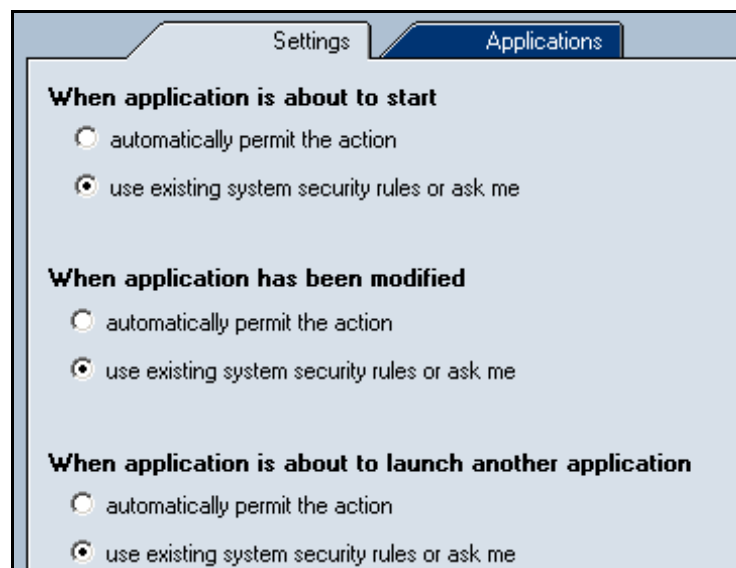


Figure 9-1 Behavior Blocking - Settings Tab

Rules in the Main tab define how the firewall will behave in the following situations:

- When application is about to start – the action is taken at the time the application launches.
- When application has been modified – the action is taken at the time an application's executable file is modified. Each time an application is started and exited, Sunbelt Personal Firewall creates a snap shot of the application parameters. The next time it starts the application, it creates a new snap shot and compares it to the previous one.
- When application is about to launch another application – the action is taken when another application is started by a application that is already running.

One of the following options can be set for each of the situations

- automatically permit the action — Sunbelt Personal Firewall does not block application startup (it accepts change of the executable file)
- use existing behavior blocking rules or ask me — a behavior blocking rule for a particular application will be used (if it exists) or user will be asked

- Click the **Applications** tab to view and edit rules for startup and change of particular applications.

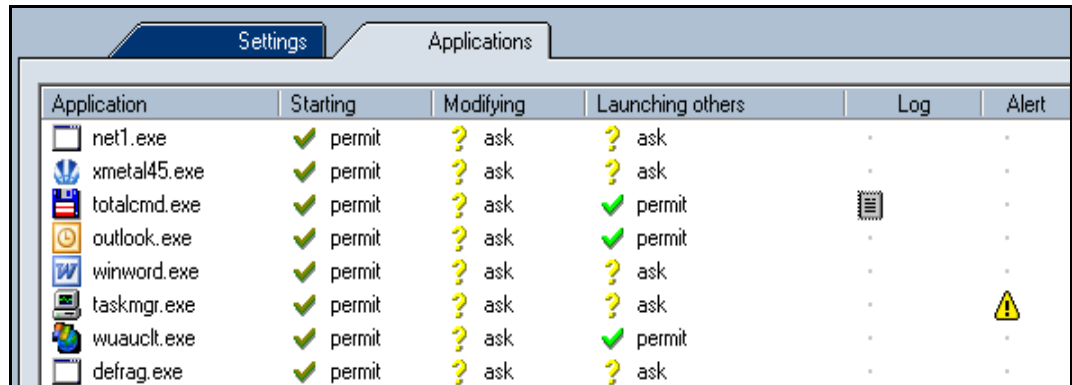


Figure 9-2 Behavior Blocking - Application Tab

These rules are created when you respond to alerts. After permitting or denying a communication alert, a rule for that application is added to this list. You cannot create rules on this tab, only edit or remove them.

- Make a selection:

To...	...select...
edit an application rule,	a rule from the list; then, click <b>Edit</b> . The <b>Behavior Block for [name of app]</b> dialog box opens. See procedure below.
remove an application from the list,	a rule from the list; then, click <b>Remove</b> .

#### To edit an application rule

- Select an application from the list.
- Click **Edit**. The **Behavior Block for [name of app]** dialog box opens.

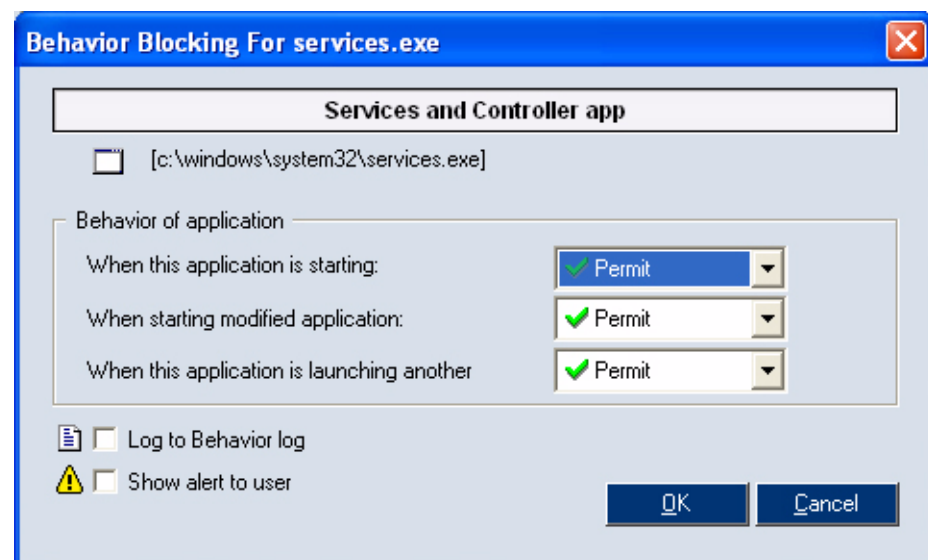


Figure 9-3 Intrusions - Behavior Blocking: Edit Application Rule

3 Make a selection:

To...	...select...
set the behavior of the application when it starts,	<i>Permit</i> , <i>Ask user</i> , or <i>Deny</i> from the <b>When this application is starting</b> drop-list.
set the behavior of the application if it starts after being modified,	<i>Permit</i> , <i>Ask user</i> , or <i>Deny</i> from the <b>When starting modified application</b> drop-list.
set the behavior for the application of it starts another application,	<i>Permit</i> , <i>Ask user</i> , or <i>Deny</i> from the <b>When this application is launching another</b> drop-list.
record communications to the behavior log,	the <b>Log to Behavior log</b> check box.
make sure the user see an application alert,	the <b>Show alert to user</b> check box.

