Kerio Control

Administrator’s Guide

Kerio Technologies

This guide provides detailed description on configuration and administration of *Kerio Control*, version *7.2.1*. All additional modifications and updates reserved. User interfaces *Kerio StaR* and *Kerio Clientless SSL-VPN* are focused in a standalone document, *Kerio Control — User's Guide*. *Kerio VPN Client* for *Windows* and *Mac OS X* is focused in the separate document *Kerio VPN Client — User's Guide*.

For current version of the product, go to http://www.kerio.com/control/download. For other documents addressing the product, see http://www.kerio.com/control/manual.

Information regarding registered trademarks and trademarks are provided in appendix A.

Products *Kerio Control* and *Kerio VPN Client* include open source software. To view the list of open source items included, refer to attachment B.

Contents

Chapter 1

Quick Checklist

In this chapter you can find a brief guide for a quick setup of *Kerio Control*. After this setup the firewall should be immediately available and able to share your Internet connection and protect your local network. For a detailed guide refer to the separate *Kerio Control — Step-by-Step Configuration* guide.

If you are unsure about any element of *Kerio Control*, simply look up an appropriate chapter in the manual. For information about your Internet connection (such as your IP address, default gateway, DNS server, etc.) contact your ISP.

Note: In this guide, the expression *firewall* represents the host where *Kerio Control* is (or will be) installed.

1. The firewall needs at least one interface connected to the local network (e.g. an *Ethernet* or *Wi-Fi* network adapter). For Internet connection, another network adapter, USB ADSL modem, PPPoE, dial up or another facility is needed.

   On *Windows*, test functionality of the Internet connection and of traffic among hosts within the local network before you run the *Kerio Control* installation. This test will reduce possible problems with debugging and error detections.

2. Run *Kerio Control* installation and in the wizard provide required basic parameters (for details, see chapter 2.4 or 2.6).

3. In your browser, open the *Kerio Control Administration* interface. This interface is available on the server at `http://localhost:4080/` (for details, see chapter 4).

4. Use the *Activation Wizard* (see chapter 5.3) to activate the product either with a valid license or as a 30-day trial version.

5. Use *Connectivity wizard* (see chapter 7.1) to set Internet connection and connection to the local network.

6. Use *Traffic Policy Wizard* (see chapter 8.1) to create basic traffic rules (rules for local traffic, Internet access and service mapping).

7. Check *DNS* module settings. Define the local DNS domain if you intend to use the hostname table and/or the DHCP server table. For details, see chapter 10.1.

8. Set user mapping from *Active Directory* or *Open Directory* domain, or create/import local user accounts and groups. Set user access rights. For details see chapter 17.

9. Enable the intrusion prevention system (see chapter 9.1).

10. Select an antivirus and define types of objects that will be scanned.

    If you choose the integrated *Sophos* antivirus application, check automatic update settings and edit them if necessary.

    External antivirus must be installed before it is set in *Kerio Control*, otherwise it is not available in the combo box.

11. Define IP groups (chapter 16.1), time ranges (chapter 16.2) and URL groups (chapter 16.4), that will be used during rules definition (refer to chapter 16.2).

12. To optimize usage of Internet connection, define bandwidth management rules (see chapter 11).

13. Create URL rules (chapter 14.2). Set *Kerio Web Filter* (chapter 14.3) and automatic configuration of web browsers (chapter 10.4).

14. Define FTP rules (chapter 14.5).

15. Using one of the following methods set TCP/IP parameters for the network adapter of individual LAN clients:

    - *Automatic configuration* — enable automatic DHCP configuration (set by default on most operating systems). Do not set any other parameters.

    - *Manual configuration* — define IP address, subnet mask, default gateway address, DNS server address and local domain name.

    Use one of the following methods to set the Web browser at each workstation:

    - *Automatic configuration* — activate the *Automatically detect settings* option (*Internet Explorer*) or specify URL for automatic configuration (other types of browsers). For details, refer to chapter 10.4.

    - *Manual configuration* — select type of connection via the local network or define IP address and appropriate proxy server port (see chapter 10.5).

Chapter 2

Installation

2.1 Product Edition

Kerio Control is available in these editions:

Windows Edition

Software application used for installation on *Microsoft Windows*.

It can be run on one server with other applications and services (such as the communication server *Kerio Connect*).

Software Appliance

Kerio Control Software Appliance (so called software appliance) is an all-in-one package of *Kerio Control* which also includes a special operating system.

Designed to be installed on a computer without an operating system, this edition is distributed as an installation disc. *Software Appliance* cannot be installed on a computer with another operating system and it does not allow to install other applications.

VMware Virtual Appliance

A virtual appliance designed for usage in *VMware* products.

VMware Virtual Appliance is a *Software Appliance* edition pre-installed on a virtual host for *VMware*. The virtual appliance is distributed as *OVF* and *VMX*.

Virtual Appliance for Parallels

A virtual appliance designed for usage in *Parallels* products.

Virtual Appliance for Parallels is a *Software Appliance* edition pre-installed on a virtual host for *Parallels*.

Kerio Control Box

Hardware device ready for network connection. It is available in two types different in performance and number of network ports.

Editions *Software Appliance*, *VMware Virtual Appliance* and *Virtual Appliance for Parallels* are referred to as *Appliance*, *Kerio Control Box* is referred to as *Box* in the document.

2.2 System requirements

For up-to-date system requirements of the software editions and for technical specifications of the *Kerio Control Box* hardware appliance, please refer to:

http://www.kerio.com/control/technical-specifications

2.3 Windows: Conflicting Software

Kerio Control can be run with most of common applications. However, there are certain applications that should not be run at the same host as *WinRoute* for this could result in collisions.

The computer where *Kerio Control* is installed (the host) can be also used as a workstation. However, it is not recommended — user interaction may affect performance of the operating system which affects *Kerio Control* performance badly.

Collision of low-level drivers

Kerio Control collides with system services and applications the low-level drivers of whose use a similar or an identical technology. The security log contains the following types of services and applications:

- The *Internet Connection Firewall / Internet Connection Sharing* system service. *Kerio Control* can detect and automatically disable this service.
- The system service *Routing and Remote Access Service (RRAS)* in *Windows Server* operating systems. This service allows also sharing of Internet connection (NAT). *Kerio Control* can detect if NAT is active in the *RRAS* service; if it is, a warning is displayed. In reaction to the alert message, the server administrator should disable NAT in the *RRAS* configuration.
  If NAT is not active, collisions should be avoided and *Kerio Control* can be used hand in hand with the *RRAS* service.
- Network firewalls — e.g. *Microsoft ISA Server*.
- Personal firewalls, such as *Sunbelt Personal Firewall*, *Zone Alarm*, *Norton Personal Firewall*, etc.
- Software designed to create virtual private networks (VPN) — i.e. software applications developed by the following companies: *CheckPoint*, *Cisco Systems*, *Nortel*, etc. There are many applications of this type and their features vary from vendor to vendor.
  Under proper circumstances, use of the VPN solution included in *Kerio Control* is recommended (for details see chapter 24). Otherwise, we recommend you to test a particular VPN server or VPN client with *Kerio Control* trial version or to contact our technical support (see chapter 27).
  Note: VPN implementation included in *Windows* operating system (based on the PPTP protocol) is supported by *Kerio Control*.

Port collision

Applications that use the same ports as the firewall cannot be run at the *Kerio Control* host (or the configuration of the ports must be modified).
If all services are running, *Kerio Control* uses the following ports:

- `53/UDP` — *DNS* module,
- `67/UDP` — *DHCP server*,
- `1900/UDP` — the *SSDP Discovery* service,
- `2869/TCP` — the *UPnP Host* service.

The *SSDP Discovery* and *UPnP Host* services are included in the UPnP support (refer to chapter 19.2).

- 4080/TCP — unsecured web interface of the firewall (refer to chapter 13). This service cannot be disabled.
- 4081/TCP — secured (SSL-encrypted) version of the firewall's web interface (see chapter 13). This service cannot be disabled.

The following services use corresponding ports by default. Ports for these services can be changed.

- 443/TCP — server of the *SSL-VPN* interface (only in *Kerio Control* on *Windows* — see chapter 25),
- 3128/TCP — HTTP proxy server (see chapter 10.5),
- 4090/TCP+UDP — proprietary VPN server (for details refer to chapter 24).

Antivirus applications

Most of the modern desktop antivirus programs (antivirus applications designed to protect desktop workstations) scans also network traffic — typically *HTTP*, *FTP* and email protocols. *Kerio Control* also provides with this feature which may cause collisions. Therefore it is recommended to install a server version of your antivirus program on the *Kerio Control* host. The server version of the antivirus can also be used to scan *Kerio Control's* network traffic or as an additional check to the integrated antivirus *Sophos* (for details, see chapter 15).

If the antivirus program includes so called realtime file protection (automatic scan of all read and written files), it is necessary to exclude directories `cache` (HTTP cache in *Kerio Control* see chapter 10.4) and `tmp` (used for antivirus check). If *Kerio Control* uses an antivirus to check objects downloaded via HTTP or FTP protocols (see chapter 15.3), the cache directory can be excluded with no risk — files in this directory have already been checked by the antivirus.

The *Sophos* integrated antivirus plug-in does not interact with antivirus application installed on the *Kerio Control* host (provided that all the conditions described above are met).

2.4 Windows: Installation

Installation packages

Kerio Control is distributed in two editions: one is for 32-bit systems and the other for 64-bit systems (see the product's download page: http://www.kerio.com/control/download).

Steps to be taken before the installation

Install *Kerio Control* on a computer which is used as a gateway connecting the local network and the Internet. This computer must include at least one interface connected to the local network (Ethernet, Wi-Fi, etc.) and at least one interface connected to the Internet. You can use either a network adapter (Ethernet, Wi-Fi, etc.) or a modem (analog, ISDN, etc.) as an Internet interface.

We recommend you to check through the following items before you run *Kerio Control* installation:

- Time of the operating system should be set correctly (for timely operating system and antivirus upgrades, etc.),
- The latest service packs and any security updates should be applied,
- TCP/IP parameters should be set for all available network adapters,
- All network connections (both to the local network and to the Internet) should function properly. You can use for example the `ping` command to detect time that is needed for connections.

These checks and pre-installation tests may protect you from later problems and complications.

Note: Basic installation of all supported operating systems include all components required for smooth functionality of *Kerio Control*.

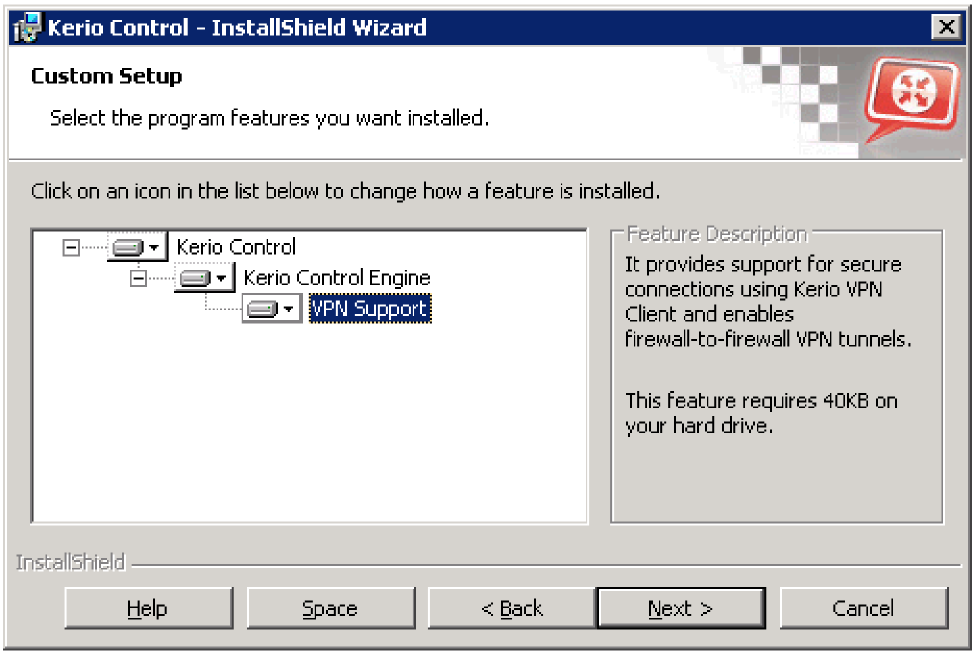
Installation and Basic Configuration Guide

Once the installation program is launched (i.e. by `kerio-control-7.1.0-2000-win32.exe`), it is possible to select a language for the installation wizard. Language selection affects only the installation, language of the user interface can then be set separately for individual *Kerio Control* components.

In the installation wizard, you can choose either *Full* or *Custom* installation. Custom mode will let you select optional components of the program:

- *Kerio Control Engine* — core of the application.
- *VPN Support* — proprietary VPN solution developed by *Kerio Technologies* (*Kerio VPN*).

Go to chapter 3 for a detailed description of all *Kerio Control* components. For detailed description on the proprietary VPN solution, refer to chapter 24.



Kerio Control - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Kerio Control
  - Kerio Control Engine
    - VPN Support

Feature Description

It provides support for secure connections using Kerio VPN Client and enables firewall-to-firewall VPN tunnels.

This feature requires 40KB on your hard drive.

Figure 2.1 Installation — customization by selecting optional components

Note: If you selected the *Custom* installation mode, the behavior of the installation program will be as follows:

- all checked components will be installed or updated,
- all checked components will not be installed or will be removed

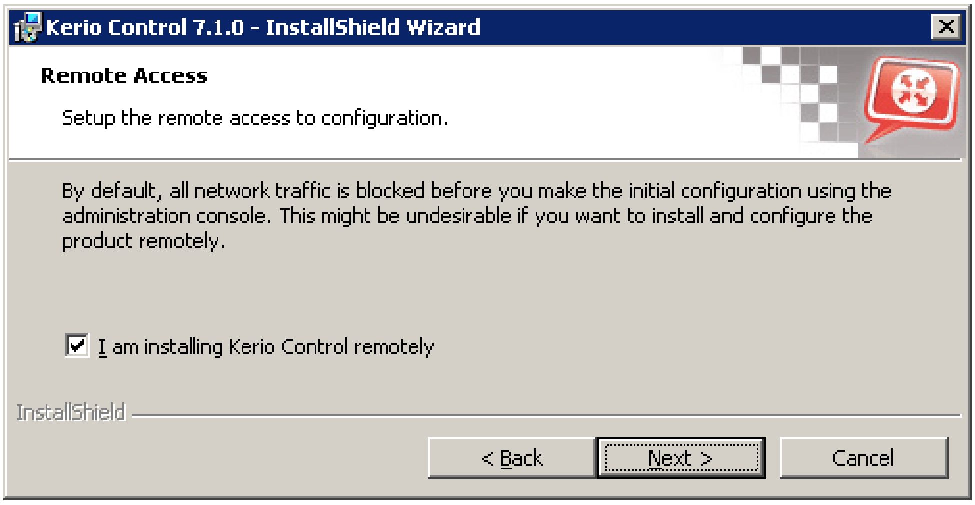
During an update, all components that are intended to remain must be ticked.

Remote Access

Immediately after the first *Kerio Control Engine* startup all network traffic will be blocked (desirable traffic must be permitted by traffic rules — see chapter 8). If *Kerio Control* is installed remotely (i.e. using terminal access), communication with the remote client will be also interrupted immediately (*Kerio Control* must be configured locally).

If it is desirable to enable remote installation and administration, communication between *Kerio Control* and the remote computer must be allowed in the installation wizard.

Note: Skip this step if you install *Kerio Control* locally. Allowing full access from a point might endanger security.



Kerio Control 7.1.0 - InstallShield Wizard

Remote Access

Setup the remote access to configuration.

By default, all network traffic is blocked before you make the initial configuration using the administration console. This might be undesirable if you want to install and configure the product remotely.

☑ I am installing Kerio Control remotely

Figure 2.2 Initial configuration — Allowing remote administration

Warning:
The remote access rule is disabled automatically when *Kerio Control* is configured using the network policy wizard (see chapter 8.1).

Conflicting Applications and System Services

The *Kerio Control* installation program detects applications and system services that might conflict with the *Kerio Control Engine*.

1. *Windows Firewall's* system components[1] and *Internet Connection Sharing*.

   These components provide the same low-level functions as *Kerio Control*. If they are running concurrently with *Kerio Control*, the network communication would not be functioning correctly and *Kerio Control* might be unstable. Both components are run by the *Windows Firewall / Internet Connection Sharing* system service.[2].

   Warning:
   To provide proper functionality of *Kerio Control*, it is *necessary* that the *Internet Connection Firewall / Internet Connection Sharing detection* is stopped and forbidden!

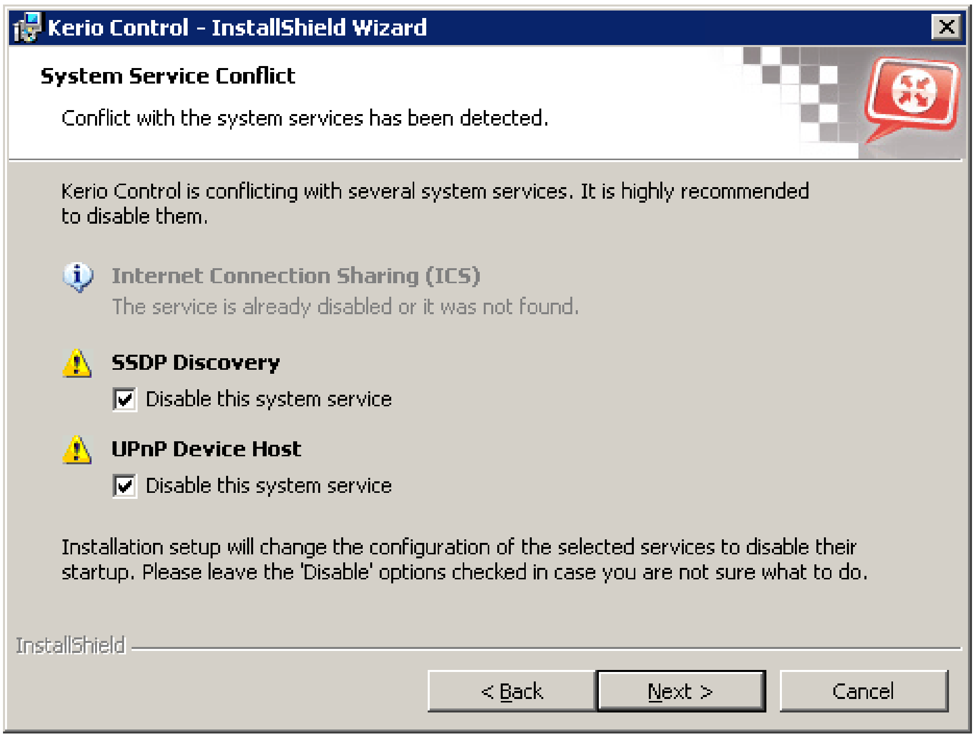
2. *Universal Plug and Play Device Host* and *SSDP Discovery Service*

   The listed services support *UPnP* protocol (Universal Plug and Play) on *Windows*. However, these services collide with the *UPnP* support in *Kerio Control* (refer to chapter 19.2).

[1] In *Windows XP Service Pack 1* and older versions, the integrated firewall is called *Internet Connection Firewall*.

[2] In the older *Windows* versions listed above, the service is called *Internet Connection Firewall / Internet Connection Sharing*.

The *Kerio Control* installation includes a dialog where it is possible to disable colliding system services.



Kerio Control - InstallShield Wizard

System Service Conflict

Conflict with the system services has been detected.

Kerio Control is conflicting with several system services. It is highly recommended to disable them.

Internet Connection Sharing (ICS)
The service is already disabled or it was not found.

SSDP Discovery
☑ Disable this system service

UPnP Device Host
☑ Disable this system service

Installation setup will change the configuration of the selected services to disable their startup. Please leave the 'Disable' options checked in case you are not sure what to do.

Figure 2.3 Disabling colliding system services during installation

By default, the *Kerio Control* installation disables all the colliding services listed. Under usual circumstances, it is not necessary to change these settings. Generally, the following rules are applied:

- The *Windows Firewall / Internet Connection Sharing (ICS)* service should be disabled. Otherwise, *Kerio Control* will not work correctly. The option is a certain kind of warning which informs users that the service is running and that it should be disabled.
- To enable support for the *UPnP* protocol in *Kerio Control* (see chapter 19.2), it is necessary to disable also services *UPnP Device Host* and *SSDP Discovery Service*.
- It is not necessary to disable the services unless you need to use the *UPnP* in *Kerio Control*.

Note:

1. Upon each startup, *Kerio Control* detects automatically whether the *Windows Firewall / Internet Connection Sharing* is running. If it is, *Kerio Control* stops it and makes a record in the *Warning* log. This helps assure that the service will be enabled/started immediately after the *Kerio Control* installation.
2. On *Windows XP Service Pack 2*, *Windows Server 2003*, *Windows Vista*, *Windows Server 2008* and *Windows 7*, *Kerio Control* registers in the *Security Center* automatically. This implies

that the *Security Center* always indicates firewall status correctly and it does not display warnings informing that the system is not protected.

Protection of the installed product

To provide the firewall with the highest security possible, it is necessary to ensure that undesirable (unauthorized) persons has no access to the critical files of the application, especially to configuration files. If the *NTFS* system is used, *Kerio Control* refreshes settings related to access rights to the directory (including all subdirectories) where the firewall is installed upon each startup. Only members of the *Administrators* group and local system account (*SYSTEM*) are assigned the full access (read/write rights), other users are not allowed access the directory.

Warning:
If the *FAT32* file system is used, it is not possible to protect *Kerio Control* in the above way. Thus, we strongly recommend to install *Kerio Control* only on *NTFS* disks.

Running the product activation wizard

Before the installation is completed, the *Kerio Control Engine* (i.e. the kernel of the program running as a system service) and *Kerio Control Engine Monitor* start.

When the installation wizard is completed, the *Kerio Control Administration* interface opens automatically in the default web browser. In this interface, the product activation wizard starts first (see chapter 5.3).

2.5 Windows: Upgrade and Uninstallation

Upgrade

Simply run the installation of a new version to upgrade *Kerio Control* (i.e. to get a new release from the *Kerio* Web pages — http://www.kerio.com/).

The installation program automatically closes the *Kerio Control Engine* and *Kerio Control Engine Monitor*.

The installation program detects the directory with the former version and updates it by replacing appropriate files with the new ones automatically. License, all logs and user defined settings are kept safely.

Note: This procedure applies to upgrades between versions of the same series (e.g. from *7.1.0* to *7.1.1*) or from a version of the previous series to a version of the subsequent series (e.g. from *Kerio Control 7.0.1* to *Kerio Control 7.1.0*). For case of upgrades from an older series version (e.g. *Kerio WinRoute Firewall 6.7.1*), full compatibility of the configuration cannot be guaranteed and it is recommended to upgrade “step by step” (e.g. *6.7.1 → 7.0.0 → 7.1.0*) or to uninstall the old version along with all files and then install the new version “from scratch”.

Warning:
Since *6.x*, some configuration parameters have been changed in version for *7.0.0*. Although updates are still performed automatically and seamlessly, it is necessary to mind the changes described above that take effect immediately upon installation of the new version. The following parameters are affected:

- *HTTP cache directory* — newly, the firewall installation directory’s `cache` subfolder is always used, typically
  `C:\Program Files\Kerio\WinRoute Firewall\cache`.
  In case that the HTTP cache is located in a different directory, it can be moved (provided that the *Kerio Control Engine* service is not running). However, such measure can be rather disserviceable as the product update actually empties the cache which may often increase its effectivity.
  For details on HTTP cache, see chapter 10.4.

