



Sunbelt Kerio **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) 2004-2005 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

Introduction	1-1
Components	1-1
Functions and Features	1-3
System Requirements	1-3
Conflicting Software	1-4
Styles and References	1-4
Installation	2-1
Install the Personal Firewall	2-1
Upgrade	2-2
Uninstall	2-2
Initial Configuration	2-2
Update Checks	2-3
Product Registration and Licensing Policy	3-1
Limited Free Edition	3-1
Product registration	3-1
Registration wizard	3-4
Firewall Components and Basic Control Features	4-1
Personal Firewall Components	4-1
Systray Icons	4-2
Firewall Behavior and Interaction with Users	5-1
Firewall Behavior	5-1
Connection Alert (unknown traffic detection)	5-2
Starting/Replacing/Launching other application Dialog	5-5
Host Intrusions Alerts	5-8
Alert Dialog Window (alerts on events)	5-9
Firewall Configuration	6-1
Configuration Dialog	6-1
Remote Admin	6-4
Preferences	6-7
Network Security	7-1
How the Firewall Policy is Applied	7-1
Rules for Applications	7-2
Network Security Predefined Rules	7-7
Trusted Area	7-9
Network security Advanced settings	7-10
Boot time protection	7-12
Detection of new network interfaces	7-13
Checking of dialed telephone numbers	7-14
Advanced Packet Filter	8-1
Packet Filter Rules	8-1
IP Groups	8-9
Internal Firewall Rules	9-1
Internal Network Traffic Rules	9-1
System Security Rules	9-4
Rules for AVG components	9-6
Intrusion Detection	10-1
Network Intrusions Prevention System (NIPS)	11-1
NIPS Settings	11-1

Host Intrusion Prevention System (HIPS)	12-1
HIPS configuration	12-1
Behavior Blocking	13-1
General Rules	13-1
Application Rules	13-2
Web Content Filtering	14-1
The Ad Blocking tab	14-1
The Privacy tab	14-5
The Exceptional sites tab (exceptions for individual servers)	14-7
Status Information	15-1
Connections and Open Ports Overview	15-1
Statistics	15-3
Logs	16-1
Logs Viewing	16-1
Logs Context Menu	16-2
Log Options	16-3
Network Log	16-5
NIPS Log	16-6
HIPS Log	16-7
Behavior Log	16-8
Web Log	16-9
Debug, Error, Warning Logs	16-10
Used open-source libraries	17-1
Glossary	18-1



Introduction

Sunbelt Kerio Personal Firewall is a software application protecting personal computers with Windows from external intrusions (typically from the Internet), viruses and data leak.

Components

Security is provided using the following components:

Network Security

This module controls all network (TCP/IP) traffic of the computer on which *Sunbelt Kerio Personal Firewall* is installed. Two types of rules can be defined for network communication:

- application rules — it is possible to permit/deny network communication for individual applications or set that *Sunbelt Kerio Personal Firewall* asks user.
- packet filter rules — advanced packet rules for network traffic can be defined (specification of IP addresses, protocols, ports, etc.). These rules can be applied either on individual applications or generally (on any application).

Sunbelt Kerio Personal Firewall includes set of predefined network security rules (i.e. for DNS, DHCP, etc.). These rules are separated from user-defined rules and they can be enabled or disabled.

Whenever *Sunbelt Kerio Personal Firewall* detects traffic which does not meet any rule, user will be asked to permit or deny the communication. Optionally, a corresponding application or packet filter rule can be created automatically upon this decision.

Behavior Blocking

The Behavior Blocking module controls running applications in the operating system. The following event types are controlled:

running applications

replacements of the application's executable file since the last startup (application replacement)

running another application by the particular application

Like in case of network traffic, rules for individual applications can be defined. These rules either permit or deny the event, eventually they ask user. If a communication does not meet any rule, *Sunbelt Kerio Personal Firewall* automatically asks user to permit or deny running the application.



Note: *Sunbelt Kerio Personal Firewall 4.x* (unlike older versions) controls running of all applications, regardless of the fact whether they participate in network communication or not. When infected, the firewall is more reliable than any antivirus (if the virus is new and it is not included in a particular virus database, antivirus is not able to detect it — *Sunbelt Kerio Personal Firewall* detects replacement of the executable file and warns user).

Network Intrusion Detection and Prevention

The *Network Intrusion Detection and Prevention System* (NIPS) can distinguish, block and log known intrusion types. For this purpose *Sunbelt Kerio Personal Firewall* uses database of known intrusions. This database is updated regularly (updated database is included in new product versions).

Host intrusion detection and prevention

Host intrusion detection and prevention system (HIPS — Host Intrusion Prevention System) detects attempts for misuse of running applications and processes to execute malicious code.

Web content filtering

This module enables the following features:

- blocking of ads (according to URI/URL rules), scripts and other Web items
- blocking of pop-up windows
- blocking of scripts (*JavaScript*, *VBScript*)
- protection from undesirable cookies storage and outflow of private data from Web application forms.

Exceptions (specific settings) can be defined for trustful servers and for cases when filtering might cause malfunctions.

Boot time protection

Sunbelt Kerio Personal Firewall's low-level driver protects the computer even when the firewall is not running (e.g. during the operation system reboot or during an installation of a new version of the firewall). This implies that the computer is protected all time it is available to external stations.

Functions and Features

The following functions and features are also provided by *Sunbelt Kerio Personal Firewall*:

Stop all traffic – Use this button (or the option in the menu) to stop all traffic on the computer on which *Sunbelt Kerio Personal Firewall* is installed (so called network lock). This function may be very helpful especially when an undesirable or a queer network activity is detected — traffic can be restored when appropriate actions are taken.

Logging – Each firewall module creates an independent log which is stored into a text file. Logs can be viewed in *Sunbelt Kerio Personal Firewall* configuration dialog. Optionally, logs can be stored on a *Syslog* server.

Connections overview and statistics – The overview provides information on established connections and ports opened by individual applications. Information on current speed and size of transmitted data in both directions is also provided for active connections. The overview is refresh automatically in predefined time intervals.

Statistics inform user on number of objects blocked by the Web content filter and number of detected intrusions per a certain time period.

Automatic update – *Sunbelt Kerio Personal Firewall* performs regular checks for new versions. Whenever a new version is detected, download and installation is offered. Checks for new versions can be also performed by hand.



Warning: *None of the versions of the Sunbelt Kerio Personal Firewall 4 can be used on Windows Server operating systems, such as Windows NT Server, Windows 2000 Server and Windows Server 2003.*

System Requirements

The following hardware and software equipment is required for *Sunbelt Kerio Personal Firewall* installation:

- Windows 98 / Me / NT 4.0 Workstation / 2000 Professional / XP Home / XP Professional operating systems
- CPU Intel Pentium or 100% compatible
- 64 MB RAM
- 8 MB of free disc space (for installation only, 10 MB recommended for log files)
- minimal screen resolution 800x600 pixels

Conflicting Software

Sunbelt Kerio Personal Firewall might conflict with certain application types which are based on identical or similar technologies as *Sunbelt Kerio Personal Firewall*. Sunbelt Software does not guarantee correct functioning of *Sunbelt Kerio Personal Firewall* nor your operating system if any of the following software applications are installed on the same operating system:

Personal firewalls

Personal firewalls (i.e. *Internet Connection Firewall* — a Windows XP component, *Zone Alarm*, *Sygate Personal Firewall*, *Norton Personal Firewall*, etc.) provide similar functions as *Sunbelt Kerio Personal Firewall*. Do not combine *Sunbelt Kerio Personal Firewall* with other firewalls.

Network firewalls




Network firewalls (i.e. *Kerio WinRoute Firewall*, *Kerio WinRoute Pro*, *Kerio WinRoute Lite*, *Microsoft ISA Server*, *CheckPoint Firewall-1*, *WinProxy* by Ositis, *Sygate Office Network*, *Sygate Home Network*, etc.) also protects the computer on which it is installed, it is therefore not necessary to use a personal firewall on such computer.



Note: To create an elementary network firewall, *Sunbelt Kerio Personal Firewall* can be combined with a router, with a router which performs translation of IP addresses (NAT) or with a proxy server — i.e. *Internet Connection Sharing* (included in newer Windows operating systems).

Styles and References

This guide uses the following styles and graphical references:

Style / Graphic	Used to:
ALL CAPS	indicate a keyboard button (Press ENTER).
BOLD	indicate a specific field, prompt, dialog, or Window (Type an IP address in the Address field).
<i>BOLD ITALIC</i>	indicate the action of clicking action buttons, Keys, links, menu bar items and menu selections (<i>OK</i> , <i>Close</i> , etc.).
<i>Italic</i>	emphasize program titles, window and web page names, key words, and “see” references. (Open the <i>Administrator Resource</i> web page).
Word>Strings	indicate a series of menu selections (Click View on the main menu bar; then, select Policy>Default).
	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

This chapter explains how to install, upgrade and uninstall Sunbelt Kerio Personal Firewall.

Install the Personal Firewall

Run the installation program (i.e. sunbeltkerio-pf-4.2.0-en-win.exe).

First, the program asks for selection of a language which will be used for guidance during the installation (English and German versions are available so far). This selection is applied only to the installation, whereas the user interface of the *Sunbelt Kerio Personal Firewall* can be switched to various language versions.

In the next step, a path where *Sunbelt Kerio Personal Firewall* will be installed can be chosen, (the C:\Program Files\Subelt\Personal Firewall path is used by default).

In this stage, default mode of the firewall is to be chosen. We recommend unexperienced users to use the default `Simple` mode. Experienced users can use the `Advanced` mode (behavior of the firewall in this mode is identical as in previous versions of the *Sunbelt Kerio Personal Firewall*). Anytime, these modes can be switched between.

Restart is necessary after a successful installation, so that the *Sunbelt Kerio Personal Firewall* low-level driver can be enabled. *Personal Firewall Engine* will be started automatically upon a restart of the operating system.



Warning: *If you intend to use Sunbelt Kerio Personal Firewall with the AVG antivirus, AVG must be installed before the Sunbelt Kerio Personal Firewall installation is initiated. If Sunbelt Kerio Personal Firewall detects the AVG antivirus when the firewall is started first time, corresponding rules will be set for the antivirus.*

Notes:

- Memory dump which can be used when the system crashes is created in Windows NT operating systems. User can send it to *Sunbelt Software* — analysis of the dump may help find and remove bugs and errors which caused the crash.
- Check an option to set memory dump generating in the operating system.
- If you use the Windows XP Service Pack 2 operating system or later, the installation program registers *Sunbelt Kerio Personal Firewall* in the *Windows Security Center*. During the installation, the firewall is registered as inactive. Upon its startup, *Sunbelt Kerio Personal Firewall* disables the integrated *Windows Firewall* if it is running.
- Under Windows 98, Me, NT 4.0 and 2000, update of the *Windows Installer* may be required unless it has been already updated (for example during another installation). Size of this update is approximately 1.8 MB. The up-to-date version of the installer must be downloaded

and installed, otherwise installation of the *Sunbelt Kerio Personal Firewall* cannot be completed!

Upgrade

Installation of a new version (upgrade) is performed in the same method as a new installation described above. It is not necessary to stop running components of the application since they will be automatically stopped and closed by the installation program.

Note: *Sunbelt Kerio Personal Firewall* includes a built-in system for automatic checks and downloads of updates.

Uninstall

Sunbelt Kerio Personal Firewall can be uninstalled using the *Add / Remove programs* option in the *Control Panel*. Files which have been created after the installation (configuration files, logs, etc.) will not be removed. After the uninstallation, these files can be either removed manually or kept for possible reinstallation.

Note: Under Windows XP Service Pack 2 and later, registration of the *Sunbelt Kerio Personal Firewall* in the *Windows Security Center* is scratched and the integrated *Windows Firewall* is enabled automatically upon uninstallation of the *Sunbelt Kerio Personal Firewall*.

Initial Configuration

Default mode of the firewall can be selected during installation of the *Sunbelt Kerio Personal Firewall*. The following modes are available:

Choice default mode of the firewall (during installation of the *Sunbelt Kerio Personal Firewall*)

- **Simple** — in this mode, the firewall enables all outgoing traffic and blocks any incoming communication. All network interfaces of the *Sunbelt Kerio Personal Firewall* host are automatically assigned to the Internet zone. The system security module is also disabled. According to these settings, the firewall never asks user and follows the default rules (the Ask action is not used by default). This behavior can be changed by modification of system and network security modules.



Note: *The only exception is confirmation of dial-up numbers — users are always asked if a new number is dialed or when a telephone number is changed, regardless of the current firewall mode.*

The Simple mode is set by default. It is recommended especially to beginners and users who cannot perform the initial configuration immediately after the installation.

- **Advanced (autodidactic mode)** — whenever an unknown communication is detected or an unknown application is started, the firewall asks user which action is to be taken and whether a rule would be created for this action. This way, step by step, a specific firewall configuration for a host and a user is being created.

If the Advanced mode is selected, the *Sunbelt Kerio Personal Firewall* detects active network interfaces of the computer on which it is installed upon the first startup. For each interface, the user is asked whether the interface is connected to a trustworthy network or not.

The Advanced mode sets the same behavior as all previous versions of the *Sunbelt Kerio Personal Firewall*. This mode is recommended to experienced users and to those users who want to use detailed custom settings.

Update Checks

Sunbelt Kerio Personal Firewall provides automatic checks for new versions. These versions, if detected, can be downloaded. Automatic checks are provided after each start of Personal Firewall Engine and then every 24 hours.

Checks for new versions can be also run by hand using the Check now button in the Overview / Preferences section of the Sunbelt Kerio Personal Firewall configuration dialog.

If you already have the latest version of Sunbelt Kerio Personal Firewall, the connection with the server is closed and the next check is scheduled. If a new version is detected, information on this version and its download is provided.

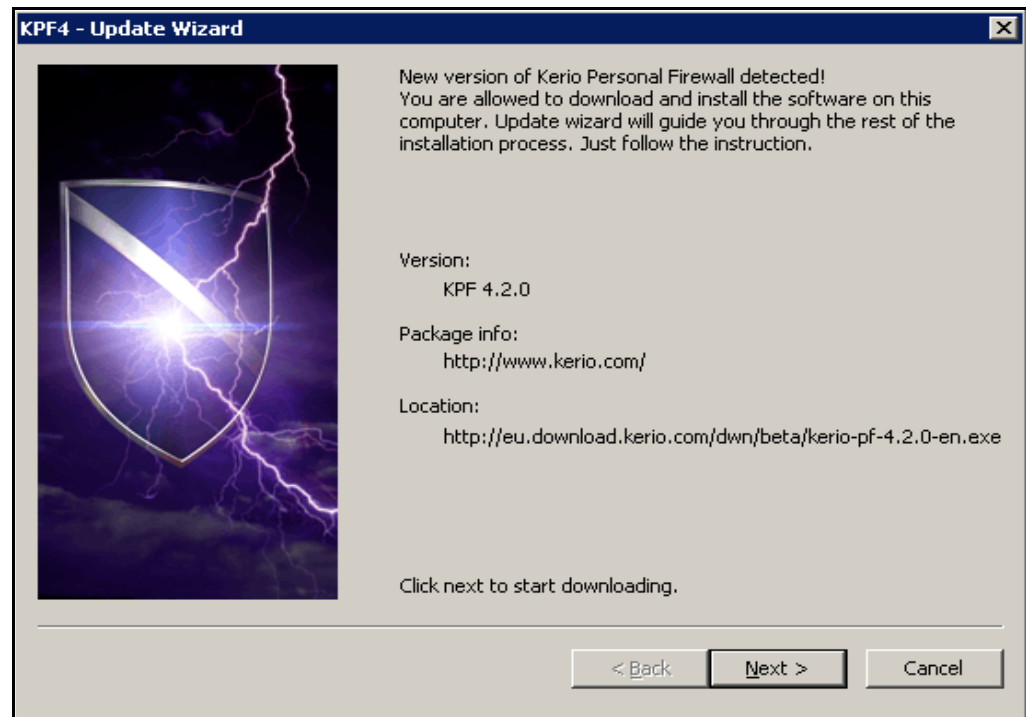


Figure 2-1 Update wizard of the Sunbelt Kerio Personal Firewall

Click on the Next button to start download of the new version and to run the installation program. Sunbelt Kerio Personal Firewall always checks signature of a downloaded file — this feature ensures that any downloaded file will be original (it is not attacked by a virus, damaged, etc.).

The system must be restarted after a new version is installed.

The download or the installation process can be stopped by the Cancel button. If the process is canceled, the update will not be offered again automatically, however, it can be run by hand whenever needed. When a new version is found, Sunbelt Kerio Personal Firewall will open the update dialog automatically.



Note: Sunbelt Kerio Personal Firewall follows special internal rules which always allow access to the server where the product can be updated and registered. Therefore, the automatic update checks cannot be blocked by inappropriate firewall settings.



Product Registration and Licensing Policy

Two editions of *Sunbelt Kerio Personal Firewall* are available: full (paid) and free (free of charge, but limited).

The same installation package is used for both version. After installation the product behaves as 30-days trial version (full version limited by time). If the product is not registered by the expiration date, it becomes free and limited. The product becomes a full version after license purchase and product registration.

Limited Free Edition

Free (unregistered) editions are limited by the following restrictions:

- It is available for personal and/or 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 *Syslog* server.
- Configuration cannot be protected by a password and it is not possible to access and administer the firewall remotely.

Technical Support

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

Product registration

Once a license for *Sunbelt Kerio Personal Firewall* is purchased, the product must be registered. Once the registration is completed, all features including those which are not available in the free edition are enabled.

Sunbelt Kerio Personal Firewall can be registered in the user interface of the firewall or at *Sunbelt Software Website*.



Note: For personal and non-commercial purposes, *Sunbelt Kerio Personal Firewall* is free and registration is not required. After 30 days from the installation, *Sunbelt Kerio Personal Firewall* starts to behave as a limited version.

For detailed information on licensing policy, refer to *Sunbelt Software Website* (<http://www.sunbelt-software.com/>).

Registration through the user interface

If a direct connection to the Internet is available to the *Sunbelt Kerio Personal Firewall*'s host, registration can be done through the firewall's user interface.

To view license and subscription information, go to the License tab under Overview.

Limited free edition before expiration of the trial period

The trial period expires 30 days after the first installation of the product on a particular host. During this period, all features of the product are available even without a license being purchased.

Basic information about the product are provided in the Product section. Click Register to run registration wizard.

Number of days left to expiration of the trial period is provided in the License section.



Figure 3-1 Overview / License — Limited free edition before expiration of the trial period

Limited free edition after expiration of the trial period

If the product is not registered by the end of the 30-days trial period, it is switched into the free, but limited edition. This means that some features of the firewall are not available any longer.

Basic information about the product are provided in the Product section. Click Register to run registration wizard.

The License informs users that the product currently operates in the unregistered limited version.



Figure 3-2 Overview / License — Limited free edition after expiration of the trial period

Licensed version

Once Sunbelt Kerio Personal Firewall is registered, all features are available without any limitation. The License provides detailed information on the current license.

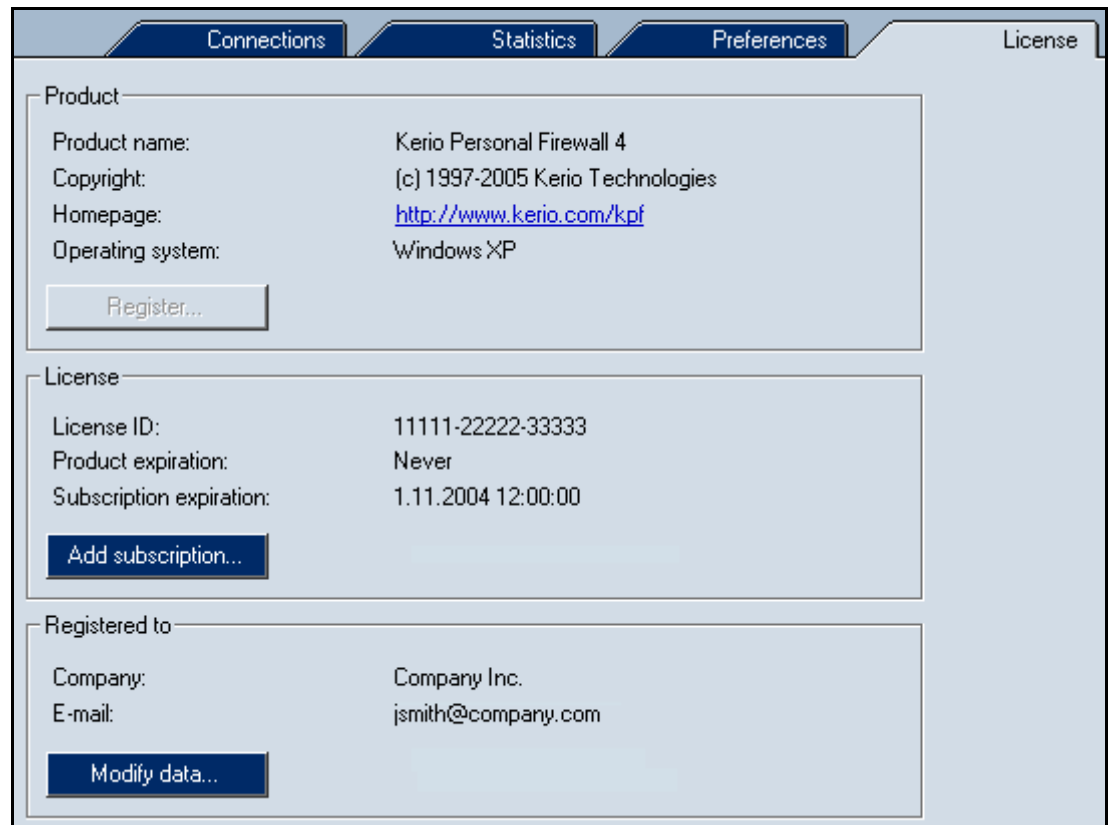


Figure 3-3 Overview / License — Licensed version

The Register button in the Product section is disabled.

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). Click Add subscription to register the purchase number to prolong the subscription. Click the button to run corresponding sections if the registration wizard.

The Registered to section provides information about the company or the person which the product is registered to. This information can be modified. The Company / Name and the Country items cannot be edited (subject of the registration cannot be changed).