4 Click **OK**. You return to the **Application Behavior Blocking** dialog box.

If you want to make quick changes to the actions for an application, there are two other ways to available to make those changes:

- Click an action under the **Modifying** or **Launching others** headings; then, toggle through the *permit*, *deny* and *ask* options.
- Right-click an action; then, make a selection from the context menu



Figure 9-4 Behavior Blocking — application rules — action selection



## Web Content Filtering

---

Use Web Content Filtering to block ads, set privacy parameters, and establish which web sites meets exceptions to the blocking rules. This chapter covers the following topics:

Section	Page
Ad Blocking, Privacy, and Site Exception parameters.	10-2
Site Exceptions	10-5

## Ad Blocking, Privacy and Site Exception Parameters

Use the **Ad Blocking** tab to set the parameters need to filter advertisements, pop-ups, and web content.

### To configure ad blocking, privacy, and site exception parameters

- 1 Click **Web**. The **Ad Blocking** tab is already selected.

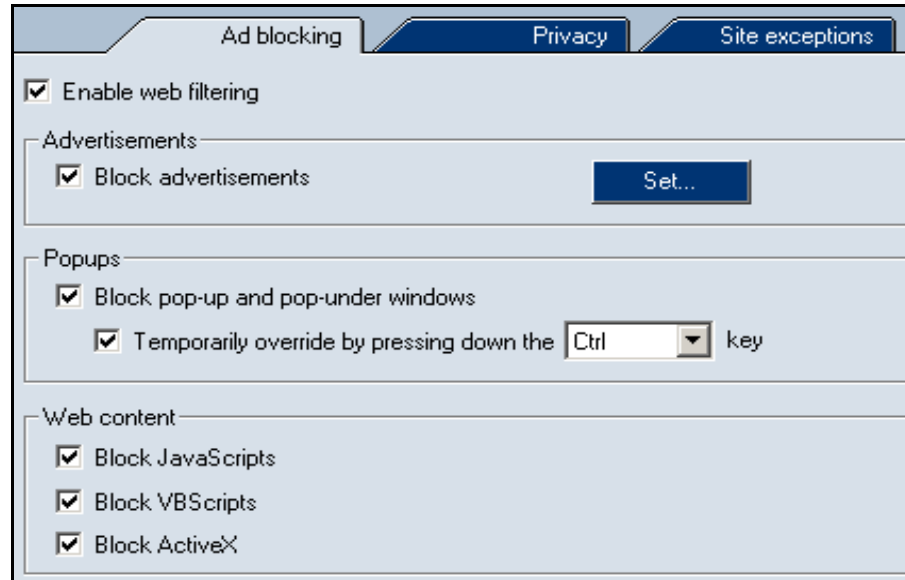


Figure 10-1 Web - Ad blocking

- 2 Select the **Enable web filtering** check box.
- 3 Make a selection:

To...	...select the...
enable web filtering	<b>Enable web filtering</b> check box.
block advertisements according to defined rules,	<b>Block advertisements check box</b> under the <b>Advertisements</b> section; then, click <b>Set...</b> See <i>To block ads by URL</i> , page 10-4.
block pop-ups and pop-under windows,	<b>Block pop-up and pop-under windows</b> check box under the <b>Popups</b> section. A pop-under window is one that opens under the active browser window.
temporarily override the pop-up and pop-under blocking using the Ctrl or F12 key,	<b>Temporarily override by pressing down the [key name] Key</b> check box under the <b>Popups</b> section. Select the Ctrl or F12 from the drop-list.
block JavaScripts,	<b>Block JavaScripts</b> check box under the <b>Web content</b> section.
block visual basic scrips,	<b>Block VBScripts</b> check box under the <b>Web content</b> section.
block ActiveX,	<b>Block ActiveX</b> check box under the <b>Web content</b> section.





**Warning:** The F12 key may cause a conflict with the Microsoft debugger. If you use the Microsoft Visual Studio, we recommend using the Ctrl key.



**Note:** The java and VB script options might cause problems displaying of some pages. If so, define special rules for such page in the Exception Sites tab, or disable the Block pop-up and pop-under windows option, and use another method to filter ads (i.e. the Block advertisements option).

- 4 Click the **Privacy** tab.
- 5 Make a selection:

To...	...select the...
filter cookies from third-party servers,	<b>Filter foreign cookies</b> check box under <b>Cookies</b> .
filter cookies that send information each time a web site is visited,	<b>Filter persistent cookies</b> check box under <b>Cookies</b> .
temporary cookies that are only used when a user opens a particular page,	<b>Filter session cookies</b> check box under <b>Cookies</b> .
block the URL address of the page from which the user opened the current page so that your browsing habits cannot be easily monitored,	<b>Deny servers to trace web-browsing</b> check box under <b>Referer</b> .
block your private information from being sent through forms on web pages,	<b>Block private information</b> check box under <b>Private Information</b> ; then, click <b>Set...</b> . The <b>Blocked private information</b> dialog box opens.