- *Supportive scripts for dial-up control* — these scripts must always be saved in the firewall installation directory’s `scripts` subfolder, typically
  `C:\Program Files\Kerio\WinRoute Firewall\scripts`
  and they all need fixed names.
  If these scripts were used int he previous version of the product, it is necessary to move them to the directory with correct names used.
  For details on dial-up configuration, see chapter 7.5.

- *Log file names* — fixed log file names are set now (`alert.log`, `config.log`, `debug.log`, etc.).
  The same path used for saving log files is kept — logs are save under the `logs` subdirectory under the firewall installation directory, typically
  `C:\Program Files\Kerio\WinRoute Firewall\logs`
  If log file names has been changed, the original files are kept and new logs are recorded in files with corresponding names.

- *Log type (Facility) and its Severity for external logging on the Syslog server* — fixed facility and severity values of individual logs of *Kerio Control* are now set. This is a fact to bear in mind while viewing firewall logs on the *Syslog* server.
  For details on log settings, see chapter 23.2.

After update, it is recommended to check *Warning* log carefully (see chapter 23.13).

Update Checker

Kerio Control enables automatic checks for new versions of the product at the *Kerio Technologies* website. Whenever a new version is detected, its download and installation will be offered automatically.

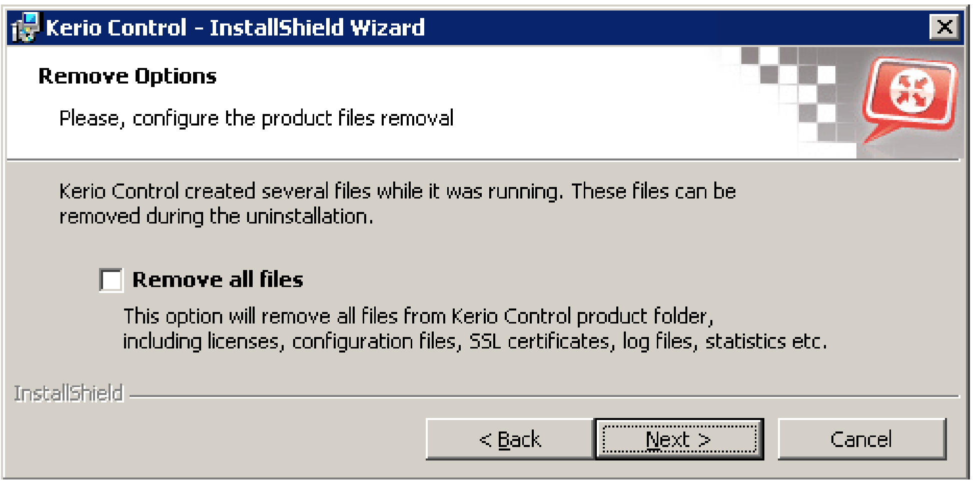
For details, refer to chapter 18.2.

Uninstallation

Before uninstalling the product, it is recommended to close all *Kerio Control* components. The *Add/Remove Programs* option in the *Control Panel* launches the uninstallation process. All files under the *Kerio Control* directory can be optionally deleted.

(the typical path is `C:\Program Files\Kerio\WinRoute Firewall`)

— configuration files, SSL certificates, license key, logs, etc.



Kerio Control - InstallShield Wizard

Remove Options

Please, configure the product files removal

Kerio Control created several files while it was running. These files can be removed during the uninstallation.

□ **Remove all files**

This option will remove all files from Kerio Control product folder, including licenses, configuration files, SSL certificates, log files, statistics etc.

Figure 2.4 Uninstallation — asking user whether files created in Kerio Control should be deleted

Keeping these files may be helpful for copying of the configuration to another host or if it is not sure whether the SSL certificates were issued by a trustworthy certification authority.

During uninstallation, the *Kerio Control* installation program automatically refreshes the original status of the *Windows Firewall / Internet Connection Sharing*, *Universal Plug and Play Device Host*) and *SSDP Discovery Service* system services.

2.6 Appliance Edition: Installation

Kerio Control in the software appliance edition is distributed:

- as an ISO of the installation CD which is used to install the system and then install the firewall either on a physical or virtual computer (*Software Appliance*),
- as a virtual appliance for *VMware* (*VMware Virtual Appliance*).

Standalone *Kerio Control* installation package for installation on previously installed *Linux* is not available.

Software Appliance / VMware Virtual Appliance installation process consists of the following simple steps:

Start of the installation

Software Appliance

ISO image of the installation CD can be burned on a physical CD and then the CD can be used for installation of the system on the target computer (either physical or virtual). In case of virtual computers, the ISO image can be also connected as a virtual CD ROM, without the need to burn the installation ISO file on a CD.
Note: Kerio Control Software Appliance cannot be installed on a computer with another operating system. Existing operating system on the target disk will be removed within the installation.

VMware Virtual Appliance

Supported *VMware* versions:

- *Workstation 6.5 and 7.0*
- *Server 2.0*
- *Fusion 2.0 and 3.0*
- *Player 2.5 and 3.0*
- *ESX 3.5 and 4.0*
- *ESXi 3.5 and 4.0*

Use an installation package in accordance with the type of your *VMware* product (see above):

- In case of products *VMware Server, Workstation* and *Fusion*, download the compressed *VMX* distribution file (`*.zip`), unpack it and open it in the your *VMware* product.
- You can import a virtual appliance directly to *VMware ESX/ESXi* from the URL of the *OVF* file — for example:

  ```
  http://download.kerio.com/dwn/control/
  kerio-control-appliance-7.1.0-2000-linux.ovf
  ```

  VMware ESX/ESXi automatically downloads the *OVF* configuration file and a corresponding disk image (`.vmdk`).

If you import virtual appliance in the *OVF* format, bear in mind the following specifics:

- In the imported virtual appliance, time synchronization between the host and the virtual appliance is disabled. However, *Kerio Control* features a proprietary mechanism for synchronization of time with public Internet time servers. Therefore, it is not necessary to enable synchronization with the host.
- Tasks for shutdown or restart of the virtual machine will be set to default values after the import. These values can be set to “hard” shutdown or “hard” reset.

However, this may cause loss of data on the virtual appliance. *Kerio Control VMware Virtual Appliance* supports so called *Soft Power Operations* which allow to shutdown or restart hosted operating system properly. Therefore, it is recommended to set shutdown or restart of the hosted operating system as the value.

The following steps are identical both for *Software Appliance* and *Virtual Appliance*.

Language selection

The selected language will be used both for *Kerio Control* installation and for the firewall's console (see chapter 3.2).

Selection of target hard disk

If the installation program detects more hard disks in the computer, then it is necessary to select a disk for *Kerio Control* installation. Content of the selected disk will be completely removed before *Kerio Control* installation, while other disk are not affected by the installation.

If there is an only hard disk detected on the computer, the installer continues with the following step automatically. If no hard disk is found, the installation is closed. Such error is often caused by an unsupported hard disk type or hardware defect.

Selection of network interface for the local network and access to administration

The installer lists all detected network interfaces of the firewall. Select an interface which is connected to the local (trustworthy) network which the firewall will be remotely administered from.

In the field, a computer may have multiple interfaces of the same type and it is therefore not easy to recognize which interface is connected to the local network and which to the Internet. To a certain extent, hardware addresses of the adapters can be a clue or you can experiment — select an interface, complete the installation and try to connect to the administration. If the connection fails, use option *Network Configuration* in the main menu of the firewall's console to change the settings (see chapter 3.2).

There can also arise another issue — that the program does not detect some or any network adapters. In such case, it is recommended to use another type of the physical or virtual (if the virtual computer allows this) adapter or install *Kerio Control Software Appliance* on another type of virtual machine. If such issue arises, it is highly recommended to consult the problem with the *Kerio Technologies* technical support (see chapter 27).

Provided that no network adapter can be detected, it is not possible to continue installing *Kerio Control*.

Setting of the local interface's IP address

It is now necessary to define IP address and subnet mask for the selected local network interface. These parameters can be defined automatically by using information from a DHCP server or manually.

For the following reasons, it is recommended to set local interface parameters manually:

- Automatically assigned IP address can change which may cause problems with connection to the firewall administration (although the IP address can be reserved on the DHCP server, this may bring other problems).
- In most cases *Kerio Control* will be probably used itself as a DHCP server for local hosts (workstations).

Completing the installation

Once all these parameters are set, the *Kerio Control Engine* service (daemon) is started. While the firewall is running, the firewall's console will display information about remote administration options and change of some basic configuration parameters — see chapter 3.2.

2.7 Appliance Edition: Upgrade

Kerio Control can be upgraded by the following two methods:

- by starting the system from the installation CD (or a mounted ISO) of the new version. The installation process is identical with the process of a new installation with an the only exception that at the start the installer asks you whether to execute an upgrade (any existing data will be kept) or a new installation (all configuration files, statistics, logs, etc will be removed). For details, see chapter 2.6.
- by update checker in the *Kerio Control Administration* interface. For details, refer to chapter 18.2

Warning:
Compared to older versions of the product (*Kerio WinRoute Firewall 6.x*), some configuration parameters have been changed in version *7.0.0*. Although updates are still performed automatically and seamlessly, it is necessary to mind the changes described above that take effect immediately upon installation of the new version.
The following parameters are affected:

- *Log file names* — fixed log file names are set now (`alert.log`, `config.log`, `debug.log`, etc.).
  The path for saving the log files is kept unchanged — logs are saved under
  `/opt/kerio/winroute/logs`
  If log file names has been changed, the original files are kept and new logs are recorded in files with corresponding names.

- *Log type (Facility) and its Severity for external logging on the Syslog server* — fixed facility and severity values of individual logs of *Kerio Control* are now set. This is a fact to bear in mind while viewing firewall logs on the *Syslog* server.
  For details on log settings, see chapter 23.2.

After update, it is recommended to check *Warning* log carefully (see chapter 23.13).

Chapter 3

Kerio Control components

Kerio Control consists of these components:

Kerio Control Engine

The core of the program that executes all product's services and functions.
On *Windows*, it runs as a service in the operating system (the service is called *Kerio Control* and it is run automatically within the system account by default).

Kerio Control Engine Monitor (Windows only)

Allows viewing and modification of the *Engine's* status (stopped / running) and setting of start-up preferences (i.e. whether *Engine* and *Monitor* should be run automatically at system start-up). It also provides easy access to the *Administration Console*. For details, refer to chapter 3.1.
Note: Kerio Control Engine is independent from the *Kerio Control Engine Monitor*. The *Engine* can be running even if there is no icon in the system tray.

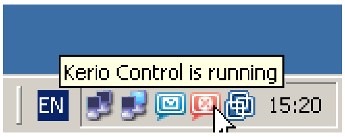
Firewall console (only in editions Appliance and Box)

The firewall's console is a simple interface permanently running on the *Kerio Control* host. It allows basic configuration of the operating system and the firewall as well as administration access recovery in case that the administration has been blocked.

Note: Since version *7.1.0*, the standalone administration application (*Kerio Administration Console*) has no longer been available.

3.1 Kerio Control Engine Monitor (Windows)

Kerio Control Engine Monitor is a standalone utility used to control and monitor the *Kerio Control Engine* status. The icon of this component is displayed on the toolbar.


Kerio Control is running

EN 15:20

Figure 3.1 Kerio Control Engine Monitor icon in the Notification Area

If *Kerio Control Engine* is stopped, a white crossed red spot appears on the icon. Starting or stopping the service can take several seconds. For this time the icon gets grey and is inactive.

By double-clicking on this icon it is possible to run the *Kerio Control Administration* that will open in the default web browser (see below). Use the right mouse button to open the following menu:

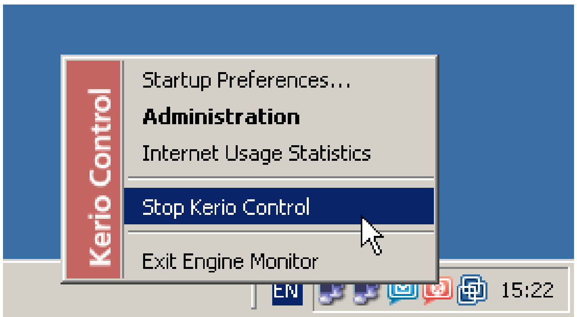


Figure 3.2 Kerio Control Engine Monitor menu

Start-up Preferences

With these options *Kerio Control Engine* and/or *Engine Monitor* applications can be set to be launched automatically when the operating system is started. Both options are enabled by default.

Administration

An option to open the *Kerio Control Administration* interface in the default web browser (calls the identical action as double-clicking on the *Engine Monitor* icon).

Internet Usage Statistics

Opens *Internet Usage Statistics* (*Kerio StaR*) in the default browser. For details, see chapter 22.

Start/Stop Kerio Control

Switches between the Start and Stop modes. The text displays the current mode status.

Exit Engine Monitor

An option to exit *Engine Monitor*. This option does not stop the *Kerio Control Engine*. The user is informed about this fact by a warning window.

Note:

1. If a limited version of *Kerio Control* is used (e.g. trial version), a notification is displayed 7 days before its expiration. This information is displayed until the expiration.
2. *Kerio Control Engine Monitor* is available in English only.

3.2 Firewall console (editions Appliance and Box)

The firewall console is a special application running on the *Kerio Control* (*Appliance* edition) host's terminal. In case of *Kerio Control Box*, it is possible to connect to the console via a serial port.

By default, the console shows only information about URL or IP address which can be used for firewall administration via the a web browser (the *Kerio Control Administration* interface). Upon authenticating by the *Admin* user's password (the main firewall administrator), this console allows to change some basic settings of the firewall, restore default settings after installation and shut down or restart the computer. If idle for some time, the user gets logged out automatically and the welcome page of the console showing details on the firewall's remote administration is displayed again.

The firewall's console provides the following configuration options:

Network interface configurations

This option allows to show or/and edit parameters of individual network interfaces of the firewall. Each interface allows definition of automatic configuration via *DHCP* or manual configuration of IP address, subnet mask and default gateway.

Note: No default gateway should be set on interfaces connected to the local network, otherwise this firewall cannot be used as agateway for the Internet access.

Remote administration policy settings

When you change the firewall's traffic policy (see chapter 8) via the *Kerio Control Administration* web interface, you may happen to block access to the remote administration accidentally.

If you are sure that the firewall's network interfaces are configured correctly and despite of that it is not possible to access the remote administration, you can use the *Remote Administration* option to change the traffic rules so that the rules do not block remote administration on any network interface.

Upon saving changes in traffic rules, the *Kerio Control Engine* service will be restarted automatically.

"Unblocking" of remote administration means that a rule is added at the top of the traffic rules table that allows access to the *Kerio Control WebAdmin* service from any computer (secured firewall web interface).

Shutting down / restarting the firewall

If you need to shut your computer down or reboot it, these options provide secure closure of the *Kerio Control Engine* and shutdown of the firewall's operating system.

Restoring default configuration

This option restores the default firewall settings as installed from the installation CD or upon the first startup of the *VMware* virtual host. All configuration files and data (logs, statistics, etc.) will be removed and it will then be necessary to execute the initial configuration of the firewall again as if a new installation (see chapter 2.6).

Restoring the default configuration can be helpful if the firewall's configuration is accidentally damaged that much that it cannot be corrected by any other means.

Chapter 4

Kerio Control administration

Kerio Control provides the *Kerio Control Administration* interface (so called *administration interface*) that allows remote and local administration of the firewall in a common web interface.

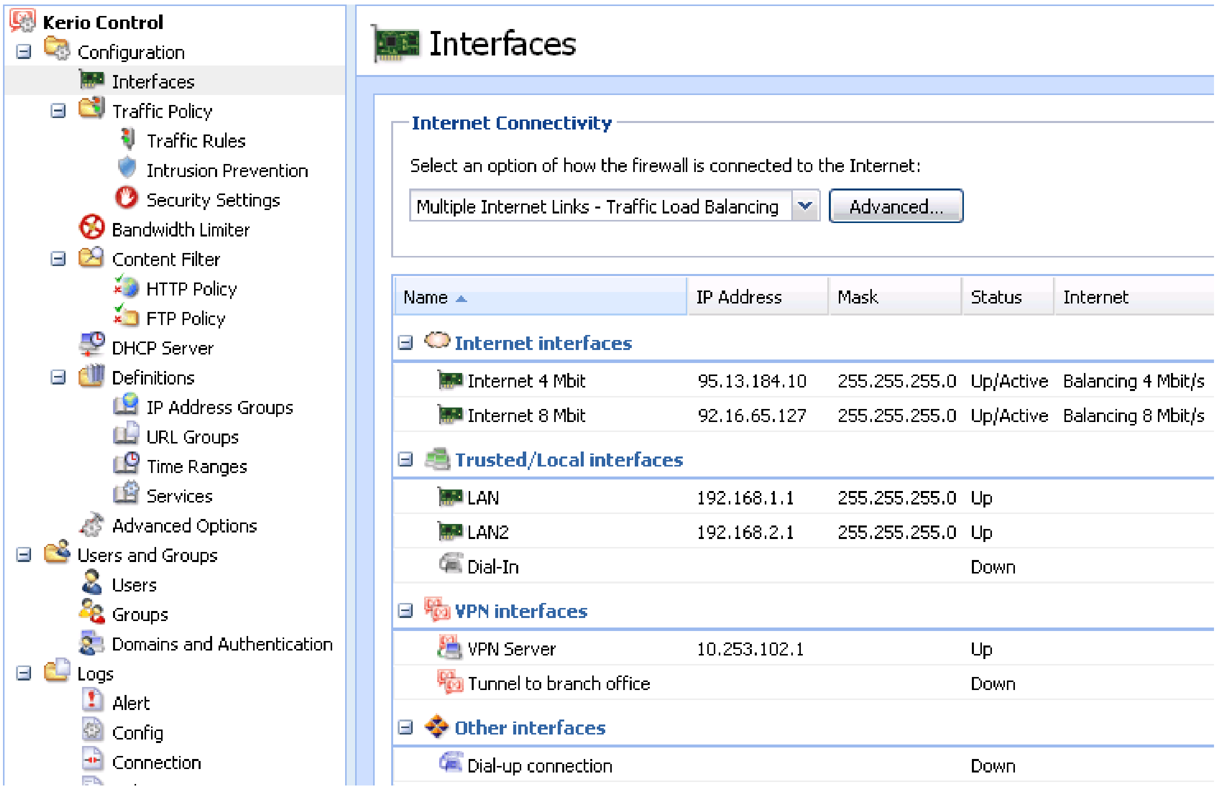
4.1 The Kerio Control Administration interface

The *Kerio Control Administration* interface is available at:

`https://server:4081/admin`

(`server` is the name or IP address of the firewall and `4081` is the port of its web interface). *HTTPS* traffic between the client and the *Kerio Control Engine* is encrypted. This protects the communication from tapping and misuse. It is recommended to use the unsecured version of the *Administration* (the *HTTP* protocol, port `4080`) only for local administration of `Kerio Control` (i.e. administration from the computer where it is installed).

Upon a successful logon to the *Administration* web interface, the main window consisting of two sections is displayed:



Internet Connectivity

Select an option of how the firewall is connected to the Internet:

Multiple Internet Links - Traffic Load Balancing

Name ▲	IP Address	Mask	Status	Internet
⊟ Internet interfaces				
Internet 4 Mbit	95.13.184.10	255.255.255.0	Up/Active	Balancing 4 Mbit/s
Internet 8 Mbit	92.16.65.127	255.255.255.0	Up/Active	Balancing 8 Mbit/s
⊟ Trusted/Local interfaces				
LAN	192.168.1.1	255.255.255.0	Up	
LAN2	192.168.2.1	255.255.255.0	Up	
Dial-In			Down	
⊟ VPN interfaces				
VPN Server	10.253.102.1		Up	
Tunnel to branch office			Down	
⊟ Other interfaces				
Dial-up connection			Down	

Figure 4.1 Main window of the Kerio Control Administration interface

- The left column contains the tree view of sections. For better transparency it is possible to hide or show individual parts of the tree (upon logon, the full tree is shown).
- The right column lists contents of the section previously selected in the left column.

In most cases, configuration changes in individual sections are performed only at the client's side (i.e. in the web browser) and get applied on the configuration file upon clicking on the *Apply* button. Therefore, it is possible to use the *Cancel* button to recover the former settings.

Individual sections of the web administration interface are described in the following chapters of this guide.

Note:

1. The *Kerio Control Administration* web interface is available in 15 languages. The *Administration* interface allows language selection by simple switching of the flag located in the top right corner of the window or by following the browser language preferences.
2. Upon the first logon to the *Kerio Control Administration* interface after installation of *Kerio Control*, activation wizard is started automatically where it is possible to register a purchased license or run the 30-day trial version and set the administration password. For a detailed description on this wizard, please refer to chapter 8.18.1.

4.2 Configuration Assistant

The configuration assistant is used for an easy instant basic configuration of *Kerio Control*. By default, it is opened automatically upon logon to the administration interface. If this feature is disabled, you can start the wizard by clicking on *Run the Configuration Assistant*.

The configuration assistant allows the following settings:

Configure Internet connection and the local network

A wizard allowing basic configuration of *Kerio Control*. Once these parameters are set, Internet connection and access to the Internet from local hosts is supposed to work. The wizard sets correct configuration of the DHCP server and the *DNS forwarder* module.
For a detailed description on the wizard, please refer to chapter 8.17.1.

Define traffic rules

Definition of basic traffic rules of the firewall. Basic rules are especially allowing NAT-based access from the local network to the Internet (IP address translation) and making selected services on local servers available from the Internet.
This tool is designed primarily for initial configuration of traffic policy. If this tool is used later, existing traffic rules get overwritten.
For details, refer to chapter 8.1.

Export your configuration

This option exports your current *Kerio Control* configuration in a package in *.tgz* (*tar* archive compressed with *gzip*).

The exported configuration can be used for firewall recovery purposes during reinstallation or to apply the configuration to another computer. *Kerio Control* configuration is compatible across individual operating systems.

Import configuration

This option loads and applies selected backup file of the firewall configuration. When a configuration is imported, differences in network interfaces are respected (added or removed interfaces, different interface names, etc.).

For detailed information on exporting and importing configuration, refer to chapter 26.1

Note: It is not necessary to use the configuration assistant or its individual features. Experienced administrators can configure *Kerio Control* without these tools.

4.3 Connectivity Warnings

When changes are being performed in *Kerio Control* configuration (settings of network interfaces, traffic rules, MAC filter and other security features) network connection can get lost between the *Kerio Control* server and the computer from which administration is realized (editions *Appliance* and *Box* can be administered only remotely from another host).

For that reason, the feature of so called connectivity warnings has been added since version *7.1.0*. When configuration changes are made which might affect connection between the *Kerio Control Administration* interface and the *Kerio Control* server, connection functionality gets checked automatically. If the connection is interrupted, *Kerio Control Administration* attempts to recover it.

In some cases it is not possible to automatically recover connection — typically after change of IP address of the interface used for *Kerio Control* administration. Then it is necessary to connect to the administration interface at the new IP address and login again (under certain conditions, change of TCP/IP configuration on the client host, configuration recovery from the DHCP server or other relevant operations may also be required).

If connection cannot be recovered within 10 minutes (or the administrator does not succeed in logging in within this time period, the server assumes that the administration has been blocked, reverts the configuration changes and recovers the existing configuration.

Chapter 5

License and Registration

A valid license is required for usage of *Kerio Control* after 30-day trial period. Technically, the product works as this:

- Immediately upon installation, the product works as a 30-day trial version. All features and options of the product are available except the *Kerio Web Filter* module and update of intrusion prevention system rules and of the integrated antivirus engine.

- Trial version can be registered for free. Registered trial version users can use technical support for the product during the trial period. Registered users can also test the *Kerio Web Filter* module, and their intrusion prevention system rules and the integrated antivirus engine are updated automatically. Registration does not prolong the trial period.

- Upon purchase of a license, it is necessary to register the product using the corresponding license key. Upon a successful registration, the product will be fully available according to the particular license policy (for details, see chapter 5.1).