Registration via the Website

Sunbelt Kerio Personal Firewall can be also registered at Sunbelt Software Website (<http://www.sunbelt-software.com>). This registration method can be used even if the Sunbelt Kerio Personal Firewall host cannot connect to the Sunbelt Software's registration server (e.g. if the communication is blocked by a network firewall).

Insert your registration number obtained against purchase of the product and your subscription number into a corresponding form. If numbers specified are valid, a corresponding license key (the license.key file) will be created. Download this file and save it into the license directory under Sunbelt Kerio Personal Firewall

(C:\Program Files\Sunbelt\Personal Firewall 4\license by default).

All features of the product will be available upon the next start of the Personal Firewall Engine service.

Registration wizard

Four steps are to be followed during registration of the Sunbelt Kerio Personal Firewall:

Step 1 — registration number

Insert the number which was delivered to you when you purchased the product (Registration key).

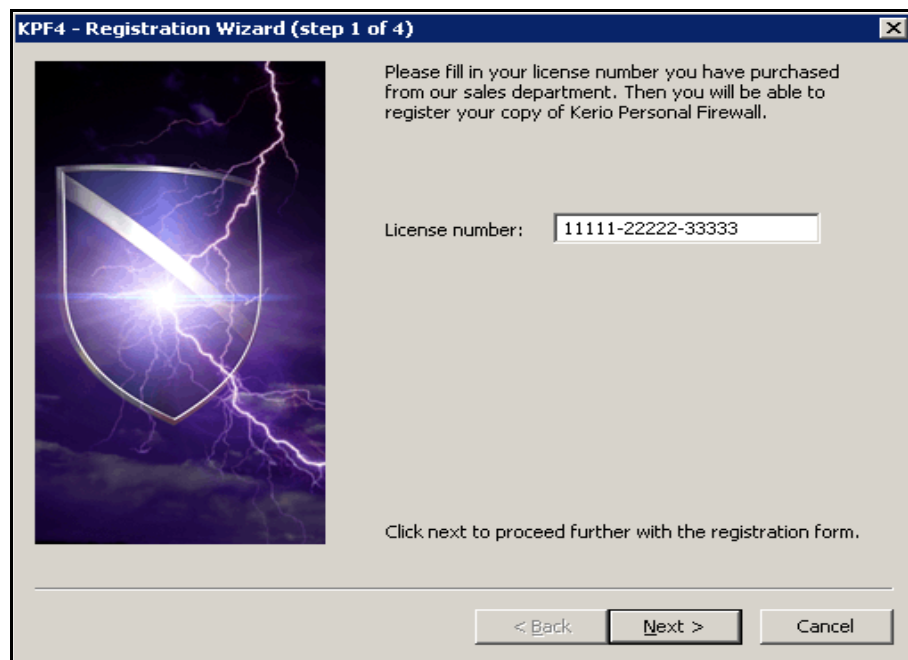


Figure 3-4 Registration wizard — Inserting registration number

Click Next to make Sunbelt Kerio Personal Firewall establish connection with the registration server and check whether the number is valid. The registration cannot be completed unless a valid registration number is used.

If connection with the registration server cannot be established (the computer cannot connect directly to the Internet, the traffic is blocked by another firewall, etc.), the wizard provides a link to the Sunbelt Software Website, where the product can be also registered.

Step 2 — contact information

In Step 2, basic information on the company or person which the firewall is registered to is required.

Figure 3-5 Registration wizard — Contact information

The Company / Name, Country and Email items are required. The other items are optional.

Step 3 — subscription

Specify purchase numbers of your subscription(s).

Figure 3-6 Registration wizard — Subscription

Use the Subscriptions textbox to add one or more purchase number obtained against your subscription purchase. Added numbers can be edited or removed. Click Next to register all specified numbers.

Upon clicking on the Next button, Sunbelt Kerio Personal Firewall establishes connection with the registration server, verifies inserted data and downloads the license key automatically (certificate).

Step 4 — finish registration process

Results of the registration process are displayed in Step 4.

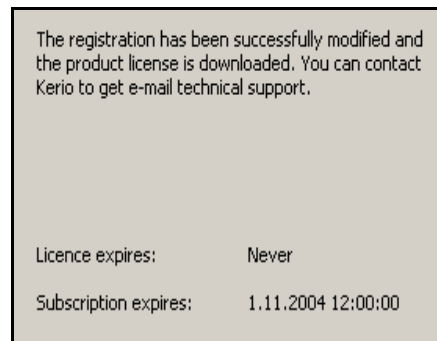


Figure 3-7Registration wizard — Information about finish registration process

Date and time of the subscription expiration is provided (time to which the user can update the product for free). If the license is time-limited, date and time of product expiration are also displayed (the License expires item).

Click Finish to close the wizard.



Note: The Personal Firewall GUI component is restarted automatically upon finishing of the registration process. This enables all features which are not available in the unregistered version.



Firewall Components and Basic Control Features

Sunbelt Kerio Personal Firewall several components and system tray features.

Personal Firewall Components

Personal Firewall Engine

Core of the Sunbelt Kerio Personal Firewall. It is running as a service (Windows NT 4.0 or later) or in the background (Windows 98 and Me).

The Personal Firewall Engine service is stored in the `kpf4ss.exe` file in the installation directory of Sunbelt Kerio Personal Firewall.

Low-level drivers

Sunbelt Kerio Personal Firewall's low-levels driver are implemented into the core of an operating system during its startup. They are located between drivers of network interfaces and the TCP/IP subsystem.

Network traffic low-level driver

The network traffic low-level driver detects and processes all incoming and outgoing IP traffic. It allows and blocks traffic in accordance with the firewall policy and controls running of applications and processes in the system.

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.

Both low-level drivers are stored in Windows system directory:

- as the `fwdrv.sys` file typically in the `C:\WINNT\system32\drivers` directory under the Windows NT and Windows 2000 operating systems
- as the `fwdrv.sys` and `khyps.sys` files, typically in the `C:\WINDOWS\system32\drivers` directory under the Windows XP operating system
- as the `fwdrv.vxd` and `khyps.sys` files, typically in the `C:\WINDOWS\system` directory under the Windows 98 and Windows Me operating systems

Personal Firewall GUI

User interface of *Sunbelt Kerio Personal Firewall* (GUI — *Graphical User Interface*).

The Personal Firewall GUI component is automatically started by the Personal Firewall Engine service (when it is started or everytime it detects that the user interface is not running). When it is running, the Personal Firewall GUI is represented by a shield icon on the System Tray.

Right-click on the icon on the System Tray to open Sunbelt Kerio Personal Firewall configuration dialog or to use another option from the menu (stopping network traffic, disabling firewall, etc.).



Figure 4-1 Sunbelt Kerio Personal Firewall icon on the Systray

The Personal Firewall GUI is represented by the `kpf4gui.exe` file which can be found in the Sunbelt Kerio Personal Firewall installation directory.

Crashdump sender

This tool sends crashdump to the *Sunbelt Software* when *Sunbelt Kerio Personal Firewall* breaks down. It is represented by the `assist.exe` file.

Libraries

The components of the *Sunbelt Kerio Personal Firewall* described 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 Kerio Personal Firewall and display of its status).
- `KTssl32_0.9.7.dll`, `libey32_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.

Support for Fast User Switching

Sunbelt Kerio Personal Firewall supports Fast User Switching in Windows XP.

Multiple Personal Firewall GUI instances can be open at any moment. In such cases Personal Firewall Engine communicates with the session which belongs to the currently active user.

After startup of the operating system and the Personal Firewall Engine service, the first instance is executed that runs under the system account (or the account under which the Personal Firewall Engine service is executed). Upon user login a new instance of the Personal Firewall GUI is executed, running with the privileges of the logged user. This instance is active until the user logs off (the instance is terminated) or the user-switch function is used (the instance is only deactivated).

Systray Icons

Sunbelt Kerio Personal Firewall's shield-shaped icon is displayed on the System Tray whenever the *Personal Firewall GUI* component is running. This component is started automatically by the *Personal Firewall Engine*.

The *Sunbelt Kerio Personal Firewall* icon also represents network activity of the computer on which the firewall is installed. Network traffic is represented by little colored bars at the bottom of the icon:



Figure 4-2 Sunbelt Kerio Personal Firewall icon on the Systray

- green bar — outgoing traffic
- red bar — incoming traffic

Double-click on the icon with the left mouse button to open the Sunbelt Kerio Personal Firewall configuration dialog. Right-click on the icon to open a menu providing the following options:



Figure 4-3 Context menu of systray icon Sunbelt Kerio Personal Firewall

Disable Firewall

This option disables the firewall. Use this option to disable all *Sunbelt Kerio Personal Firewall* modules (network communication filtering, monitoring of launched applications, intrusions detection and Web content filtering).

This option disables the firewall for certain necessary periods, such as during tests or debugging (i.e. network connection failures). We do not recommend you to use the *Disable Firewall* for long — the firewall would not function and your computer would not be protected.

When *Sunbelt Kerio Personal Firewall* is disabled, the icon striked-through.



Figure 4-4 Sunbelt Kerio Personal Firewall Systray icon— Firewall disabled

This option disables the firewall and switches into the Enable Firewall mode. The Enable Firewall option can then be used for the firewall recovery.



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

Stop all traffic

This option blocks all network traffic (network lock).

If this option is enabled, the “do not enter” sign is displayed on the *Sunbelt Kerio Personal Firewall* shield icon.



Figure 4-5 Sunbelt Kerio Personal Firewall Systray icon — Stop all traffic

This option in the menu changes to the Enable traffic option — it can be used to refresh the traffic applying the current firewall settings and rules.

In case that a 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.

Anytime the Personal Firewall Engine service is started up, the Disable Firewall and Stop all traffic options are set to default modes. For security reasons it is not recommended to leave the firewall disabled after the system startup. Stopping all traffic might cause problems for example during user login.

Configuration

Use this option to open the *Sunbelt Kerio Personal Firewall* configuration dialog.

Register

This option runs registration wizard. If Sunbelt Kerio Personal Firewall has been already registered, the option will not be available in the menu.

About

The “About” window provides information on versions of individual Sunbelt Kerio Personal Firewall components as well as links to corresponding Web pages.

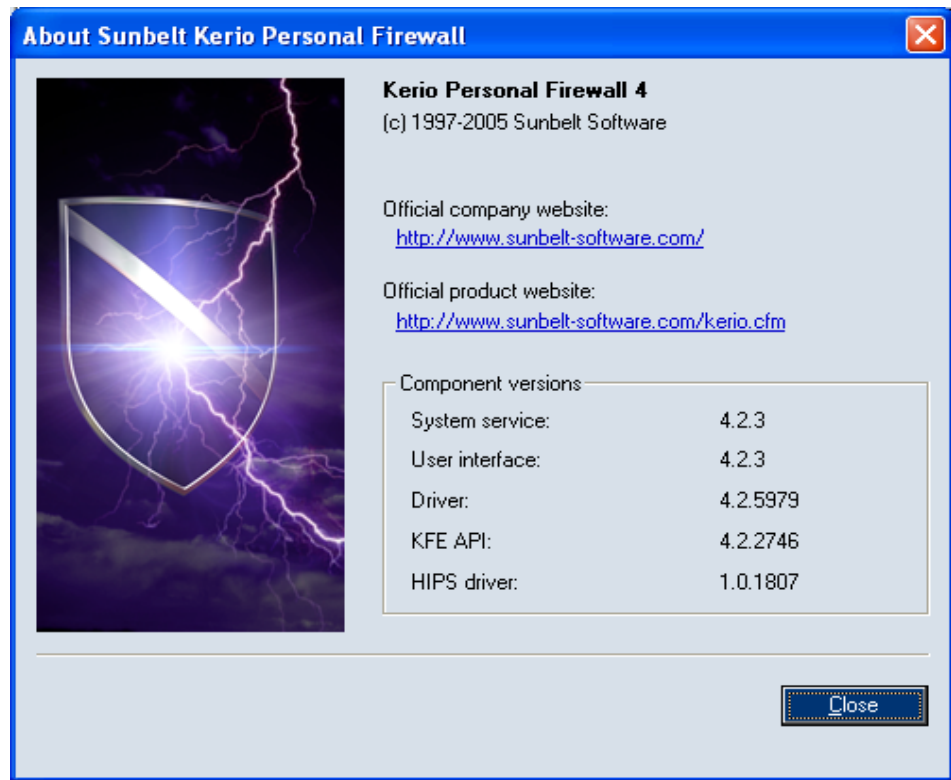


Figure 4-6 About window

Exit

Use this option to stop the Personal Firewall Engine service and to close the Personal Firewall GUI (all open windows and application dialogs will be closed and the icon on the Systray will be hidden).

Sunbelt Kerio Personal Firewall can be reactivated by choosing the Firewall Engine option from the Start > Programs > Sunbelt Kerio > Personal Firewall 4 menu, or by running the service in the Administrative Tools / Services control panel.

When Sunbelt Kerio Personal Firewall is closed, the low-level driver starts to allow all outgoing and incoming traffic — the computer is not protected any longer.

If access to the firewall administration requires a password and the user is authenticated, the Logout item is also available in the context menu.



Firewall Behavior and Interaction with Users

Firewall Behavior

Data transmission within the Internet is performed through TCP/IP protocols. These protocols are also used for most of traffic within local networks. The essential protocol is IP (Internet Protocol). Packets of this protocol carry the rest of information (they encapsulate other protocols). Sunbelt Kerio Personal Firewall controls all IP packets — this implies that it is able to catch them, get essential information and then either let them into the system or filter them out. Logs on all events, detected intrusions etc. are provided as well.

Sunbelt Kerio Personal Firewall is based on so called stateful inspection. This means that the firewall decides according to information acquired from the detected packet as well as with respect to information about the previous communication. A log is created for each permitted connection (or a pseudo-connection in case of UDP and ICMP) and the firewall blocks all packets which do not belong to this connection. Stateful inspection of the network communication is more efficient and more secure than packet filtering.

If the Advanced mode is selected during the installation of the Sunbelt Kerio Personal Firewall, the firewall works in so called self-taught mode. Anytime unknown network traffic is detected, a dialog will be displayed through which the particular traffic can be permitted or denied, either for the single situation or for any further connections (permanently). If traffic is permitted/denied permanently, a corresponding rule is created automatically and users will not be asked about the particular traffic anymore.



Note: *The same method is used for checking of running applications.*

By modifying rules for applications or advanced packet filter rules, a user (or the administrator) can specify further traffic filtering rules. Only packets meeting required criteria or those that belong to permitted connections (see information on the stateful inspection) are let through the firewall.

Warning dialogs are displayed “Always on Top”. If more than one event (attempts for connection establishment, intrusion attempts, etc.) are detected at a time, they are queued. When the dialog which is currently on top is confirmed, another one is displayed.

Connection Alert (unknown traffic detection)

The *Connection Alert* dialog (asks user whether the connection will be permitted or denied) informs users when *Sunbelt Kerio Personal Firewall* detects an unknown traffic. In this dialog, the user/administrator decides whether the traffic will be permitted or denied and if a corresponding rule is to be created.



Note: *The way how Sunbelt Kerio Personal Firewall will behave when a network connection is detected are defined by parameters in the Network Security section. The Connection Alert dialog is opened if no corresponding rule is found or the rule asks user explicitly.*



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



Figure 5-1 Connection alert (unknown traffic detection)

The *Alert* dialog provides the following information and options:

Traffic direction and zone

The colored stripe informs users of traffic direction (incoming or outgoing) and the location which a remote point belongs to (trusted IP addresses or the Internet).



Figure 5-2 Connection alert — Traffic direction and zone

The color of the stripe and the first part of the text represent the direction of the connection:

- Outgoing connection alert — outgoing connection (connection from a local to a remote point). Outgoing connections are represented by a green stripe.
- Incoming connection alert — incoming connection (connection from a remote to a local point). Incoming connection is represented by a red stripe.

The location where the IP address of a particular remote point belongs to is displayed in parenthesis:

- Trusted area — group of trusted IP addresses
- Internet — any IP address which is not included in the Trusted area

Local application and Remote point

Basic information on an connection can be found below the colored stripe:

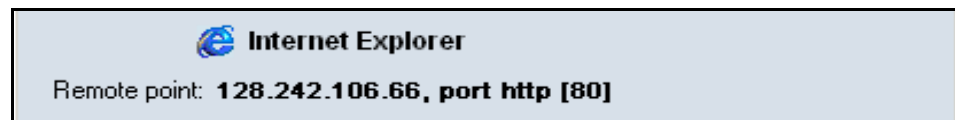


Figure 5-3 Connection alert — Local application and remote point

- application icon and its description 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 for executables will be used.
- remote point DNS 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. Translation of IP addresses to DNS names can be enabled/disabled globally, for example in the Overview / Connections context dialog.

- remote point (in case of standard services, the name of the service is displayed in addition to the port number)

Place the mouse pointer over the application name (description) to view a tooltip informing on a full path to the application's executable file.



Figure 5-4 Connection alert — Full path to the application

Actions

The three following actions can be taken within the dialog:



Figure 5-5 Connection alert — Actions

- Use the Permit button to allow the connection.
- Use the Deny button to block the traffic.
- Check the Create a rule for this communication and don't ask me again option to create a rule for the particular communication. The system will remember the action that will be taken with this connection and create a corresponding rule. Later when identical connection is detected, Sunbelt Kerio Personal Firewall will automatically take an action meeting this rule (Permit or Deny).



Note: Created rules can be edited or removed using the Sunbelt Kerio Personal Firewall Administration dialog in the Applications tab of the Network Security section.

- Use the Details button to view detailed information on the connection and on a corresponding local application. Click on this button again to hide this information.

Click on the Details button to view the following information:

Detailed information on the connection and local application

In the description box there are details about the connection (direction, protocol, local/remote endpoint address and port number) and communicating application (name of executable file including the full file path, description of the application, date of file creation, the date of last change and the date which the file was last opened).



Figure 5-6 Connection alert — Detailed information on the connection and local application

Create an advanced rule



Figure 5-7 Connection alert — Create an advanced rule

Check the Create an advanced filter rule option to create (instead of a standard application rule) an additional advanced rule which can be used to set details such as parameters for communication (IP addresses, ports, etc.), a local application, time validity, etc.

Click on the Advanced filter rule... button to open a dialog for an advanced definition of a packet filter rule. In this dialog a selected rule can be easily customized. Advanced rules can be edited or

removed anytime using the Packet Filter button in the Sunbelt Kerio Personal Firewall Administration dialog in the Applications tab of the Network Security section.



Note: The specific traffic in question is paused while the *Connection Alert* dialog is opened (the data is queued by *Sunbelt Kerio Personal Firewall* in its memory buffer). If the user reacts too slow, the application might consider this status as a network error (server not available) after a certain period (typically a few seconds).

Starting/ Replacing/ Launching other application Dialog

The *Starting/Replacing/Launching other application* dialog informs users that *Sunbelt Kerio Personal Firewall* has detected an attempt to startup an application or to run an application by another one. Decide whether the action will be permitted or denied and whether an appropriate rule will be created. The application will not be opened unless permitted by user.



Note: The way how *Sunbelt Kerio Personal Firewall* will behave when applications are started is defined by rules in the *System Security* section. The *Starting/Replacing/Launching other application* dialog is opened if no corresponding rule is found or the rule asks user explicitly.



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

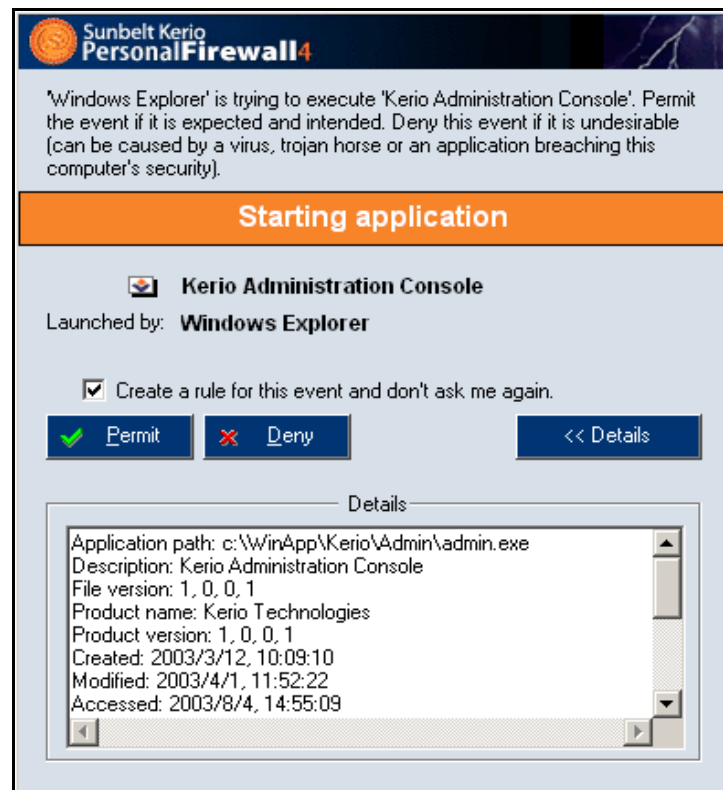


Figure 5-8 Starting/Replacing/Launching other application dialog

The Starting/Replacing/Launching other application dialog provides the following information:

Description

A brief description of a particular event and a general recommendation which action should be used are provided in the dialog header.

'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 5-9 Starting/Replacing/Launching other application dialog — Event description



Note: If description of the application (or the file name if there is no description available) is too long, it will be shortened to 32 only and three dots will be added at the end to inform that the item is not displayed complete.

Name

Information on which event type was detected is displayed in the colored field:

Starting application

Figure 5-10 Starting/Replacing/Launching other application dialog — Event

- Starting application — an application is to be launched
- Replacing application — executable file of an application is to be replaced
- Application is launching other application — the running application is attempting to launch another application

Icon and application name

Icon and description of the application are provided below below the information on application type. 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 5-11 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 tooltip providing full path to the executable file of the corresponding application.


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

Figure 5-12 Starting/Replacing/Launching other application dialog — Full path to the application

Action

Select an action which will be taken for this application.