- 6 Click the **Site exceptions** tab.
- 7 To add a web server for which special filter rules will be defined, click **Add...** See *To add a site exception, page 10-5*.
- 8 Make a selection:

To...	...select...
edit a web server for which special filter rules will be defined,	a web server from the list; then, click <b>Edit</b> .
remove a web server,	a web server from the list; then, click <b>Remove</b> .

- 9 Click **OK** to save the information and close the **Sunbelt Personal Firewall** window, or click **Apply** to save the information and keep the window open.

### To block ads by URL

- 1 Click **Web**; then, **Set...** on the **Ad Blocking** tab. The **Advertisement blocking by URL** dialog box opens.

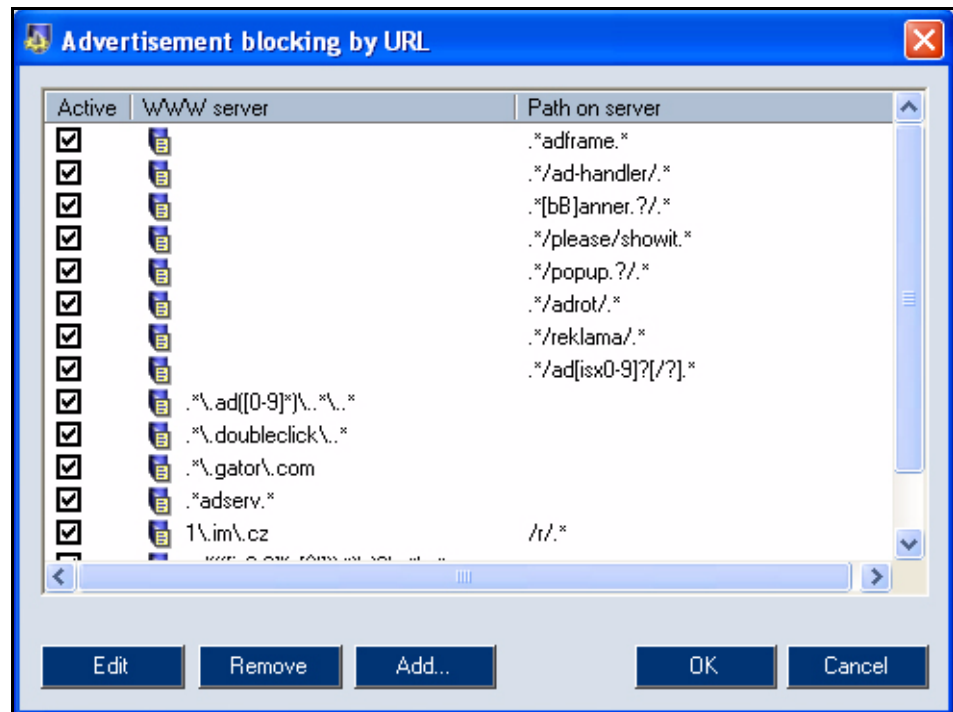


Figure 10-2 Web - Advertisement Blocking by URL

- 2 To add a server to the list, click **Add...** See To add a web server to the advertisement blocking list, below.
- 3 Make a selection:

To...	...select...
edit a web server,	a web server from the list; then, click <b>Edit</b> .
remove a web server,	a web server from the list; then, click <b>Remove</b> .

- 4 Click **OK**. You return the **Ad Blocking** tab.

### To add a web server to the advertisement blocking list

- 1 Click **Web**; then **Set** on the **Ad Blocking** tab. The **Advertisement blocking by URL** dialog box opens.
- 2 Click **Add...** The **Advertisement filter editing** dialog box opens.
- 3 Type the name of the web server in the **WWW server** field.
- 4 If you want to block a path to a specific object on the server, type the path in the **Path on server** field.
- 5 Click **OK**.

## Site Exceptions

Exceptions for individual Web servers are helpful especially when the general content filter rules cause certain Web pages or some of their items to not function properly (i.e. new windows cannot be opened, it is not possible to login through an email address, etc.). Sometimes they are completely blocked.

Before you define a rule exception for a server, consider carefully whether the server is trustworthy or not, and the types of objects (scripts, cookies, private data) that are required for smooth functionality. The Exception tab includes one predefined rule. This rule allows automatic Microsoft updates and allows updates from windowsupdate.microsoft.com.

### To add a site exception

- 1 Click **Web**; then the **Site exceptions** tab.
- 2 Click **Add...**. The Edit exception site dialog box opens.