There is actually no difference between the trial and full version of *Kerio Control* except being or not being registered with a valid license. This gives each customer an opportunity to install and test the product in a particular environment during the trial period. Then, once the product is purchased, the customer can simply register the installed version by the purchased license number (see chapter 5.4). This means that it is not necessary to uninstall the trial version and reinstall the product.

In case that the 30-day trial period has expired, functionality of *Kerio Control* is limited. Upon registration with a valid license number (received as a response to purchase of the product), *Kerio Control* is available with full functionality again.

The product license also defines number of users who can use the product. The basic license starts at 5 users. Number of users can be increased by purchasing a so called add-on license. For details on number of licensed users, see chapter 5.2.

5.1 Licenses, optional components and Software Maintenance

Kerio Control has the following optional components: *Sophos* antivirus (refer to chapter 15) or/and the *Kerio Web Filter* module for web pages rating (see chapter 14.3). These components are licensed individually.

License keys consist of the following information:

***Kerio Control* license**

Kerio Control basic license Its validity is defined by the two following factors:

- Update right expiration date — specifies the date by which *Kerio Control* can be updated for free. When this date expires, *Kerio Control* keeps functioning, however, it cannot be updated. The time for updates can be extended by purchasing and registration of so called *Software Maintenance*.
- Product expiration date — since this date, functionality of *Kerio Control* will be limited. Full functionality can be restored by purchasing and registration of a valid license.

License of the integrated *Sophos* antivirus

This license is defined by the two following dates:

- Update right expiration date (independent of *Kerio Control*) — when this date expires, the antivirus keeps functioning, however, neither its virus database nor the antivirus can be updated yet. The time for updates can be extended by purchasing so called *Software Maintenance*.
- Plug-in expiration date — specifies the date by which the *Sophos* antivirus stops functioning and cannot be used anymore.

> ***Warning:***
> Owing to persistent incidence of new virus infections we recommend you to use always the most recent antivirus versions.

Kerio Web Filter license

This license is defined by the date of expiration of the module's functionality. After this date, the *Kerio Web Filter* module is blocked and cannot be used any longer. However, its functionality can be extended by purchasing so called *Software Maintenance*.

Software Maintenance

Software Maintenance (referred to as *subscription* in previous versions of the product) is a right to update the product for certain time. If Software Maintenance expires, it is still possible to keep using the existing version of the product, but it is not longer possible to update for versions released after the expiration date. Updates will be available again upon purchasing of *Software Maintenance* for a new period.

Note:

1. Registration of *Kerio Control* generates a so called license key (the `license.key` file — see chapter 26.1). If your license key gets lost for any reason (e.g. after the hard drive breakdown or by an accidental removal, etc.), you can simply use the basic product's purchase number to recover the license. The same method can be used also for change of the firewall's operating system (*Windows / Software Appliance / VMware Virtual Appliance / Virtual Appliance for Parallels*) — the license keys cannot be used across different

operating systems. If the license number gets lost, contact the *Kerio Technologies* sales department.

2. Refer to the *Kerio Technologies* website (http://www.kerio.com/control/) to get up-to-date information about licenses, subscription extensions, etc.

5.2 Deciding on a number of users (licenses)

Kerio Control 7 uses a new system of Internet access monitoring, better corresponding to the product's licensing and usage policy. *Kerio Technologies* licenses this software as a server with the *Admin* account and 5 user accounts in the basic license. Users can be added in packages of five users.

User is defined as a person who is permitted to connect to *Kerio Control* and its services. Each user can connect from up to five different devices represented by IP addresses, including VPN clients.

If any user tries to connect from more than five devices at a time, another user license is used for this purpose. Although the product formerly did not limit number of connected users, it used to consider each IP address connected to the server as one user which might have caused situations where one user used up available licenses even by connecting from two device at a time.

> ***Warning:***
> *Kerio Control* does not limit number of defined user accounts (see chapter 17). However, if the maximal number of currently authenticated users is reached, no other user can connect.

5.3 Activation Wizard

First logon to the *Kerio Control Administration* interface after the installation automatically runs the product activation wizard. This wizard allows to register the product with a purchased license or activate the 30-day trial version and set some basic *Kerio Control* parameters.

Language selection

This page allows to select language. This language will be used by the activation wizard and it will also be set as a default language after the first logon to the administration interface. Once logged in, language settings can be changed as needed.

Internet Connection

On this page, the wizard checks whether Internet connection is available, allowing online registration of the product.

In editions *Appliance* and *Box*, if Internet connection cannot be detected, the wizard allows to change configuration of network interfaces. Select an interface connected to the Internet, configuration method (DHCP, static configuration or PPPoE) and specify required parameters. This procedure can be taken until Internet connection starts working.

On *Windows*, it is necessary to set Internet connection directly in the properties of the particular network adapter.

It is also possible to select offline registration and set Internet connection later.

Time zone, date and time settings (editions Appliance and Box)

Registration as well as many *Kerio Control* features (user authentication, logs, statistics, etc.) require correct setting of date, time and time zone on the firewall.

Select your time zone and check (and change, if necessary) date and time settings. It is recommended to enable synchronization of time against a time server (NTP servers of *Kerio Technologies* are used for this purpose).

Online activation

Online activation allows registering of serial number of the purchased product or the 30-day trial version.

Registration of purchased license

For registration you will need all purchased license numbers — number of the basic product, numbers of optional components, numbers of add-on licenses (adding users to an existing license) and number of Software Maintenance (right to update the product for a particular period).

- First, insert the license number of the basic product and enter the security code displayed in the picture (protection from violating of the registration server).
- In the next step, all license numbers that have been registered so far are displayed. Add other unregistered numbers if you have any (add-on licenses, Software Maintenance, etc.).
- On the next page, you can edit your registration details.
- Upon a successful registration, a license key will be generated and the product will be activated with a valid license.

Registration of the trial version

If you want to test the 30-day trial version, you can also register it. This type of registration is tentative and it is not obligatory.

Registration of the trial version allows to test also features unavailable in the unregistered version (the *Kerio Web Filter* module, updates of the integrated antivirus engine and the intrusion prevention system). The registration provides you with free technical support for the entire trial period.

Registration of the trial version does not prolong the trial period.

Offline activation

For offline activation you will need a file with the license key for the particular operating system (usually `license.key`). You can have this file saved from your previous installation of *Kerio Control*.

If you do not have the license key file (or you change operating system), it is possible to register license at the *Kerio Technologies* website (http://www.kerio.com/, option *Support* → *Register You License* in the main menu).

In the registration, specify correctly the operating system you will use the license on (*Windows* or *Linux*). The license can be used for any platform but the license key is always generated for the particular platform only. Once registered successfully, you can download the generated license key and use it for offline activation of the product.

Unregistered trial version

If it is not possible to complete the registration for any reason (e.g. Internet connection or license key file is not available at the moment), it is possible to click on *Skip Registration* to activate an unregistered 30-day trial version. the product can be registered later by using links available on the welcome page of the administration interface.

Admin password

On the last page of the activation wizard, it is required to enter the *Admin* password — i.e. the password of the main administrator of the firewall. Username *Admin* with this password is then used for:

- Access to the remote administration of the firewall via the web administration interface (see chapter 4),
- In case of editions *Appliance* and *Box* also for logon to the firewall's console (see chapter 3.2).

Remember this password or save it in a secured location and keep it from anyone else!

5.4 License information and registration changes

The license information are displayed on the *Kerio Control Administration* welcome page (the first item in the tree in the left part of the window — this section is displayed automatically whenever the *Kerio Control* administration is entered).

License information

License number

License number of the basic product.

Software Maintenance expiration date

Date until when the product can be upgraded for free.

Product functionality expiration date

Date when the product expires and stops functioning (only for trial versions or special license types).

Number of licensed users

Maximal number of users who can be using *Kerio Control* at a time (for details, see chapter 5.2).

Company

Name of the company (or a person) to which the product is registered.

Server

Name of the server (computer or device), on which *Kerio Control* is running.

Operational system

Operating system of the server (for editions *Appliance* and *Box*, *Linux* is displayed).

Changing registration

Depending on the current license, links are displayed at the bottom of the image:

1. For unregistered versions:

    - *Become a registered trial user* — registration of the trial version.

      Registration of the trial version allows to test also features unavailable in the unregistered version (the *Kerio Web Filter* module, updates of the integrated antivirus engine and the intrusion prevention system). The registration provides you with free technical support for the entire trial period.

    - *Register product with a purchased license number* — registration of purchased license numbers for the product.

      Once purchased, the product must be registered. Otherwise, it will keep behaving as a trial version!

2. For registered versions:

    - *Update registration information* — this option allows to add license numbers of optional components, Software Maintenance (right to update the product for a certain period) or add-on licenses (adding users to existing license), or to edit registration details of the company or person to which the product is registered.

- *Install License* — this option allows to import a license file (`*.key`) generated within your registration at the *Kerio Technologies* website or saved from a previous installation of *Kerio Control*.

  The license file cannot be used across different operating systems (*Windows / Appliance /Box*). If you are changing your operating system, it is necessary to use the basic product license number to register the product again (if you happen to lose the license number, please contact the *Kerio Technologies* sales department).

In any of the cases described, the registration wizard will be started where basic data are required and additional data can also be defined. This wizard is similar to the product activation wizard (see chapter 5.3).

New version notifications

If the update checker is enabled (refer to chapter 18.2), the *A new version is available, click here for details...* notice is displayed whenever a new version is available. Click on the link to open the dialog where the new version can be downloaded and the installation can be started (for details, see chapter 18.2).

Running the configuration assistant

The last link on the welcome page opens so called configuration assistant where you can set basic configuration of *Kerio Control* easily and in an instant and where it is also possible to import or export configuration.

5.5 Subscription / Update Expiration

Kerio Control automatically informs administrators of an upcoming license expiry date and/or of expiry of the right for updates (Software Maintenance) of the basic product, integrated *Sophos* antivirus or the *Kerio Web Filter* module. These alert only inform the administrator that they should prolong the Software Maintenance or renew the corresponding license.

Administrators are informed in the following ways:

- Bubble message is displayed (these messages are displayed by *Kerio Control Engine Monitor* — on *Windows* only),
- Notification informing about license and/or Software Maintenance expiry by an information box upon logon to the *Kerio Control Administration* interface.
- Notification of product expiration in the firewall's web interface upon opening of an Internet web page.

Note: Kerio Control administrators can also set posting of license or Software Maintenance expiration alerts by email or SMS (see chapter 20.4).

Bubble alerts (Windows)

Seven days before the date, *Kerio Control Engine Monitor* starts to display the information about number of days remaining to the Software Maintenance or license expiration several times a day (in regular intervals).

This information is displayed until *Kerio Control* or any of its components stops functioning or until Software Maintenance expires. The information is also no longer displayed upon registration of Software Maintenance or license of a particular component.

Notifications in the administration interface

Starting with the 30th day before the license or Software Maintenance expiration, warning is displayed informing about number of days left to expiration or stating that it has already expired. The warning also contains a link to the *Kerio Technologies* website where you can find detailed subscription information as well as purchase a new license or Software Maintenance for an upcoming period.

The warning stops being displayed when the license number of the new Software Maintenance is registered (refer to chapter 5.4).

Notification in the web interface

This notification is displayed for time-limited licenses (e.g. NFR license) or time-limited versions (Beta ans RC versions). Starting on day seven before *Kerio Control* expiration upon opening of a web page in the Internet, the browser gets redirected to a special page of the firewall's web interface. This page informs user about number of days remaining to the product expiration date (to the date where the product stops fully function.

Note: Final versions with valid "standard" license is not limited by time.

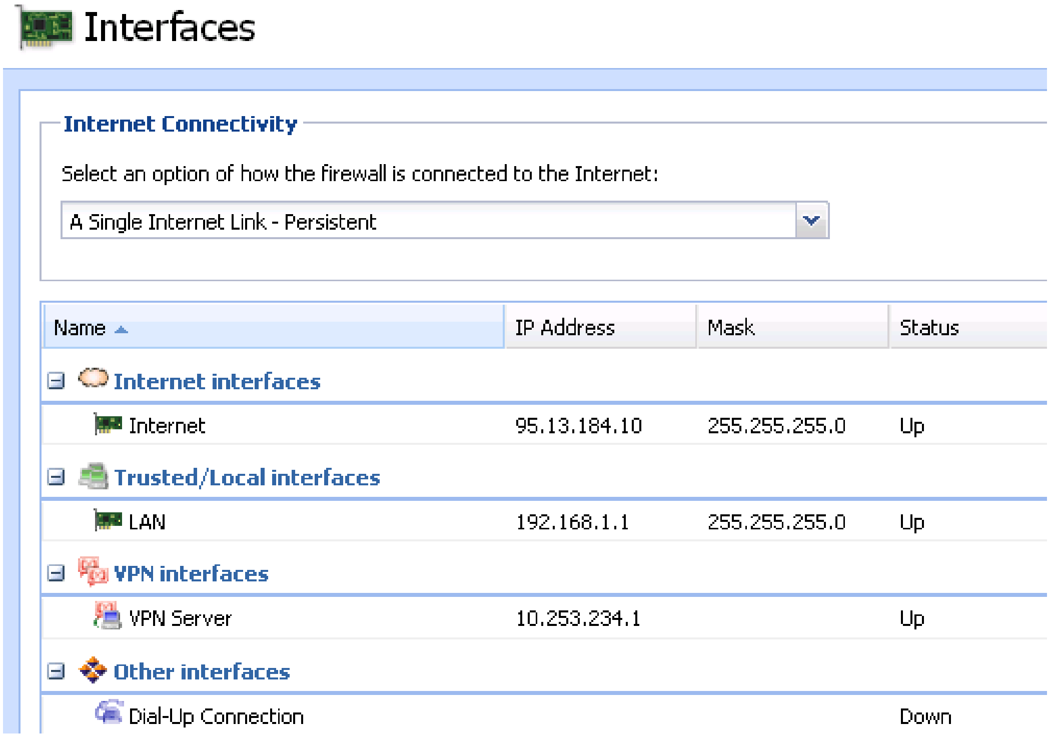
Chapter 6

Network interfaces

Kerio Control is a network firewall. This implies that it represents a gateway between two or more networks (typically between the local network and the Internet) and controls traffic passing through network adapters (*Ethernet*, *Wi-Fi*, dial-ups, etc.) which are connected to these networks.

Kerio Control functions as an IP router for all *Kerio Control's* network interfaces installed within the system.[3] The linchpin of the firewall's configuration therefore is correct configuration of network interfaces.

Network interfaces of the firewall can be viewed and configured in the *Administration* web interface under *Configuration* → *Interfaces*.



Interfaces

Internet Connectivity

Select an option of how the firewall is connected to the Internet:

A Single Internet Link - Persistent

Name ▲	IP Address	Mask	Status
⊟ Internet interfaces			
Internet	95.13.184.10	255.255.255.0	Up
⊟ Trusted/Local interfaces			
LAN	192.168.1.1	255.255.255.0	Up
⊟ VPN interfaces			
VPN Server	10.253.234.1		Up
⊟ Other interfaces			
Dial-Up Connection			Down

Figure 6.1 Network interfaces

[3] If you want to disable *Kerio Control* for any of these interfaces, go to the adapter's properties and disable *Kerio Control* (the *Kerio Control's* low level driver).
However, for security reasons and to guarantee full control over the network traffic, it is strongly unrecommended to disable *Kerio Control's* low level driver on any network adapter!
Kerio Control in editions *Appliance* and *Box* always works with all network interfaces in "UP" status.

Hint:
Network interfaces as well as other basic *Kerio Control* parameters can be easily set with the Connectivity Wizard (see chapter 7.1). You can open this wizard by clicking on *Configure in wizard* under *Interfaces* or from the *Configuration Assistant* (see chapter 4.2) on the administration interface welcome page.

6.1 Groups of interfaces

To simplify the firewall's configuration and make it as comfortable as possible, network interfaces are sorted in groups in *Kerio Control*. In the firewall's traffic rules, these groups as well as individual interfaces can be used in *Source* and *Target* (refer to chapter 8.3). The main benefit of groups of interfaces is that in case of change of internet connection, addition of a new line, change of a network adapter etc., there is no need to edit traffic rules — simple adding of the new interface in the correct group will do.

In *Kerio Control*, the following groups of interfaces are defined:

- *Internet interfaces* — interfaces which can be used for Internet connection (network cards, wireless adapters, dial-ups, etc.),
- *Trusted / Local interfaces* interfaces connected to local private networks protected by the firewall (typically *Ethernet* or *Wi-Fi* cards),
- *VPN interfaces* — virtual network interfaces used by the *Kerio VPN* proprietary solution (VPN server and created VPN tunnels — for details, refer to chapter 24),
- *Other interfaces* — interfaces which do not belong to any of the groups listed above (i.e. a network card for DMZ, idle dial-up, etc.).

Groups of interfaces cannot be removed and it is not possible to create new ones (it would not be of any help).

During the initial firewall configuration by *Connectivity wizard* (see chapter 7.1), interfaces will be sorted in correct groups automatically. This classification can be later changed (with certain limits — e.g. VPN server and VPN tunnels cannot be moved from the *VPN interfaces* group).

To move an interface to another group, drag it by mouse to the desired destination group or select the group in properties of the particular interface — see below.

Note: If the initial firewall configuration is not performed by the wizard, all interfaces (except VPN interfaces) are set as *Other interfaces*. Before you start creating traffic rules, it is recommended to define correctly interfaces for Internet connection as well as interfaces for the local network — this simplifies definitions of the rules significantly.

6.2 Viewing and configuring Ethernet ports (Kerio Control Box)

Kerio Control Box contains four or eight Gigabit Ethernet ports. On software level, individual ports can be set as individual interfaces, added to switch or disabled. In small networks, *Kerio Control* can be used not only to secure Internet gateway but also as a switch — it is not necessary to use any other device.

Ethernet configuration options:

- *Standalone interface* — the port will be used as a standalone Ethernet interface.

  Such port is usually used for connection to the Internet (add it to the group *Internet interfaces*) or for connection of a separate segment of the LAN (group *Trusted / Local interfaces*) or DMZ zones (group *Other interfaces*).

- *Switch for LAN* — port will be a part of the switch which, in *Kerio Control*, behaves as one *Ethernet* interface.

  By default, the switch belongs to the group *trusted / Local interfaces* and is used for connection of local workstations, servers, switches, routers and other devices which make infrastructure of the local network.

- *Not assigned* — the port will be inactive. This can be used for example for temporary disconnection of the computer of a network segment connected to the port.

6.3 Special interfaces

Interfaces include also the following special items:

VPN server

This interface is used as a server for connection of the proprietary VPN client (*Kerio VPN Client* — this solution can be downloaded for free from http://www.kerio.com/control/download). VPN servers are always sorted in the *VPN interfaces* group.
Double-click on this interface or click on *Edit* to edit settings and parameters of the VPN server. The *VPN server* interface cannot be removed.
For detailed information on the proprietary solution *Kerio VPN*, refer to chapter 24.

Dial-In (on Windows only)

This interface represents the server of the *RAS* service (dial-up connection to the network) on the *Kerio Control* host. This interface can be used for definition of traffic rules (see chapter 8) for RAS clients which are connecting to this server.
Dial-In interfaces are considered as trustworthy (clients connected via this interface use it to access the local network). This interface cannot be either configured or removed. If you do not consider RAS clients as parts of trustworthy networks for any reason, you can move the *Dial-In* interface to *Other interfaces*.

Note:

1. If both RAS server and *Kerio Control* are used, the RAS server must be configured to assign clients IP addresses of a subnet which is not used by any segment of the local network. *Kerio Control* performs standard IP routing which might not function unless this condition is met.
2. For assigning of IP addresses to RAS clients connecting directly to the *Kerio Control* host, *it is not possible* to use the *Kerio Control's* DHCP server. For details, see chapter 10.2.

6.4 Viewing and editing interfaces

In the list of interfaces, *Kerio Control* shows parameters related to firewall's configuration and operations:

Name

The unique name used for interface identification within *Kerio Control*. It should be clear for easy reference, e.g. *Internet* for the interface connected to the Internet connection.
The name can be edited later (see below) with no affect on *Kerio Control's* functionality.
The icon to the left of the name represents the interface type (network adapter, dial-up connection, VPN server, VPN tunnel).
Note: Unless the name is edited manually, this item displays the name of the adapter as assigned by the operating system (see the *Adapter name* entry).

IP Address and Mask

IP address and the mask of this interface's subnet.
If the more IP addresses are set for the interface, the primary IP address will be displayed. On *Windows*, the address assigned to the interface as first is considered as primary.

Status

Current status of the interface (up/down).

Internet

This information indicates the method the interface uses for Internet connection (primary/secondary connection, bandwidth used).

Details

Adapter identification string returned by the device driver.

System Name

The name of the adapter (e.g. “LAN connection 2”). The name is for reference only.

Gateway

IP address of the default gateway set for the particular interface.

DNS

IP address of the primary DNS server set on the interface.

MAC

Hardware (MAC) address of a corresponding network adapter. This entry is empty for dial-ups as its use would be meaningless there.

Use the buttons at the bottom of the interface list to remove or edit properties of the chosen interface. If no interface is chosen or the selected interface does not support a certain function, appropriate buttons will be inactive.

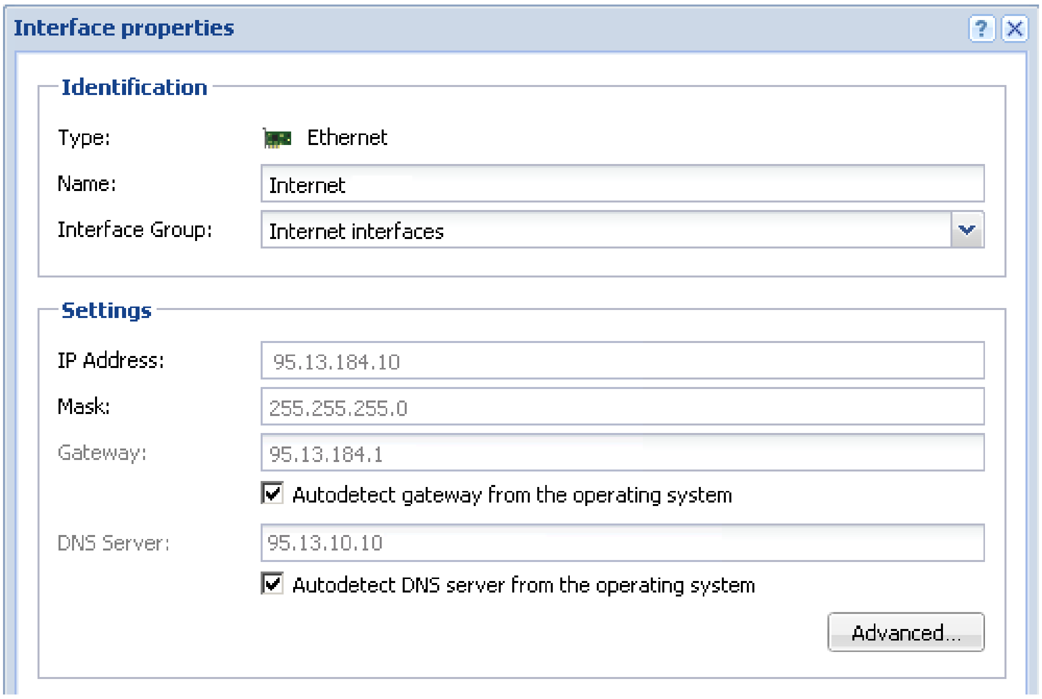
Add VPN Tunnel / Add → VPN tunnel

Use this option to create a new server-to-server VPN tunnel. Details on the proprietary *Kerio VPN* solution are provided in chapter 24.

Note: In editions *Appliance* and *Box*, it is also possible to add new interfaces (PPTP or PPPoE connections) — see section 6.5. If *Kerio Control* is installed on *Windows*, it is necessary to define new connections by standard methods right in the operating system.