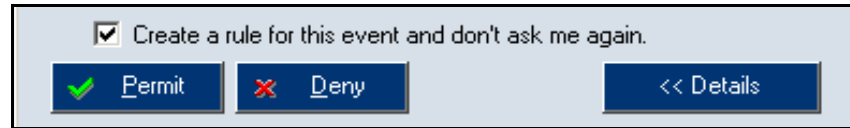


Figure 5-13 Starting/Replacing/Launching other application dialog — Actions

- Use the Permit button to allow the application.
- Select the Deny button to block the application.
- Check the Create a rule for this event and don't ask me again option to create a rule (in System Security / Applications). Next time this event is detected, the rule will be applied without asking user.
- Click on the Details button to view detailed information on the started application (eventually also information about application by which it is launched)

Details

Open the Details section to view information on the starting application, eventually also information about application by which it is launched (full path to the executable file, description of the application, version number, date when the file was created/modified, the latest date of when the file was accessed, etc.).

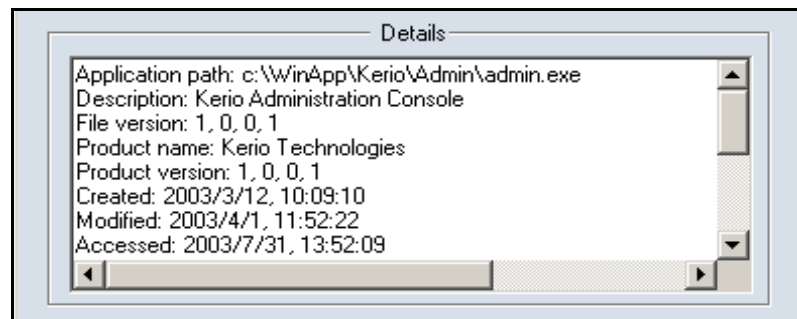


Figure 5-14 Starting/Replacing/Launching other application dialog — Details

Host Intrusions Alerts

The *Intrusion attempt blocked* dialog warns user that *Sunbelt Kerio Personal Firewall* detected a host intrusion attempt and blocked it.



Note: *The Intrusion attempt blocked dialog is displayed when there is no corresponding exception defined for the applications involved or if the Do not display warnings for these event types option is disabled.*

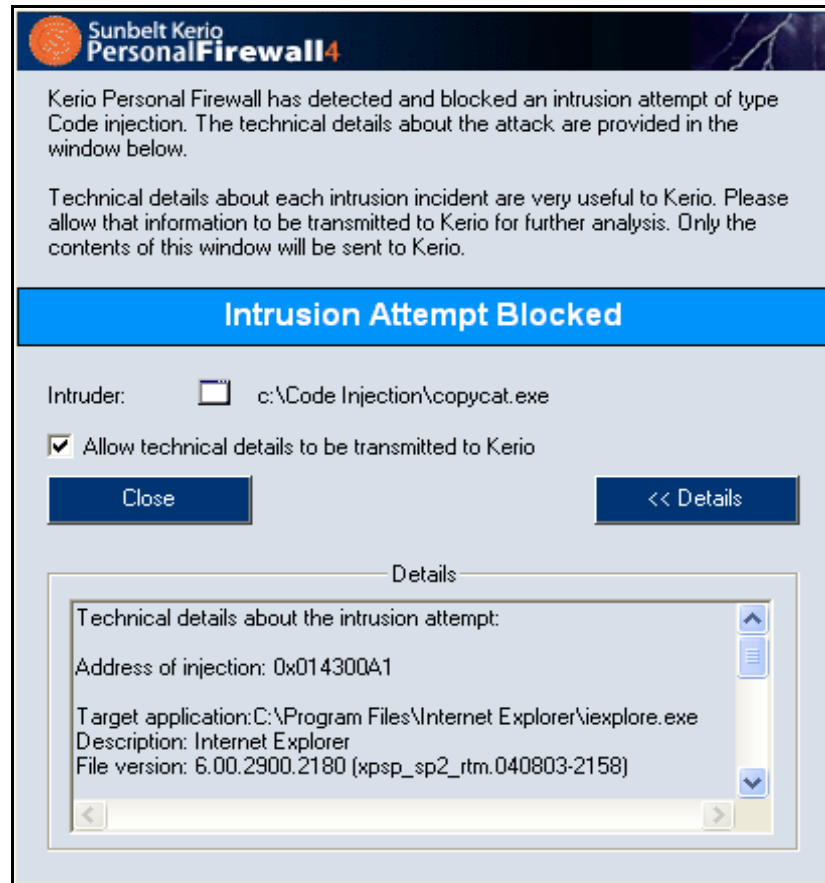


Figure 5-15 Host intrusion alert

Event description

At the top of the dialog window, a description of the event detected is provided, including recommended response.

Event name

The light-blue strip provides information that an intrusion attempting to get into the host system has been detected. The following intrusion types can be detected:

- Buffer overflow.
- Code injection.

The icon and paths to applications

Right below the event name, paths to the target and injector applications as well as corresponding icons can be found (see figure 16). If the application does not use any icon, the standard system icon for executable files is used.

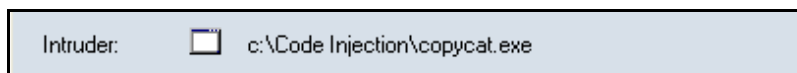


Figure 5-16 Code injection detected — Icons and intrusion description

In case of Buffer overflow events, only the process where the intrusion was detected is provided (see figure 17).



Figure 5-17 Buffer overflow detected — Icon and intrusion description

Allow intrusion attempt information sending

The Allow technical details to be transmitted to Sunbelt option which is enabled by default allows Sunbelt developers use information about intrusions to improve the detection system. Only the contents of the warning dialog will be sent to Sunbelt Software.

Close

Use this button to close the warning dialog. It is recommended to check intrusion details in the HIPS log upon closing the dialog.

Intrusion details

The Details section provides detailed information about both the attacked and the attacking application (only the process in case of Buffer overflow) — full path to their executable files, application description, version number, etc.

Alert Dialog Window (alerts on events)

You can enable the `Alert` dialog in *Sunbelt Kerio Personal Firewall* rules or by running a corresponding application. This dialog will appear when a packet is sent or received that meets the conditions of the rule. A window providing information on the connection will be displayed in the right bottom corner of the screen. If other events meeting the rule are detected while this window is open, they will be queued. The queue can be listed in both directions using the arrow buttons.



Warning: If you close the Alert dialog (by clicking on the cross button at the right top of the window or using the `Alt+F4` keys), all queued alerts will be removed, regardless of the fact that they have been displayed or not!

Network Connection Alert

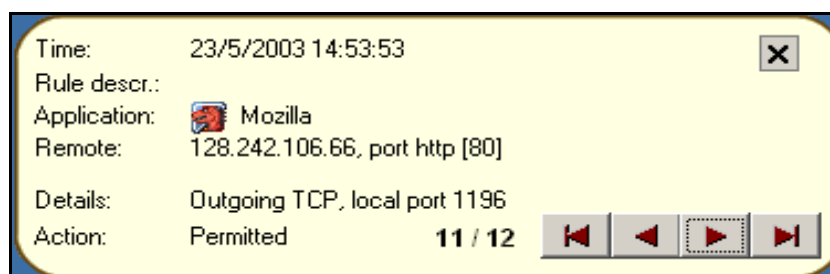


Figure 5-18 Network Connection Alert

The Alert window provides the following information:

- Time — date and time when the connection was initiated
- Rule descr. — description (name) of a used traffic rule: Application startup,
- Application change (change of the executable file of the application) or Application launches another application
- Application — icon and name of the local application used for the communication (if this application has no icon, a default system icon will be used; if no name is available for the application, the name of the corresponding executable file will be displayed)
- Remote — IP address and port of the remote computer (if a name can be identified using DNS, this name will be displayed instead of the IP address; the protocol name will be displayed before the port number for standard services)
- Details — connection details: direction (Outgoing or Incoming), protocol and local port
- Action — action which has been taken (Permitted or Denied)
- sequence number of the alert in the queue (the total count of alerts will grow when new alerts are generated by Sunbelt Kerio Personal Firewall)
- buttons to list in the alert queue — function of buttons from left to right: go to the first/previous/next/last alert

Example of Starting Application Alert

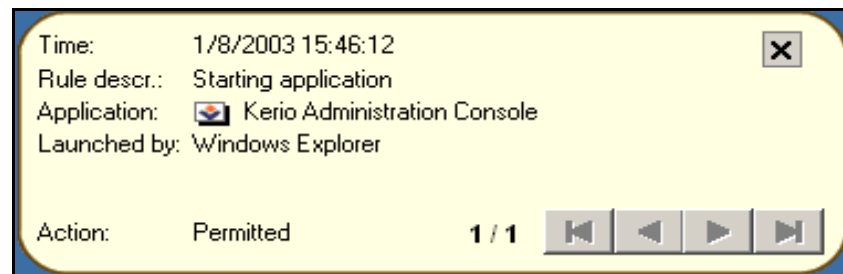


Figure 5-19 Starting Application Alert

The Alert dialog includes the following items:

- Time — date and time of the event
- Rule descr. — description of detected event:
 - Starting application — an application was started
 - Replacing application — replacement of application's executable file
 - Application is launching other application — the running application is attempting to launch another application
- Application — icon and name of a local application participating in the communication (if no icon is available, the standard system icon will be used; if application name is not available, name of a corresponding executable file without extension will be displayed)
- Launched by — name (description) of an application by which the application is launched
- Action — action that was Permitted by a corresponding rule (starting application Permitted/ Denied).



Firewall Configuration

Configuration Dialog

Sunbelt Kerio Personal Firewall parameters can be set and status information can be viewed in the configuration dialog. Use one of the following methods to enter this dialog:

- double-click on the Sunbelt Kerio Personal Firewall icon located on the Systray
- right-click on the icon and select the Configuration option in the context menu

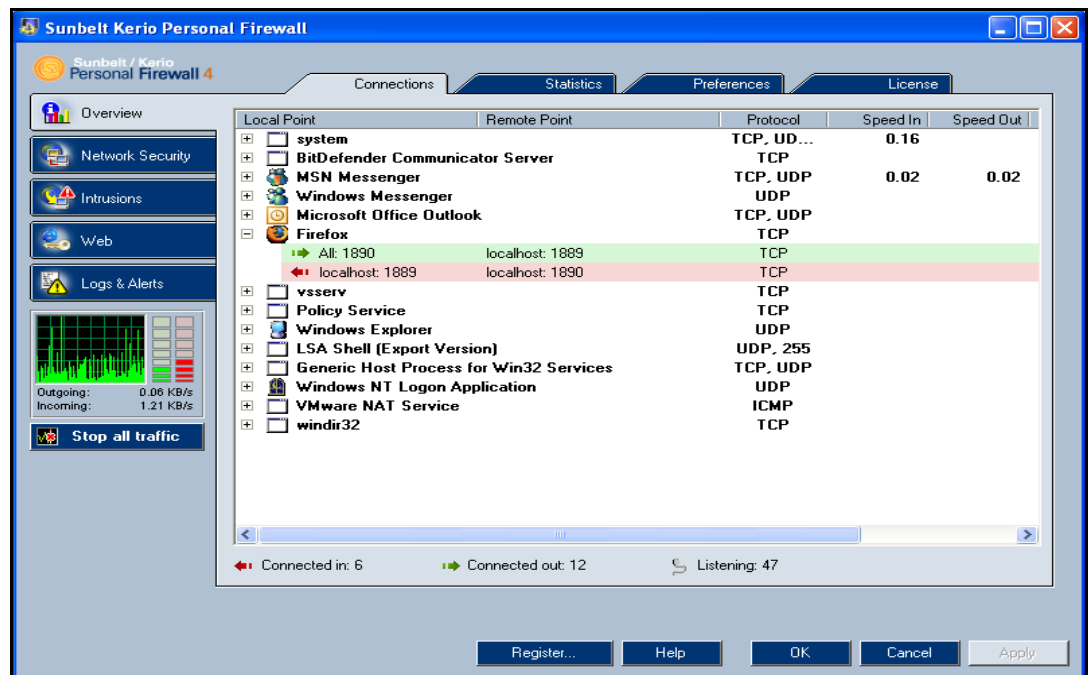


Figure 6-1 Sunbelt Kerio Personal Firewall Configuration Dialog

Use tabs on the left to switch between individual sections:

- 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

Chart at the bottom of the dialog window shows traffic load of a particular network interface. The green bar next to the chart represents current speed of outgoing traffic, whereas the red bar shows current speed of incoming traffic. Click on the chart to switch between the line graph and the bar graph. Place the mouse pointer over the chart to view a tooltip giving statistics of network traffic:

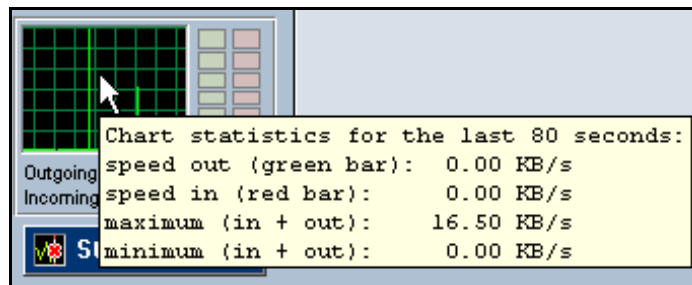


Figure 6-2 Configuration Dialog — Traffic load of a particular network interface

- speed out (green bar) — current speed of outgoing traffic
- speed in (red bar) — current speed of incoming communication
- maximum (in+out) — top speed record
- minimum (in+out) — bottom speed record

Use the Stop all traffic button to block all network traffic (all connections will be stopped immediately). This function can be helpful for example when communication which was supposed to be denied has been permitted by mistake. If this option is used, it is replaced by the Enable traffic option.

If traffic is stopped, this will be shown by the icon and the Enable traffic text below the button.



Figure 6-3 Configuration Dialog — Stop all traffic / Enable traffic



Note: The Stop all traffic / Enable traffic option is also available from the context menu called through the Sunbelt Kerio Personal Firewall icon displayed on the Systray.

Buttons at the dialog bottom provide the following functions:

- OK — saves all changes and closes the configuration dialog
- Cancel — closes the dialog without saving changes
- Apply — saves and applies all changes and leaves the dialog open



Note: Changes in configuration can be done in only tab of one section at a time. If you attempt to switch to another tab or to another section, the system seeks possible changes that could have been made since the last save. If some changes are detected, Sunbelt Kerio Personal Firewall asks users whether they should be saved or canceled.

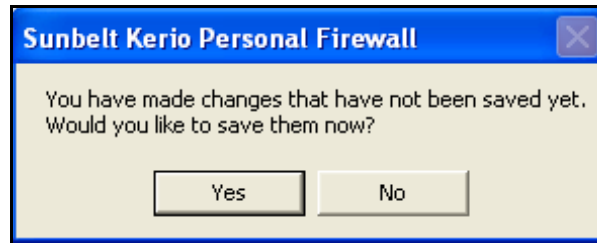


Figure 6-4 Configuration Dialog — Confirm storing of changes

Protected Configuration

It is possible to set Sunbelt Kerio Personal Firewall configuration so that it can be accessed only through a password authentication (only authorized users are then allowed to modify settings). In such case unauthorized users are allowed only to view the configuration. Password will be required if a configuration change is attempted.



Figure 6-5 Password protected

After insertion of a correct password a particular user will be logged-in. This user will be authorized to change the configuration.

We recommend authorized users to logout after the desirable changes are done so that no unauthorized user can modify the configuration. Use the Logout option in the context menu accessible through the icon in the Systray, or the Logout button in Overview / Preferences. If a user does not log out, the configuration can be accessed and modified unless the Personal Firewall Engine service is closed.

Remote Admin

Sunbelt Kerio Personal Firewall can be also administered remotely (from a remote station — not from the one where the *Personal Firewall Engine* service is running). Two alternatives of remote administration are available:

- access to the configuration — all settings and functions available through the configuration dialog can be accessed from a remote computer. Dialogs during events (initialization of applications, network communication) and notifications on events can be viewed only through the computer where the *Personal Firewall Engine* is running.
- session is redirected — all dialogs and notifications will be also redirected to a particular remote station.

Access from a remote workstation

The following steps must be followed for a successful remote access to the *Personal Firewall Engine*:

- 1 Allowing remote administration and setting a password which will be used for access to the administration

Remote access to the Personal Firewall Engine is available only through a successful user authentication (password request). Enable the Enable password protection and the Allow remote administration of this computer options in the Overview / Preferences section. Set a password if not specified yet.

- 2 Running the *Personal Firewall GUI* at a remote computer

- If Sunbelt Kerio Personal Firewall 4.x is installed on the remote computer, select and run the Remote Firewall Administration from the Sunbelt program group.
- If Sunbelt Kerio Personal Firewall is not installed on the remote computer, copy the kpf4gui.exe, KTIbeay32_0.9.7.dll, KTssleay32_0.9.7.dll and KTzlib.dll files or the trans subdirectory (if you intend to use another language version of the interface than the English one) from the local workstation (typically from the C:\Program Files\Sunbelt\Personal Firewall 4 directory) and run it on the remote workstation.

- 3 Authentication to access the *Personal Firewall Engine*

Use one of the methods of running *Personal Firewall GUI* described above to open the authentication dialog where you can login to the *Personal Firewall Engine*.

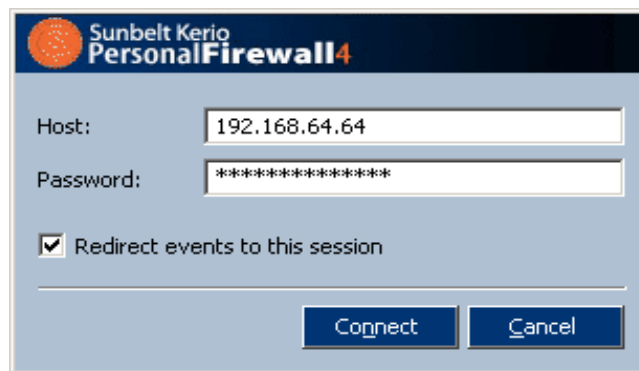


Figure 6-6 Access from a Remote workstation

Address

DNS name or IP address of the computer on which the *Personal Firewall Engine* service is running. After a successful connection this name or the IP address will be displayed:

- in the header of the configuration window



Figure 6-7 Remote administration — Header of the configuration window

- in tooltip accessible through the icon on the Systray



Figure 6-8 Remote administration — Icon on the Systray

Password

Password through which the administration can be accessed (see step 1).

Redirect events to this session

Check this option to redirect all dialogs and notifications to the remote computer.

This option enables thorough control of the *Sunbelt Kerio Personal Firewall* from a remote computer. It is not recommended to use this option if you want to perform a single-shot modification of the configuration.

Click on the **Connect** button to establish connection with a remote workstation.



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

When connected successfully to the *Personal Firewall Engine*, the *Sunbelt Kerio Personal Firewall* icon with a symbol of remote connection (R — remote) is displayed in the System Tray. The context menu provides the following functions:

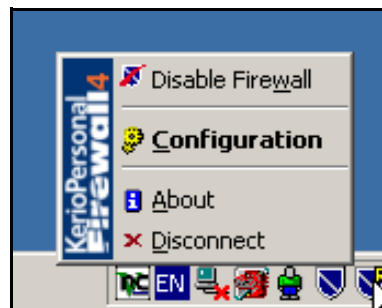


Figure 6-9 Remote administration — Context menu of the Systray icon

Disable firewall

Deactivates the firewall (all security functions are disabled).

Configuration

Use this option to enter the configuration dialog where all settings which are available on the local host can be done (except for disabling of network communication).

About

Information about versions of individual *Sunbelt Kerio Personal Firewall* components as well as license of the firewall and expiration date in case of a trial version (the same information which is provided when a user is connected locally).

Disconnect

Disconnection from the remote *Personal Firewall Engine* administration and closing the *Personal Firewall GUI* on the computer from which the remote access has been performed.



Note: *Unlike in case of local administration, 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).*

Preferences

User preferences and advanced firewall parameters can be set in the Overview / Preferences section.

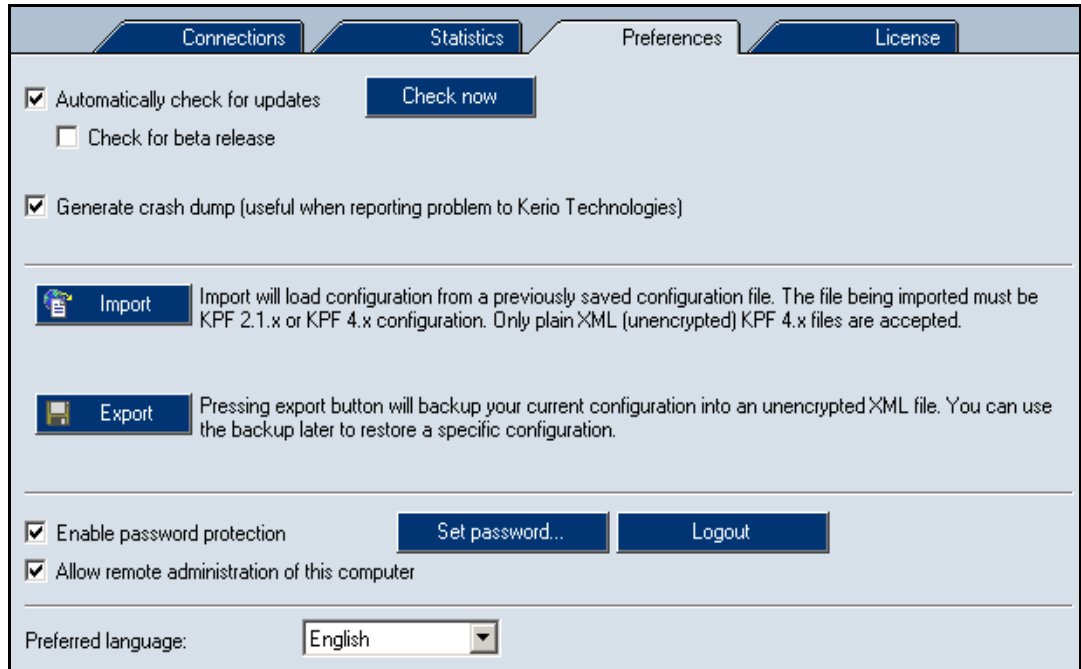


Figure 6-10 Overview / Preferences section

Automatically check for updates

Enables/disables automatic checks for new versions. We recommend to enable this option to provide maximal security (new versions include updates of intrusion database, bugs are removed, etc.).

Check now

Use this button to check for new version of *Sunbelt Kerio Personal Firewall* immediately. If a new version is found at the update server, download and installation will be offered. If not, user will be informed that no new version is available (the latest version is already installed at the computer).