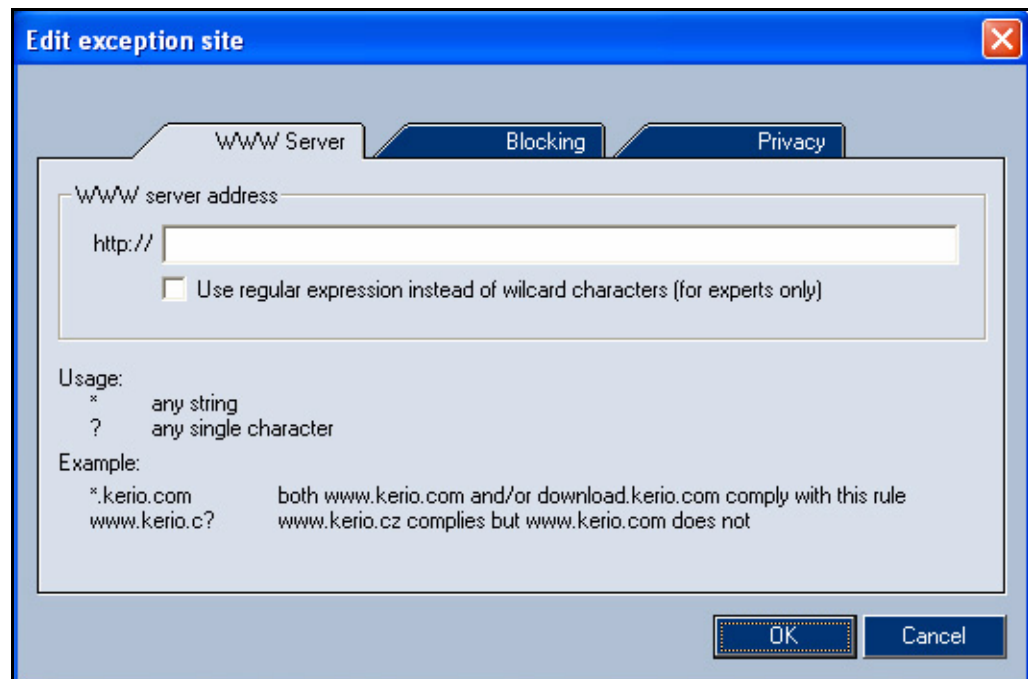


Figure 10-3 Web - Add/Edit Site Exception Rule

- 3 Type the URL of the server in the **http://** field.
- 4 To add blocking and privacy information specific to this site instead of using the general parameters set on the **Ad Blocking** and **Privacy** tabs in the main window, click the **Blocking** and **Privacy** tabs; then set the parameters. See *To add blocking privacy, and site exception parameters, page 10-2*.



## Logs & Alerts

---

Logs store the history of module: Network, System, Intrusions and Web. The other logs (Error, Warning and Debug) store information about Sunbelt Personal Firewall processes. This information can help the Sunbelt technical support team to solve possible problems with the firewall. This chapter covers the following topics:

Section	Page
Viewing Logs and Alerts	11-2
Context Menu	11-3
Log Options	11-4
Network Log	11-5
NIPS Log	11-6
HIPS Log	11-7
Behavior Log	11-8
Web Log	11-9
Debug, Error, and Warning Logs	11-10

## Viewing Logs and Alerts

Log files are stored in the logs in a subdirectory where Sunbelt Personal Firewall is installed (typically C:\Program Files\Sunbelt\Personal Firewall 4\logs). The file has the .log extension (i.e. network.log). An index file is included in each log. This file has the .idx extension (i.e. network.log.idx).

### To view module logs and set logging parameters

- 1 Click Logs & Alerts. The **Logs** tab opens.

Line	C...	Application	D...	Local point	Remote point	Protocol	Descri
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	172.16.1.128:3957	194.108.44.6:53	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	192.168.81.41:1593	192.168.81.1:53	UDP	Permit
4...	1	svchost.exe	→	192.168.81.41:3957	192.168.81.1:53	UDP	Permit
4...	1	ashwebsv....	→	172.16.1.128:2145	217.11.249.137:80	TCP	Permit
4...	1	ashwebsv....	→	172.16.1.128:2147	194.228.110.30:80	TCP	Permit
4...	1	firefox.exe	→	172.16.1.128:2150	194.108.44.19:80	TCP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	System	→	172.16.1.128:138	172.16.1.255:138	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	firefox.exe	→	172.16.1.128:2155	194.108.44.19:443	TCP	Permit
4...	1	firefox.exe	→	172.16.1.128:2156	194.108.44.19:443	TCP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit
4...	1	firefox.exe	→	172.16.1.128:2165	194.108.44.19:443	TCP	Permit
4...	1	svchost.exe	→	169.254.127.219:68	169.254.127.218:67	UDP	Permit

Figure 11-1 Logs & Alerts - Logs Tab

- 2 Click a module tab at the bottom to view information specific to that module.
- 3 To re-order the log items in a particular list, click a column heading.

For technical reasons (data size), complete log files are not downloaded to the disc. Only the part that will be viewed is downloaded. Therefore, the following difficulties may occur:

- Logs display slowly.
- When re-ordering the columns only the part of the log that is being viewed is displayed. The items re-ordered again to view another part of the log.



**Note:** The Error, Warning and Debug logs are not available from the Sunbelt Personal Firewall user interface. They can only be viewed only as files.

## Context Menu

Set basic parameters for the Logs & Alerts section using the context menu.

### To set basic parameters using the context menu

- 1 Click **Logs & Alerts**. The **Log** tab opens.
- 2 Right-click inside the tab to open a context menu providing options for a particular log:

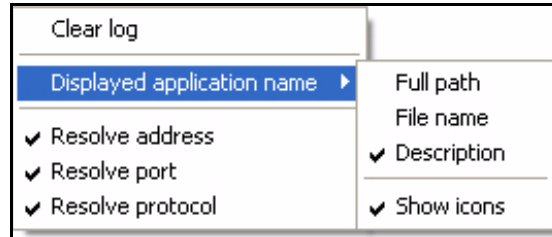


Figure 11-2 Logs & Alerts - The Log Context Menu

- 3 Make a selection:

To...	...select...
remove all data from the log file,	Clear log.
determine how the application names are listed,	Displayed application name; then select one of the following from the sub-menu: <ul style="list-style-type: none"> <li>• Full path – full path to the application's executable file</li> <li>• File name – name of the application's executable</li> <li>• Description – description of the application (if it is not available, name of the executable without the extension is displayed)</li> <li>• Show icons – display the application or system icon for an application.</li> </ul>
list the computer by name instead of IP address,	Resolve address. If a name is not found, the IP address will be listed.
list the service name instead of port numbers,	Resolve port.
list the protocol names instead of the protocol numbers,	Resolve protocol.



**Note:** Some logs do not provide all of the items mentioned above, i.e. network communication is not displayed for the System log. Therefore Resolve address, Resolve port and Resolve protocol functions are not available.

The Displayed application name and Resolve address/port/protocol options are applied globally. Their settings influences all logs, the Overview>Connections section, Connection alert and Starting/Replacing application dialogs, and the Alert window.

## Log Options

Use the Settings tab to set general log parameters and options.