Modify

Click on *Edit* to view and/or modify parameters of the selected interface.



Interface properties

Identification

Type: Ethernet

Name: Internet

Interface Group: Internet interfaces

Settings

IP Address: 95.13.184.10

Mask: 255.255.255.0

Gateway: 95.13.184.1

☑ Autodetect gateway from the operating system

DNS Server: 95.13.10.10

☑ Autodetect DNS server from the operating system

Figure 6.2 Editing interfaces

In *Kerio Control*, it is specify to specify a special name for each interface (names taken from the operating system can be confusing and the new name may make it clear). It is also possible to change the group of the interface (Internet, secure local network, another network — e.g. configuration of DMZ), default gateway and DNS servers.

In *Appliance Edition*, it is possible to set all parameters of the network interface in this dialog.

For dial-ups it is also possible to set login data and dialing options (see chapter 7.5).

For *VPN server* and VPN tunnels, a dialog for setting of the *VPN server* (see chapter 24.1) or a VPN tunnel (refer to chapter 24.3) will be opened.

Remove

Removes the selected interface from *Kerio Control*. This can be done under the following conditions:

- the interface is an inactive (disconnected) VPN tunnel,
- the network adapter is not active or it is not physically present,
- the interface is a dial-up which no longer exists in the system.

Network cards and dial-ups defined in the operating system as well as established VPN tunnels cannot be removed in *Kerio Control*.

Note:

1. Records related to network cards or dial-ups that do not exist any longer (those that have been removed) do not affect *Kerio Control's* functionality — such interfaces are considered as inactive (as in case of a hung-up dial-up).
2. When an adapter is removed, the *Nothing* value is automatically used for corresponding items of all traffic rules where the interface was used. These rules will be disabled. This ensures that the traffic policy is not endangered (for details, refer to chapter 8.3).

Dial or Hang Up / Enable, Disable

Function of these buttons depend on the interface selected:

- For dial-up, PPTP and PPPoE connections, the *Dial* and *Hang-up* buttons are available and they are used to handle the line by hand.
  Note: Users with appropriate rights can also control dial-ups in the user web interface (see chapter 17.2 and the *Kerio Control — User's Guide*).
- For VPN tunnels, the *Enable* and *Disable* buttons are available that can be used to enable /disable the VPN tunnel selected for details, see chapter 24.3).
  In the *Software Appliance / VMware Virtual Appliance* edition, it is also possible to block individual network adapters.
- If the *Dial-in* interface or a VPN server is selected, these buttons are inactive.

6.5 Adding new interface (editions Appliance and Box)

In editions *Appliance* and *Box*, *Kerio Control* allows to add new network interfaces (PPTP and PPPoE connections).

Click the *Add* button to display a menu and select the type of the new interface.

The new interface needs an easily identifiable name that will be shown in *Kerio Control* and it needs to be added to a group of interfaces (this item can be changed as desired any time later).

The following data is also required depanding on the connection:

- *PPTP* — PPTP server, username and password,
- *PPPoE* — interface (Ethernet), username and password. If you set the interface to Any

— *Kerio Control* will automatically select the appropriate interface which will be used for conenction.

—

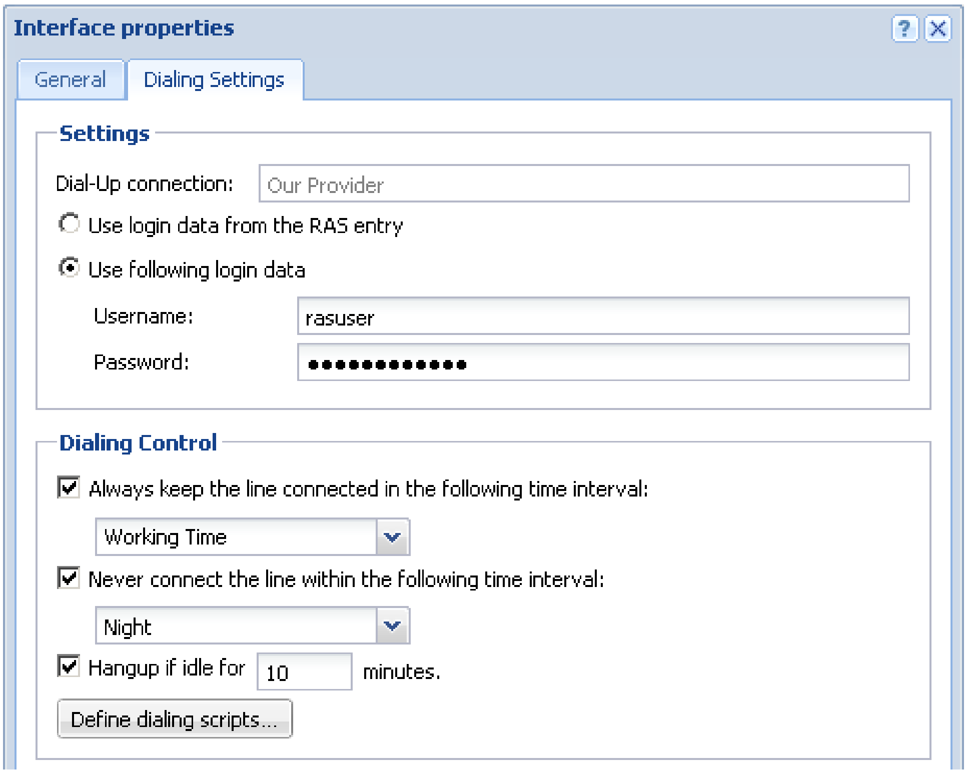
Optionally, you can specify IP address of a specific DNS server which will then be used as the primary DNS server for Internet connections via this interface.

The *Dialing settings* can be used to set time intervals in which the connection should be established persistently and when it should be disconnected. Out of these intervals, the link will demand manual dialing (either in the administration interface or in the user web interface — see *Kerio Control — User's Guide*). The link can be hung up automatically after defined period of idleness (for details, see section 6.6).

Note: The PPPoE connection can be defined in properties of the particular *Ethernet* interface. We recommend this method if you use only one PPPoE connection via this interface.

6.6 Advanced dial-up settings

For dial-ups, the interface settings dialog (see chapter 6) includes also the *Dialing settings* tab where specific parameters for dial-up connections can be set:



Interface properties

General | Dialing Settings

Settings

Dial-Up connection: Our Provider

○ Use login data from the RAS entry

● Use following login data

Username: rasuser

Password: •••••••••••••

Dialing Control

☑ Always keep the line connected in the following time interval:

Working Time

☑ Never connect the line within the following time interval:

Night

☑ Hangup if idle for 10 minutes.

Figure 6.3 Interface properties — dialing settings

Login information

If login data for the particular dial-up connection change, it can be updated here or it is also possible to use the data saved in the operating system (if saved there).

Time intervals for persistent connection and persistent hang-up

Under certain circumstances it may be needed that dial on demand works only within a certain time period (typically in working hours) and that the link is hung-up outside this range. With respect to cost rates of individual providers, it can sometimes be most efficient to keep the link up persistently even in times with dense network communication.

For these purposes, it is possible to set time intervals for persistent connection and/or hang-up.

If the time intervals overlap, the interval in which the link is hung-up rules over the other. Out of these intervals, the link will demand manual connection (either in the administration interface or in the user web interface — see *Kerio Control User's Guide*). *Kerio Control* on *Windows* also supports the mode of automatic dialing of the link in response to queries from the local network (so called on-demand dialing — see chapter 7.5).

Note:

1. If a static route over a dial-up is defined in *Kerio Control* routing table, this link will be dialed whenever a packet is routed through there. Settings for the interval within which the link should be hung-up persistently will be ignored in this case.
   For details, see chapter 19.1.
2. The dialing settings do not include an explicit option of connection recovery upon failures. In case of connection outage, connection will or will not be recovered in dependence on the current mode of the link:
   - If the link should be connected persistently at the moment of the failure, the connection is recovered automatically.
   - If the connection is set to be hung-up at the moment of the outage, the connection will not be recovered.
   - In mode of on-demand dial (i.e. outside the intervals defined), connection will be recovered in response to the first request (i.e. packet sent from the local network to the Internet).

Automatic hangup when idle

Dial-ups are usually charged by connection time. When no data are transferred via the connection, there is no reason to keep the link up. Therefore, it is possible to set also idleness time after which the link will be hung-up automatically.

For optimal idleness timeout length, it is necessary to know how the Internet connection is charged in the particular case. If the idleness timeout is too short, it may result in too frequent hanging up and dialing of the link which might be very uncomfortable and in certain cases even increase connection costs.

Note: In the time interval where persistent connection of the link is set (see above), the idleness timeout is ignored.

6.7 Supportive scripts for link control (Windows)

In some cases there is a special need of running a program or a script (execute a batch command) along with dialing or hanging up a link. This can be helpful for example if a special type of modem is used that must be controlled by a special program provided by its developers.

Kerio Control allows launching any program or a command in the following situations: *Before dial*, *After dial*, *Before hang-up* or/and *After hang-up*. In case of the *Before dial* and *Before hang-up* options, the system does not wait for its completion after startup of the program.

Scripts for control of dial-ups must be located in the `scripts` subdirectory of the firewall's installation directory, typically

```
C:\Program Files\Kerio\WinRoute Firewall\scripts
```

(Attention! This directory does not exist in the default installation — it is therefore necessary to create it!).

The script names must have the following names:

- `BeforeDial.cmd` — before dial,
- `AfterDial.cmd` — after dial,
- `BeforeHangup.cmd` — before hangup,
- `AfterHangup.cmd` — after hangup.

Each script first accepts the parameter of full name of the connection currently being dialed or hung up (name in the *Kerio Control* interface).

Possible errors (e.g. if you allow an action but the particular script does not exist) are recorded in the *Error* log (see chapter 23.8).

Note: If the name of the dial-up includes blanks, it will be automatically put in quotes upon the script call, which guarantees correct transmission of the full name in an only parameter of the script. However, it is more suitable to use names without blanks and diacritics for dial-ups. Interfaces in *Kerio Control* can be renamed any time needed.

Warning:
On *Windows*, *Kerio Control* is running as a service. Therefore, external applications and operating system's commands will run in the background only (in the *SYSTEM* account). The same rules are applied for all external commands and external programs called by scripts. Therefore, it is not highly unrecommended to use interactive applications (i.e. applications with user interaction) for the actions described above. Interactive application would be running "in background" until the system restart or killing of the particular process. Under specific circumstances, such application might also block other dials or hang-ups.
In editions *Appliance* and *Box*, supportive scripts for dial-ups are not supported.

Chapter 7

Configuring Internet connection and the local network

The basic function of *Kerio Control* is connection of the local network to the Internet via one or more Internet connections (Internet links). Depending on number and types of Internet links, *Kerio Control* provides various options of Internet connection:

Single Internet Link

The most common connection of local networks to the Internet. In this case, only one Internet connection is available and it is used persistently (typically *Ethernet*, *Wi-Fi*, *ADSL* or cable modems). It is also possible to use dial-like links which can be connected persistently — typically *PPPoE* connections.

A Single Internet Link — Dial On demand (Windows only)

This type of connection is fit for links which are charged by connection time — typically modems for analog or *ISDN* links. The link is down by default and *Kerio Control* dials it in response to a query demanding access from the local network to the Internet. If no data are transferred via the link for some time, *Kerio Control* hangs it up to reduce connection costs.

This mode is available only in *Kerio Control* for *Windows*. *Kerio Control* in editions *Appliance* and *Box* does not support dial-ups.

Multiple Internet Links — Failover

Where reliability (availability of the Internet connection) is an issue and two Internet links are available, the connection failover feature can help. If the primary link fails, *Kerio Control* switches to the secondary link automatically. Users may therefore notice just a very short disconnection of the Internet connection. When the connection on the primary link is recovered, *Kerio Control* automatically switches back to it. For most part of users, this operation takes so short to be even noticeable.

Multiple Internet Links   Traffic Load Balancing

If throughput (connection speed) is an issue, *Kerio Control* can use multiple links concurrently and spread data transferred between the LAN and the Internet among these links. In standard conditions and settings, this also works as connection failover — if any of the links fails, transferred data are spread among the other (working) links.

In all cases, *Kerio Control* works in the mode of shared Internet connection. Sharing uses the NAT (IP address translation) technology, hiding the entire local network behind a public IP address of the firewall (or multiple addresses — depending on the type of Internet connection applied). *Kerio Control* can also be used as a neutral router (router without NAT). However, this mode is not the best connection of the LAN to the Internet — it requires expert configuration and advanced security.

This involves selection of the Internet connection type in the *Configuration* → *Interfaces* section of the *Kerio Control* configuration, setting corresponding interfaces for connection to the Internet and definition of corresponding traffic rules (see chapter 8.3).

7.1 Connectivity Wizard

For easy configuration of network interfaces, Internet connection and local network, *Kerio Control* provides *Connectivity Wizard*. This wizard can be run from the *Configuration Assistant* (see chapter 4.2) or by clicking on the *Configure in wizard* link under *Configuration Interfaces*.

Typically, the connectivity wizard is used for initial configuration of Internet connection and local network. If used later, the wizard tends to respect the existing firewall configuration as much as possible. If it detects specific settings which are not compatible, detailed information is displayed and the wizard closes. *Kerio Control* administrator then can edit this setting manually or make necessary configuration changes without even using the wizard. One of these "incompatible" settings is for example *DHCP server* (see chapter10.2) in the manual configuration mode or on-demand dial of Internet connection (*Kerio Control* on Windows).

Internet connection mode

The first section focuses on selection of mode for Internet connection:

- *Single Internet Link* — connection with a single leased or dial-up link (see chapter 7.2).
- *Two Internet Links with Traffic Load Balancing* — two links will be always used for Internet connection, increasing connection speed (throughput) — see chapter 7.3.
- *Two Internet Links with Failover* — the primary link is used for Internet connection, with a secondary link ready as a failover link (see chapter 7.4).

Detailed descriptions of individual connection modes are provided in the following chapters.

Note: Kerio Control on *Windows* also enables on demand dial of Internet connection. This mode cannot be set in the wizard. For details, see chapter 7.5.

Selecting Internet interfaces

In dependence on the selected connection mode it is also necessary to choose interface(s) connected to the Internet.

The wizard allows to edit settings of the default gateway and DNS servers for individual interfaces (by default, configuration detected in the firewall's operating system is used).

Kerio Control in editions *Appliance* and *Box* also allows to set IP address and subnet mask of individual interfaces.

The wizard does not allow setting of dial-up connection parameters (phone number, login data, etc.).

Selecting an interface for local network and setting DHCP server

The next page allows to select an interface connected to the local network.

The interface of the local network will be used as the default gateway (or also as a DNS server) for hosts in the LAN. For this reason, the interface must have a fixed IP address and therefore it cannot be configured by DHCP.

It is supposed that exactly one interface is currently connected to the local network. Interfaces which are used neither for Internet connection or for the local network are added to the *Other Interfaces* group. If the local network consists of multiple segments connected to different firewall interfaces, then you can simply add all uninvolved interfaces to the group *Trusted / Local Interfaces*.

While selecting an interface for the local network, it is also possible to enable automatic configuration of local hosts by the *Kerio Control* DHCP server (recommended). This option enables the DHCP server in automatic configuration mode — it is not necessary to set anything. If you do not want to use the *Kerio Control* DHCP server, it is kept disabled which should guarantee avoiding possible collisions.

Summary and application of the new configuration

On the last page of the wizard, new connection configuration is summarized.

This is the last chance to cancel the changes. The configuration will be applied upon its confirmation.

7.2 Internet Connection With A Single Link

Requirements

The *Kerio Control* hosting computer must be connected to the Internet by a leased line (typically *Ethernet* or *Wi-Fi* card). Parameters of this interface will be set with use of information supplied by the ISP provider or they can be configured automatically with the DHCP protocol.

It is also possible to use a dial-like link which can be connected persistently — typically *PPPoE* connections. *Kerio Control* will keep this type of link connected persistently (in case of connection failure, the connection is automatically recovered immediately).

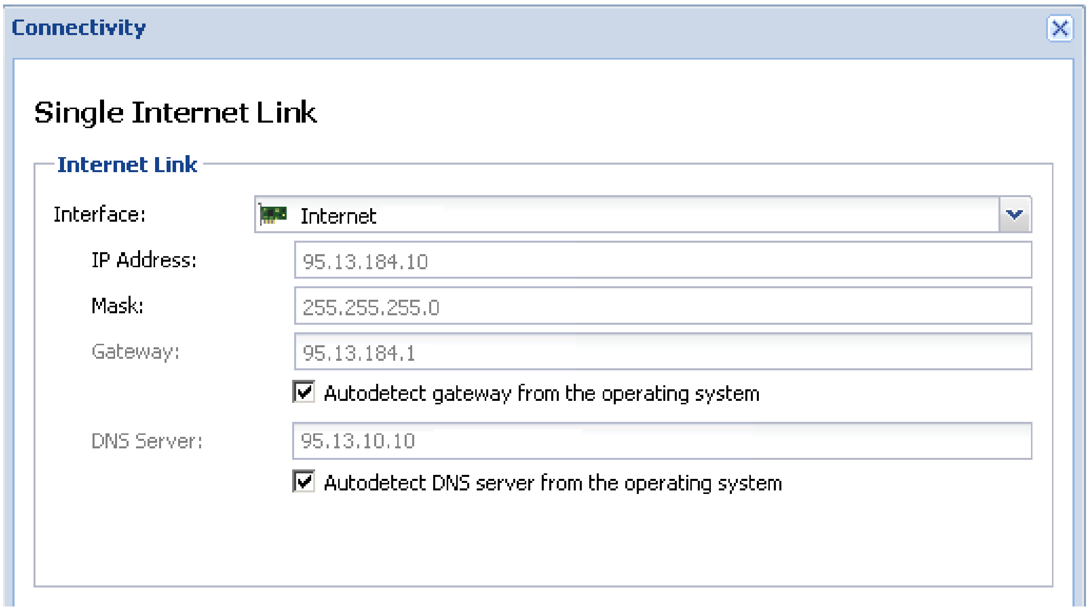
This connection type also requires one or more network cards for connection of individual segments of the LAN. Default gateway must *NOT* be set on any of these cards!

Hint:
On *Windows*, it is recommended to check functionality of both the Internet connection before installing *Kerio Control*:

Configuration with the wizard

1. On the first page of the *Connectivity wizard* (see chapter 8.1), select the option *A Single Internet Link*.

2. On the next page of the wizard, select a network interface (Internet link). As a preselection, the interface where *Kerio Control* detected the default gateway is used. Therefore, in most cases the appropriate adapter is already set within this step.



Connectivity

Single Internet Link

Internet Link

Interface: Internet

IP Address: 95.13.184.10

Mask: 255.255.255.0

Gateway: 95.13.184.1

☑ Autodetect gateway from the operating system

DNS Server: 95.13.10.10

☑ Autodetect DNS server from the operating system

Figure 7.1 Connectivity wizard — selection of an interface for the Internet connection

The wizard allows to change configuration of the default gateway and DNS servers on the selected interface. In editions *Appliance* and *Box*, it is also possible to set IP address and subnet mask.

If you choose *PPPoE* connection, username and password is required.

Note: If the more IP addresses are set for the interface, the primary IP address will be displayed. On *Windows*, the address assigned to the interface as first is considered as primary.

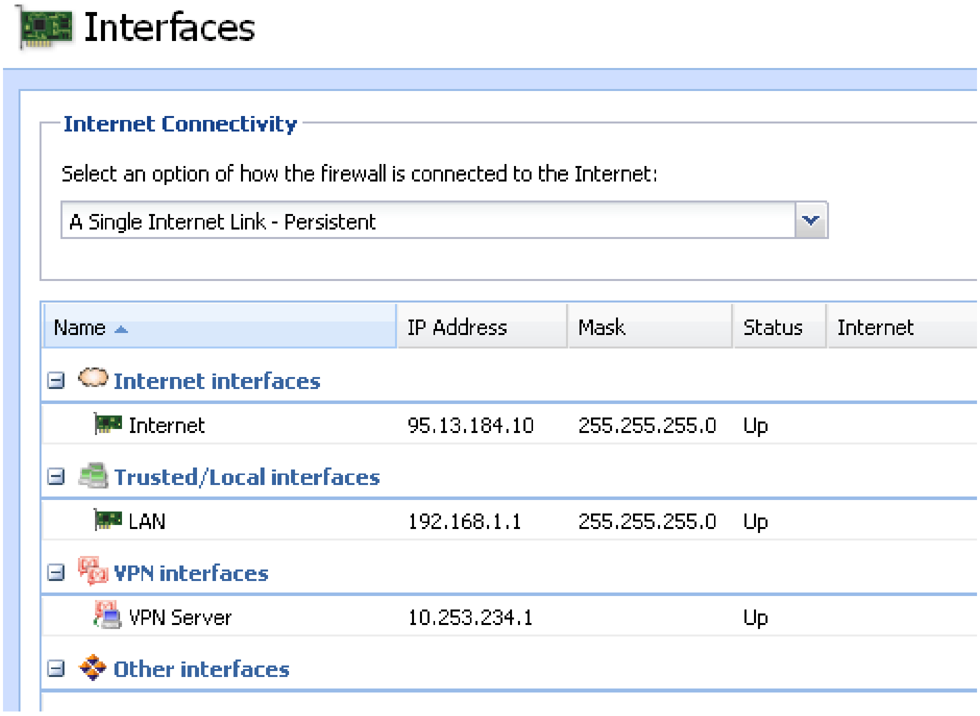
For details on network interfaces, see chapter 6.

3. On the next page of the wizard, select interface connected to the local network. If multiple interfaces are connected to the local network, select the interface you are currently using

for connection to the *Kerio Control* administration. Then move the other adapters to the group *Trusted / Local Interfaces*.

Resulting interface configuration

When you finish set-up in *Connectivity wizard*, the resulting configuration can be viewed under and edited if desirable.



Interfaces

Internet Connectivity

Select an option of how the firewall is connected to the Internet:

A Single Internet Link - Persistent

Name	IP Address	Mask	Status	Internet
Internet interfaces				
Internet	95.13.184.10	255.255.255.0	Up	
Trusted/Local interfaces				
LAN	192.168.1.1	255.255.255.0	Up	
VPN interfaces				
VPN Server	10.253.234.1		Up	
Other interfaces				

Figure 7.2 Network interfaces — connection by a single leased link

The *Internet Interfaces* groups includes only card *Internet* selected in the second page of the wizard. Only the *LAN* adapter selected on the third page of the wizard is included in the group *trusted / Local Interfaces*.

Other interfaces are considered as not used and added to the group *Other Interfaces*. For these interfaces, it will be necessary to define corresponding traffic rules manually (e.g. DMZ creation rule). If the interface configuration does not correspond with the real network configuration, edit it (e.g. if the firewall uses multiple interfaces for the local network, move corresponding interfaces to the group *Trusted / Local Interfaces*).

It is also possible to add new interfaces to the *Internet Interfaces* group. Packets will then be routed to corresponding target networks in accordance with the system routing table (see also chapter 19.1) and IP address translation will be applied (NAT). However, such configuration is not significantly helpful in place.

Warning:
It is necessary that in the *Single Internet Link* mode the default gateway is set only at the “main” Internet interface! If *Kerio Control* detects more default gateways, error is announced. Solve this problem immediately, otherwise traffic from the firewall and the LAN to the Internet will not work correctly.

7.3 Network Load Balancing

If at least two Internet links are available, *Kerio Control* can divide traffic in parts sent by either of them. The benefits of such solution are evident — Internet connection throughput gets better (i.e. speed of data transmission between the LAN and the Internet increases) and response time gets shorter for connections to servers in the Internet. If special traffic policy is not defined (so called *policy routing* — see chapter 8.5), then individual links are also backed-up mutually (see also chapter 7.4) — in case of failure of one of the lines, the traffic is routed via another.