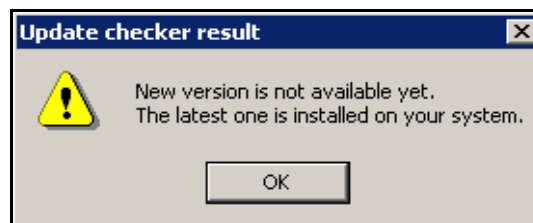


Figure 6-11 Check for new version — New version is not available

Check for beta release

Enable this option to perform checks for released beta versions along with checks for new full versions. Beta versions are program versions that are just being developed and tested. Therefore, their smooth functionality is not guaranteed and bugs may occur.

Use the `Check for beta release` option if you intend to participate in product testing for details refer to <http://www.sunbelt-software.com/>, *Beta Sections*). If you are not interested in the participation and you want to use a functioning version, disable this option.

Generate crash dump

Use this option to enable generation of debugging information which could be used after a possible *Sunbelt Kerio Personal Firewall* crash. If the *Personal Firewall Engine* or the *Personal Firewall GUI* crashes and this option is available, a file including memory data will be created and the *Assist* utility which enables to send crash information (compressed memory information and selected logs) to *Sunbelt Software* (for analysis) will be launched automatically.

In case of an operating system failure, the *Sunbelt Kerio Personal Firewall* can send a memory crashdump to the *Sunbelt Software's* technical support department for detailed analysis. One minute after the *Personal Firewall Engine* service is started, the disc is checked for a new crashdump. If it is detected, the *Assist* tool is started that analyzes it and decides whether it has anything in common with *Sunbelt Kerio Personal Firewall*. If so, user can confirm its sending to *Sunbelt Software* where it would be analyzed..

Crash dump is sent in a compressed format. Content of the following system registry path will be also packed to this file:

HKEY_CURRENT_USER\Software\Sunbelt\Personal Firewall 4.



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

Configuration

This section provides functions for Sunbelt Kerio Personal Firewall back-up, its recovery and Sunbelt Kerio Personal Firewall 2.1.x configuration backup restoration.

Use the Import button to open the file. Sunbelt Kerio Personal Firewall can open and download configuration file in the following formats:

- *Sunbelt Kerio Personal Firewall 4.x* unencrypted (the XML format with the `.cfg` extension)
- *Sunbelt Kerio Personal Firewall 2.1.x* (with the `.conf` extension) — import of older configuration (back-up)

Click on the Export button to save the file. This way you can back-up the unencrypted configuration file for later use or for its use on another computer.



Note: Encrypted configuration files cannot be imported.

Enable password protection

Set password which will be used to access the Sunbelt Kerio Personal Firewall configuration. If the configuration is password protected, it can be only viewed. Users are allowed to change configuration after a successful password authentication.

Users can log out using the Logout button — password will be required before further changes. It is also possible to log out through the context menu which can be found in the Systray

Click on the Set password... button to open a dialog where password can be edited.

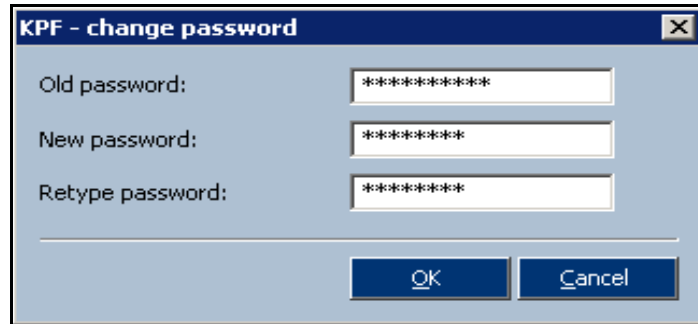


Figure 6-12 Enable password protection

Insert your current password into the Old password entry (only authorized users are allowed to edit password). This entry is inactive if not defined yet (after the Sunbelt Kerio Personal Firewall is installed, when the configuration is removed, etc.). Use the New password entry to specify a new password and conform it using the Retype password entry.



Note: Remote administration of the Sunbelt Kerio Personal Firewall is available only to users authenticated through the password. If the Enable password protection option is disabled, remote administration cannot be enabled (the following option is not available).

Allow remote administration of this computer

Use this option to enable an internal firewall rule which allows connection to the *Sunbelt Kerio Personal Firewall* administration from a remote station. Remote administration is disabled by default.

For detailed information on remote administration refer to chapter.

Preferred language

Select preferred language for the Sunbelt Kerio Personal Firewall user interface. Click on the OK or the Apply button to restart the interface. Next time the configuration dialog or the context menu is opened, this language will be used.

Language versions (localizations) are available in the trans subdirectory in the directory where the Sunbelt Kerio Personal Firewall is installed. The Personal Firewall Engine detects which language versions are available and then any language version can be selected from the Preferred language menu.

Preferred language also affects selection of the most relevant help file. If no corresponding help file for the language is found, Sunbelt Kerio Personal Firewall will attempt to open the English help file automatically. If not even the English version is detected, help file will not be opened.



Note: *Help files are saved in the directory where Sunbelt Kerio Personal Firewall is installed. Context help files are provided in the Microsoft HTML Help format and they are called kpf4-<language_abbreviation>.chm (language_abbreviation is a language name represented by two characters)*

If Sunbelt Kerio Personal Firewall finds out that a particular localization file does not correspond with the current version of the user interface, user will be informed about this fact by an alert. This fact would not affect functionality of the firewall, however, some texts and labels may not be up-to-date or provided only in English.



Network Security

The most important part of the *Sunbelt Kerio Personal Firewall* configuration is definition of network communication rules. The following three rule types are available:

- Rules for applications — simple rules defining how the firewall will behave during network communication in trusted areas and in the Internet. These rules are generated automatically. This process is based on the user's reactions to dialogs regarding unknown network traffic. For details see below.
- Advanced Packet Filter — detailed rules for network communication (optional configuration of IP addresses, protocol, ports, application, etc.). Rules for packet filters can be either defined by hand in the Sunbelt Kerio Personal Firewall configuration dialog or generated automatically according to user's reactions to connection alerts
- Predefined network security rules — Sunbelt Kerio 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).
- The network security module can be enabled/disabled through the Enable Network Security module option in the Applications tab of the Network Security section. If the option is unchecked, all described rule types are unavailable.

How the Firewall Policy is Applied

When a particular communication is detected, individual firewall modules apply rules one by one in a defined order. If the communication meets a rule, a corresponding action will be taken and no more rules will be tested.

Rules of individual *Sunbelt Kerio Personal Firewall* modules are applied as follows:

- 1 Intrusion detection system (IDS)
- 2 Stateful inspection of the network traffic (automatically lets in/out packets which belong to permitted connections),
- 3 Internal rules for *Sunbelt Kerio 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: Individual firewall components may be disabled — corresponding rules will not be applied on detected communication. Internal firewall rules cannot be switched off.

Rules for Applications

Rules for applications can be viewed and modified in the Applications tab of the Network Security section.



Note: The following information is for such cases when Sunbelt Kerio Personal Firewall is in the Advanced mode. In the Simple mode, all outgoing traffic is allowed and all incoming communication is denied for any application (both for trusted zone and the Internet) and no rules are automatically created.

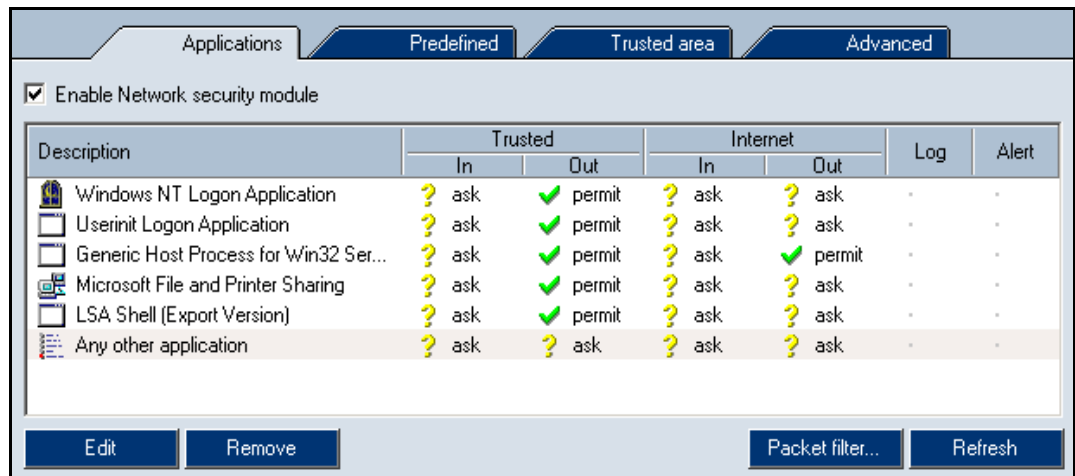


Figure 7-1 Network Security / Applications sections — Rules for applications

At most one rule can be defined for each application. Order of the rules is not important.

Each rule is defined by the following items:

Description

Application icon and description. If an application has no icon, a system icon for executable files will be used. If no description is available for an application, the name of its executable file (without extension) will be displayed.

Note: Icons and descriptions of applications cannot be edited in *Sunbelt Kerio Personal Firewall*.

Trusted, Internet

Setting of parameters for how a particular application will behave during connection from/to a *Trusted* area or from/to the *Internet* (*In* — incoming connection; *Out* — outgoing connection).

For each zone and direction one of the following actions can be selected:

- permit — allows the connection
- deny — blocks the connection
- ask — Sunbelt Kerio Personal Firewall asks the user to either permit or deny the connection. Anytime a new connection is detected, the Connection Alert dialog is opened and the user decides how the firewall will react.



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


Description	Trusted		Internet		Log	Alert
	In	Out	In	Out		
 Mozilla	? ask	✓ permit	? ask	✓ permit		

Figure 7-2 Rules for Applications — Rule for the *Mozilla* web browser

Example: Rule for the *Mozilla* Web browser — see the screenshot above

Web browsers are typical client applications which connect to Web servers. Outgoing connection (Out) from these applications can be permitted (Permit). Because Web servers do not open a connection to the client, we can Deny incoming connections for *Mozilla* or we set the Ask action so that such connection attempts will be always reported and the firewall will ask the user to take an appropriate action.

Log

Check this option to log all communication which would meet the rule into the Network log, regardless of the action which has been taken (both permitted and denied connections will be logged).

Alert

Check this option if you want Sunbelt Kerio Personal Firewall to display an alert anytime a connection meeting this rule is detected. The message will appear in the Alert dialog window, regardless of whether the connection is permitted or denied.

This function can be helpful for example when a connection is denied and we want to find out when the remote points repeat the connection attempt.

Use the Edit button to edit a selected rule (see below). Use the Remove button to remove a selected rule. The Refresh button can be used to refresh the rule list (when the Applications tab is open, an interaction between the firewall and user may arise and rules may be added or modified).

Default Rule

The Another application rule (so called default rule) is always placed at the end of the list of network traffic rules for applications. This rule applies to network traffic which does not match with any other rule. Default rule is highlighted in the rule list. It cannot be removed.



- 1 **Note:** *Actions can be set in the Any other application rule to switch between firewall modes:*
 - *If at least one ask action is in the rule, the firewall works in the Advanced mode — whenever an unknown traffic is detected, user is asked to take an action; the traffic is handled according to his/her decision.*
 - *If only the permit and/or deny actions are set in the rule for both zones and both directions, the firewall works in the Simple mode — if an unknown traffic is detected, a corresponding action is taken without asking the user.*
- 2 *The default rule is also used as a “template” for new rules which are created automatically in correspondance with interaction with the user. For security reasons, action selected by the user is set only for for zone and direction corresponding with detected traffic. The other actions are adopted from the default rule.*

Example: In the default rule, the ask action is used for all traffic zones and directions. The user runs a Web browser and connects to a server in the LAN which belongs to the trustworthy zone. The firewall informs the user about an unknown traffic. The user permits the traffic and enables the option of creating of a new rule. In the new rule, the permit action will be set for outgoing traffic in the trustworthy zone, and the ask action will be set both for incoming traffic in the trustworthy zone and both directions in the Internet zone (this action will be adopted from the default rule).

Applications							Predefined	Trusted area	Advanced
<input checked="" type="checkbox"/> Enable Network security module									
Description	Trusted		Internet		Log				
	In	Out	In	Out					
Internet Explorer	? ask	✓ permit	? ask	? ask	-				
Any other application	? ask	? ask	? ask	? ask	-				

Figure 7-3 Rules for applications — Default rule and created rule for web browser

The behavior that is described above must be considered when actions are set for the default rule. It is recommended to set the `ask` action for all zones and directions in case of self-taught mode or `deny` for blocking any unknown traffic without asking the user.

Options

The following options are available for the rules:

- 1 Right-click on the `Description` column to open the context menu providing the following functions:

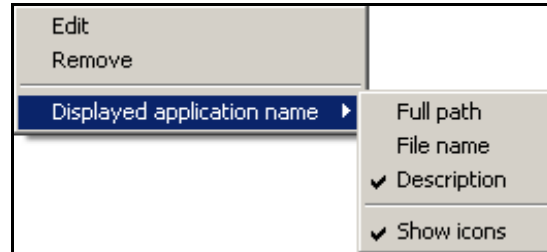


Figure 7-4 Rules for applications — Context menu

- Edit — opens a dialog where a selected rule can be edited (see below)
- Remove — removes a selected rule
- Displayed application name — use this option to define how the application name will be displayed:
 - Full path to the file
 - File name without the path
 - Description of the application

Use the `Show icon` option to enable/disable application icons before application names or descriptions.

- 2 Click on an action (in the Trusted or the Internet column):
 - left-click to switch between the Permit, Deny and Ask actions
 - right-click to open a context menu and select an action.



Figure 7-5 Rules for applications — Actions

Edit

Click on the Edit edit button in the context menu to modify a selected rule. In this dialog you can set actions for individual zones and traffic directions, logging and parameters for sending alerts to users.

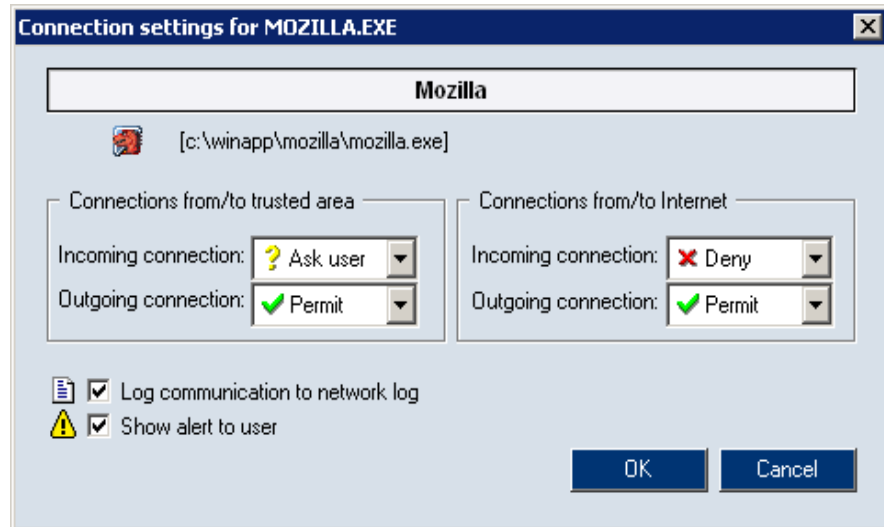


Figure 7-6 Rules for applications — Dialog for rule definition

Description of an application is displayed at the top of the dialog. Below this description, icon and full path to the application executable file is given. This information cannot be edited.

In the center of the dialog window actions for individual zones and traffic directions can be set.

Check the Log communication to network log option to enable logging of communication meeting this rule to the Filter log.

Use the Show alert to user option to enable the Alert dialog for connections meeting this rule.

Network Security Predefined Rules

Sunbelt Kerio Personal Firewall includes several predefined rules. These rules are independent from individual applications (they are applied globally). User decides whether individual predefined rules will be used or not. These rules can be modified.

Predefined rules for network traffic can be found in the **Predefined** tab of the **Network Security** section.

Applications				Predefined		Trusted area	
<input checked="" type="checkbox"/> Enable predefined network security							
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 7-7 Network Security / Predefined section — Predefined rules

Rules in this tab cannot be added nor removed. Actions for Trusted area and the Internet can be set for each rule. To switch between actions (Permit/Deny) click on a corresponding field.



Note: The Ask action (asking user whether the traffic will be allowed or not) is not available for predefined rules.

Check/uncheck the Enable predefined network security option to enable/disable predefined rules for network communication. If this option is not checked, predefined rules are ignored and Sunbelt Kerio Personal Firewall uses only application rules and advanced packet filter rules.

Use the Set to defaults button to restore actions for predefined rules to default values.

Predefined Rules

Brief descriptions on predefined network security rules are provided in this section.

Internet Group Management Protocol

The *IGMP* used for subscription or unsubscription to/from groups of multicast users. This protocol can be misused easily and that is why it is disabled by default. We recommend you not to enable this protocol unless you run applications which use multicast technologies (typically for transmission of audio or video data through the Internet).

Ping and Tracert in, Ping and Tracert out

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

First, a possible attacker tests whether an elected IP address responds to control messages. Blocking these messages will make your computer “invisible” and reduces chance of possible intrusions.

All incoming *Ping* and *Tracert* messages (from the Internet) are blocked by default. These messages are allowed from the trusted area (administrator can for example 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

Rule 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 for translation of computer names to IP addresses. At least one connection to a DNS server must be permitted to enable definition through DNS names.

Virtual Private Network

Virtual private network (VPN) is a secure connection of two local networks (or connection of a remote client to a local network) via the Internet using an encrypted channel (so called tunnel). The *Virtual Private Network* rule allows/denies VPN establishment through the *PPTP* protocol (*Microsoft's* proprietary protocol).

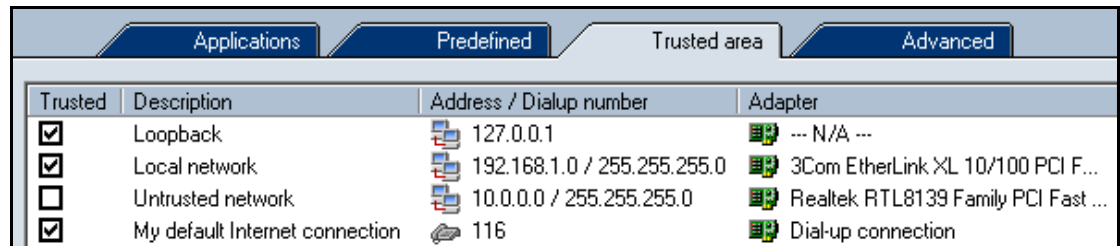
Broadcasts

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

Trusted Area

Two types of IP groups are distinguished for Sunbelt Kerio Personal Firewall application rules: 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. Address which are not defined as trusted will be added to Internet zone automatically.

To define your trusted area go the Trusted area tab in the Network Security section.



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

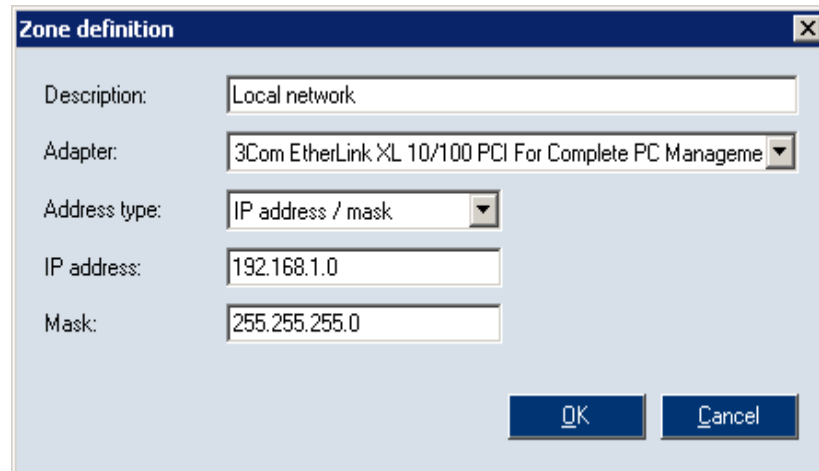
Figure 7-8 Network security / Trusted area section — Trusted area definition

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

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

Trustworthy zone definition

Use the Add or the Edit button to define an item of the trusted area (or double-click on a selected item to Edit it).



Zone definition

Description: Local network

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

Address type: IP address / mask

IP address: 192.168.1.0

Mask: 255.255.255.0

OK Cancel

Figure 7-9 Trustworthy zone definition

Description

Item description. For reference only. It is recommended to provide description of the IP range, network, etc.

Adapter

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 which is not connected into the particular network, the packet is considered untrusted.

Use the --- Any --- option if you want that Sunbelt Kerio Personal Firewall does not check adapters from which packets with a particular IP address was sent.

Address type

Type of a trusted area item:

- 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



Note: *The All addresses option can only be used with a particular adapter (“network connected to this interface”). If it had been possible to combine this option with the --- Any --- option in the Adapter item, all IP addresses would have belonged to the trusted area. This would be irrelevant and such setting is not allowed by Sunbelt Kerio Personal Firewall (the OK button is not active).*

If a dial-up is selected in the Adapter entry, firewall's behavior can be set upon each change of a telephone number in the Zone definition dialog.

Network security Advanced settings

The Advanced tab in the Network security section provides options for advanced settings of the security and logging of undesirable traffic.