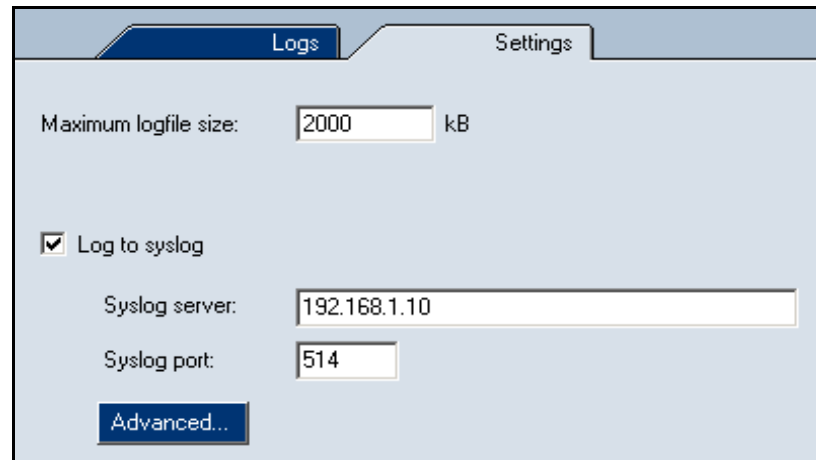


Figure 11-3 Logs & Alerts - Settings

### To set log and alert parameters

- 1 Click **Logs & Alerts**; then the **Settings** tab.
- 2 Type the maximum size (in kilobytes) for the log file in the **Maximum log file size** field. If the size is exceeded, the file is removed and a new log is started.
- 3 To log files to the syslog server, select the **Log to syslog** check box; then do the following:
  - Type the Syslog server IP address in the **Syslog server** field.
  - Type the Syslog port number in the **Syslog port** field.
  - Click **Advanced...** to open the **Advanced syslog settings** dialog box and select the items that will be logged to the syslog.

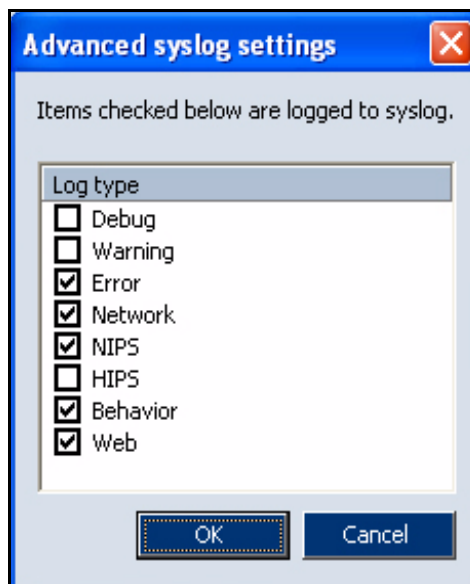


Figure 11-4 Logs & Alerts Advanced Syslog Settings

- 4 Click **OK** to save the settings and close the **Sunbelt Personal Firewall** window, or click **Apply** to save the settings and keep the window open.

## Network Log

The Network tab lists information on network traffic that meets an application or packet filter rule. Traffic is not logged unless the Log communication to network log option is enabled. The Network log provides the following information:

Line	Count	Date	Application	Direction	Local...	Remote point	Protoc
0	1	06/Aug/2003 16:55:10	 Mozilla	 out	ferda...	128.242.10...	TCP
1	1	06/Aug/2003 16:55:12	 Mozilla	 out	ferda...	128.242.10...	TCP

Figure 11-5 Logs & Alerts - Network log

- Line — line where the item can be found in the log.
- Count — number of time the item is recorded in the log. If one record is repeated in sequence, it is logged once and the real count is expressed by a number).
- Date — date and time the event was logged.
- Description — description of a particular packet filter rule.
- Application — name of a local application participating in the particular network communication.



**Note:** Both a description the applications and the full paths to their executable files are saved into the log file. Therefore, you can switch between the two items and select which one is displayed.

- Direction — direction of the connection
- Local point — local IP address (name of the computer)
- Remote point — IP address (name) of the remote computer
- Protocol — used communication protocol (TCP, UDP, etc.)
- Action — action which was taken:
  - permitted — the communication was permitted
  - denied — the communication was denied
  - asked>permitted — user was asked through the Connection alert dialog and the communication was permitted
  - asked>denied — user was asked through the Connection alert dialog and the communication was denied



## NIPS Log

The NIPS tab lists information about detected network intrusions. The NIPS log lists the following information:

Logs		Settings				
Line	Count	Date	Description	Direction	Source of attack	Attack class
742	1	03/Nov/2004 09:10:30	PortScan	in	62.141.3.139	network-scan
743	1	03/Nov/2004 09:10:51	PortScan	in	62.141.3.139	network-scan
744	1	03/Nov/2004 09:39:11	DOS Teardrop attack	in	217.11.251.145	attempted-dos
745	1	03/Nov/2004 10:44:52	ICMP L3retriever Ping	in	192.168.44.137	attempted-recon
746	1	03/Nov/2004 15:31:26	PortScan	in	62.141.3.139	network-scan
747	1	03/Nov/2004 15:32:00	PortScan	in	62.141.3.139	network-scan
748	1	03/Nov/2004 15:41:36	ICMP L3retriever Ping	in	192.168.44.137	attempted-recon
749	1	03/Nov/2004 16:07:49	ICMP L3retriever Ping	in	192.168.44.137	attempted-recon
750	1	03/Nov/2004 16:31:21	DOS Teardrop attack	in	217.11.251.145	attempted-dos

Figure 11-6 Logs & Alerts - NIPS log

- Line — line where the item can be found in the log.
- Count — number of time the item is recorded in the log. If one record is repeated in sequence, it is logged once and the real count is expressed by a number).
- Date — date and time the event was logged
- Description — name (description) of detected intrusion
- Direction — direction of the intrusion (intrusions might be also initiated from local computers)
- Source of attack — IP address (or DNS name) of the remote host from which the attack came, if identifiable (attacks can be sent from false IP addresses).
- Attack class — the class the attack belongs to
- Priority — priority group to which the attack is sorted by Sunbelt Personal Firewall
- Action — action performed by Sunbelt Personal Firewall when the attack was detected (permitted — attack permitted, denied — attack denied)

## HIPS Log

The HIPS tab lists information about detected attacks to applications. Blocked attacks are highlighted in red.