Note:

1. Network load balancing is applied only to outbound traffic via the default route. If the routing table (see chapter 19.1) defines a route to a destination network, traffic to the network will always be routed through the particular interface.
2. Network load balancing does not apply to the traffic of the firewall itself. This traffic is processed directly by the operating system and, therefore, the standard routing is applied here (the default route with the lowest metric value will always be used).

Requirements

The computer hosting *Kerio Control* must have two network interfaces for connection to the Internet, i.e. leased (*Ethernet*, *Wi-Fi*) or persistently connected dial-up links (*PPPoE*). Usual dial-ups (analog modem, *ISDN*) are not suitable, because it is not possible to dial on demand in the network load balancing mode.

This connection type also requires one or more network cards for connection of individual segments of the LAN. Default gateway must *NOT* be set on any of these cards (cards for the LAN)!

Both the primary and the secondary link may be configured automatically by the DHCP protocol. In that case, *Kerio Control* looks all required parameters up in the operating system.

Hint:
On *Windows*, it is recommended to check functionality of individual Internet links yet before installing *Kerio Control*: The following testing methods can be applied (to both links):

- If these links are two dial-ups, connect one after the other and check access to the Internet.
- If one link is leased and the other a dial-up, test the leased link connection first and then dial the other one. Dialing of the link opens (creates) a new default route via this link which allows us to test Internet connection on the secondary link.
- In case of two leased links, the simplest way is to disable one of the connections int he operating system and test the other (enabled) link. And, as implied, test the other in the same way when the first link is checked.

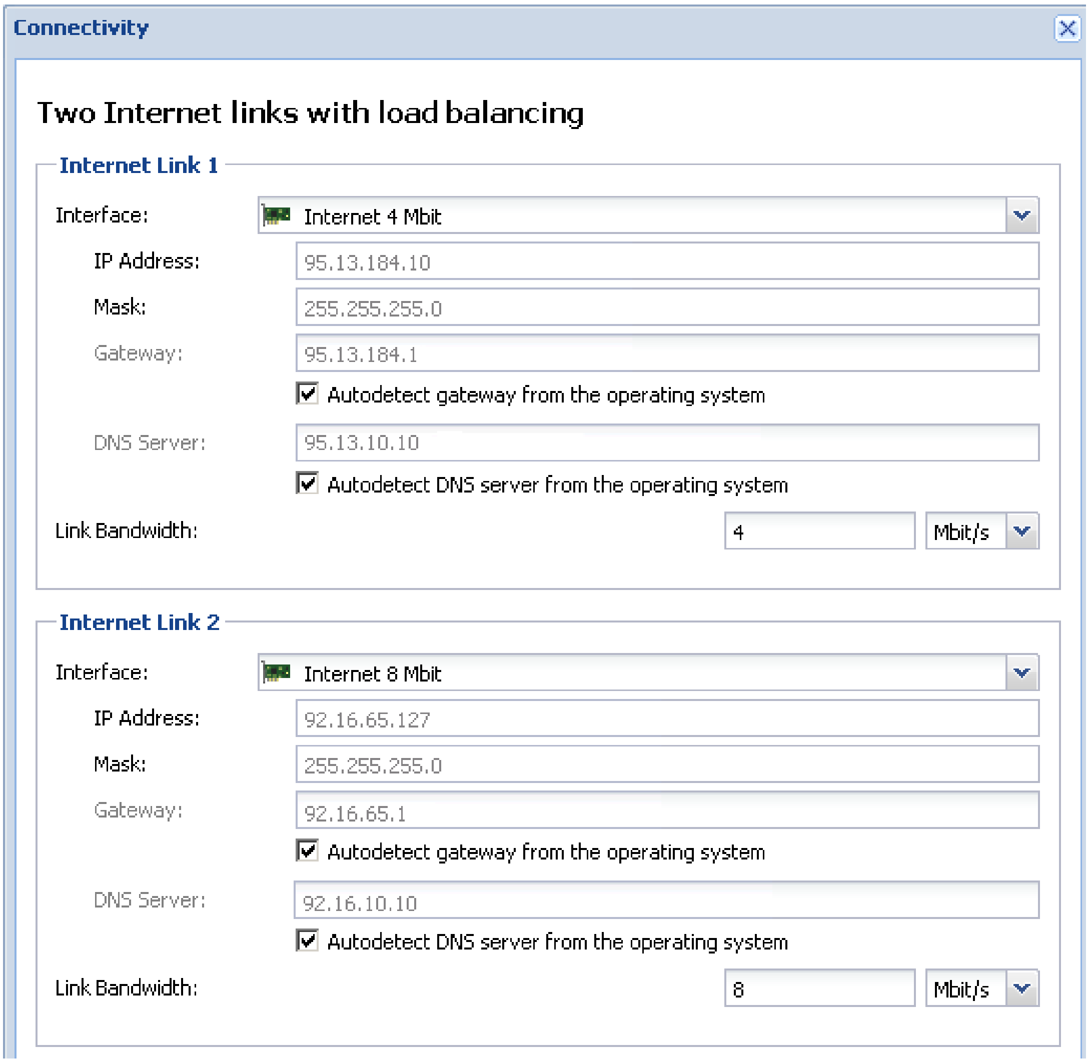
This method can be applied to any number of Internet lines.

Configuration with the wizard

1. On the first page of the *Connectivity wizard* (see chapter 8.1), select the option *Two Internet Links With traffic Load Balancing*.
2. On the second page of the interface, select two interfaces to be used as Internet links with traffic load balance.

   The wizard allows to change configuration of the default gateway and DNS servers on the selected interface. In editions *Appliance* and *Box*, it is also possible to set IP address and subnet mask. If you choose *PPPoE* connection, username and password is required.

   For each link, specification of bandwidth is required (i.e. traffic speed). The absolute value of the link speed is not important (however, just for reference reasons, it should correspond with the link speed suggested by the ISP). The important aspect is the ratio of speed between individual links — it determines how Internet traffic will be divided among these links.



Connectivity

Two Internet links with load balancing

Internet Link 1

Interface: Internet 4 Mbit

IP Address: 95.13.184.10

Mask: 255.255.255.0

Gateway: 95.13.184.1

☑ Autodetect gateway from the operating system

DNS Server: 95.13.10.10

☑ Autodetect DNS server from the operating system

Link Bandwidth: 4 Mbit/s

Internet Link 2

Interface: Internet 8 Mbit

IP Address: 92.16.65.127

Mask: 255.255.255.0

Gateway: 92.16.65.1

☑ Autodetect gateway from the operating system

DNS Server: 92.16.10.10

☑ Autodetect DNS server from the operating system

Link Bandwidth: 8 Mbit/s

Figure 7.3 Connectivity wizard — load balancing with two Ethernet links

Example:
Let us suppose there are two Internet links available. You set their bandwidth values to *4 Mbit/s* and *8 Mbit/s*. Total (proposed) speed of the Internet connection is therefore *12 Mbit/s*, while one link provides one third of this capacity and the other link provides two thirds. Simply said, one third of overall Internet traffic will be routed through one link and the resting two thirds through the other one.

Note: If the more IP addresses are set for the interface, the primary IP address will be displayed. On *Windows*, the address assigned to the interface as first is considered as primary.

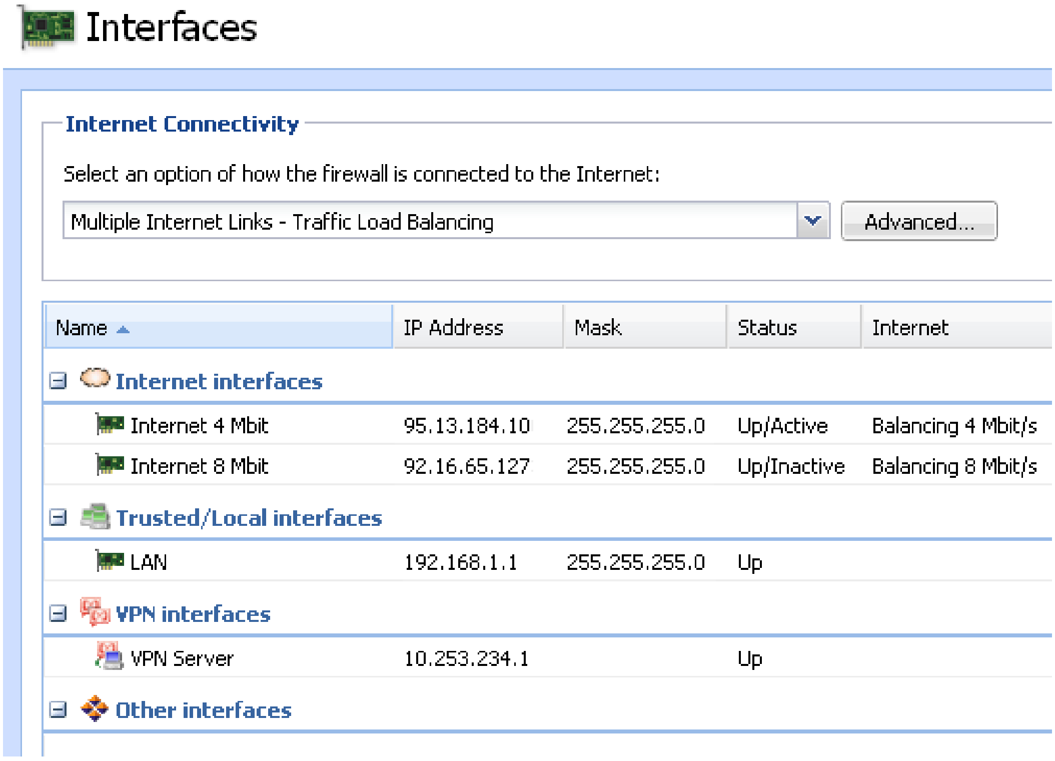
For details on network interfaces, see chapter 6.

3. On the next page of the wizard, select interface connected to the local network. If multiple interfaces are connected to the local network, select the interface you are currently using

for connection to the *Kerio Control* administration. Then move the other adapters to the group *Trusted / Local Interfaces*.

Resulting interface configuration

When you finish set-up in *Connectivity wizard*, the resulting configuration can be viewed under *Configuration* → *Interfaces* and edited if desirable.



Interfaces

Internet Connectivity

Select an option of how the firewall is connected to the Internet:

Multiple Internet Links - Traffic Load Balancing

Name	IP Address	Mask	Status	Internet
Internet interfaces				
Internet 4 Mbit	95.13.184.10	255.255.255.0	Up/Active	Balancing 4 Mbit/s
Internet 8 Mbit	92.16.65.127	255.255.255.0	Up/Inactive	Balancing 8 Mbit/s
Trusted/Local interfaces				
LAN	192.168.1.1	255.255.255.0	Up	
VPN interfaces				
VPN Server	10.253.234.1		Up	
Other interfaces				

Figure 7.4 Configuration of interfaces — network traffic load balancing

The *Internet interfaces* group includes the *Internet 4Mbit* and the *Internet 8Mbit* link selected as an interface for Internet traffic load balancing on the third page of the wizard.

The *Internet* column shows proposed speed of individual links (see above). The *Status* column informs of the current status of the link (up/down) as well as of the fact whether the link is active, i.e. whether connection on this Internet link is working and part of Internet traffic can be routed through it.

For any new link added to the *Internet interfaces* group, the default speed of *1 Mbit/s* will be set. Then it is possible and also recommended to edit the proposed link speed in the interface settings (see chapter 6) with respect to its real speed, which makes the balancing efficient and working smoothly.

Only the *LAN* adapter selected on the third page of the wizard is included in the group *trusted / Local Interfaces*.

Other interfaces are considered as not used and added to the group *Other Interfaces*. For these interfaces, it will be necessary to define corresponding traffic rules manually (e.g. DMZ creation rule). If the interface configuration does not correspond with the real network configuration, edit it (e.g. if the firewall uses multiple interfaces for the local network, move corresponding interfaces to the group *Trusted / Local Interfaces*).

> ***Hint:***
> Speed of one or more links can be set even for *0 Mbit/s*. Such links will then not be used for network traffic load balancing, but for traffic routing in accordance with specific traffic rules (see chapter 8.5). However, availability of these links will still be tested and the links will serve as alternative for case that all the other links fail.

Advanced settings (optimization, dedicated links, etc.)

In basic configuration, network load balancing is applied automatically with respect to their proposed speeds (see above). It is possible to use traffic rules to modify this algorithm (e.g. by dedicating one link for a particular traffic). This issue is described in detail in chapter 8.5.

Advanced Settings

Probe hosts

Functionality of individual Internet links is regularly tested by sending an *ICMP* request for a response (*PING*) to certain hosts or network interfaces. By default, the default gateway of the particular link is used as the probe host. If the default gateway is not available, the tested link is not working (correctly).
If the primary default gateway (i.e. the default gateway set for the tested link) cannot be used as the testing computer by any reason, it is possible to specify IP addresses of other (one or more) testing computers upon clicking on *Advanced*. If at least one of the tested devices is available, the Internet connection in question is considered as functioning.
The specified probe hosts will be used for testing of availability of *all* Internet links. Therefore, the group of testing computers should include a few hosts belonging to various subnets of the Internet.
Note:

1. Probe hosts must not block *ICMP Echo Requests* (*PING*) since such requests are used to test availability of these hosts — otherwise the hosts will be always considered as unavailable. This is one of the cases where the default gateway cannot be used as the testing computer.
2. Probe hosts must be represented by computers or network devices which are permanently running (servers, routers, etc.). Workstations which are running only a few hours per day are irrelevant as probe hosts.
3. *ICMP* queries sent to probe hosts cannot be blocked by the firewall's traffic rules.

VPN tunnels

During recovery over the primary link, *Kerio Control* may automatically disconnect and reconnect all VPN tunnels. If this option is disabled, VPN tunnels will stay connected over the failover link which may it probable that forwarding between private networks would not be correct.

7.4 Connection Failover

Kerio Control allows guarantee Internet connection by an alternative (back-up) connection (so called connection failover). This connection failover is launched automatically whenever failure of the primary connection is detected. When *Kerio Control* finds out that the primary connection is recovered again, the secondary connection is disabled and the primary one is re-established automatically.

Requirements

The computer hosting *Kerio Control* must have two network interfaces for Internet connection: a leased line (*Ethernet*, *Wi-Fi*) or a dial-up with persistent connection (*PPPoE*) for primary connection and a leased line or a dial-up for secondary (failover) connection.

This connection type also requires one or more network cards for connection of individual segments of the LAN. Default gateway must *NOT* be set on any of these cards (cards for the LAN)!

Both the primary and the secondary link may be configured automatically by the DHCP protocol. In that case, *Kerio Control* looks all required parameters up in the operating system.

Warning:
Connection failover is relevant only if performed by a persistent connection (i.e. the primary connection uses a network card or a persistently connected dial-up). Failing that, the secondary connection would be activated upon each hang-up of the primary link automatically.

Hint:
On *Windows*, it is recommended to check functionality of both the primary and the secondary link out before installing *Kerio Control*:

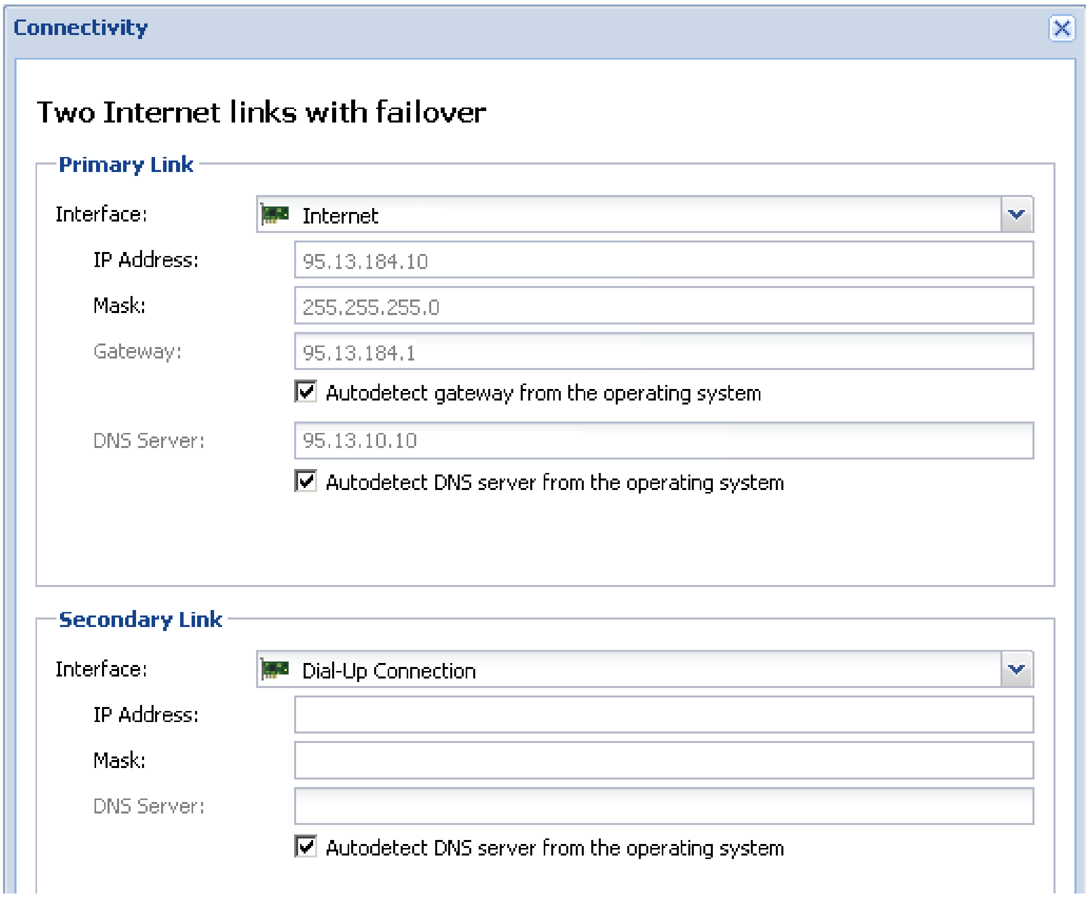
- If these links are two dial-ups, dial one after the other and check the Internet connection.
- If the primary link is leased and the secondary a dial-up, test the primary link connection first and the secondary connection second. Dialing of the link opens (creates) a new default route via this link which allows us to test Internet connection on the secondary link.
- In case of two leased links, the simplest way is to disable one of the connections int he operating system and test the other (enabled) link. And, as implied, test the other in the same way when the first link is checked.

Configuration with the wizard

1. On the first page of the *Connectivity wizard*, select the option *Two Internet Links With Failover*.
2. In the second step of the wizard, select a network interface to be used for the primary connection (leased or persistent link) and for the secondary connection (leased or dial-up link). If you choose *PPPoE* connection, username and password is required.

   The wizard allows to change configuration of the default gateway and DNS servers on the selected interface. In editions *Appliance* and *Box*, it is also possible to set IP address and subnet mask. If you choose *PPPoE* connection, username and password is required.

   For details on network interfaces, see chapter 6.
3. On the next page of the wizard, select interface connected to the local network. If multiple interfaces are connected to the local network, select the interface you are currently using for connection to the *Kerio Control* administration. Then move the other adapters to the group *Trusted / Local Interfaces*.



Connectivity

Two Internet links with failover

Primary Link

Interface: Internet

IP Address: 95.13.184.10

Mask: 255.255.255.0

Gateway: 95.13.184.1

☑ Autodetect gateway from the operating system

DNS Server: 95.13.10.10

☑ Autodetect DNS server from the operating system

Secondary Link

Interface: Dial-Up Connection

IP Address:

Mask:

DNS Server:

☑ Autodetect DNS server from the operating system

Figure 7.5 Connectivity wizard — leased dial-up link failover

Resulting interface configuration

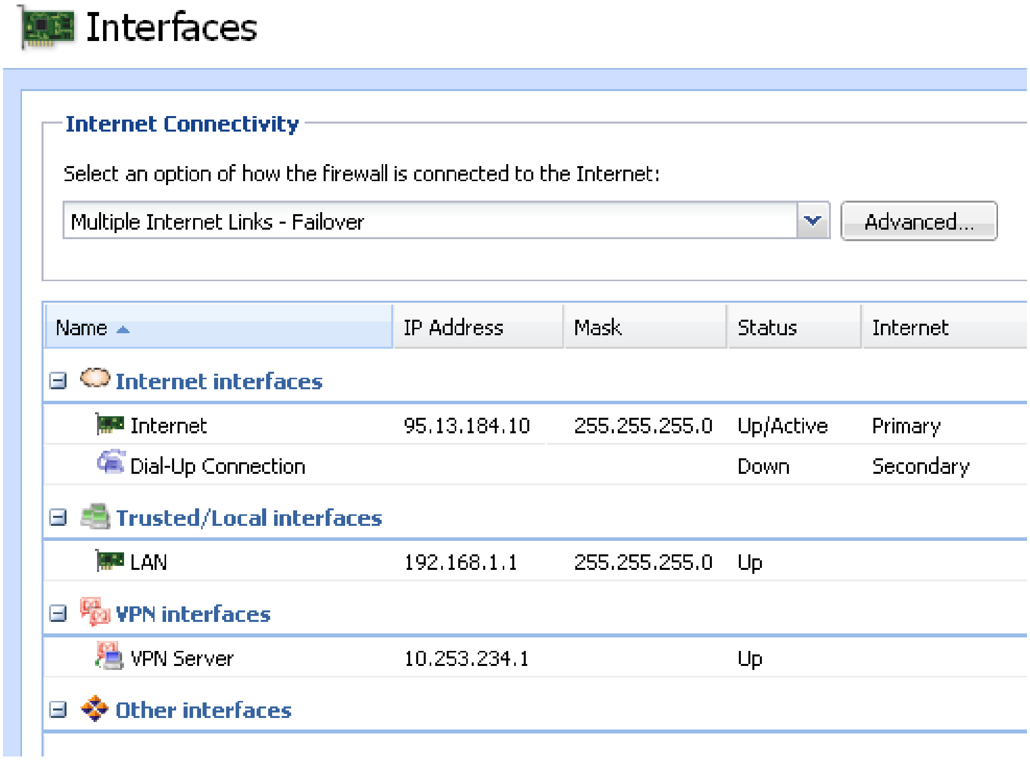
When you finish set-up in *Connectivity wizard*, the resulting configuration can be viewed under *Configuration* → *Interfaces* and edited if desirable.

The *Internet interfaces* group includes the *Internet* and the *Dial-up* link selected as primary and secondary (failover) on the second page of the wizard. The information provided in the *Internet* column states which link is used for primary and which one for secondary connection. The *Status* column informs of the link status (up/down) as well as of the fact whether the link is active (just being used as Internet connection at the moment) or not.

Only the *LAN* adapter selected on the third page of the wizard is included in the group *trusted / Local Interfaces*.

Other interfaces are considered as not used and added to the group *Other Interfaces*. For these interfaces, it will be necessary to define corresponding traffic rules manually (e.g. DMZ creation rule). If the interface configuration does not correspond with the real network configuration, edit it (e.g. if the firewall uses multiple interfaces for the local network, move corresponding interfaces to the group *Trusted / Local Interfaces*).

To change settings of primary and secondary connection, use corresponding options in the interface edit dialog (see chapter 6) or use the context menu called up by right-clicking on



Interfaces

Internet Connectivity

Select an option of how the firewall is connected to the Internet:

Multiple Internet Links - Failover

Name	IP Address	Mask	Status	Internet
Internet interfaces				
Internet	95.13.184.10	255.255.255.0	Up/Active	Primary
Dial-Up Connection			Down	Secondary
Trusted/Local interfaces				
LAN	192.168.1.1	255.255.255.0	Up	
VPN interfaces				
VPN Server	10.253.234.1		Up	
Other interfaces				

Figure 7.6 Configuration of interfaces — Internet connection failover

the corresponding link. However, under any circumstances, always a single link can be set as primary connection and a single one as secondary.