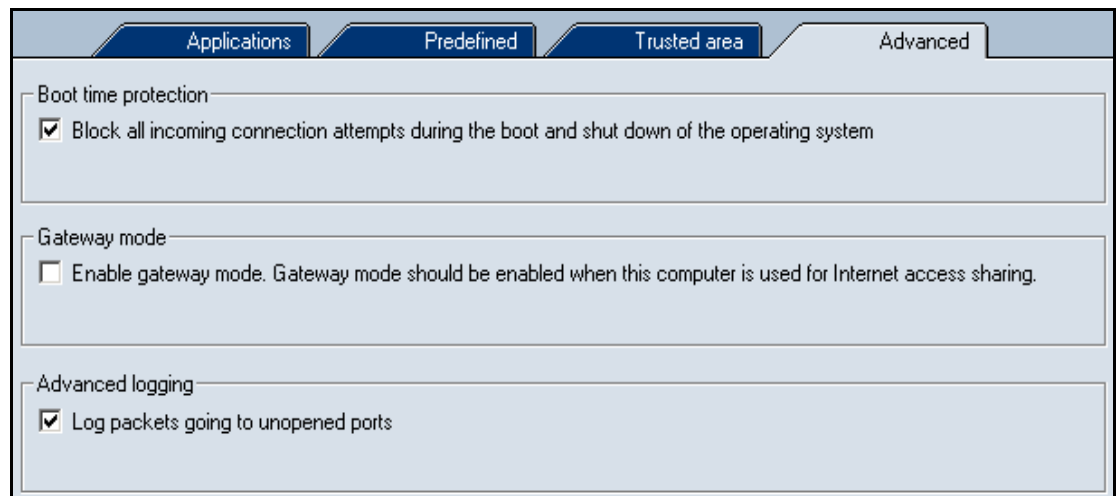


Figure 7-10 Network Security / Advanced section

Boot time protection

Check/uncheck 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 of the option can be useful for testing and troubleshooting purposes (e.g. to solve problems with remote administration of the host protected by Sunbelt Kerio Personal Firewall).

For security reasons, it is recommended not to 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 Kerio Personal Firewall will let through packets with destination ports at which no local application is running, or packets with destination IP addresses which are not local.

Do not use this option unless Sunbelt Kerio Personal Firewall is really running on the Internet Gateway, otherwise protection of the local computer might be seriously reduced!



Note: The Enable Gateway Mode option can be also used to allow communication of the operating system which is run within VMWare (<http://www.vmware.com/>) if Sunbelt Kerio Personal Firewall protects host system. If this option is disabled, Sunbelt Kerio Personal Firewall will block all packets routed to the operating system within the VMWare.

If Sunbelt Kerio Personal Firewall is used for proxy server protection, it is not necessary to enable this option (proxy server behaves as a client on the local computer).

Advanced logging

Use the `Log packets going to unopened ports` option to enable logging of detected packets which include destination ports which do not belong to any process in the local operating system. These packets are dropped automatically, however, they might point at an intrusion attempts (port scanning).



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

Boot time protection

The Sunbelt Kerio Personal Firewall's network traffic low-level driver protects computer even when the firewall is not running. Typically, this situation arrives upon startup of the operating system (the time between activation of network connections and the moment when the service is started) and during update of the product (during installation of a new version of Sunbelt Kerio Personal Firewall, the service is stopped automatically and it is started again when the server is restarted), or when the Personal Firewall Engine service is not launched upon start of the operating system for any reason.

This function is enabled by default. It can be disabled/enabled in the firewall's GUI whenever necessary (the Advanced tab under Network security).

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

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

Detection of new network interfaces

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



Note: Trustworthy network is a network computers of which are considered as secure by a user. Typically, it is a local network which is protected from internet attacks by a network firewall. Sunbelt Kerio Personal Firewall enables definition of various specific actions for trustworthy networks and other for the rest of the Internet.

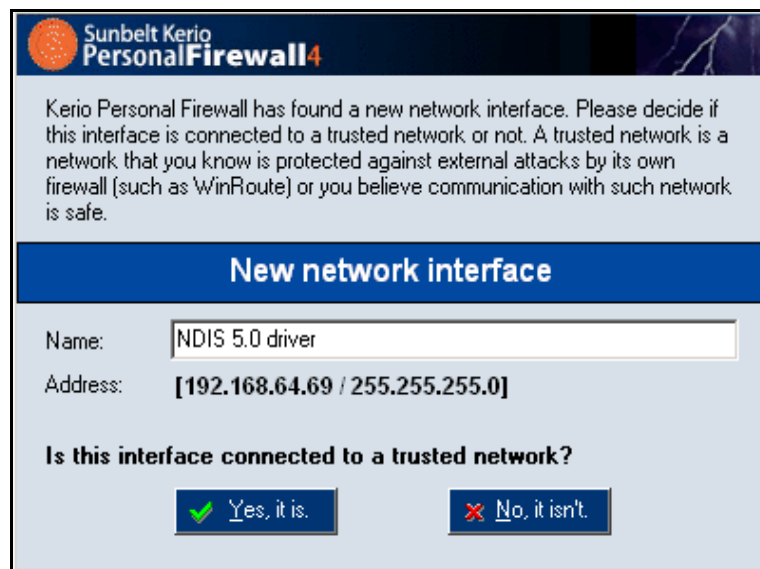


Figure 7-11 Detection of new network interfaces

The Name entry is specified by a name of a corresponding network adapter. The Address item provides information of IP address of this adapter and the mask of the network which it is connected to. Name of the interface can be edited (it is recommended to 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.

By clicking the Yes, it is button, the subnet to which the interface is connected will be added to the group of trustworthy IP addresses (Trusted area). If No, it isn't is clicked, the network will be considered as a part of the Internet.

- 1 Anytime, group of trustworthy IP addresses can be edited.
- 2 Whenever any other interface is added or enabled or an interface is connected to a new subnet, *Sunbelt Kerio Personal Firewall* detects it and the *New network interface* dialog is opened.
- 3 As to dial-ups, the telephone number which is being dialed is displayed. User can enable or disable this connection.

Sunbelt Kerio 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 of dialed telephone numbers

Sunbelt Kerio Personal Firewall can detect and block changes of telephone numbers of dialed lines. This protects users from undesirable redirecting of dial-ups to high-price services. Connections may be redirected without letting the user know (for example by an ActiveX object on a Web page). If a change of a telephone number is detected, *Sunbelt Kerio Personal Firewall* asks user to accept or reject the change. If the change is rejected, the line is hung-up immediately. Thanks to this feature, users are protected from undesirable and expensive connections.

How it works

Upon the first unknown dial-up connection, the firewall asks user whether the interface is connected to a trustworthy network (like in case of a new network adapter. The dial-up will be considered as an interface in the Network security / Trusted zone section.

After the user is asked whether the adapter should be accepted to the trusted zone, a dialog providing information on the new telephone number is opened.



Figure 7-12 Detection of new dial-up number

In this dialog, user can set various parameters of the interface as well as the way the firewall will behave upon a change of a dial-up number.

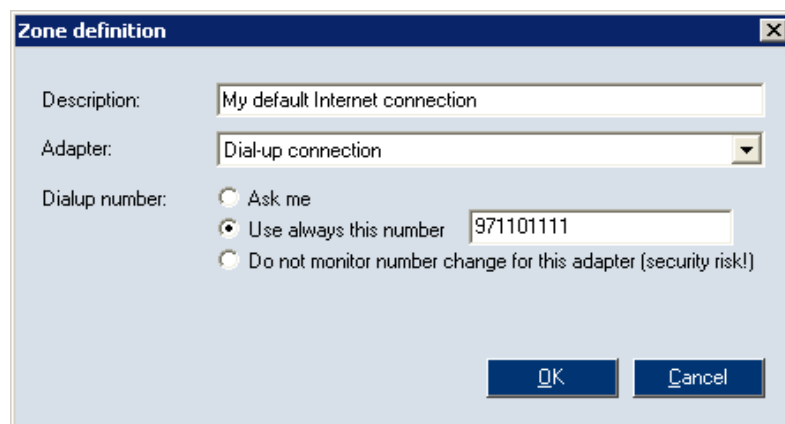


Figure 7-13 Checking of dialing telephone numbers settings

The following options are available for the Dialup number item:

- **Ask** — whenever a number is dialed, Sunbelt Kerio Personal Firewall asks user to accept or reject this number. If the change is accepted, the firewall remembers this dial-up 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 makes the firewall suppose that the dial-up number is not to be changed. Whenever a change of the dial-up number is detected, the New dial-up number dialog is displayed and the user is asked to accept or reject the change.



Figure 7-14 Dial-up number changed

The Dial-up number item provides the new telephone number (the number which is currently set for the dial-up connection). The Adapter item provides a name of the dial-up connection.

Click Yes, continue to make Sunbelt Kerio Personal Firewall accept the number, allow for dialing the line and remember the new number, or No, hang up to reject the change and hang up the line.

- **Do not monitor number change** — the firewall ignores changes of the dial-up number and always permits the line to be dialed. This option can be used for example for 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!



Advanced Packet Filter

The packet filter allows for definition of advanced rules for specific network communication. Besides selection of a local application and traffic direction, protocol, remote IP addresses, remote and local ports and other parameters can be defined.

Rules for packet filter can be defined as follows:

- By hand — click on the Packet Filter... button in the Applications tab of the Network Security section to 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 is opened when a connection which does not meet any rule is detected; if the Create an advanced filter rule option is checked, a packet filter rule will be created instead of a standard rule.



Note: Advanced packet filter does not distinguish between trusted area and the Internet (an IP address, subnet, IP group, etc. are always specified in the rule).

Packet Filter Rules

Rules for advanced packet filters can be viewed in the Filter Rules tab of the Advanced Packet Filter dialog window.

Rules are ordered in a list. Anytime a network connection is detected, the list is tested rule by rule from the top downwards and the first rule which the traffic meets is applied. Use the Up and Down buttons or Ctrl + up arrow and Ctrl + down arrow key combinations to reorder the list according to your liking and needs. More complex combinations of filtering rules can be defined thanks to these features.

Filter rules		IP Groups					
	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 8-1 Packet filter rules

Packet filter rules can be optionally classified by groups. Participation of a rule in a group does not influence the system of rule appliance since rules in all groups are always tested. This implies that these groups are for reference only. Rule groups are displayed on the left of the Filter Rules tab.

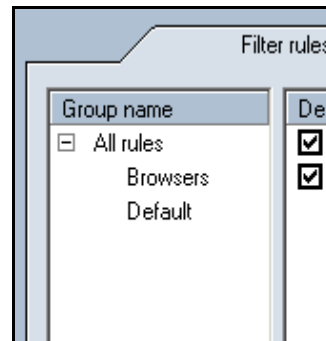


Figure 8-2 Rule groups of packet filter

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.

Use the following buttons below the group list to handle packet filter rules:

- Edit — opens dialog for modification of a selected rule (this dialog can also be opened by double-clicking on a selected rule)
- Add — adds a new rule to the end of the list
- Insert — inserts a selected rule to the current position (this rule will precede a marked rule)
- Remove — removes a selected rule



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.

Rule Definition and Modification

Clicking on the **Add**, **Insert** or **Edit** button opens a dialog for definition of a packet filter rule. A rule is defined by the following parameters:

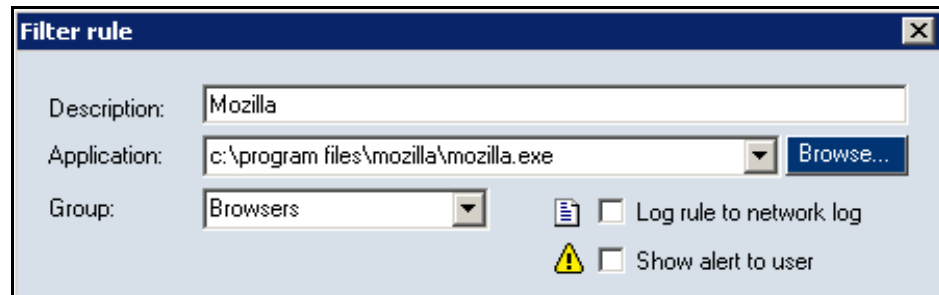


Figure 8-3 Packet filter rule

Description

Rule description/name. We recommend you to insert a brief rule description (purpose, application name, etc.). This description is used for your reference only. The name of a particular local application which participates in the communication is inserted for automatically generated rules.

Application

Local application to which the rule is applied. This application can be either inserted by hand (full path to a corresponding executable file), selected from a menu (menu of applications used for other rules is offered) or searched on the disc (use the **Browse...** button to open a standard system dialog from which an application can be run).

You can also create a general filtering rule which will be applied on all applications. This can be done through the any option or by leaving the Application item blank.

Group

Rule group in which the rule will be included. Participation of a rule in a group does not influence the system of rule appliance — the entire rule list is always tested. This implies that these groups are used for reference only.

Use the Group item to choose a group from the menu or to add a new group by inserting a new group name — the rule will be automatically included to this group. All rules are added to the Default group by default. The same method is applied on rules which are generated automatically.

Log rule to network log

Enables/disables logging of communication meeting this rule into the Network log.

Show alert to user

Check this option to enable the Alert dialog whenever traffic meeting this rule is detected.



Figure 8-4 Packet filter rule — Protocols

Protocol

Set parameters for protocols to which the rule will be applied. 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 we leave the Protocol entry empty, the rule will be applied to any protocol.



Note: *If an application uses TCP and UDP protocols at various ports, two different packet filter rules must be defined.*

Click on the Add or Edit button to open a dialog for protocol definition.

Figure 8-5 Packet filter rule — Protocol addition

The protocol is specified by a designated number in the IP packet header. This number can be defined directly through the Number entry. Use the Name option to select from a menu of predefined protocols.

You can use the Description text field to enter a description for your reference. It can be viewed in this dialog only.

The Codes item will be available in the dialog if ICMP is selected. Use this entry to specify type of ICMP messages which the rule will be applied on.

Figure 8-6 Packet filter rule — ICMP

Types of messages are defined by number codes (individual codes are separated by comas). If the Codes entry is not specified, the rule will be applied on all types of ICMP messages.

Click on the Select button to open a special dialog for definition of types of ICMP messages. Select appropriate types of ICMP messages. Click on the OK button and codes of the types you have defined will be inserted into the Codes entry automatically.

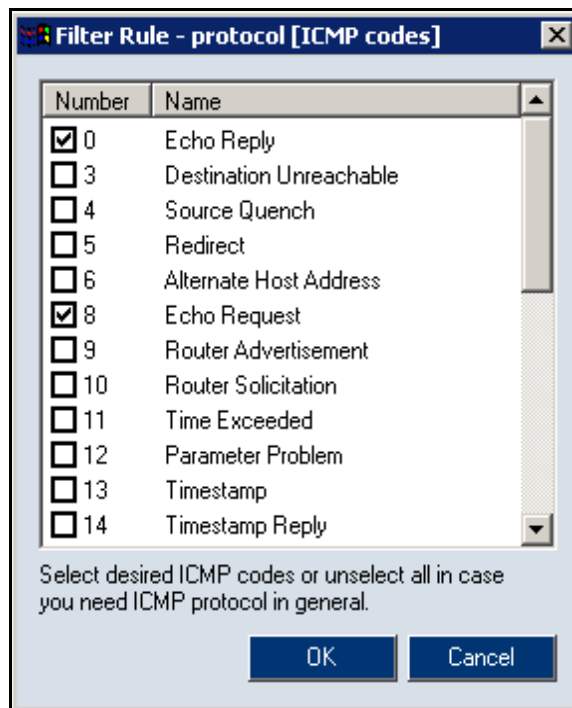


Figure 8-7 Packet filter rule — Types of ICMP messages

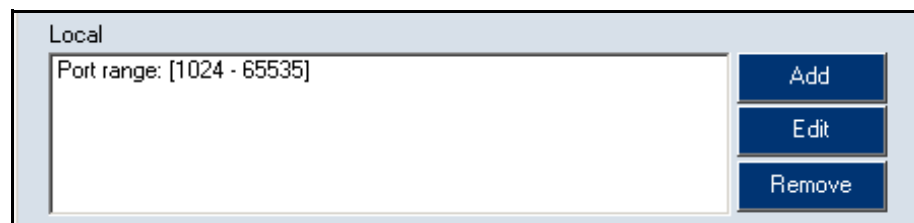


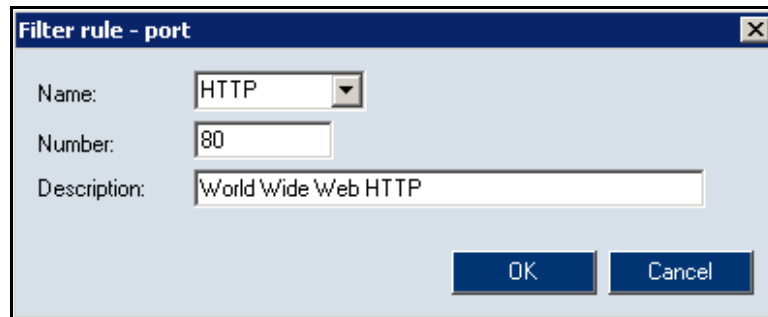
Figure 8-8 Packet filter rule — Port

Local

Specify parameters for the local point. Sunbelt Kerio Personal Firewall uses all local IP addresses implicitly including the loopback IP addresses. For this reason local parameters can be specified only by ports.

Use the Add button to add a single port (Add port) or a port range (Add port range). Multiple ports and port ranges can be specified — this way any port group can be covered easily.

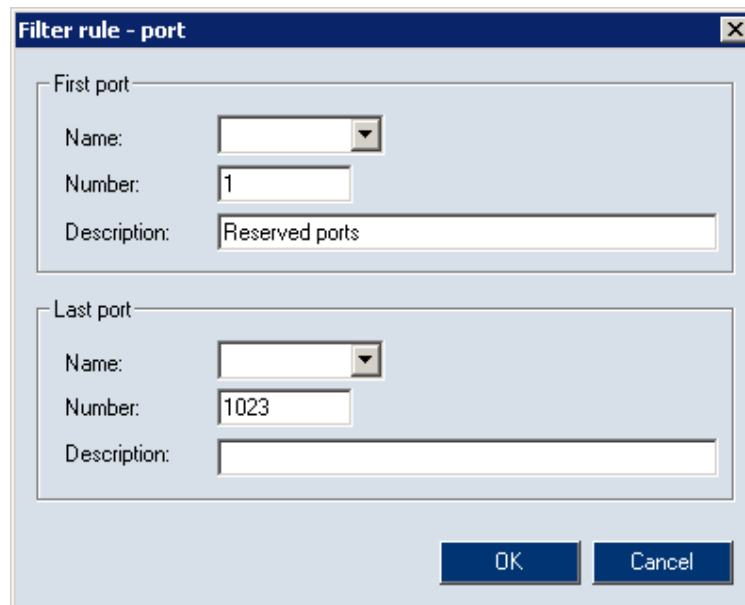
The port can be specified either by specification of the Number entry (only values included in the 1-65535 are valid) or by selection of a predefined service in the Name item. You can use the Description entry to describe the port or the service (for reference only).



The screenshot shows a dialog box titled "Filter rule - port". It contains three fields: "Name:" with a dropdown menu set to "HTTP", "Number:" with a text box containing "80", and "Description:" with a text box containing "World Wide Web HTTP". At the bottom right, there are "OK" and "Cancel" buttons.

Figure 8-9 Packet filter rule — Addition of port

The dialog for range specification consists of two essential entries: First port (first port in the range) and Last port (last port in the range).



The screenshot shows a dialog box titled "Filter rule - port" with two sections. The "First port" section has "Name:" (empty dropdown), "Number:" (text box with "1"), and "Description:" (text box with "Reserved ports"). The "Last port" section has "Name:" (empty dropdown), "Number:" (text box with "1023"), and "Description:" (empty text box). "OK" and "Cancel" buttons are at the bottom right.

Figure 8-10 Packet filter rule — Addition of port range

Remote

Specification of remote point of a connection. IP address, port or both can be specified. The rule will be applied if the packet will contain any of defined IP addresses and one of the defined ports.

Figure 8-11 Packet filter rule — Remote IP address (computer) and port (service)

Either individual ports (Add port) or a port range (Add port range) can be defined. The dialog is the same as for the Local point — see above.

Use the following methods to specify IP address:

- a single IP address (Add address)

Figure 8-12 Packet filter rule — Addition of IP address

- IP address range (Add address range) — enter first and last address of the range

Figure 8-13 Packet filter rule — Addition of IP address from IP address range

subnet (Add address / mask) — specify subnet address and a corresponding mask

Figure 8-14 Packet filter rule — Addition of subnet

IP address group (Add IP group) — use the Select option to select one from the menu of IP addresses defined through the IP Groups tab (see below)

Figure 8-15 Packet filter rule — Addition of IP address group

Individual methods can be combined.



Figure 8-16 Packet filter rule — Direction of the traffic and action settings

Direction

Direction of the traffic which the rule will be applied to: Both directions, Incoming or Outgoing connection.

Traffic direction is represented by direction of an initial packet which starts the connection.

Action

Action which will be taken by Sunbelt Kerio Personal Firewall when a connection meeting this rule is detected:

- Permit — allows the connection
- Deny — blocks the connection

Packet filter rules details

It is important to be aware of how individual parts of a rule and their items are related to be able to define rules effectively.

- The logical relations among Protocol, Local and Remote are “and”. This implies that only traffic which meets all the conditions will meet the rule.
- The logical relation between items included in one item (protocols, IP addresses and ports) is “or”.
- Example: The Remote item consists of two port ranges : 80-88 and 8000-8080. The rule will be met when a remote port belongs to one of these ranges.
- The logical relation between the “IP address” and “port” items in the Remote entry is “and”. Example: The Remote entry is specified by the IP address 65.131.55.1 and the port number 80. This condition will be met by traffic which includes a remote computer with the IP address 65.131.55.1 at the port number 80.

Notes Specific to Packet Filter Definition

The Protocol, Local and Remote entries are closely related. A user should follow the following rules to ensure smooth functionality of the rule:

- 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 port numbers are not applicable as they are used only for traffic through TCP or UDP protocols.
- Application service is specified by port numbers and by protocols. In the packet filter rule dialog, a service is represented by port only — the protocol must be entered by hand.
Example: Suppose we want to create a rule for incoming HTTP connections (i.e. to enable access to a Web server on a computer which is protected by *Sunbelt Kerio Personal Firewall*), we will take the following steps:
 - Add port in the Local section. Select the HTTP service — this will automatically set the port value to 80.
 - Go to the Protocol section to set TCP, which is used by the HTTP service.
- The most common traffic model 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 free local port (an unknown port) from the operating system that will be used for the connection. This implies that, unlike the server port (which must be always known), any free port can be used temporarily for a client.

These facts should be considered during packet filter definition. The problem will be better understood through the two following examples:

Example 1: We intend to enable access to a Web server on a local computer with IP address 60.80.100.120. We can achieve this by definition of the following rule:

- 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 will be running at a remote host; port is not known yet, that is why we specify the IP address only)

Example 2: We intend to block connections to the Web server with IP address 90.80.70.60. This is how we define the rule:

- Protocol — [6] TCP
- Local — we leave this entry empty (client port cannot be specified yet)
- Remote — Port: [80] HTTP, Address: 90.80.70.60 (specification of the remote server)

IP Groups

IP groups enable easier definition of packet filter rules. These groups can be used for specification of the `Remote` entry in the dialog for packet filter rule definition (see above).