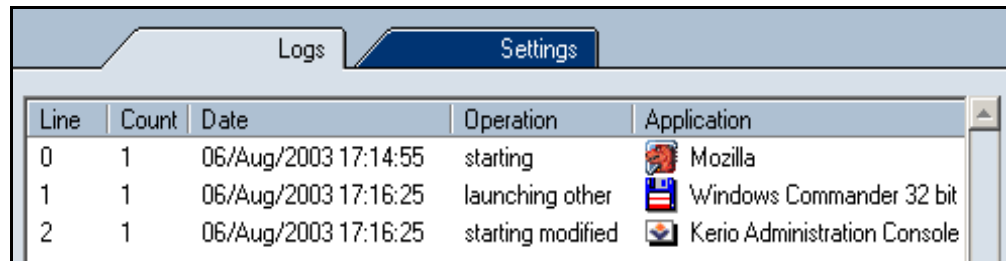
Line	Count	Date	Action	Intrusion Type	Description
0	1	07/Feb/2005 11:13:56	denied	Code injection	Process 'c:\copycat.exe' is trying to inject dangerous c
1	1	11/Apr/2005 09:43:24	denied	Code injection	Process c:\copycat.exe injected dangerous code into
2	1	11/Apr/2005 09:44:05	denied	Code injection	Process c:\copycat.exe injected dangerous code into
3	1	11/Apr/2005 09:45:53	denied	Code injection	Process c:\copycat.exe injected dangerous code into
4	1	11/Apr/2005 09:53:44	denied	Code injection	Process c:\copycat.exe injected dangerous code into

Figure 11-7 Logs & Alerts - HIPS log

- Line — line where the item can be found in the log.
- Count — number of time the item is recorded in the log. If one record is repeated in sequence, it is logged once and the real count is expressed by a number).
- Date — date and time the event was logged
- Action — actions taken by Sunbelt Personal Firewall in response to the attack (permitted or denied)
- Attack class — name of the detected attack

## Behavior Log

The Behavior tab lists information about running applications that meet the corresponding rules in Application Behavior Blocking in the Intrusions section. The Behavior log provides the following information:



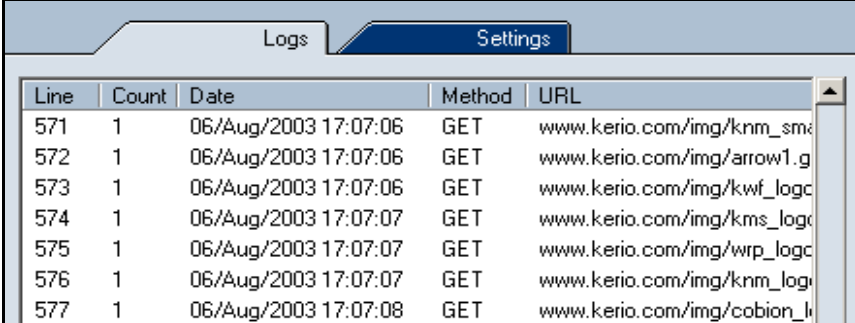
Line	Count	Date	Operation	Application
0	1	06/Aug/2003 17:14:55	starting	Mozilla
1	1	06/Aug/2003 17:16:25	launching other	Windows Commander 32 bit
2	1	06/Aug/2003 17:16:25	starting modified	Kerio Administration Console

Figure 11-8 The Logs section — The Behavior log

- Line — line where the item can be found in the log.
- Count — number of time the item is recorded in the log. If one record is repeated in sequence, it is logged once and the real count is expressed by a number).
- Date — date and time the event was logged
- Operation — operation type:
  - starting — the application is starting
  - starting modified — executable file of the application has been changed
  - launching other — the application is launching another application
- Application — application name (with respect to the Displayed application name parameter)
- Subject — this item represents name of an application started by the original application (with respect to the Displayed application name parameter)
- Action — action which was taken:
  - permitted — running the application has been permitted
  - denied — running the application has been denied
  - asked>permitted — user was asked through the Starting/Replacing application alert, and starting the application was permitted
  - asked>denied — user was asked through the Starting/Replacing/Launching other application dialog and starting the application was denied

## Web Log

The Web tab lists information about objects blocked by the Web content filter. This log is not configurable. The Web log provides the following information:



Line	Count	Date	Method	URL
571	1	06/Aug/2003 17:07:06	GET	www.kerio.com/img/KNM_smc
572	1	06/Aug/2003 17:07:06	GET	www.kerio.com/img/arrow1.g
573	1	06/Aug/2003 17:07:06	GET	www.kerio.com/img/kwf_logc
574	1	06/Aug/2003 17:07:07	GET	www.kerio.com/img/kms_logc
575	1	06/Aug/2003 17:07:07	GET	www.kerio.com/img/wrp_logc
576	1	06/Aug/2003 17:07:07	GET	www.kerio.com/img/KNM_logc
577	1	06/Aug/2003 17:07:08	GET	www.kerio.com/img/cobion_li

Figure 11-9 The Logs section — The Web log

- Line — line where the item can be found in the log.
- Count — number of time the item is recorded in the log. If one record is repeated in sequence, it is logged once and the real count is expressed by a number).
- Date — date and time the event was logged
- Method — method used by the HTTP protocol (GET or POST)
- URL — URL address of the page to which the method is applied
- Subject — type of blocked item (referer, cookie, blockPopups)
- Value — value of this item (content of the Referer: item, information in cookie or rule which was used to block the ad)
- Action — type of action taken (Removed — the item was removed from the Web page, Blocked — the item was blocked by ad rules)

Information provided within the Value item depends on the type of blocked object:

- Advertisement — the Value column lists information on the rule that was applied
- the Referer item — the Value column lists URL address of the page to which the item refers
- Script — the Value column lists the filtered object type (JavaScript, VBScript or ActiveX).
- blockPopups — the ON expression in the Value column informs users that pop-up and pop-under window blocking is enabled for the particular page.