Advanced Settings

Probe hosts

Functionality of individual Internet links is regularly tested by sending an *ICMP* request for a response (*PING*) to certain hosts or network interfaces. By default, the default gateway of the particular link is used as the probe host. If the default gateway is not available, the tested link is not working (correctly).

If the primary default gateway (i.e. the default gateway set for the tested link) cannot be used as the testing computer by any reason, it is possible to specify IP addresses of other (one or more) testing computers upon clicking on *Advanced*. If at least one of the tested devices is available, the Internet connection in question is considered as functioning.

The specified probe hosts will be used for testing of availability of *all* Internet links. Therefore, the group of testing computers should include a few hosts belonging to various subnets of the Internet.

Note:

1. Probe hosts must not block *ICMP Echo Requests* (*PING*) since such requests are used to test availability of these hosts — otherwise the hosts will be always considered as unavailable. This is one of the cases where the default gateway cannot be used as the testing computer.

2. Probe hosts must be represented by computers or network devices which are permanently running (servers, routers, etc.). Workstations which are running only a few hours per day are irrelevant as probe hosts.
3. *ICMP* queries sent to probe hosts cannot be blocked by the firewall's traffic rules.

VPN tunnels

During recovery over the primary link, *Kerio Control* may automatically disconnect and reconnect all VPN tunnels. If this option is disabled, VPN tunnels will stay connected over the failover link which may it probable that forwarding between private networks would not be correct.

7.5 Connection with a single leased link - dial on demand (Windows)

If the *Kerio Control* host is connected to the Internet via dial-up, *Kerio Control* can automatically dial the connection when users attempt to access the Internet. *Kerio Control* on *Windows* allows automatic dialing of the link in response to queries from the local network. This feature is called dial on demand.

Note: In editions *Appliance* and *Box*, dial on demand is not supported.

Requirements

The corresponding device must be installed on the *Kerio Control* (usually an analog or an ISDN modem) and the corresponding dial-up connection must be created in the operating system. It is not necessary to define and save login data in the dial-up settings, this information can be defined directly in *Kerio Control*. This connection type also requires one or more network cards for connection of individual segments of the LAN. Default gateway must *NOT* be set on any of these cards!

We recommend you to create and test a dial-up connection before installing *Kerio Control*.

Warning:
Before configuring the LAN and the firewall for a Internet link dialed on demand, please pay special attention to the information provided in chapter 26.5. Correct configuration of the network with respect to specific qualities and behavior of on demand dial helps to avoid subsequent problems.

Configuration

The dial on demand mode cannot be configured in the connectivity wizard — to set network interfaces, go to *Configuration / Interfaces*.

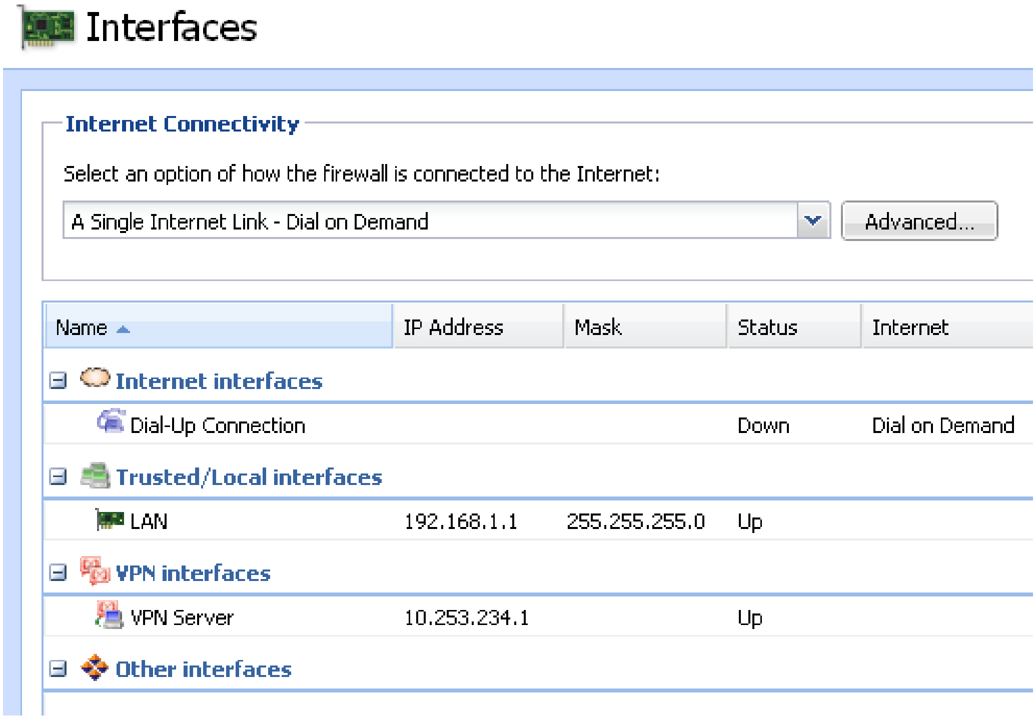
Add *Dial-Up* connection to the group *Internet interfaces*. In interface properties it is necessary to set this interface as a dial on demand link (this information is displayed in the column *Internet*).

To *Trusted / Local Interfaces*, add all interfaces connected to the local network.

Other interfaces will stay in the group *Other Interfaces*. For these interfaces, it will be necessary to define corresponding traffic rules manually (e.g. DMZ creation rule).

The *Internet interfaces* group can include multiple dial-ups. However, only one of these links can be set for on-demand dialing. If another link is dialed manually, *Kerio Control* will route packets to the corresponding destination network in accordance with the system routing table (see also chapter 19.1) and perform IP address translation (NAT). However, such configuration would be of any use. It is therefore recommended to keep only a single on-demand-dial link in the *Internet interfaces* group.

To change the dial-on-demand link, use the corresponding option in the interface edit dialog (see chapter 6) or use the context menu (by right-clicking on the link).



Interfaces

Internet Connectivity

Select an option of how the firewall is connected to the Internet:

A Single Internet Link - Dial on Demand

Name	IP Address	Mask	Status	Internet
⊟ Internet interfaces				
Dial-Up Connection			Down	Dial on Demand
⊟ Trusted/Local interfaces				
LAN	192.168.1.1	255.255.255.0	Up	
⊟ VPN interfaces				
VPN Server	10.253.234.1		Up	
⊟ Other interfaces				

Figure 7.7 Configuration of interfaces — an on-demand dial link

Warning:
In the *Dial on Demand* mode, default gateway must NOT be set on any network interface of the firewall! On-demand dialing is based on absence of the default gateway (if no route exist in the routing table where a packet would be directed, *Kerio Control* create a default gateway by dialing an Internet link).

For details on network interfaces, see chapter 6.

Advanced dialing settings

You can use the *Advanced* button to set dial-up parameters — e.g. intervals where the line is supposed to be persistently connected or hung up as well as supportive scripts for dialing and hanging of the line. For detailed information on these settings, see chapter 6.6.

Chapter 8

Traffic Rules

Traffic Rules belongs to of the basic *Kerio Control* configuration. All the following settings are displayed and can be edited within the table:

- security (protection of the local network including the *Kerio Control* host from Internet intrusions
- IP address translation (or NAT, *Network Address Translation* — technology which enables transparent access of the entire local network to the Internet with one public IP address only)
- access to the servers (services) running within the local network from the Internet (port mapping)
- controlled access to the Internet for local users

Traffic policy rules can be defined in *Configurations* → *Traffic Policy* → *Traffic Rules*. The rules can be defined either manually (advanced administrators) or using the wizard (recommended).

It is recommended to create basic traffic rules and later customize them as desired. Advanced administrators can create all the rules according to their specific needs without using the wizard.

8.1 Network Rules Wizard

To run the traffic policy wizard, click on the *Configure in wizard* button under *Configuration* → *Traffic Policy* → *Traffic Rules*.

The network rules wizard demands only the data that is essential for creating a basic set of traffic rules. The rules defined in this wizard will enable access to selected services to the Internet from the local network, and ensure full protection of the local network (including the *Kerio Control* host) from intrusion attempts from the Internet.

Requirements of the wizard

To use the wizard, the computer or device hosting *Kerio Control* needs:

- at least one active adapter connected to the local network,
- at least either one active adapter connected to the Internet or at least one telephone or PPPoE connection is defined. This connection is not required to be established at the moment of the wizard's startup.

Step 1 — confirmation

To guarantee reliable *Kerio Control* functionality after the wizard is used, all existing rules are removed and substituted by rules created automatically upon the new data. Unless this is the initial configuration (upon *Kerio Control* installation), the wizard asks you if you really wish to overwrite the existing traffic rules.

The existing traffic policy is substituted by new rules after completing the entire process after confirmation of the last step. This means that during the process the wizard can be stopped and canceled without losing existing rules.

Step 2 — making Kerio Control services available from the Internet

On the second page of the wizard, select *Kerio Control* services to be available from the Internet:

- *Kerio VPN Server* — connection to the *Kerio Control's* VPN server. Enable this service if you want to create VPN tunnels and/or connect remotely to the local network by using *Kerio VPN Client*. For details see chapter 24.

- *Server Kerio SSL-VPN (HTTPS)* — the *Kerio Clientless SSL-VPN* interface (available only in *Kerio Control* on Windows). This option allows HTTPS traffic on the standard port (443). For details see chapter 25.

- *Kerio Control Administration* — enables remote administration of *Kerio Control*. This option allows HTTPS traffic on port 4081 (port of the administration interface cannot be changed).

Step 3 — mapping of other services

On the third page, you can make any other services on the firewall or servers in the local network available from the Internet (mapping).

Each mapping rule contains the following parameters:

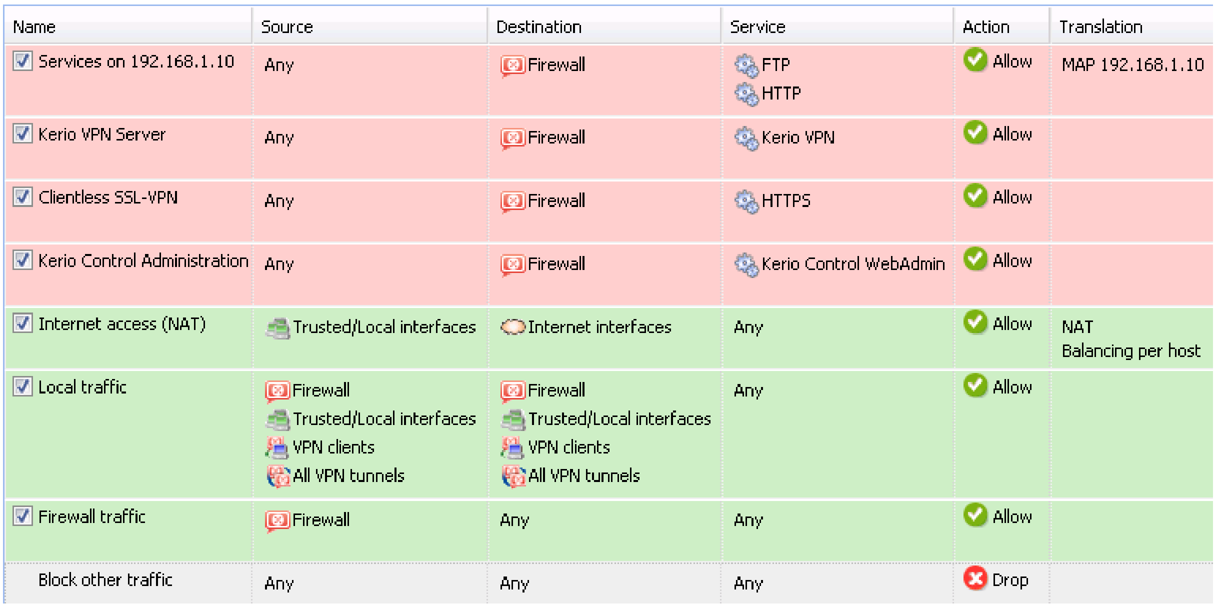
- Mapped service — services can be chosen either from the list of defined services (see chapter 16.3) or it is possible to define another service by its protocol and port number.

- Destination host — firewall or IP address of the local server on which the service is running.

Rules Created by the Wizard

The traffic policy is better understood through the traffic rules created by the Wizard in the previous example.

These rules are not affected by the selected type of Internet connection (the wizard, pages 2 and 3).



Name	Source	Destination	Service	Action	Translation
☑ Services on 192.168.1.10	Any	Firewall	FTP HTTP	✓ Allow	MAP 192.168.1.10
☑ Kerio VPN Server	Any	Firewall	Kerio VPN	✓ Allow	
☑ Clientless SSL-VPN	Any	Firewall	HTTPS	✓ Allow	
☑ Kerio Control Administration	Any	Firewall	Kerio Control WebAdmin	✓ Allow	
☑ Internet access (NAT)	Trusted/Local interfaces	Internet interfaces	Any	✓ Allow	NAT Balancing per host
☑ Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	✓ Allow	
☑ Firewall traffic	Firewall	Any	Any	✓ Allow	
Block other traffic	Any	Any	Any	✗ Drop	

Figure 8.1 Traffic Policy generated by the wizard

Services on...

These two rules are examples of mapped services on local servers. For each local server, one rule will be created following the pattern *Services on <IP address of the server>* or *Services on the firewall*.
These services will be available at IP addresses of all "outbound" interfaces of the firewall (i.e. interfaces in the group *Internet interfaces*).

Kerio Control Administration, Kerio VPN Server, Clientless SSL-VPN

These rules allow access to administration of *Kerio Control*, VPN server and the *Kerio Clientless SSL-VPN* interface. Individual rules are created only if the particular services were selected on the second page of the wizard.

Internet access (NAT)

This rule sets that in all packets routed from the local network to the Internet, the source (private) IP address will be replaced by the address of the Internet interface through which the packet is sent from the firewall.
The *Source* item of this rule includes the *Trusted / Local interfaces* group and the *Destination* item includes group *Internet interfaces*. This makes the rule applicable to any network configuration. It is not necessary to change this rule whenever a new segment of the LAN is connected or Internet connection is changed.

Note: On *Windows*, the *Trusted / Local interfaces* group includes also a *Dial-In* interface, i.e. all *RAS* clients connecting to this server can access the Internet with the *NAT* technology by default.

Local Traffic

This rule allows all traffic between local hosts and the firewall (i.e. the computer where *Kerio Control* is installed). In this rule, items *Source* and *Destination* include the *Trusted / Local interfaces* group (see chapter 6) and the special group *Firewall*.

If creating of rules for *Kerio VPN* was set in the wizard (the wizard, page 5), the *Local Traffic* rule includes also special address groups *All VPN tunnels* and *All VPN clients*. This implies that, by default, the rule allows traffic between the local network (firewall), remote networks connected via VPN tunnels and VPN clients connecting to the *Kerio Control's* VPN server.

Note:

1. Access to the *Kerio Control* host is not limited as the wizard supposes that this host belongs to the local network. Limitations can be done by modification of an appropriate rule or by creating a new one. An inconvenient rule limiting access to the *Kerio Control* host might block remote administration or it might cause some Internet services to be unavailable (all traffic between the LAN and the Internet passes through this host).
2. On Windows, the *Trusted / Local interfaces* group includes also a *Dial-In* interface by default. This means that the *Local Traffic* rule also allows traffic between local hosts and *RAS* clients/VPN clients connected to the server.

Firewall Traffic

This rule enables access to certain services from the *Kerio Control* host. It is similar to the *NAT* rule except from the fact that this rule does not perform IP translation (this host connects to the Internet directly).

Default rule

This rule drops all communication that is not allowed by other rules. The default rule is always listed at the end of the rule list and it cannot be removed.

The default rule allows the administrator to select what action will be taken with undesirable traffic attempts (*Deny* or *Drop*) and to decide whether packets or/and connections will be logged.

Note: To see detailed descriptions of traffic rules refer to chapter 8.3..

8.2 How traffic rules work

The traffic policy consists of rules ordered by their priority. When the rules are applied, they are processed from the top downwards and the first rule is applied that meets connection or packet parameters — i.e. order of the rules in the list is key. The order of the rules can be changed with the two arrow buttons on the right side of the window.

An explicit rule denying all traffic is shown at the end of the list. This rule cannot be edited or removed. If there is no rule to allow particular network traffic, then the “catch all” deny rule will discard the packet.

Note:

1. Unless any other traffic rules are defined (by hand or using the wizard), all traffic is blocked by a special rule which is set as default.
2. To control user connections to WWW or FTP servers and filter contents, use the special tools available in *Kerio Control* for these purposes (see chapter 14) rather than traffic rules.

8.3 Definition of Custom Traffic Rules

The traffic rules are displayed in the form of a table, where each rule is represented by a row and rule properties (name, conditions, actions — for details see below) are described in the columns. Left-click in a selected field of the table (or right-click a rule and choose the *Edit...* option in the context menu) to open a dialog where the selected item can be edited.

To define new rules press the *Add* button. Move the new rule within the list using the arrow buttons.

Name

Name of the rule. It should be brief and unique so that the table is easy-to-use.

Checkboxes next to names can be either checked to activate or unchecked to disable the particular rule. If a particular field is empty, *Kerio Control* will ignore the rule. This means that you need not remove and later redefine these rules when troubleshooting a rule.

The background color of each row with this rule can be defined as well. Use the *Transparent* option to make the background transparent (background color of the whole list will be used, white is usually set). Colors allow highlighting of rules or distinguishing of groups of rules (e.g. rules for incoming and outgoing traffic).

Note: Names and background colors of the rules are used for better reference and greater comfort they do not influence the firewall’s functionality.

Source, Destination

Definition of the source or destination of the traffic defined by the rule.

A new source or destination item can be defined after clicking the *Add* button:

- *Host* — the host IP address or name (e.g. `192.168.1.1` or `www.company.com`)

> ***Warning:***
> If either the source or the destination computer is specified by DNS name, *Kerio Control* tries to identify its IP address while processing a corresponding traffic rule.
> If no corresponding record is found in the cache, the *DNS forwarder* forwards the query to the Internet. If the connection is realized by a dial-up which is currently hung-up, the query will be sent after the line is dialed. The corresponding rule is disabled unless IP address is resolved from the DNS name. Under certain circumstances denied traffic can be let through while the denial rule is disabled (such connection will be closed immediately when the rule is enabled again).
> For the reasons mentioned above we recommend you to specify source and destination computers only through IP addresses in case that you are connected to the Internet through a dial-up!

- *IP range* — e.g. `192.168.1.10—192.168.1.20`
- *Subnet with mask* — subnet defined by network address and mask

  (e.g. `192.168.1.0/255.255.255.0`)
- *IP address group* — a group of addresses defined in *Kerio Control* (refer to chapter 16.1)
- *Interfaces* — selection of an interface or a group of interfaces from which the packet comes in (*Source*) or via which they are sent out (*Destination*).

  Groups of interfaces allow creation of more general rules independent from any particular network configuration (e.g. it is not necessary to change such rules when Internet connection is changed or when a new LAN segment is added). It is recommended to define traffic rules associated with groups of interfaces wherever possible. For details on network interfaces and groups of interfaces, see chapter 6.

  Note: Only the *Internet interfaces* and the *Trusted / Local interfaces* group can be used in traffic rules. Another method is used to add interfaces for *Kerio VPN*(see below). The *Other interfaces* group includes interfaces of various types that were not filed in another group. For this reason, traffic rules for such group would not be of much use.
- *VPN* — virtual private network (created with *Kerio VPN*). This option can be used to add the following items:

  1. *Incoming VPN connections (VPN clients)* — all VPN clients connected to the *Kerio Control* VPN server via the *Kerio VPN Client*,
  2. *VPN tunnel* — network connected to this server from a remote server via the VPN tunnel The *All* option covers all networks connected by all VPN tunnels defined which are active at the particular moment.

For detailed information on the proprietary VPN solution integrated in *Kerio Control*, refer to chapter 24.

- *Users* — users or groups that can be chosen in a special dialog

  The *Authenticated users* option makes the rule valid for all users authenticated to the firewall (see chapter 12.1). Use the *User(s) from domain* option to add users/groups from mapped directory services domains or from the local user database (for details, refer to chapter 17).

  > ***Hint:***
  > Users/groups from various domains can be added to a rule at a moment. Select a domain, add users/groups, choose another domain and repeat this process until all demanded users/groups are added.

  In traffic rules, user are represented by IP address of the host they are connected (authenticated) from. For detailed description on user authentication, refer to chapter 12.1.

  Note:

  1. If you require authentication for any rule, it is necessary to ensure that a rule exists to allow users to connect to the firewall authentication page. If users use each various hosts to connect from, IP addresses of all these hosts must be considered.
  2. If user accounts or groups are used as a source in the Internet access rule, automatic redirection to the authentication page nor NTLM authentication will work. Redirection requires successful establishment of connection to the destination server.
     If traffic policy is set like this, users must be told to open the authentication page (see chapters 13 and 12.1) in their browser and login before they are let into the Internet.
     This issue is described in detail in chapter 8.6.

- *Firewall* — a special address group including all interfaces of the host where *Kerio Control* is running. This option can be used for example to permit traffic between the local network and the *Kerio Control* host.

Use the *Any* button to replace all defined items with the *Any* item (this item is also used by default for all new rules). This item will be removed automatically when at least one new item is added.

Use the *Remove* button to remove all items defined (the *Nothing* value will be displayed in the item list). This is helpful when rules are changed — it is not necessary to remove items one by one. Whenever at least one item is added, the *Nothing* value will be removed automatically. If the *Nothing* value is kept for the *Source* or/and *Destination* item, a corresponding rule is disabled.

The *Nothing* value takes effect when network interfaces (see chapter 6) and users or groups (see chapter 17) are removed. The *Nothing* value is automatically used for all *Source*, *Destination* or/and *Service* items of rules where a removed interface (or a user account, a group or a service) has been used. Thus, all these rules are disabled.

Definition of rules with the *Nothing* value in any column is not of any use — it is more useful to use the checkbox in the *Name* column instead to disable a rule.

Note: Removed interfaces cannot be replaced by the *Any* value, otherwise the traffic policy might be changed fundamentally (e.g. an undesirable traffic might be allowed).

Service

Definition of service(s) on which the traffic rule will be applied. Any number of services defined either in *Configurations* → *Definitions* → *Services* (see chapter 16.3) or using protocol and port number (or by port range — a dash is used to specify the range) can be included in the list.

Use the *Any* button to replace all defined items with the *Any* item (this item is also used by default for all new rules). Whenever at least one new service is added, the *Any* value removed automatically.

Use the *Remove* button to remove all items defined (the *Nothing* value will be displayed in the item list). Whenever at least one service is added, the *Nothing* value will be removed automatically. If the *Nothing* value is kept in the *Service* column, the rule is disabled.

The *Nothing* value is important for removal of services (see chapter 16.3). The *Nothing* value is automatically used for the *Service* item of rules where a removed service has been used. Thus, all these rules are disabled. Inserting the *Nothing* value manually is not meaningful —a checking box in the *Name* column can be used instead.

Note: If there is a protocol inspector for a certain service in *Kerio Control*, it is applied to all corresponding traffic automatically. If desired to bypass the protocol inspector for certain traffic, it is necessary to define this exception in the particular traffic rule. For detailed information, see chapter 8.7.

Action, Log and DSCP

Action determines method that will be applied by *Kerio Control* when a given packet has passed all the conditions for the rule (the conditions are defined by the *Source*, *Destination* and *Service* items):

- *Permit* — traffic will be allowed by the firewall.
- *Deny* — client will be informed that access to the address or port is denied. The client will be warned promptly, however, it is informed that the traffic is blocked by firewall.
- *Drop* — all packets that fit this rule will be dropped by firewall. The client will not be sent any notification and will consider the action as a network outage. The action

is not repeated immediately by the client (the client expects a response and tries to connect later, etc.).