IP groups can be viewed and defined in the `IP Group` tab of the `Advanced Packet Filter` window.

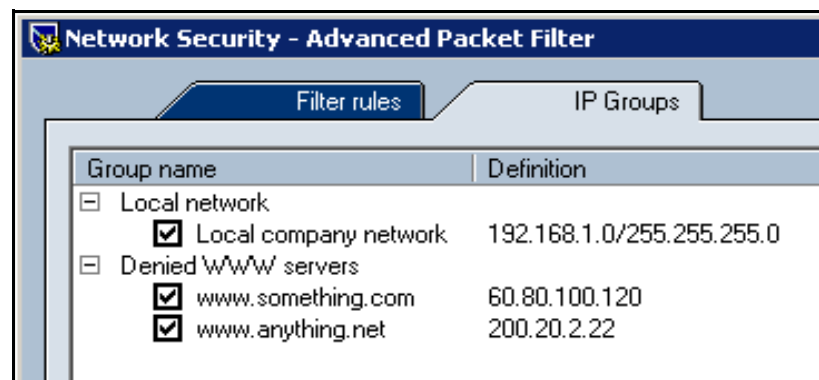


Figure 8-17 Packet filter — IP address groups

The window consists of the two following columns:

- Group name — name of an IP group. Use the plus button to view a list of all items included in a particular group
- Definition — definitions of individual items of a particular group

Uncheck an item to disable a rule temporarily. This can be helpful for example when testing or debugging — it is not necessary to remove items and then define them again.

Click on the Add button (or the Edit button to edit a selected item) to open a dialog for IP group definition.

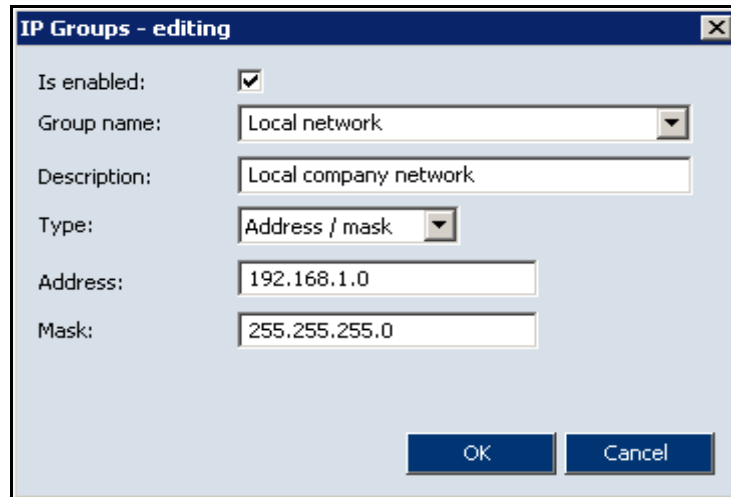


Figure 8-18 Packet filter — Addition of IP address group

Is enabled

Check/uncheck this option to enable/disable the item. This option is identical to the matching field next to the item name in the IP Groups tab (see above). If the Is enabled is unchecked, 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 by 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 First address 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)



Internal Firewall Rules

Sunbelt Kerio Personal Firewall includes predefined rules which allow network communication for exceptional cases (e.g. license registration, product update etc.) and startup of some applications (system components).

Internal firewall rules are prior to user-defined rules. Internal rules cannot be disabled nor modified.

Internal Network Traffic Rules

These rules enable allowance of network traffic between individual *Sunbelt Kerio Personal Firewall* components during local or remote administration, connections to *Sunbelt Software* registration or check-for-new-version servers, etc.

Internal network traffic rules are hidden — they are not displayed in *Personal Firewall GUI*.

Remote configuration

This rule enables connection of the *Personal Firewall GUI* to the *Personal Firewall Engine*. If remote administration is allowed, connections from any host are allowed. If not, only 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 enables 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 of the Personal Firewall Engine with the GUI

This rule allows the *Personal Firewall Engine* to connect to the *Personal Firewall GUI* (displaying of 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 Kerio Personal Firewall components to send DNS queries to any DNS server. DNS queries are used for mapping of host names which are later used for various purposes, such as displaying in Personal Firewall GUI, resolution of 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 of crashdump files to Sunbelt Kerio Technologies is enabled, this rule allows sending files 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 is used for corresponding webpages that sends Personal Firewall Engine information about blocked pages. Traffic is performed by TCP protocol through a special port (44501).

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

Update checker

This rule allows to access download servers where new versions of *Sunbelt Kerio Personal Firewall* are available.



Note: 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

*) Resolution of IP address and port's proxy server is performed automatically by the *Sunbelt Kerio Personal Firewall* (the information is resolved from configuration of the operating system).

Product registration

This rule enables registration of Sunbelt Kerio Personal Firewall license 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

*) Resolution of IP address and port's proxy server is performed automatically by the *Sunbelt Kerio Personal Firewall* (the information is resolved from configuration of the operating system).

Syslog

If logging to Syslog server is enabled, this rule enables connection of the Personal Firewall Engine 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

These rules allow startup of various components of the operating system on which the Sunbelt Kerio Personal Firewall is installed. Internal system security rules can be found in the System Security / Applications section. These rules cannot be removed, however, users can set actions, logging or/and notices for them.

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:\WINDOWS 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)

1 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

2 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

3 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

4 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

5 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 Kerio Personal Firewall components

These rules allow running individual Sunbelt Kerio Personal Firewall applications 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 Kerio 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

Rules for AVG components

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



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

Figure 9-1 Network Security — Rules for AVG components

- The first rule allows the *AVG E-mail Scanner* component to communicate with mailservers (all data between the mail client and servers will pass through *E-mail Scanner*).
- The second rule allows automatic updates of *AVG* and virus database at corresponding servers.

Rules for *AVG* can be changed and/or removed by a user. If these rules are removed, *Sunbelt Kerio Personal Firewall* will treat communication of *AVG* 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

In the *Intrusions* section, protection from various intrusion types can be set, as follows:

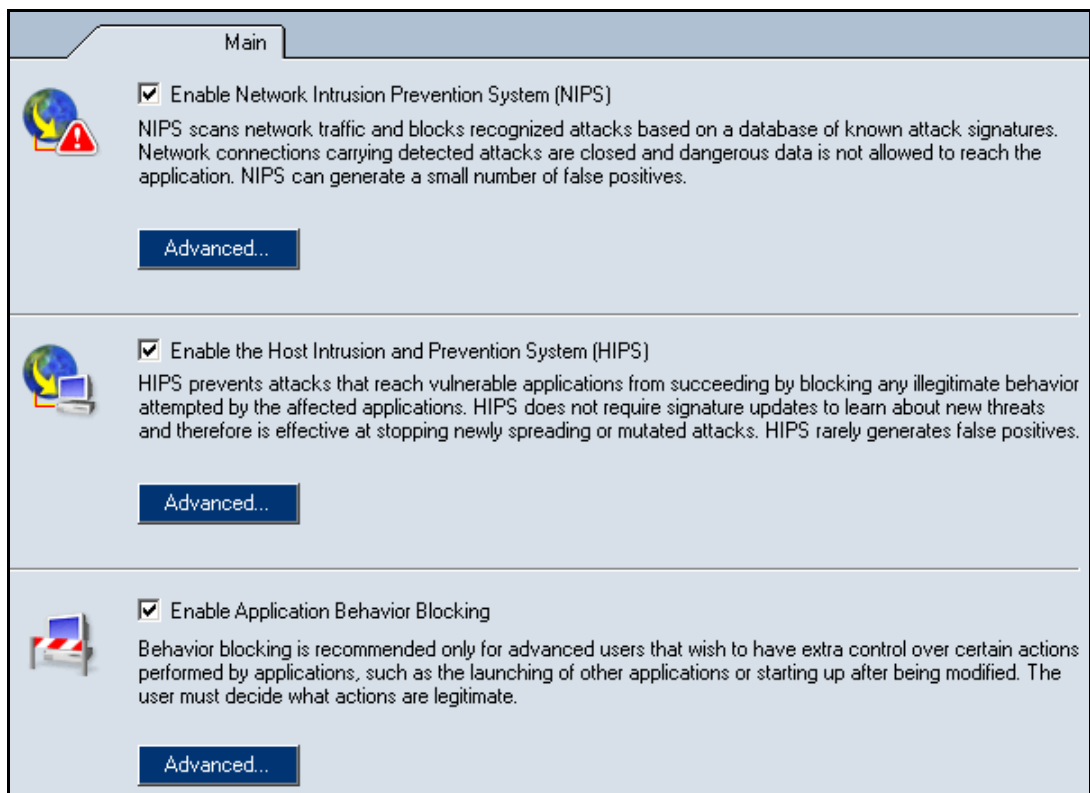


Figure 10-1 The Intrusions section

- Network intrusion prevention system (NIPS) — this system recognizes and blocks various types of network intrusions by blocking network connections that might be used for transfer of dangerous data.
- Host intrusion detection and prevention system (HIPS) — this system recognizes and blocks technologies used by intruders or viruses to run malicious codes. HIPS is helpful especially for recognition of new or modified viruses.
- Behavior blocking — this system enables to monitor behavior of applications, such as starting of an application by another process or application modification. This method is extremely helpful especially for recognition of new viruses.



Network Intrusions Prevention System (NIPS)

Sunbelt Kerio Personal Firewall is able to detect and block many known network intrusion types. For this purpose it uses its internal intrusion database. The database can be automatically updated every time a new version of the firewall is installed (therefore, we recommend you to perform update of Sunbelt Kerio Personal Firewall anytime it is alerted).

The Sunbelt Kerio Personal Firewall contains the Network Intrusion Detection and Prevention System (NIPS) which is compatible with Snort, the open-source IDS (<http://www.snort.org/>).

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

NIPS Settings

NIPS (Network Intrusion Prevention System) parameters can be set in the `Intrusions` section (see figure <Undefined Cross-Reference>).

Use the `Enable NIPS module` option to enable/disable the intrusion prevention system.



Figure 11-1 Intrusion Detection — NIPS Settings

Sunbelt Kerio Personal Firewall distinguishes between three intrusion types:

- High priority intrusions — critical intrusions which might for example damage the operating system, cause data leak, etc.
- Medium priority intrusions — intrusions which cause for example blocking of certain services, malfunctions of network connection, etc.
- Low priority intrusions — low-level danger intrusions (equivocal network activities, errors in protocols, invalid data format, etc.)

Firewall behavior can be set for individual types using the following options:

- Action — firewall's reactions to attacks of a particular type (Permit, Deny).
- Generally spoken, it is recommended to deny all High priority and Medium priority intrusion types — do not permit intrusions of these types unless necessary (i.e. for testing, etc.). Low priority intrusions are allowed by default — their blocking might cause malfunctioning of certain services.
- Log to intrusion log — logs all detected intrusions of a particular type into the Intrusions log (see chapter <Undefined Cross-Reference>).

Use the Details button to open a window providing outline of intrusions of the particular type.

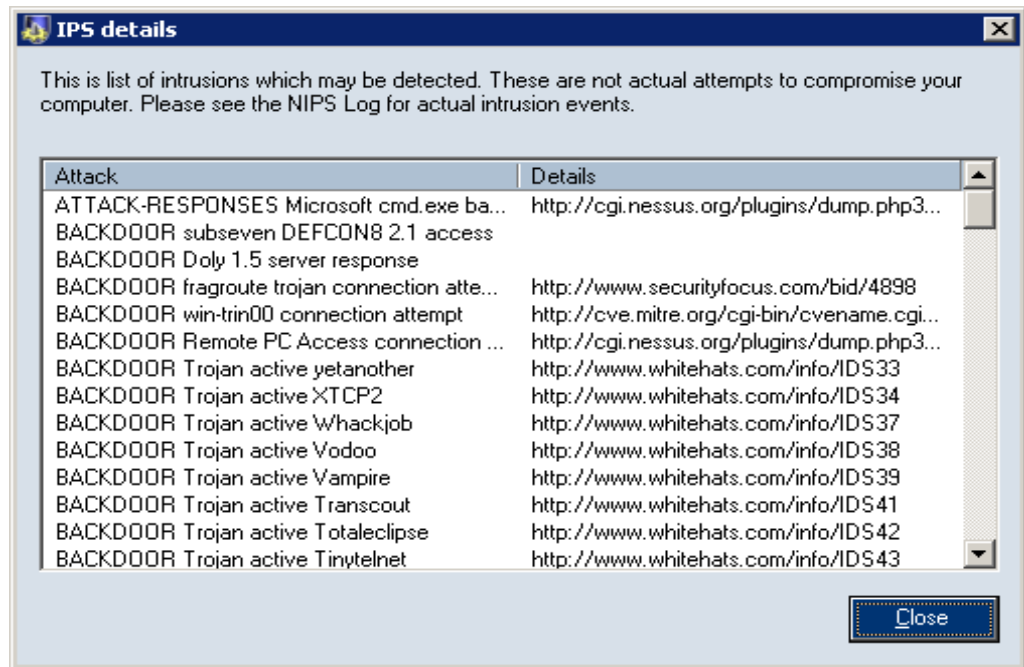


Figure 11-2 Intrusion Detection — Details of intrusions

The dialog provides name or description of the attack (the Attack column) and class of the intrusion (the Class column). Sunbelt Kerio Personal Firewall uses the Snort type of IDS — for detailed information on individual attacks and attack types go to the <http://www.snort.org/> website.

So called Port Scanning is a special attack type (detection of open ports on a particular computer). Such attacks cannot be blocked if any ports of the user are open (closed ports are blocked automatically), they can only be detected. Use the Log to intrusions log option to enable/disable logging information on Port Scanning to the Intrusions log.



Host Intrusion Prevention System (HIPS)

HIPS targets detection and prevention from special technologies used by users or viruses to run malicious codes. Legitimate application usually do not apply such technologies. Disabling of these technologies helps to protect you from security leaks in applications running at the server. *HIPS* protects even from new security leaks which cannot be detected by other detection systems (since new attack types might not be in their databases yet).

HIPS configuration

Parameters of the intrusion detection system can be set in the Intrusions section.

HIPS can detect and filter out the two most wide spread technologies used for execution of malicious codes: *Buffer Overflow* and *Code Injection* (injects malicious code into another process).

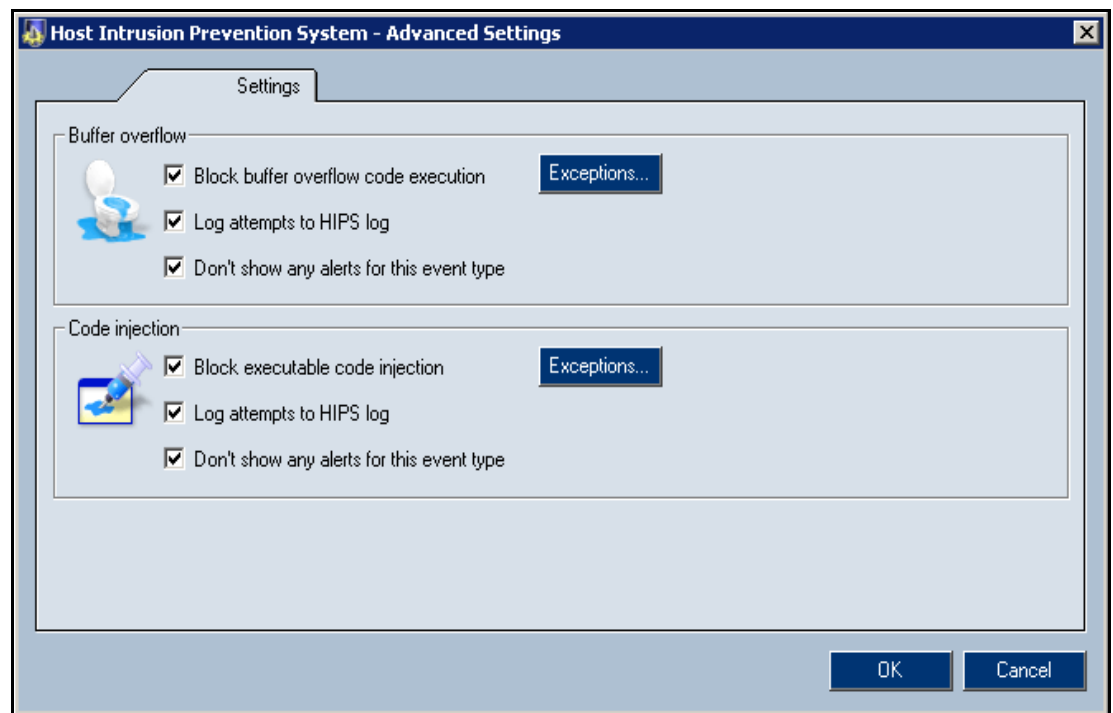


Figure 12-1 Intrusion Detection — Setting the intrusion prevention module

Buffer Overflow

The Buffer Overflow technology misuses insufficient control of application's input data. Unless size of read data is limited and controlled, an attacker may overwrite return address of the running program and execute their own code. However, this code is executed from the buffer reserved for data. This is then considered as a non-standard behaviour and detected by the HIPS module. Possible attempts on execution of possibly dangerous actions (process execution, file opening, network connection establishing, etc.) are blocked.

Block buffer overflow code execution

This option allows to disable running a code in case of a buffer overflow.

Log attempts to HIPS log

If this option is enabled, all detected intrusions are logged in the HIPS log.

Don't show any alerts for this event type

Check this option to disable alert windows for intrusion attempts.

Use the Exceptions button to specify an executable to which this attack type check will not apply. Before setting an exception, check if the attempt is not a real intrusion.

Code Injection

The Code Injection technology is based on misusing of authorization of another running trustworthy process. The infected application (with corresponding authorization) writes a malicious executable code in the memory space of the process or it connects to the dynamic library of the process. By special calling of the operating system, the code is executed. This way the attacker makes their code being executed using the authorization of the trustworthy process.

The HIPS module detects and blocks execution of codes written by special calling of the operating system to the memory of a trustworthy process. In such cases, functionality of attacked application is usually not interfered.

Block executable code injection

Check this option to block executable code injection.

Log attempts to HIPS log

If this option is enabled, all detected intrusions are logged in the HIPS log

Don't show any alerts for this event type

Check this option to disable alert windows for intrusion attempts.

The Code injection technology is used by various legitimate applications — these applications will not function correctly. For such cases, Sunbelt Kerio 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.



Behavior Blocking

Sunbelt Kerio Personal Firewall controls all applications in the operating system, regardless of whether they are deployed into network communication or not. Therefore it can detect when an application is infected by a new virus or attacked by a Trojan horse immediately (it usually takes some time when an antivirus is used — a new virus must be detected and then an appropriate virus database must be found).

Go to the Behavior Blocking section to set behavior blocking parameters (parameters for application control).

Check/uncheck the Enable Behavior Blocking option to enable/disable control of starting applications. If this option is disabled, running applications is ignored by Sunbelt Kerio Personal Firewall.

General Rules

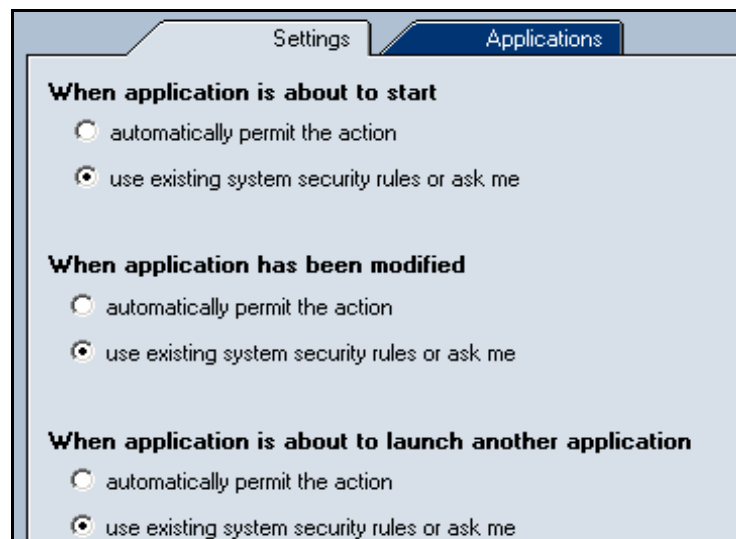


Figure 13-1 Behavior Blocking — General rules

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

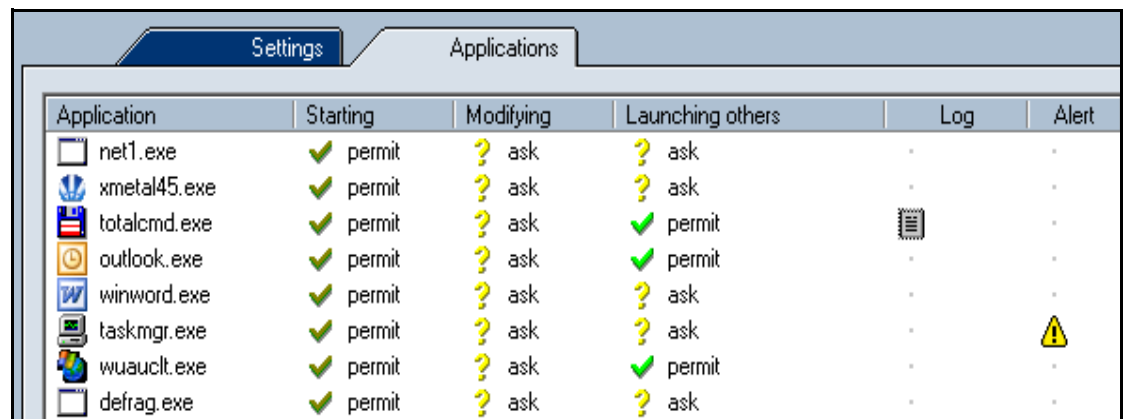
- When application is about to start — application startup
- When application has been modified — modification of application's executable file (by the startup a check-out summary of the executable is performed and it is compared with the summary stored in the Sunbelt Kerio Personal Firewall database)
- When application is about to launch another application — startup of another application by the running application

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

- automatically permit the action — Sunbelt Kerio 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

Application Rules

Go to the Applications tab in the Behavior Blocking section to view and edit rules for startup and change of particular applications.