## **Debug, Error, Warning Logs**

The Error, Warning and Debug logs are not available from the Sunbelt Personal Firewall's user interface — they can only be opened as files in the Logs sub-directory of the directory where Sunbelt Personal Firewall is installed (typically C:\Program Files\Sunbelt\Personal Firewall 4\logs). The file itself has the .log extension (e.g. error.log).

### **Debug Log**

The Debug log lists detailed information on all processes of Sunbelt Personal Firewall.

### **Error Log**

The Error log lists errors that seriously affect Sunbelt Personal Firewall functionality (i.e. the Firewall Engine cannot start).

### **Warning Log**

The Warning log lists less important errors (i.e. an error detected when a new version verification is performed, etc.).



## Open-source libraries

---

This product includes the following open-source libraries:

### **libiconv**

Libiconv converts from one character encoding to another through Unicode conversion.

Copyright ©1999-2003 Free Software Foundation, Inc.

Author: Bruno Haible

### **OpenSSL**

Toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

### **zlib**

Zlib is a general purpose data compression library.

Copyright ©1995-2003 Jean-Loup Gailly and Mark Adler.



## Glossary

---

### **Application protocol**

Application protocols are transmitted in packets of TCP or UDP protocol. They are used for transmission of user (application) data. In addition to standard application protocols which are available (i.e. SMTP, POP3, HTTP, FTP, etc.), application programmers may use a custom (non-standard) method for communication.

### **Buffer**

A region of memory reserved for use as an intermediate repository in which data is temporarily held while waiting to be transferred between two locations or devices. For instance, a buffer is used while transferring data from an application, such as a word processor, to an input/output device, such as a printer.

### **Cookie**

Information in text format that the server stores at a client (Web browser). It is used for later identification of a user when the same server/site is opened again. Cookies can be misused for monitoring which sites have been visited by a user, or they can be used for visit counter.

### **DHCP**

Acronym for Dynamic Host Configuration Protocol. A TCP/IP protocol that enables a network connected to the Internet to assign a temporary IP address to a host automatically when the host connects to the network. See also IP address, TCP/IP. Compare dynamic SLIP.

### **DNS**

Acronym for Domain Name System. The hierarchical system by which hosts on the Internet have both domain name addresses (such as `bluestem.prairienet.org`) and IP addresses (such as `192.17.3.4`). The domain name address is used by human users and is automatically translated into the numerical IP address, which is used by the packet-routing software. DNS names consist of a top-level domain (such as `.com`, `.org`, and `.net`), a second-level domain (the site name of a business, an organization, or an individual), and possibly one or more sub-domains (servers within a second-level domain). See also domain name address, IP address. 2. Acronym for Domain Name Service. The Internet utility that implements the Domain Name System. DNS servers, also called name servers, maintain databases containing the addresses and are accessed transparently to the user. See also Domain Name System (definition 1), DNS server.

### **Firewall**

A tool (usually a software product) for protection from intrusions and from data outflow. Two basic firewall types are available:

- network firewall — protects computers of a network. Usually, it is used as a gateway (router) through which the particular network is connected to the Internet.

- personal firewall — protects one computer (user's workstation). Unlike network firewalls, it can match network communication with a particular application, change its behavior accordingly to interaction with users, etc.

Note: In this guide the word firewall represents Sunbelt Personal Firewall.

## **IDS**

Acronym for Intrusion Detection System. A type of security management system for computers and networks that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, both inside and outside the organization. An IDS can detect a wide range of hostile attack signatures, generate alarms, and, in some cases, cause routers to terminate communications from hostile sources.

## **ICMP**

Acronym for Internet Control Message Protocol. A protocol used for transmission of control messages. Several types of such messages are available, such as a report that the destination is not available, redirection request or response request (used in the PING command).

## **IGMP**

Acronym for Internet Group Membership Protocol. A protocol used by IP hosts to report their host group memberships to any immediately neighboring multicast routers.

## **IP**

Acronym for Internet Protocol. A protocol transmitting all Internet protocols in its data part. The header of this protocol provides essential routing information, such as source and destination IP address (which computer sent the message and to which computer the message should be delivered).

## **Packet**

A packet is a file that is sent between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, web page request, etc.) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into smaller chunks or *packets* so the file can be easily sent. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a file may travel different routes through the Internet. However, when they all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

## **Packet Filtering**

On the Internet, packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet mangling and Network Address Translation (NAT). Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion.

In a software firewall, packet filtering is done by a program called a packet filter. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides to prevent it from passing (called DROP) or allow it to pass (called ACCEPT).

## **POP3**

## **Port**

The most essential information in TCP and UDP packet is the source and destination port. The IP address identifies a computer in the Internet, whereas a port identifies an application running on the computer. Ports 1-1023 are reserved for standard services and the operating system, whereas ports 1024-65535 can be used by any application. In a typical client to server connection, usually the destination port is known (connection is established for this port or UDP datagram is sent to it). The source port is then assigned by the operating system automatically.



**PPTP**

Acronym for Point-to-Point Tunneling Protocol. An extension of the Point-to-Point Protocol used for communications on the Internet. PPTP was developed by Microsoft to support virtual private networks (VPNs), which allow individuals and organizations to use the Internet as a secure means of communication. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection. See also virtual network.