Note: It is recommended to use the *Deny* option to limit the Internet access for local users and the *Drop* option to block access from the Internet.

The following actions can be taken to log traffic:

- *Transferred Data Chart* — network traffic load timeline. These charts can be viewed under *Status* → *Traffic Charts* (see chapter 21.2).
- *Log packets* — packets matching the rule (permitted, denied or dropped, according to the rule definition) will be logged in the *Filter* log.
- *Log connections* — connections matching this rule will be logged in the *Connection* log (only for permit rules). Individual packets included in these connections will not be logged.

  Note: Connection cannot be logged for blocking and dropping rules (connection is not even established).

In allowed traffic, corresponding packets can be marked by a certain *DSCP* value. This value is used for bandwidth limiting (reducing of data transfer speed) or its reservation for the particular traffic (see 11). In "unmarked" packets, this item's value is *0*.

Translation

Source or/and destination IP address translation.

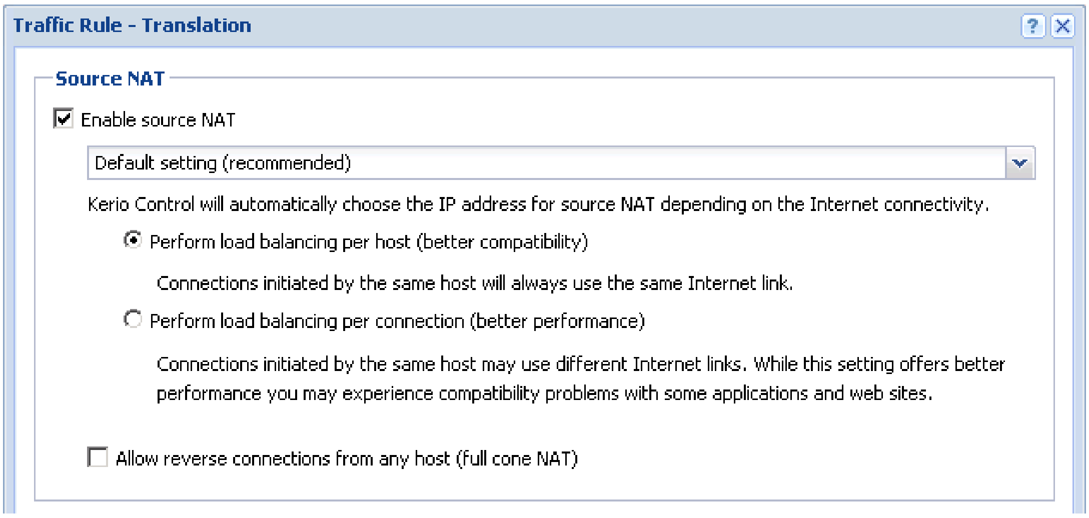
Source IP address translation (NAT — Internet connection sharing)

The source IP address translation can be also called IP masquerading or Internet connection sharing. The source (private) IP address is substituted by the IP address of the interface connected to the Internet in outgoing packets routed from the local network to the Internet. Therefore, the entire local network can access the Internet transparently, but it is externally considered as one host.

Source address translation is used in traffic rules applied to traffic from the local private network to the Internet. In other rules (traffic between the local network and the firewall, between the firewall and the Internet, etc.), NAT is meaningless. For detailed information and examples of rules, refer to chapter 8.4.

For source address translation, *Kerio Control* offers these options:

Automatic IP address selection



Traffic Rule - Translation

Source NAT

☑ Enable source NAT

Default setting (recommended)

Kerio Control will automatically choose the IP address for source NAT depending on the Internet connectivity.

● Perform load balancing per host (better compatibility)

Connections initiated by the same host will always use the same Internet link.

○ Perform load balancing per connection (better performance)

Connections initiated by the same host may use different Internet links. While this setting offers better performance you may experience compatibility problems with some applications and web sites.

□ Allow reverse connections from any host (full cone NAT)

Figure 8.2 Traffic rule — NAT — automatic IP address selection

By default, in packets sent from the LAN to the Internet the source IP address will be replaced by IP address of the Internet interface of the firewall through which the packet is sent. This IP address translation method is useful in the general rule for access from the LAN to the Internet (see chapter 8.4), because it works correctly in any Internet connection configuration and for any status of individual links (for details, see chapter 7).

If *Kerio Control* works in the mode of network traffic load balancing (see chapter 7.3), you can select a method which will be used for spreading the traffic between the LAN and the Internet over individual Internet links:

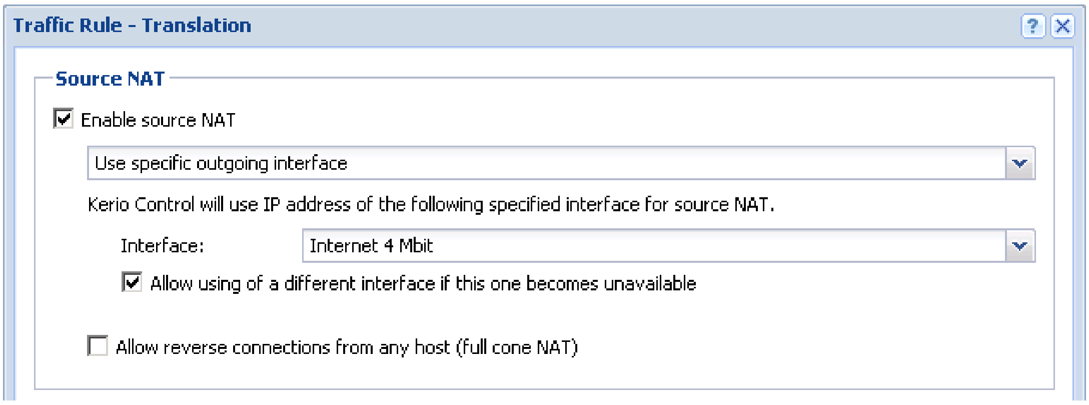
- *Load balancing per host* — all traffic from the specific host (client) in the LAN will always be routed via the same Internet link. All connections from the client will be established from the same source IP address (the public address of the particular interface of the firewall). This method is set as default, because it guarantees the same behavior as in case of clients connected directly to the Internet. However, load balancing dividing the traffic among individual links may be not optimal in this case.
- *Load balancing per connection* — for each connection established from the LAN to the Internet will be selected an Internet link to spread the load optimally. This method guarantees the most efficient use of the Internet connection's capacity. However, it might also introduce problems and collisions with certain services. The problem is that individual connections are established from various IP addresses (depending on the firewall's interface from which the packet is sent) which may be considered as an attack at the destination server which might result in closing of the session, blocking of the traffic, etc.

If another type of Internet connection is used (a single leased link, on demand dialing or connection failover), these options have no effect on *Kerio Control's* functionality.

Hint:
For maximal efficiency of the connection's capacity, it is possible to combine both load balancing methods. In the general rule for access from the LAN to the Internet, use load balancing per connection and add a rule for specific services (servers, clients, etc.) which will employ the load balancing per host method. For details, see also chapter 8.4.

NAT to IP address of a specific interface

It is possible to select a specific interface which will be used for the source NAT in outgoing packets. This also determines that packets will be sent to the Internet via this specific link. This allows definition of rules for sending of a specific traffic through a selected — so called *policy routing* — see chapter 8.5.


Traffic Rule - Translation

Source NAT

☑ Enable source NAT

Use specific outgoing interface

Kerio Control will use IP address of the following specified interface for source NAT.

Interface: Internet 4 Mbit

☑ Allow using of a different interface if this one becomes unavailable

□ Allow reverse connections from any host (full cone NAT)

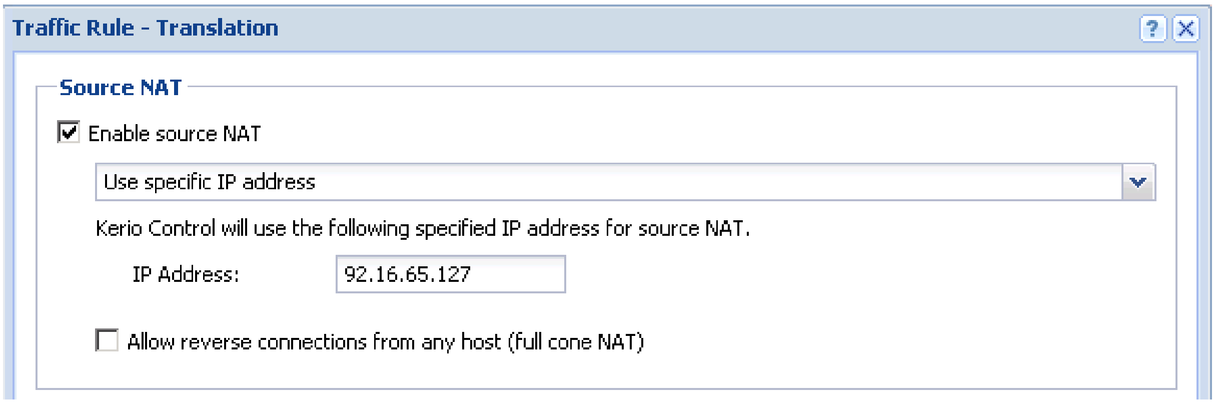
Figure 8.3 Traffic rule — NAT — NAT with specific interface (its IP address)

If the selected Internet link fails, Internet will be unavailable for all traffic meeting criteria (specific services, clients, etc.) specified by this rule. To prevent from such situations, it is possible to allow use of an alternative (back-up) interface (link) for cases of the link's failure. If set as suggested, *Kerio Control* will behave like in mode of automatic interface selection (see above) if the such failure occurs.

NAT with a specified IP address

It is also possible to specify an IP address for NAT which will be used as the source IP address for all packets sent from the LAN to the Internet. This option is available above all to keep the environment compatible with older *Kerio Control* versions. However, use of a fixed IP address has many limitations:

- It is necessary to use an IP address of one of the firewall's Internet interfaces. If any other address is used (including even local private addresses). NAT will not work correctly and packets sent to the Internet will be dropped.
- For obvious reasons, specific IP address cannot be used for NAT in the Internet connection failover and the network traffic load balancing modes.



Traffic Rule - Translation

Source NAT

☑ Enable source NAT

Use specific IP address

Kerio Control will use the following specified IP address for source NAT.

IP Address: 92.16.65.127

☐ Allow reverse connections from any host (full cone NAT)

Figure 8.4 Traffic rule — NAT — NAT with specific IP address

Full cone NAT

For all NAT methods it is possible to set mode of allowing of incoming packets coming from any address — so called *Full cone NAT*.

If this option is off, *Kerio Control* performs so called *Port restricted cone NAT*. In outgoing packets transferred from the local network to the Internet, *Kerio Control* replaces the source IP address of the particular interface by public address of the firewall (see above). If possible, the original source port is kept; otherwise, another free source port is assigned. As to incoming traffic, only packets sent from the same IP address and port from which the outgoing packet was sent are let in. This translation method guarantees high security — the firewall will not let in any packet which is not a response to the sent request.

However, many applications (especially applications working with multimedia, Voice over IP technologies, etc.) use another traffic method where other clients can (with direct connection established) connect to a port "opened" by an outgoing packet. Therefore, *Kerio Control* supports also the *Full cone NAT* mode where the described restrictions are not applied for incoming packets. The port then lets in incoming packets with any source IP address and port. This translation method allows running of applications in the private network that would either work only partially or they would not work at all.

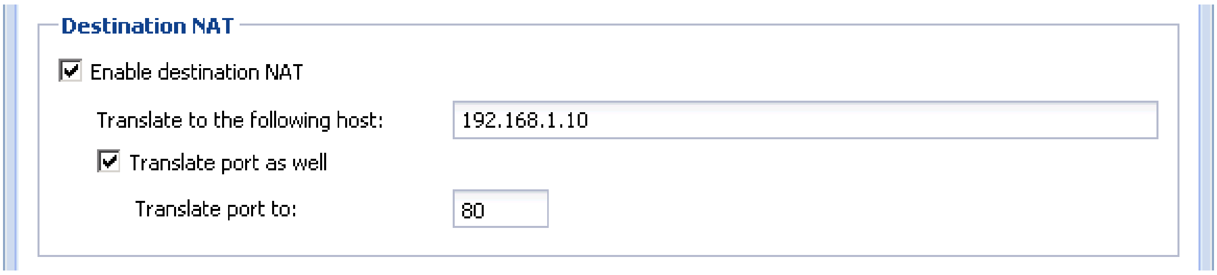
For example of using of *Full cone NAT* for VoIP applications, refer to chapter 8.8.

Warning:
Use of *Full cone NAT* brings certain security threats — the port opened by outgoing connection can be accessed without any restrictions being applied. For this reason, it is recommended to enable *Full cone NAT* only for a specific service (i.e. to create a special rule for this purpose).
By any means do not allow Full cone NAT in the general rule for traffic from the local network to the Internet[4]*!* Such rule would significantly decrease security of the local network.

Destination NAT (port mapping):

Destination address translation (also called port mapping) is used to allow access to services hosted in private local networks behind the firewall. All incoming packets that meet defined rules are re-directed to a defined host (destination address is changed). This actually "moves" to the Internet interface of the *Kerio Control* host (i.e. IP address it is mapped from). From the client's point of view, the service is running on the IP address from which it is mapped (usually on the firewall's IP address).

Options for destination NAT (port mapping):



Destination NAT

☑ Enable destination NAT

Translate to the following host: 192.168.1.10

☑ Translate port as well

Translate port to: 80

Figure 8.5 Traffic rule — destination address translation

- *No Translation* — destination address will not be modified.
- *Translate to* — IP address that will substitute the packet's destination address. This address also represents the IP address of the host on which the service is actually running.

  The *Translate to* entry can be also specified by DNS name of the destination computer. In such cases *Kerio Control* finds a corresponding IP address using a DNS query.

  > ***Warning:***
  > We recommend you not to use names of computers which are not recorded in the local DNS since rule is not applied until a corresponding IP address is found. This might cause temporary malfunction of the mapped service.

- *Translate port to* — during the process of IP translation you can also substitute the port of the appropriate service. This means that the service can run at a port that is different from the port where it is available from the Internet.

  Note: This option cannot be used unless only one service is defined in the *Service* entry within the appropriate traffic rule and this service uses only one port or port range.

For examples of traffic rules for port mapping and their settings, refer to chapter 8.4.

Valid on

Time interval within which the rule will be valid. Apart from this interval *Kerio Control* ignores the rule.

The special *Always* option can be used to disable the time limitation (nothing is displayed in the *Traffic Policy* dialog).

When a denying rule is applied and/or when an allowing rule's appliance terminates, all active network connections matching the particular rule are closed immediately.

Protocol inspector

Selection of a protocol inspector that will be applied on all traffic meeting the rule. The menu provides the following options to select from:

- *Default* — all necessary protocol inspectors (or inspectors of the services listed in the *Service* entry) will be applied on traffic meeting this rule.
- *None* — no inspector will be applied (regardless of how services used in the *Service* item are defined).
- *Other* — selection of a particular inspector which will be applied to traffic meeting this rule (all *Kerio Control's* protocol inspectors are available). No other protocol inspector will be applied to the traffic, regardless of settings of services in the *Service* section.

  Do not use this option unless the appropriate traffic rule defines a protocol belonging to the inspector. Functionality of the service might be affected by using an inappropriate inspector.

  For more information, refer to chapter 8.7.

Note: Use the *Default* option for the *Protocol Inspector* item if a particular service (see the *Service* item) is used in the rule definition (the protocol inspector is included in the service definition).

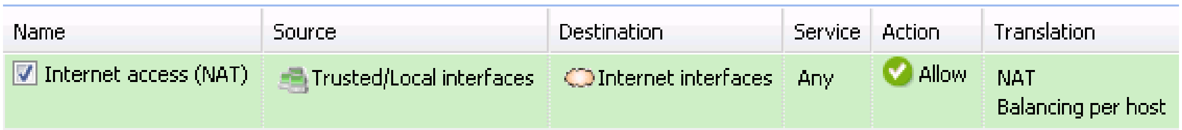
8.4 Basic Traffic Rule Types

Kerio Control traffic policy provides a range of network traffic filtering options. In this chapter you will find some rules used to manage standard configurations. Using these examples you can easily create a set of rules for your network configuration.

IP Translation (NAT)

IP translation (as well as Internet connection sharing) is a term used for the exchange of a private IP address in a packet going out from the local network to the Internet with the IP address of the Internet interface of the *Kerio Control* host. This technology is used to connect local private networks to the Internet by a single public IP address.

The following example shows an appropriate traffic rule:



Name	Source	Destination	Service	Action	Translation
☑ Internet access (NAT)	Trusted/Local interfaces	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.6 A typical traffic rule for NAT (Internet connection sharing)

Source

The *Trusted / Local interfaces* group. This group includes all segments of the LAN connected directly to the firewall. If access to the Internet from some segments is supposed to be blocked, the most suitable group to file the interface into is *Other interfaces*.

If the local network consists of cascaded segments (i.e. it includes other routers), it is not necessary to customize the rule in accordance with this fact — it is just necessary to set routing correctly (see chapter 19.1).

Destination

The *Internet interfaces* group. With this group, the rule is usable for any type of Internet connection (see chapter 7) and it is not necessary to modify it even it Internet connection is changed.

Service

This entry can be used to define global limitations for Internet access. If particular services are defined for IP translations, only these services will be used for the IP translations and other Internet services will not be available from the local network.

Action

To validate a rule one of the following three actions must be defined: Permit, Drop, Deny.

Translation

In the *Source NAT* section select the *Default settings* option (the primary IP address of the interface via which packets go out from the *Kerio Control* host will be used for NAT). This also guarantees versatility of this rule — IP address translation will always be working correctly, regardless the Internet connection type and the particular link type via which the packet will be sent to the Internet.

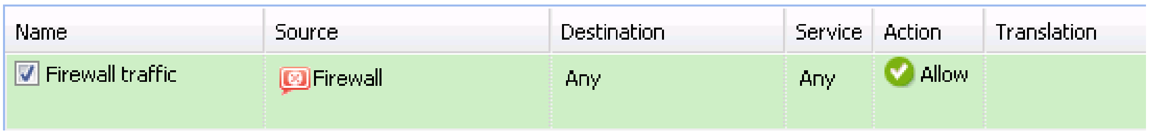
> ***Warning:***
> The *No translation* option should be set in the *Destination address translation* section, otherwise the rule might not function. Combining source and destination IP address translation is relevant under special conditions only.

Placing the rule

The rule for destination address translation must be preceded by all rules which deny access to the Internet from the local network.

Note: Such a rule allows access to the Internet from any host in the local network, not from the firewall itself (i.e. from the *Kerio Control* host)!

Traffic between the firewall and the Internet must be enabled by a special rule. Since *Kerio Control* host can access the Internet directly, it is not necessary to use NAT.



Name	Source	Destination	Service	Action	Translation
☑ Firewall traffic	Firewall	Any	Any	✓ Allow	

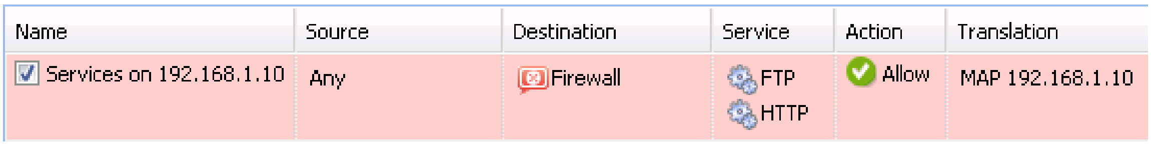
Figure 8.7 Rule for traffic between the firewall and hosts in the Internet

Port mapping

Port mapping allows services hosted on the local network (typically in private networks) to become available over the Internet. The locally hosted server would behave as if it existed directly on the Internet (public address of the *Kerio Control* host).

Kerio Control allows to access mapped services also from local networks. This avoids problems with different DNS records for the Internet and the local network.

Traffic rule for port mapping can be defined as follows:



Name	Source	Destination	Service	Action	Translation
☑ Services on 192.168.1.10	Any	Firewall	FTP HTTP	✓ Allow	MAP 192.168.1.10

Figure 8.8 Traffic rule that makes the local web server available from the Internet

Source

Mapped services can be accessed by clients both from the Internet and from the local network. For this reason, it is possible to keep the *Any* value in the *Source* entry (or it is possible to list all relevant interface groups or individual groups — e.g. *Internet* and *LAN*).

Destination

The *Kerio Control* host labeled as *Firewall*, which represents all IP addresses bound to the firewall host.
This service will be available at all addresses of the interface connected to the Internet. To make the service available at a particular IP address, use the *Host* option and specify the IP address (see the multihoming example).

Service

Services to be available. You can select one of the predefined services (see chapter 16.3) or define an appropriate service with protocol and port number.
Any service that is intended to be mapped to one host can be defined in this entry. To map services for other hosts you will need to create a new traffic rule.

Action

Select the *Allow* option, otherwise all traffic will be blocked and the function of port mapping will be irrelevant.

Translation

In the *Destination NAT (Port Mapping)* section select the *Translate to IP address* option and specify the IP address of the host within the local network where the service is running.

Using the *Translate port to* option you can map a service to a port which is different from the one where the service is available from the Internet.

> ***Warning:***
> In the *Source NAT* section should be set to the *No Translation* option. Combining source and destination IP address translation is relevant under special conditions only.

Note: For proper functionality of port mapping, the locally hosted server must point to the *Kerio Control* firewall as the default gateway. Port mapping will not function well unless this condition is met.

Placing the rule

As already mentioned, mapped services can be accessed also from the local network. During access from the local network, connection is established from the local (private) IP address to an IP address in the Internet (the firewall's public IP address). If the rule for mapped service is preceded by a rule allowing access from the local network to the Internet, according to this rule the packet would be directed to the Internet and then dropped. Therefore, it is recommended to put all rules for mapped services *at the top* of the table of traffic rules.

Note: If there are separate rules limiting access to mapped services, these rules must precede mapping rules. It is usually possible to combine service mapping and access restriction in a single rule.

Multihoming

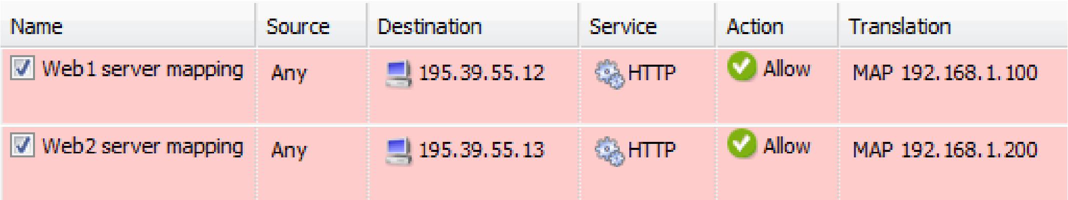
Multihoming is a term used for situations when one network interface connected to the Internet uses multiple public IP addresses. Typically, multiple services are available through individual IP addresses (this implies that the services are mutually independent).

Let us suppose that in the local network a web server `web1` with IP address `192.168.1.100` and a web server `web2` with IP address `192.168.1.200` are running in the local network. The interface connected to the Internet uses public IP addresses `195.39.55.12` and `195.39.55.13`. We want the server `web1` to be available from the Internet at the IP address `195.39.55.12`, the server `web2` at the IP address `195.39.55.13`.

The two following traffic rules must be defined in *Kerio Control* to enable this configuration:

Source

Any (see the previous example referring to mapping of single service).



Name	Source	Destination	Service	Action	Translation
☑ Web1 server mapping	Any	195.39.55.12	HTTP	✓ Allow	MAP 192.168.1.100
☑ Web2 server mapping	Any	195.39.55.13	HTTP	✓ Allow	MAP 192.168.1.200

Figure 8.9 Multihoming — web servers mapping

Destination

An appropriate IP address of the interface connected to the Internet (use the *Host* option for insertion of an IP address).