Application	Starting	Modifying	Launching others	Log	Alert
net1.exe	✓ permit	? ask	? ask	.	.
xmetal45.exe	✓ permit	? ask	? ask	.	.
totalcmd.exe	✓ permit	? ask	✓ permit	☰	.
outlook.exe	✓ permit	? ask	✓ permit	.	.
winword.exe	✓ permit	? ask	? ask	.	.
taskmgr.exe	✓ permit	? ask	? ask	.	⚠
wuauclt.exe	✓ permit	? ask	✓ permit	.	.
defrag.exe	✓ permit	? ask	? ask	.	.

Figure 13-2 Behavior Blocking — Application rules

These rules are based on interaction with user when an unknown application is started. Rules cannot be created by hand, they can only be edited or removed.

An action that firewall will take after startup (Starting), after the executable file is changed (Modifying) and when another application is run by this application (Launching others) can be set for each application. Actions can be defined:

- 1 right from the menu of applications — click on an action to switch between the following actions: permit, deny and ask
- 2 right-click on an action and select an action from the context menu



Figure 13-3 Behavior Blocking — application rules — action selection

- 3 In the dialog for rule modification. Use the Edit button or the Edit option in the context menu to open the dialog.

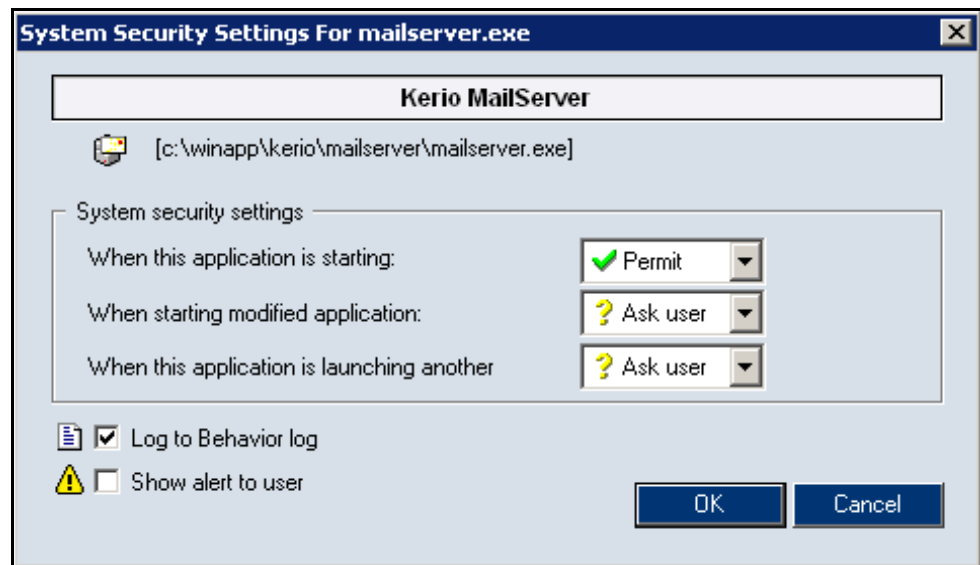


Figure 13-4 Behavior Blocking — Editing of application rule

- In the dialog header, description, icon and full path to the application's executable file is provided.
- Use the Behavior Blocking settings entry to enable setting actions for the described situations.
- Check or uncheck the Log to system log option to enable/disable log activity for the application (startup, change of the executable file or running another application by this application)
- Check or uncheck the Show alert to user option to enable/disable the Alert dialog for cases when the application is activated.



Web Content Filtering

Two main content filtering functions are available in Sunbelt Kerio Personal Firewall:

- Ad blocking (blocking of banners, pop-up windows, etc.)
- Privacy protection (control of outgoing data and stored cookies)

The Ad Blocking tab

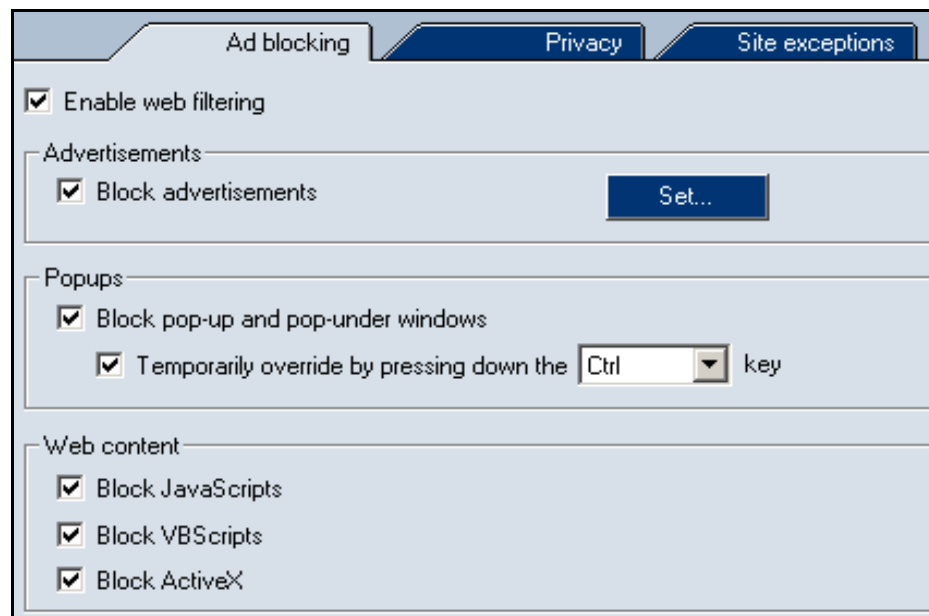


Figure 14-1 Sekce WWW / Ad blocking — Options

Sunbelt Kerio Personal Firewall provides the following ad blocking options:

Block advertisement

Use this option to block ads according to the defined rules. Use the **Set** button to open a dialog for definition of these rules (see below).

Block pop-up and pop-under windows

Use this option to deny automatic opening of undesirable browser windows (*popup* is a window opened over an active browser window; *pop-under* is a window opened under an active browser window).

Temporarily override by pressing down the ... key

If this option is enabled, holding down a selected key (*Ctrl* or *F12*) will temporarily disable pop-up and pop-under windows blocking (i.e. unless a page is loaded).

The *Sunbelt Kerio Personal Firewall* icon on the Systray indicates when pop-up and pop-under blocking is disabled.



Figure 14-2 Systray icon — Pop-up filter disabled



Warning: The *F12* key may collide with the *Microsoft* debugger. If you use the *Microsoft Visual Studio*, we recommend you to use the *Ctrl* key.

Block JavaScript, Block VBScript

Enable these options to filter all commands of the corresponding script run from a website.



Note: *These options might cause problems with displaying of some pages. If so, define special rules for such pages 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).*

These options might cause problems in displaying of some pages or malfunctions — in such cases modify firewall settings as described in the previous item.

Ad Filtering Rules

Click on the **Set** button to open a dialog where ad filtering rules can be edited, removed or added.

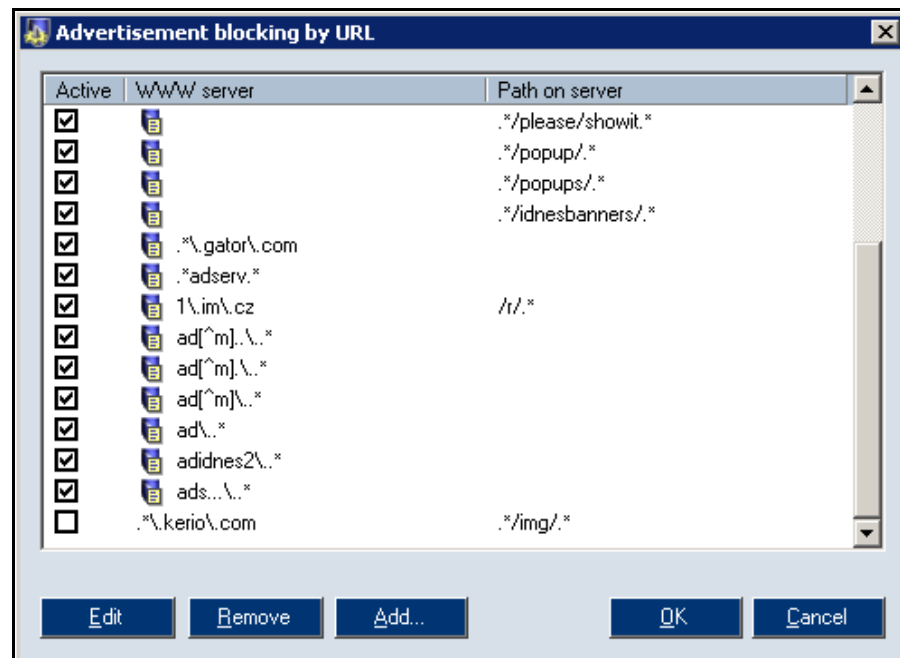


Figure 14-3 Ad Filtering Rules

Each rule consists of two parts — Server part (name or IP address of a particular Web server) and Local part (relative address of a particular object at the server).

Only one of these items can be specified.

- If the WWW Server item is empty, the rule will be applied on the specified relative address at any server.
- If the Path on server entry is empty, the rule will be applied on any object at the specified server (this Web server then cannot be accessed)

Use matching fields in the Active column to enable/disable individual rules. This way rules can be disabled temporarily (it is not necessary to remove rules and add them later).

Use the Edit, Remove and Add buttons to edit or remove selected rules or to add a new one. Sunbelt Kerio Personal Firewall includes set of predefined rules (marked with an icon). Predefined rules cannot be edited nor removed, they can only be enabled or disabled.

Sunbelt Kerio Personal Firewall includes database of predefined rules. These rules are marked with a corresponding icon. Predefined rules cannot be modified or removed, they only can be enabled or disabled. The database is updated whenever a new version of Sunbelt Kerio Personal Firewall is installed. Only parameters of the Active column will be kept after an update (rules which have been disabled by the user will not be enabled during an update).

Click on the Add or the Edit button to define ad filtering rules. Such rules consist of two parts:

- WWW server — name of a WWW server
- Path on server — path to an object (object localization) placed on the server

Both the wildcard characters or the regular expressions (more complex definitions for experienced users) can be used for this definition.

Rule Definition using Wildcard Characters

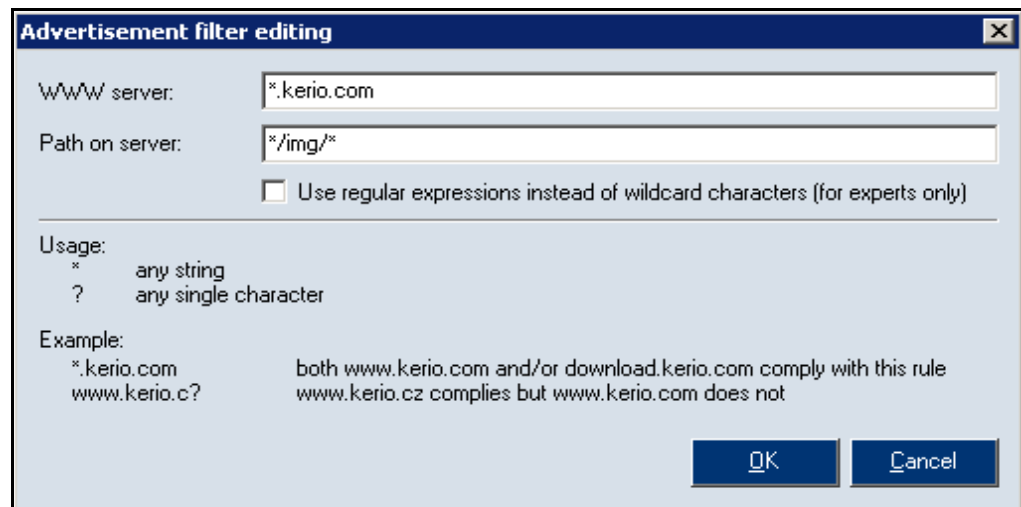


Figure 14-4 Definition of Ad Filtering Rule — Using Wildcard Characters

If the Use regular expressions instead of wildcard characters is disabled, the following wildcard characters can be used for definition of the WWW server and the Path on server entries:

- * (asterisk) — represents any number of characters (even an empty string)
- ? (question mark) — represents any single character

Examples:

- The WWW server entry is defined by the string `*.sunbelt.com`. Unlike for example `www.akerio.com`, WWW servers `www.sunbelt-software.com` or `download.sunbelt.com` will match with this string.
- The WWW server entry contains the string `www.sunbelt.f?`. WWW servers `www.sunbelt-software.fr` or `www.sunbelt.fx` will match with this string, WWW server `www.sunbelt-software.com` will not.

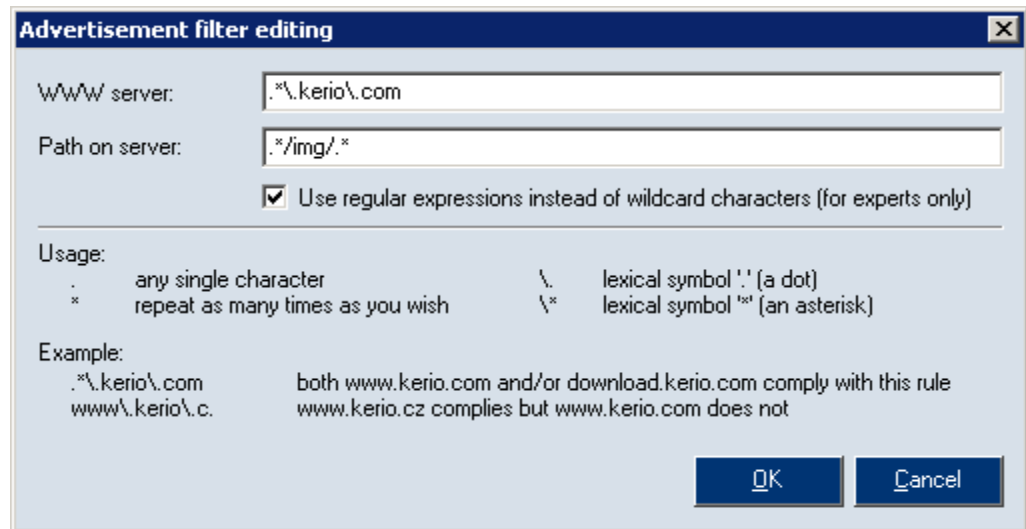
Rule Definition using Regular Expressions

Figure 14-5 Definition of Ad Filtering Rule — Using regular expressions

If the Use regular expressions instead of wildcard characters is enabled, the WWW server and the Path on server entries must be defined using regular expressions (POSIX standard). Regular expressions can be used to specify any string using special symbols:

A few basic characters are usually sufficient for Web server and Web object definitions:

- `.` (dot) — represents any character in a string.
- `*` (asterisk) — represents any number (even zero) of repetition of the previous symbol.
- Example: The `.*` expression represents any number of characters.
- `\` (backslash) — is used for specification of a character which is used as a special symbol in the regular expression.
Example: The `\.` expression represents the “dot” character.

Example (refer to the screenshot):

- The Server Part item is defined by the `.*ad\.anything\.*` expression.
- This expression means that server name must include the `ad.anything.` string — i.e. `ad.anything.net`, `1ad.anything.com`, `img.ad.anything.cx`, etc.
- The Local Part is defined by the `*/img/*` expression.
- This implies that relative address of the object must include the `/img/` string — i.e. `/img/banner.gif`, `/data/img/bar.jpg` or `/img/`.

For detailed information on regular expressions go to: <http://www.gnu.org/software/grep/>

The Privacy tab

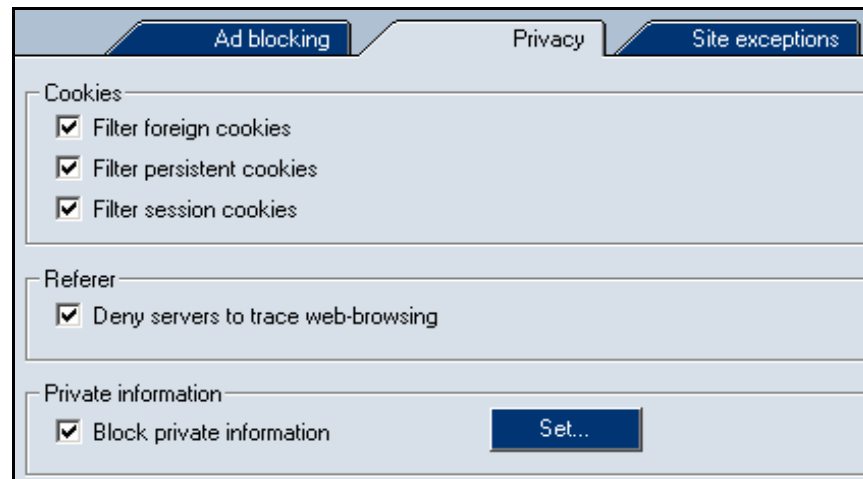


Figure 14-6 Sekce WWW / Praivacy — User privacy protection

The Privacy tab provides the following options for user privacy protection:

Filter foreign cookies

Filtering of both persistent and session cookies from third-party servers (Third party cookies).

These cookies are downloaded from servers independent from the page itself (i.e. ad cookies).

Filter persistent cookies

This option can be used to filter persistent cookies.

These cookies contain information which can be sent to a particular Web server whenever the page is visited again by the user — the server is informed that the user has already visited the page, this user's preferences and other information.

Filter session cookies

This option filters temporary cookies (the cookies are saved during one session only —until the Web browser is closed). These cookies are used only if the user opens a particular page (or a particular server or a server in a particular domain) again within the same session — that are removed when the all windows of the browser are closed.

Note: Even if filtering of all types of cookies is enabled, a cookie may be saved under certain circumstances. This situation arrives, for example, when a cookie is saved by a script on a Web page — this is not a type of network traffic and therefore Sunbelt Kerio Personal Firewall does not detect such actions. However, filtering of cookies does not allow to send any cookie to the server, so that saved cookies are unusable. This implies that the firewll protects user's privacy even in these cases.

Deny servers to trace web-browsing

Blocks the Referer item in HTTP header.

This item includes URL address of the page from which the user opened the current page. Browsing of users can be easily monitored using the Referer item.

Block private information

This option blocks sending private user data through forms on Web pages.

Click on the Set button to open a dialog where private data which will not be allowed to send and which will be blocked by Sunbelt Kerio Personal Firewall can be specified.

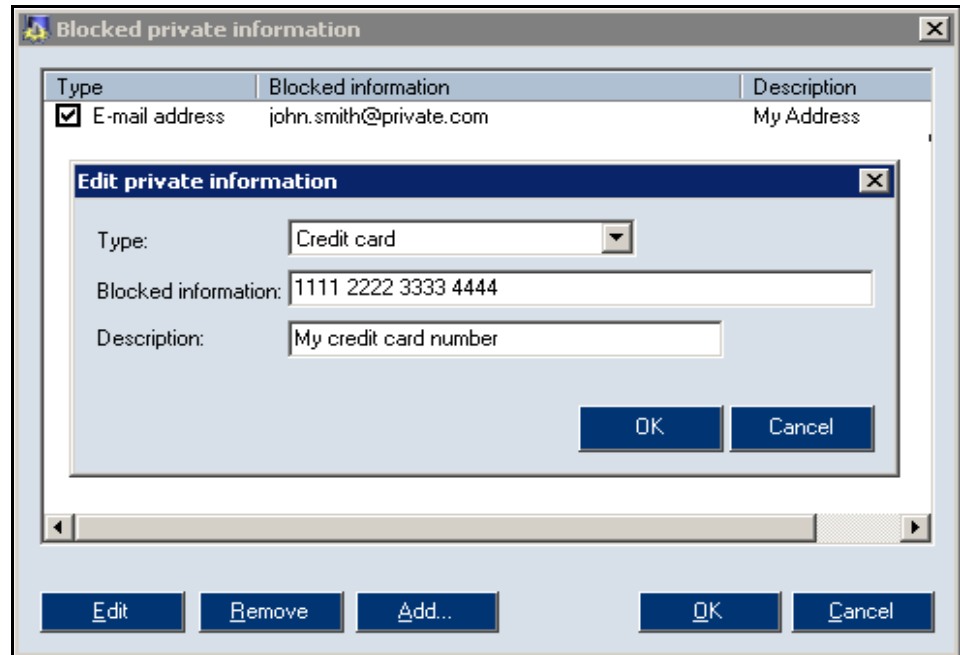


Figure 14-7 Definition of private information

Define the following items to specify private user data which will be protected:

- Type — information type (i.e. email address, credit card number, etc.). This item is for reference only and it is not related to the field type on a Web page.
- Blocked information — string which will be blocked by Sunbelt Kerio Personal Firewall. Warning: Private information is not case-sensitive.
- Description — description of the private information (for reference only).

The Exceptional sites tab (exceptions for individual servers)

Web servers for which special Web content filter rules will be defined can be specified in the Exception sites tab.

Web server	Foreign cookies	Pers. cookie	Sess. cookie	Referer	Popups	Privacy
.*\windowsupdate\.microsoft\.com	✓ Allow	✓ Allow	✓ Allow	✓ Allow	✓ Allow	✓ Allow
*.kerio.com	✗ Suppress	✗ Suppress	✓ Allow	✗ Suppress	✓ Allow	✓ Allow
.*\kerio\.cz	✗ Suppress	✓ Allow	✓ Allow	✗ Suppress	✓ Allow	✓ Allow

Figure 14-8 Sekce WWW / Site exceptions — Specific settings for www servers

Exceptions for individual Web servers can be helpful especially when general content filter rules (in the Ad blocking and Privacy tabs) cause that certain Web pages or some of their items do not function (i.e. new windows cannot be opened, it is not possible to login through an email address, etc.), or that they will be completely blocked (according to ads filtering rules). Before you define an exceptional rules for a server, consider carefully whether the server is trustful or not and which types of objects (scripts, cookies, private data) are really required for smooth functionality of pages on this server.

The Exception tab includes one predefined rule. This rule allows automatic Microsoft updates and allows updates from windowsupdate.microsoft.com.

Use the Add or the Edit button to open a dialog where exceptions can be defined.