**SMTP****TCP**

Acronym for Transmission Control Protocol. TCP is a secure protocol that is used to send a data transmission through a virtual channel (connection). It is used as a transmission protocol for most application protocols, such as SMTP, POP3, HTTP, FTP, Telnet, etc.

**TCP/IP**

TCP/IP is a general term for protocols used in communication over the Internet. Data is divided into data items called packets within individual protocols. Each packet consists of a header and a data part. The header includes routing information (i.e. source and destination address) and the data part contains transmitted data.

The Internet protocol stack is divided into several levels. Packets of lower protocols encapsulate parts of higher-level protocols in their data parts (i.e. packets of TCP protocol are transmitted in IP packets).

**UDP**

Acronym for User Datagram Protocol. A protocol without a connection. This implies that it does not create any connection and data is transmitted in individual messages (so called datagrams). UDP does not warrant reliable data delivery (datagrams can be lost during transmission). However, unlike transmission through TCP protocol, it provides faster data transmission (it is not necessary to establish connections or provide reliability control, confirmation is not demanded, etc.). UDP protocol is used especially for transmission of DNS queries, audio files, video files, or other types of streaming media which promote speed over reliability.

**VPN**

Acronym for Virtual Private Network. Nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines. 2. A WAN (wide area network) formed of permanent virtual circuits (PVCs) on another network, especially a network using technologies such as ATM or frame relay.

# Index

- A**
- Advertisement Blocking List
    - add web server to 10-4
  - Alerts
    - application 5-6
    - connection 5-3
    - for connections with rules 5-10
    - host intrusion 5-8
  - Application Alert 5-6
  - Application Behavior Blocking 9-9
  - Application Rules
    - additional options 7-6
    - defining 7-4
    - settings 7-5
  - AVG Component Rules 8-6
- B**
- Behavior Log 11-8
  - Block ads by URL 10-4
  - Boot-time Protection 7-24
- C**
- Components 1-3
  - Components and Control Features 4-1
    - Components 4-2
    - system tray icons 4-2
  - Configure
    - ad blocking parameters 10-2
    - privacy parameters 10-2
    - site exception parameters 10-2
  - Conflicting Software 1-5
  - Connection Alert 5-3
  - Connection Alerts 5-3
  - Connections with Rules 5-10
  - Context Menu
    - set basic parameters 11-3
- D**
- Debug Log 11-10
- E**
- Error Log 11-10
- F**
- Firewall Behavior and User Interaction 5-1
    - application alert 5-6
    - connection alert 5-3
    - connection alerts 5-3
    - connections with rules 5-10
    - host intrusion alert 5-8
    - Overview 5-2
  - Firewall Configuration 6-1
    - interface 6-2
    - set preferences 6-9
    - working with network connections 6-5
    - working with statistics 6-7
  - Firewall Preferences 6-9
    - back-up and restore config files 6-11
    - configuration 6-11
    - configure 6-9
    - password protection 6-11
    - preferred language 6-14
    - remote administration 6-12
    - set password 6-12
  - Functions and Features 1-4
- H**
- HIPS Log 11-7
  - Host Intrusion Alert 5-8
  - HostIntrusion and Prevention System 9-5
- I**
- Installation
    - before you install 2-2
    - initial settings 2-8
    - installation 2-2
    - uninstall 2-9
    - upgrading current version 2-10
    - upgrading to new version 2-8
  - Interface 6-2
    - action buttons 6-4
    - modules 6-2
    - network traffic graph 6-3
  - Internal Firewall Rules 8-1
    - AVG component rules 8-6
    - network traffic rules
      - Network Traffic Rules 8-2
      - system security rules 8-4
  - Intrusion Detection 9-1
    - Application Behavior Blocking 9-9
    - HIPS 9-5
    - intrusions 9-2
    - NIPS 9-3
- L**
- Log
    - behavior 11-8
    - debug 11-10
    - error 11-10
    - HIPS 11-7
    - network 11-5
    - NIPS 11-6
    - warning 11-10
    - web 11-9

Log Options  
set 11-4

Logging Parameters  
set 11-2

Logs and Alerts 11-1  
viewing 11-2

## **M**

Module Logs  
view 11-2

## **N**

Network Connections 6-5  
manage options 6-6

Network Intrusion Prevention System 9-3

Network Log 11-5

Network Security 7-1  
advanced settings 7-23  
application rules 7-3  
boot-time protection 7-24  
detecting new network interfaces 7-25  
how rules are applied 7-2  
packet filter rules 7-7  
Predefined Rules 7-20  
rules 7-2  
trusted area 7-22  
verifying dialed numbers 7-26  
what is it? 7-2

NIPS Log 11-6

## **O**

Overview 1-2

## **P**

Packet Filter Rules  
adding a rule 7-10  
inside 7-9  
IP groups 7-18  
manually define 7-7  
proper functionality 7-9  
protocol parameters 7-15

parameters  
ad blocking 10-2  
privacy 10-2  
site exception 10-2

Predefined Rules  
manage 7-20

Purchasing and Product Registration 3-1  
free vs full version 3-2  
purchasing SKPF 3-2  
Registration 3-3

## **R**

References 1-5

## **S**

Site Exceptions  
add 10-5

Statistics 6-7  
viewing statistics for specific time frame 6-8

Styles 1-5

Styles and references 1-5

System Requirements 1-4

System Security Rules 8-4

System Tray Icons 4-2

## **U**

Uninstalling SKPF 2-9

Upgrading 2-8, 2-10

## **V**

Viewing Logs and Alerts 11-2

## **W**

Warning Log 11-10

Web Content Filtering 10-1  
ad blocking parameters 10-2  
privacy parameters 10-2  
site exception parameters 10-2  
site exceptions 10-5

Web Log 11-9

Web Server  
add to advertisement blocking list 10-4