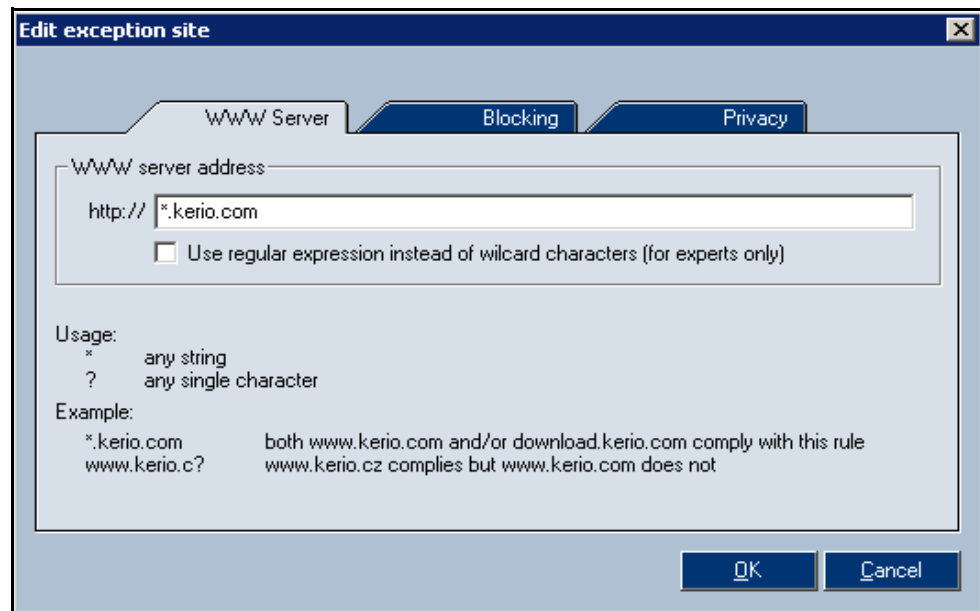


Figure 14-9 Exception definition for WWW server

Use the WWW Server tab to specify Web server name. Names can be specified by wildcard characters or by regular expressions.

The Blocking and the Privacy tabs provide similar functions as the same tabs in the Web section. However, in this case individual parameters are applied for a selected Web server only.



Status Information

Connections and Open Ports Overview

Open the Connections tab in the Overview section to view the list of active connections and open ports used by individual applications. This overview of connections makes users aware of which applications are actively involved in current network communication and which applications are waiting for connections.

A port is considered open when:

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

List of applications which include at least one open port can be found in the Connections tab.

Local Point	Remote Point	Protocol
All: 44336	-----	TCP
All: 81	-----	TCP
Mozilla		
All: 1137	Loopback: 1136	TCP
Loopback: 1136	Loopback: 1137	TCP
VNC server for Win32		
All: 5900	-----	TCP
All: 5800	-----	TCP
Domain Name System (DNS) Server		
All: domain	-----	TCP

Figure 15-1 Overview / Connections — Overview of active connections and open ports used by individual applications

The first line represents each application's icon and name (description) — if the application has no icon, the default system icon for executable files will be used; if no description (name) is available, the name of the file without the extension will be displayed. Click on the [+] button next to the application icon to view or on the [-] button to hide open ports currently used by the application.

The other lines provide information on individual open connections. Outgoing connections are green, incoming connections are red. Individual columns provide detailed information on each connection:

Local Point

Local IP address (or a corresponding DNS name) and port (or name of a service in case of a standard service).

The following special names can be used instead of a DNS name:

- All — port is open at all local IP addresses (IP address 0.0.0.0)
- Loopback — local loopback IP address (127.0.0.1)

Remote Point

IP address (or DNS name) and port number (or a service name) of a particular remote point. The same information for the local IP address and port is provided (see above).

Protocol

Used protocol (TCP, UDP, or both).

Speed In, Speed Out

Current speed of incoming (In) and outgoing (Out) data of the particular connection in kilobytes per second (KB/s).

Bytes In, Bytes Out

Total extent of incoming (In) and outgoing (Out) data within the particular connection.



Note: *In case of a port which waits for an incoming connection, only the local IP address, local port and protocol are available.*

Summary of Open Ports and Established Connections

Current number of active connections and open ports is displayed at the bottom of the Connections tab (in the status line):

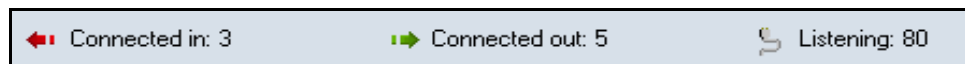


Figure 15-2 Overview / Connections — Summary of open ports and established connections

- Connected in — number of established incoming connections
- Connected out — number of established outgoing connections
- Listening — number of ports at which application wait for connection

Statistics

In the Overview / Statistics section you can view system statistics for intrusion detection and Web content filter.

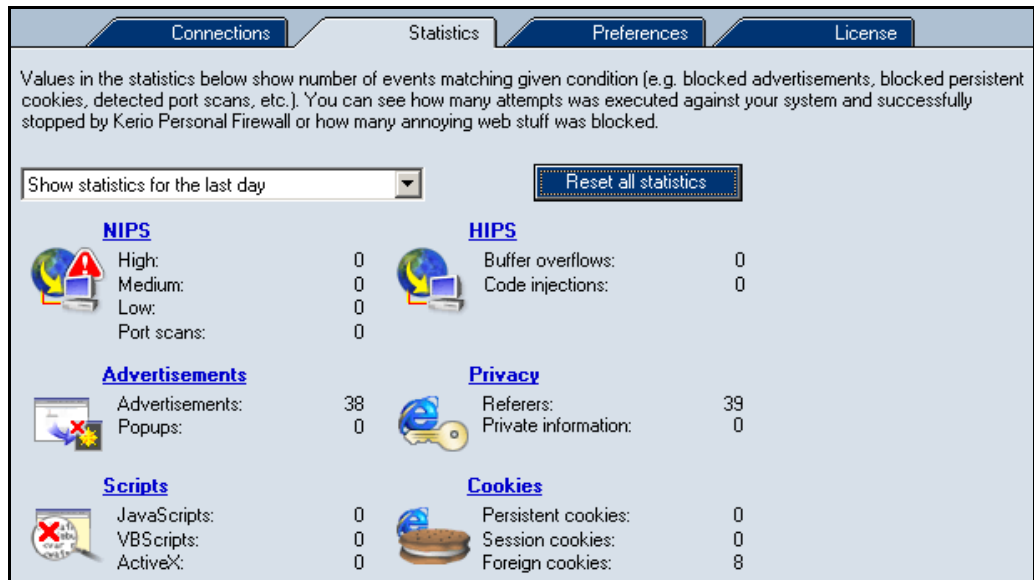


Figure 15-3 Overview / Statistics — Statistics on number of blocked intrusions and undesirable Web items

Use the Show statistics for the last ... entry to view statistics for a selected time range:

- hour — last hour
- day — last day
- week — last week
- month — last month

The Reset all statistics button can be used to reset all monitored statistics. This action must be confirmed by the user.

Statistics are divided into the following groups according to their types. Click on a group name to view corresponding statistics — WWW, HIPS, or NIPS.

NIPS

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

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

- 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 of the following types:

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



Logs

Logs are files where history of certain items is stored. Sunbelt Kerio Personal Firewall provides a log for each module (Network, System, Intrusions and Web).

The other logs (Error, Warning and Debug) store information on processes of Sunbelt Kerio Personal Firewall. This information can for example help the Sunbelt Software technical support to solve your possible problems with the firewall.

Log files are stored in the logs subdirectory of the directory where Sunbelt Kerio 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 (for scanning) is included in each log. This file has the .idx extension (i.e. network.log.idx).

Logs Viewing

Individual firewall module logs can be viewed and logging parameters can be set in the Logs & Alerts section.

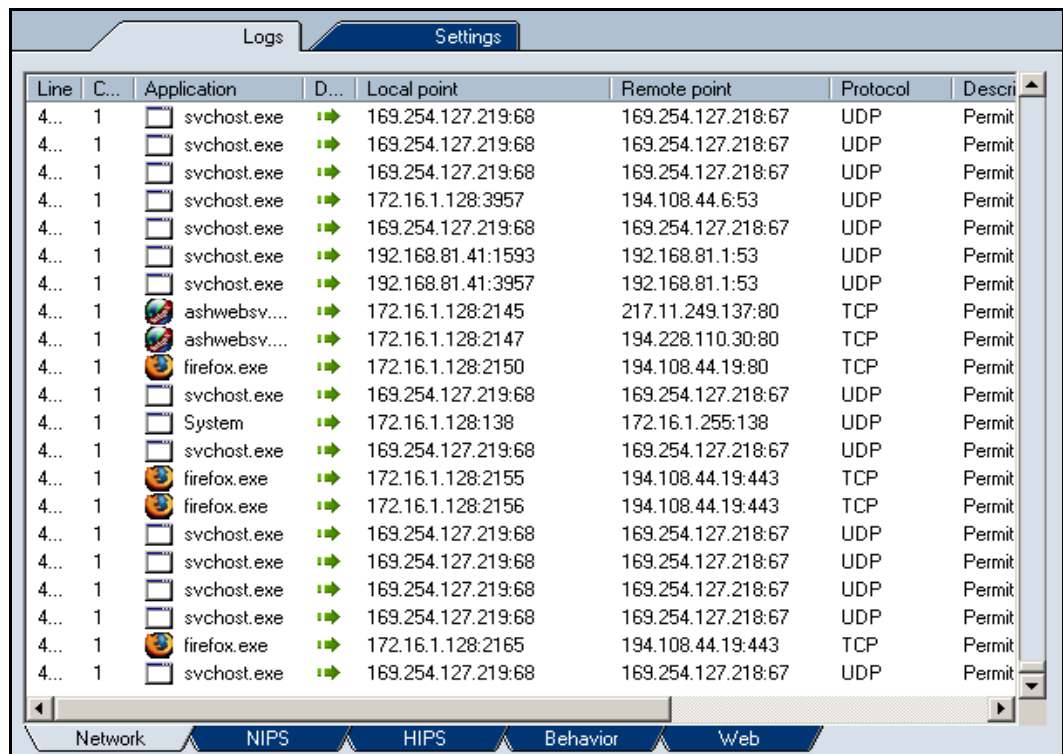


Figure 16-1 The Logs section — Log viewing

The Logs section includes tabs with logs for individual firewall modules. Each tab is focused on a certain part of a particular log file. Click on a column name to reorder the log items.

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

- Logs display slowly.
- In ordering by columns only currently viewed part of the log is displayed. Information must be ordered again after another part of the log is viewed.



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

Logs Context Menu

Right-click on the log tab to open a context menu providing options for a particular log:

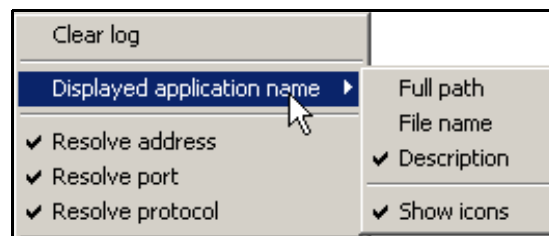


Figure 16-2 The Logs section — The Network log context menu

Clear log

Clears the log. All data will be removed from a corresponding file. Removed files cannot be refreshed.

Displayed application name

The way how application names will be displayed:

- Full path — full path to the application's executable file
- File name — name of the application's executable
- Description — description of the application (if it is not available, name of the executable without the extension is displayed)

Check/ uncheck the `Show icons` option to enable/disable showing icons (the system icon for executables will be used if the application has no icon).

Resolve address

Names of computers will be displayed instead of IP addresses.

Computer names are found through DNS. Unless a name is found, IP address will be displayed.

Resolve port

Names of services will be displayed instead of port numbers (this function is available only for standard services defined in the `services` system file).

Resolve protocol

Names of protocols will be displayed instead of protocol numbers (this function is available only for standard protocols defined in the protocols system file).



Note: Some logs do not provide all items mentioned above — i.e. no network communication is 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 setting influences all logs, the Overview / Connections section, Connection alert and Starting / Replacing application dialogs and the Alert window. View configuration is also described in corresponding chapters.

Log Options

The following parameters and log options (applied generally on all Sunbelt Kerio Personal Firewall logs) can be set in the Settings tab of the Logs & Alerts section:

The screenshot shows a configuration window with two tabs: 'Logs' and 'Settings'. The 'Settings' tab is active. It contains the following fields and options:

- Maximum logfile size: 2000 kB
- Log to syslog
- Syslog server: 192.168.1.10
- Syslog port: 514
- Advanced... button

Figure 16-3 Logs / Settings — Maximum logfile size

Maximum log file size

Maximal size of a log file (in kilobytes). If the size is exceeded, the file will be removed and a new log will be started.

Log to Syslog

Check/uncheck this option to enable/disable sending selected files to Syslog server.

Specify Syslog server through name and IP address of the corresponding Syslog server and define the Syslog port entry with number of the port on which the Syslog server is running (514 by default).

Click on the Advanced... button to open a dialog for selection of Sunbelt Kerio Personal Firewall logs which will be sent to the Syslog server.

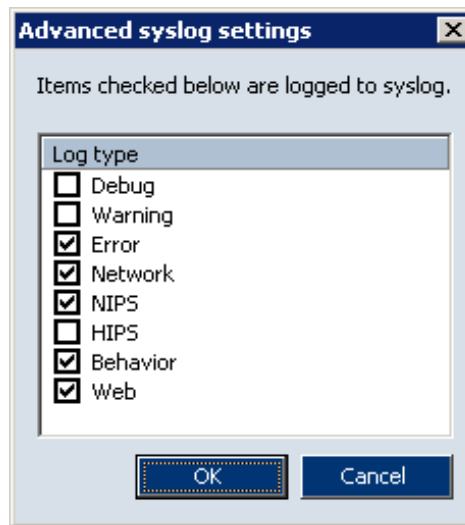


Figure 16-4 Advanced Syslog settings

Network Log

Information on network traffic which is meeting an application rule or a 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 16-5 The Logs section — The Network log

- Line — log line number
- Count — number of records (if one record is repeated in sequence, it is logged only once and the real count is expressed by a numeral)
- Date — date and time when the event was logged
- Description — description of a particular packet filter rule
- Application — name of a local application (according to the Displayed application name parameter) participating in the particular network communication.



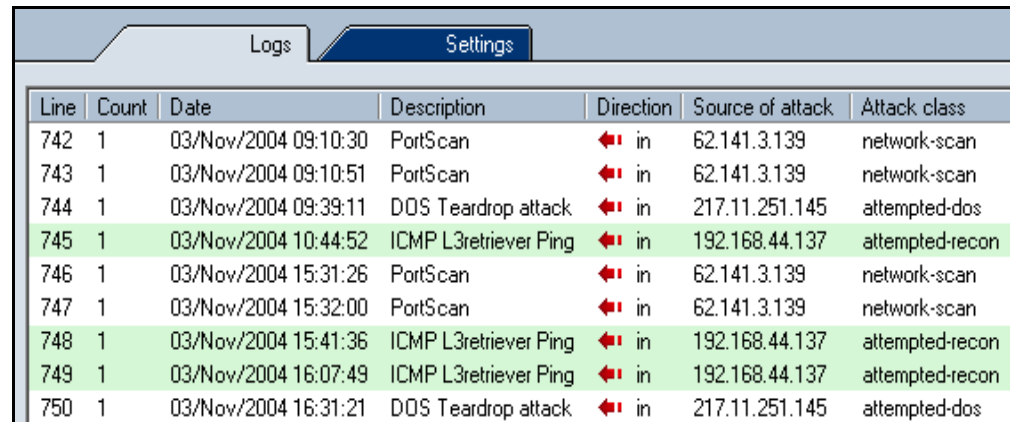
Note: Both description of applications and full paths to their executable files are saved into the log file. Therefore, you can switch between the two items and select which one will be displayed.

- Direction — direction of the connection (in — to a local computer, out — from a local computer)
- 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 has been permitted
 - denied — the traffic has been denied
 - asked → permitted — user was asked through the Connection alert dialog and the communication has been permitted
 - asked → denied — user was asked through the Connection alert dialog and the communication has been denied

NIPS Log

Information on detected network intrusions is logged into the NIPS log. Only network intrusions belonging to the types where the Log to NIPS log option is enabled are logged.

The NIPS log provides the following information:



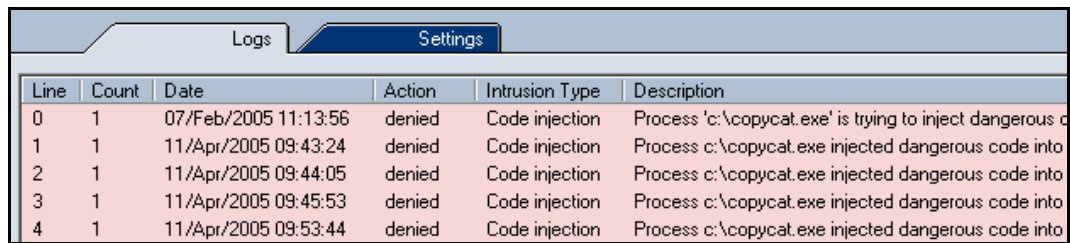
Line	Count	Date	Description	Direction	Source of attack	Attack class
742	1	03/Nov/2004 09:10:30	PortScan	in	62.141.3.139	network-scan
743	1	03/Nov/2004 09:10:51	PortScan	in	62.141.3.139	network-scan
744	1	03/Nov/2004 09:39:11	DOS Teardrop attack	in	217.11.251.145	attempted-dos
745	1	03/Nov/2004 10:44:52	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 16-6 The Logs section — The NIPS log

- Line — log line number
- Count — number of identical records
- Date — date and time when 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 Kerio Personal Firewall
- Action — action performed by Sunbelt Kerio Personal Firewall when the attack was detected (permitted — attack permitted, denied — attack denied)

HIPS Log

The HIPS log keeps information on detected attacks to applications. Attacks of those groups are logged where the Log attempts to HIPS log option is enabled. Detected yet unblocked attacks are marked white, blocked attacks are 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 code into
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 16-7 The Logs section — The HIPS log

- Line — log line number
- Count — number of identical logs
- Date — date and time where the event was logged
- Action — actions taken by Sunbelt Kerio Personal Firewall as a response to the attack (permitted or denied)
- Attack class — name of the attack detected

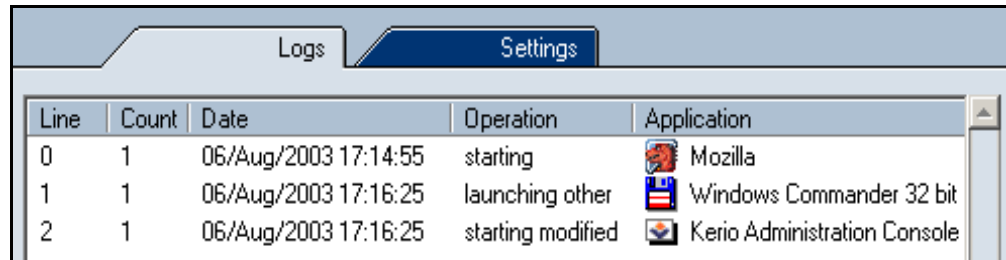
In the context menu, select an item (i.e. type of information) to be displayed:

- Description — attack description.
- Full path — the item provide information about the full path to both the source and the target application.
- File name — name of the target file.

Behavior Log

Information on running applications which meet corresponding rules in the Behavior Blocking / Applications section is stored in the Behavior log. The Log to Behavior log option must be enabled for a particular rule to enable the log.

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

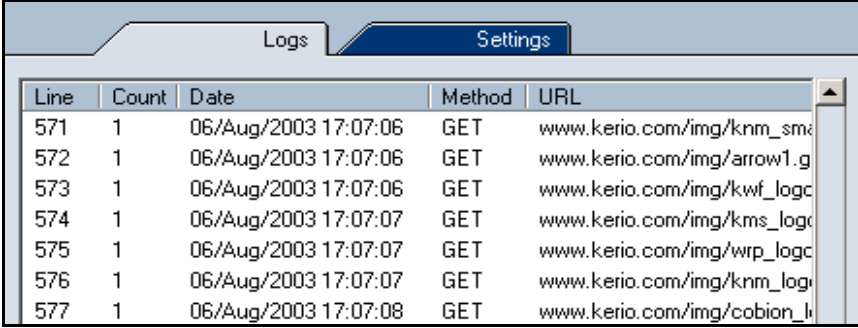
Figure 16-8 The Logs section — The Behavior log

- Line — log line number
- Count — number of identical records
- Date — date and time when 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 Æ permitted — user was asked through the Starting/Replacing application dialog and start of the application has been permitted
 - asked Æ denied — user was asked through the Starting/Replacing/Launching other application dialog and start of the application has been denied

Web Log

Information on objects blocked by the Web content filter is logged into the Web log. This log is not configurable — if the Web content filter is enabled, all filtered objects are logged.

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/ksm_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/ksm_logc
577	1	06/Aug/2003 17:07:08	GET	www.kerio.com/img/cobion_li

Figure 16-9 The Logs section — The Web log

- Line — log line number
- Count — number of identical records
- Date — date and time when the event was logged
- Method — used method of the HTTP protocol (GET or POST)
- URL — URL address of the object (of the page) to which the method is applied
- Subject — type of the blocked item of a Web page (referer, cookie, blockPopups — pop-up or pop-under windows)
- Value — value of this item (content of the Referer: item, information in cookie or rule which was used to block the ad)
- Action — action which was 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 a type of the blocked object (see the Subject item):

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

Debug, Error, Warning Logs

The Error, Warning and Debug logs are not available from the Sunbelt Kerio Personal Firewall's user interface — they can only be opened as files in the Logs subdirectory of the directory where Sunbelt Kerio 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 includes detailed information on all processes of Sunbelt Kerio Personal Firewall.

Error Log

Errors which seriously affect functionality of Sunbelt Kerio Personal Firewall (i.e. the Personal Firewall Engine cannot be started) are logged into the Error log.

Warning Log

Less important errors are logged into the Warning log (i.e. an error detected when a check for new version is performed, etc.).



Used 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.

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.

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 Kerio Personal Firewall.

ICMP

ICMP (Internet Control Message Protocol) is 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).

IP

IP (Internet Protocol) is 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).

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.

TCP

TCP (Transmission Control Protocol) is used for reliable data transmission through so called 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

UDP (User Datagram Protocol) is a so called connectionless protocol. 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.