Service

Service which will be available through this interface (the *HTTP* service in case of a Web server).

Action

Select the *Allow* option, otherwise all traffic will be blocked and the function of port mapping will be irrelevant.

Translation

Go to the *Destination NAT (Port Mapping)* section, select the *Translate to IP address* option and specify IP address of a corresponding Web server (`web1` or `web2`).

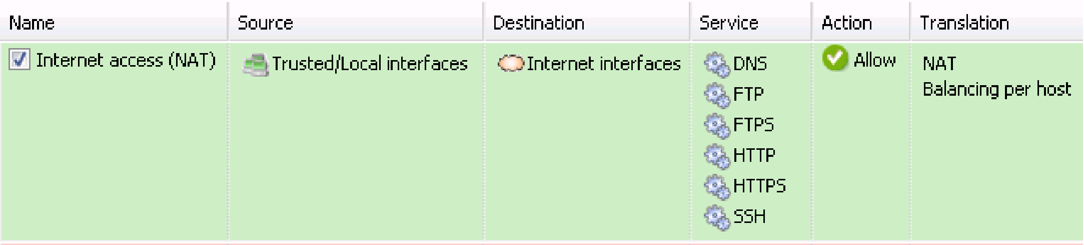
Limiting Internet Access

Sometimes, it is helpful to limit users access to the Internet services from the local network. Access to Internet services can be limited in several ways. In the following examples, the limitation rules use IP translation. There is no need to define other rules as all traffic that would not meet these requirements will be blocked by the default "catch all" rule.

Other methods of Internet access limitations can be found in the *Exceptions* section (see below).

Note: Rules mentioned in these examples can be also used if *Kerio Control* is intended as a neutral router (no address translation) — in the *Translation* entry there will be no translations defined.

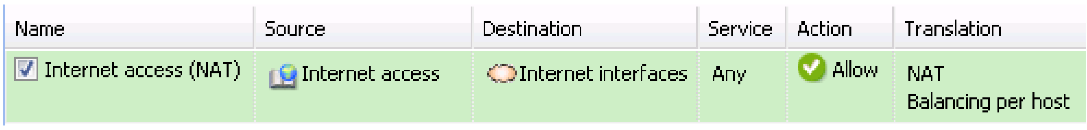
1. Allow access to selected services only. In the translation rule in the *Service* entry specify only those services that are intended to be allowed.



Name	Source	Destination	Service	Action	Translation
☑ Internet access (NAT)	Trusted/Local interfaces	Internet interfaces	DNS FTP FTPS HTTP HTTPS SSH	✓ Allow	NAT Balancing per host

Figure 8.10 Internet connection sharing — only selected services are available

2. Limitations sorted by IP addresses. Access to particular services (or access to any Internet service) will be allowed only from selected hosts. In the *Source* entry define the group of IP addresses from which the Internet will be available. This group must be formerly defined in *Configuration → Definitions → Address Groups* (see chapter 17.5).

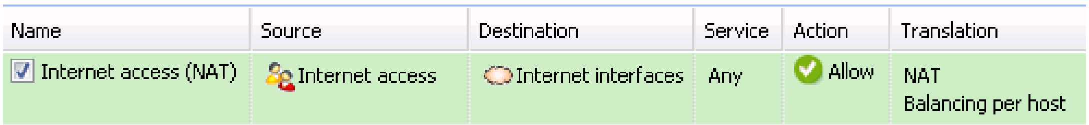


Name	Source	Destination	Service	Action	Translation
☑ Internet access (NAT)	Internet access	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.11 Only selected IP address group(s) is/are allowed to connect to the Internet

Note: This type of rule should be used only if each user has his/her own host and the hosts have static IP addresses.

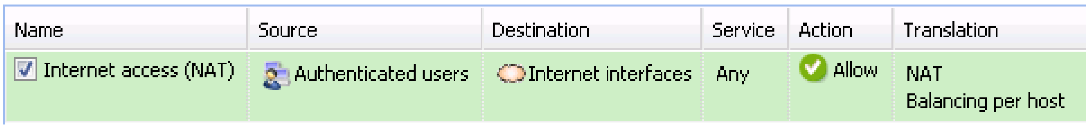
3. Limitations sorted by users. Firewall monitors if the connection is from an authenticated host. In accordance with this fact, the traffic is permitted or denied.



Name	Source	Destination	Service	Action	Translation
☑ Internet access (NAT)	Internet access	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.12 Only selected user group(s) is/are allowed to connect to the Internet

Alternatively you can define the rule to allow only authenticated users to access specific services. Any user that has a user account in *Kerio Control* will be allowed to access the Internet after authenticating to the firewall. Firewall administrators can easily monitor which services and which pages are opened by each user (it is not possible to connect anonymously).



Name	Source	Destination	Service	Action	Translation
☑ Internet access (NAT)	Authenticated users	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.13 Only authenticated users are allowed to connect to the Internet

For detailed description on user authentication, refer to chapter 12.1.

Note:

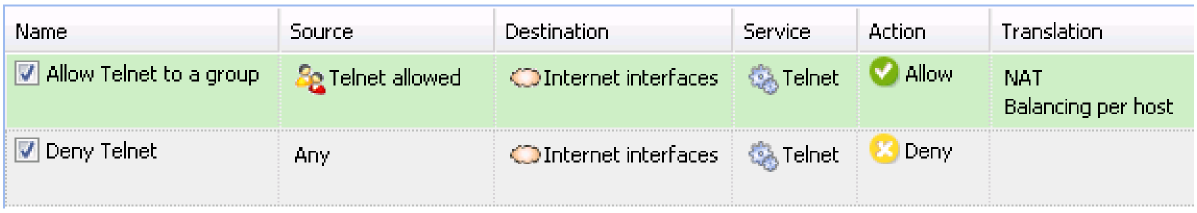
1. The rules mentioned above can be combined in various ways (i.e. a user group can be allowed to access certain Internet services only).
2. Usage of user accounts and groups in traffic policy follows specific rules. For detailed description on this topic, refer to chapter 8.6.

Exclusions

You may need to allow access to the Internet only for a certain user/address group, whereas all other users should not be allowed to access this service.

This will be better understood through the following example (how to allow a user group to use the *Telnet* service for access to servers in the Internet). Use the two following rules to meet these requirements:

- First rule will deny selected users (or a group of users/IP addresses, etc.) to access the Internet.
- Second rule will deny the other users to access this service.



Name	Source	Destination	Service	Action	Translation
☑ Allow Telnet to a group	Telnet allowed	Internet interfaces	Telnet	✓ Allow	NAT Balancing per host
☑ Deny Telnet	Any	Internet interfaces	Telnet	✗ Deny	

Figure 8.14 Exception — Telnet is available only for selected user group(s)

8.5 Policy routing

If the LAN is connected to the Internet by multiple links with load balancing (see chapter 7.3), it may be needed that one link is reserved for a certain traffic, leaving the rest of the load for the other links. Such a measure is useful if it is necessary to keep important traffic swinging (email traffic, the informational system, etc.), i.e. not slowed down by secondary or even marginal traffic (web browsing, online radio channels, etc.). To meet this crucial requirement of an enterprise data traffic, it is necessary to consider and employ, besides the destination IP address, additional information when routing packets from the LAN to the Internet, such as source IP address, protocol, etc. This approach is called *policy routing*.

In *Kerio Control*, policy routing can be defined by conditions in traffic rules for Internet access with IP address translation (NAT). This approach brings wide range of options helping to meet all requirements for routing and network load balancing.

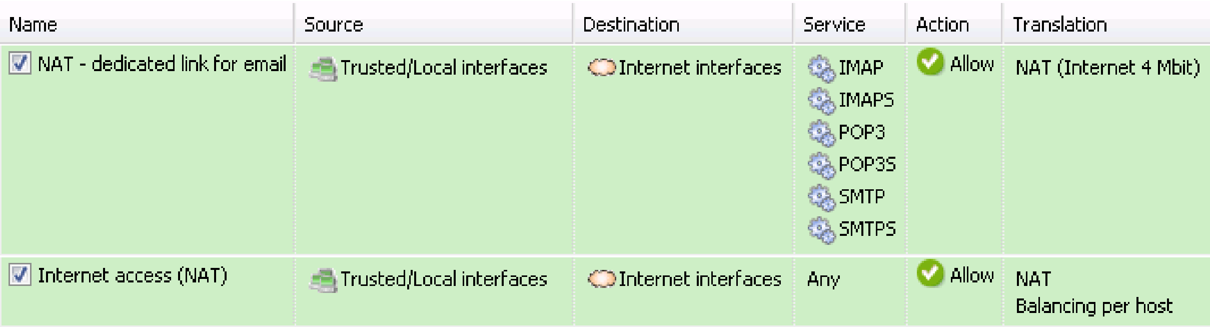
Note: Policy routing traffic rules are of higher priority than routes defined in the routing table (see chapter 19.1).

Example: A link reserved for email traffic

Let us suppose that the firewall is connected to the Internet by two links with load balancing with speed values of *4 Mbit/s* and *8 Mbit/s*. One of the links is connected to the provider where the mailserver is also hosted. Therefore, it is desirable that all email traffic (*SMTP*, *IMAP*, *POP3* protocols and their secured versions) is routed through this link.

Define the following traffic rules to meet these requirements:

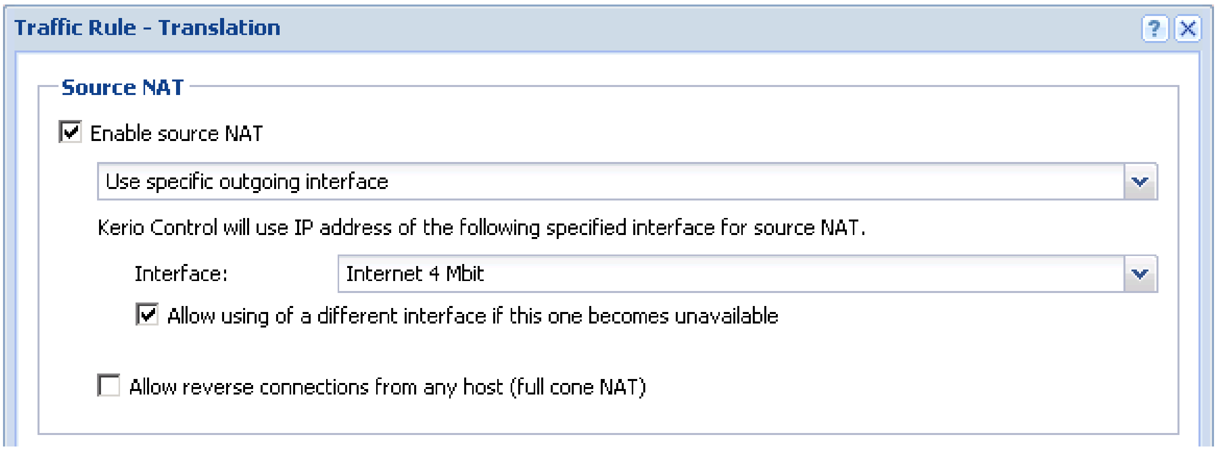
- First rule defines that NAT is applied to email services and the *Internet 4 Mbit* interface is used.
- The other rule is a general NAT rule with automatic interface selection (see chapter 8.4).



Name	Source	Destination	Service	Action	Translation
☑ NAT - dedicated link for email	Trusted/Local interfaces	Internet interfaces	IMAP IMAPS POP3 POP3S SMTP SMTPS	✓ Allow	NAT (Internet 4 Mbit)
☑ Internet access (NAT)	Trusted/Local interfaces	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.15 Policy routing — a link reserved for email traffic

Setting of NAT in the rule for email services is shown in figure 8.16. It is recommended to allow use of a back-up link for case that the reserved link fails. Otherwise, email services will be unavailable when the connection fails.



Traffic Rule - Translation

Source NAT

☑ Enable source NAT

Use specific outgoing interface

Kerio Control will use IP address of the following specified interface for source NAT.

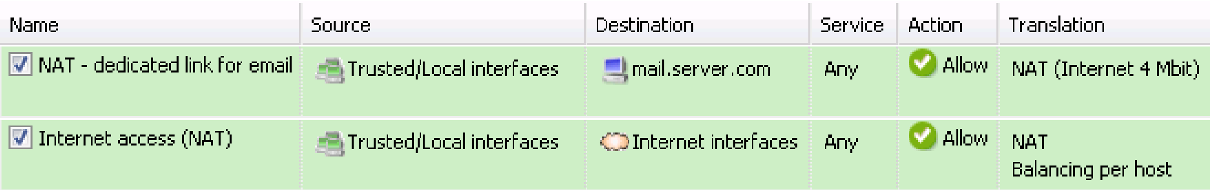
Interface: Internet 4 Mbit

☑ Allow using of a different interface if this one becomes unavailable

☐ Allow reverse connections from any host (full cone NAT)

Figure 8.16 Policy routing — setting NAT for a reserved link

Let us suppose that the mailserver provides also *Webmail* and *CalDAV* services which use *HTTP(s)* protocol. Adding these protocols in the first rule would make all web traffic routed through the reserved link. To reach the desired goal, the rule can be modified by reserving the link for traffic with a specific server — see figure 8.17.



Name	Source	Destination	Service	Action	Translation
☑ NAT - dedicated link for email	Trusted/Local interfaces	mail.server.com	Any	✓ Allow	NAT (Internet 4 Mbit)
☑ Internet access (NAT)	Trusted/Local interfaces	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.17 Policy routing — a link reserved for a specific server

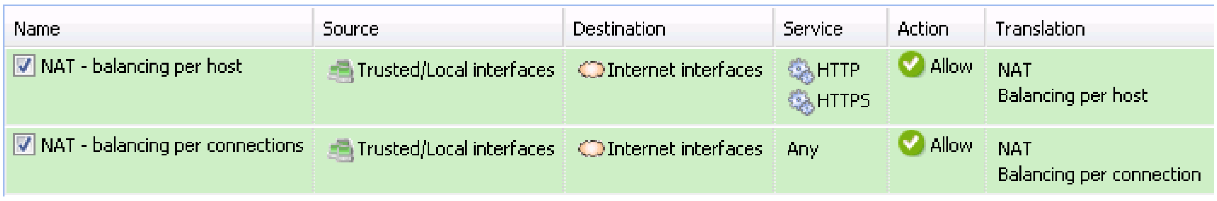
Note: In the second rule, automatic interface selection is used. This means that the *Internet 4Mbit* link is also used for network traffic load balancing. Email traffic is certainly still respected and has higher priority on the link reserved by the first rule. This means that total load will be efficiently balanced between both links all the time.
If you need to reserve a link *only* for a specific traffic (i.e. route other traffic through other links), go to*Configuration* → *Interfaces* and set the speed of the link to *0 Mbit/s*. In this case the link will not be used for automatic load balancing. Only traffic specified in corresponding traffic rules will be routed through it.

Example: Optimization of network traffic load balancing

Kerio Control provides two options of network traffic load balancing: per host (clients) or per connection (for details, refer to chapter 8.3). With respect to variability of applications on individual hosts and of user behavior, the best solution (more efficient use of individual links) proves to be the option of load balancing per connection. However, this mode may encounter problems with access to services where multiple connections get established at one moment (web pages and other web related services). The server can consider source addresses in individual connections as connection recovery after failure (this may lead for instance to expiration of the session) or as an attack attempt (in that case the service can get unavailable).

This problem can be bridged over by policy routing. In case of “problematic” services (e.g. *HTTP* and *HTTPS*) the load will be balanced per host, i.e. all connections from one client will be routed through a particular Internet link so that their IP address will be identical (a single IP address will be used). To any other services, load balancing per connection will be applied — thus maximally efficient use of the capacity of available links will be reached.

Meeting of the requirements will be guaranteed by using two NAT traffic rules — see figure 8.18. In the first rule, specify corresponding services and set the *per host* NAT mode. In the second rule, which will be applied for any other services, set the *per connection* NAT mode.



Name	Source	Destination	Service	Action	Translation
☑ NAT - balancing per host	Trusted/Local interfaces	Internet interfaces	HTTP HTTPS	✓ Allow	NAT Balancing per host
☑ NAT - balancing per connections	Trusted/Local interfaces	Internet interfaces	Any	✓ Allow	NAT Balancing per connection

Figure 8.18 Policy routing — load balancing optimization

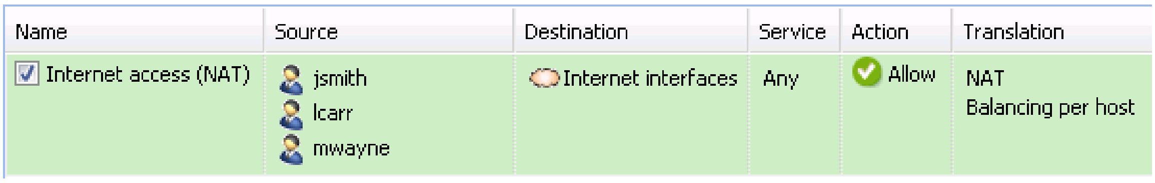
8.6 User accounts and groups in traffic rules

In traffic rules, source/destination can be specified also by user accounts or/and user groups. In traffic policy, each user account represents IP address of the host from which user is connected. This means that the rule is applied to users authenticated at the firewall only (when the user logs out, the rule is not effective any longer). This chapter is focused on various issues relating to use of user accounts in traffic rules as well as hints for their solution.

Note: For detailed information on traffic rules definition, refer to chapter 8.3.

How to enable certain users to access the Internet

How to enable access to the Internet for specific users only? Assuming that this problem applies to a private local network and Internet connection is performed through NAT, simply specify these users in the *Source* item in the NAT rule.



Name	Source	Destination	Service	Action	Translation
☑ Internet access (NAT)	jsmith lcarr mwayne	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.19 This traffic rule allows only selected users to connect to the Internet

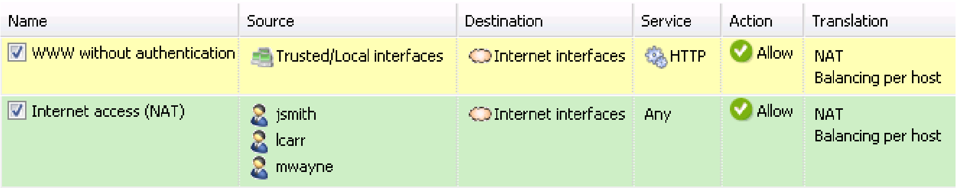
Such a rule enables the specified users to connect to the Internet (if authenticated). However, these users must open the *Kerio Control* interface's login page manually and authenticate (for details, see chapter 12.1).

However, with such a rule defined, all methods of automatic authentication will be ineffective (i.e. redirecting to the login page, NTLM authentication as well as automatic authentication from defined hosts). Automatic authentication (redirection to the login page) is performed at the very moment of establishing connection to the Internet. However, this NAT rule blocks any connection unless the user is authenticated.

Enabling automatic authentication

The automatic user authentication issue can be solved easily as follows:

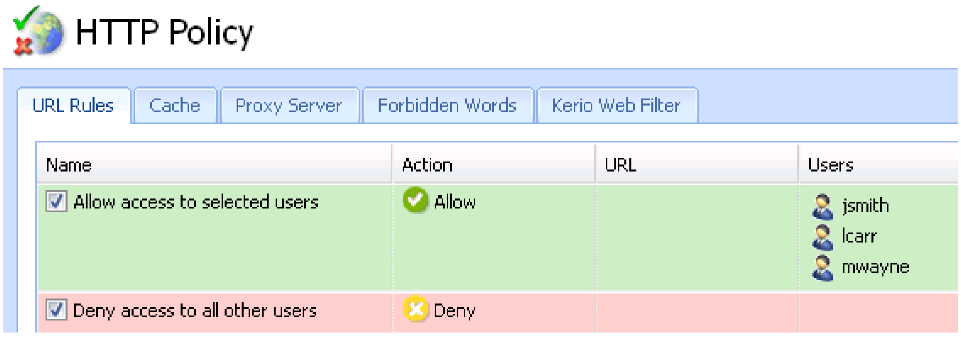
- Add a rule allowing an unlimited access to the *HTTP* service before the NAT rule.



Name	Source	Destination	Service	Action	Translation
☑ WWW without authentication	Trusted/Local interfaces	Internet interfaces	HTTP	✓ Allow	NAT Balancing per host
☑ Internet access (NAT)	jsmith lcarr mwayne	Internet interfaces	Any	✓ Allow	NAT Balancing per host

Figure 8.20 These traffic rules enable automatic redirection to the login page

- In URL rules (see chapter 14.2), allow specific users to access any Web site and deny any access to other users.



Name	Action	URL	Users
☑ Allow access to selected users	✓ Allow		jsmith lcarr mwayne
☑ Deny access to all other users	✗ Deny		

Figure 8.21 These URL rules enable specified users to access any Web site

User not authenticated yet who attempts to open a Web site will be automatically redirected to the authentication page (or authenticated by NTLM, or logged in from the corresponding host). After a successful authentication, users specified in the *NAT* rule (see figure 8.20) will be allowed to access also other Internet services. As well as users not specified in the rules, unauthenticated users will be disallowed to access any Web site or/and other Internet services.

Note: In this example, it is assumed that client hosts use the *Kerio Control DNS Forwarder* or local DNS server (traffic must be allowed for the DNS server). If client stations used a DNS server in the Internet (this configuration is not recommended!), it would be necessary to include the *DNS* service in the rule which allows unlimited Internet access.

8.7 Partial Retirement of Protocol Inspector

Under certain circumstances, appliance of a protocol inspector to a particular communication might be undesirable. To disable specific protocol inspection, define corresponding source and destination IP addresses and a traffic rule for this service that will define explicitly that no protocol inspector will be used.

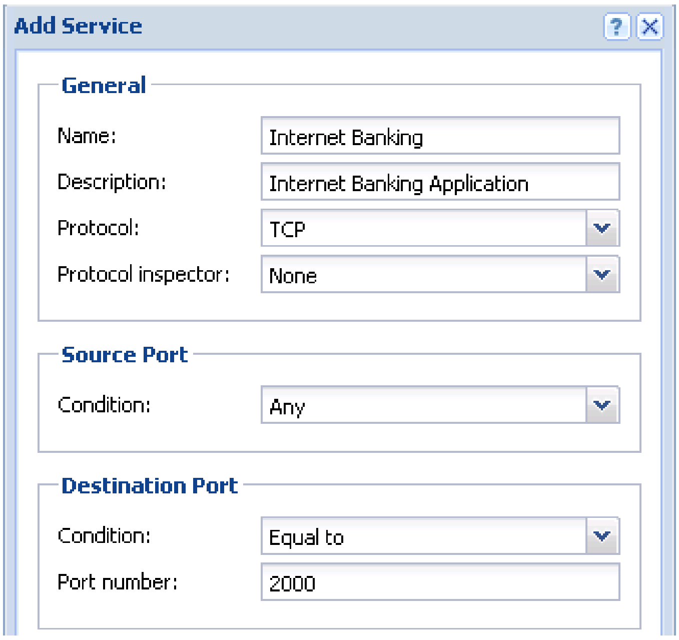
Example

A banking application (client) communicates with the bank's server through its proper protocol which uses TCP protocol at the port 2000. Supposing the banking application is run on a host with IP address `192.168.1.15` and it connects to the server `server.bank.com`.

This port is used by the *Cisco SCCP* protocol. The protocol inspector of the *SCCP* would be applied to the traffic of the banking client under normal circumstances. However, this might affect functionality of the application or endanger its security.

A special traffic rule, as follows, will be defined for all traffic of the banking application:

1. In the *Configuration* → *Definitions* → *Services* section, define a service called *Internet Banking*: this service will use TCP protocol at the port 2000 and no protocol inspector is used by this communication.



Add Service

General

Name:	Internet Banking
Description:	Internet Banking Application
Protocol:	TCP
Protocol inspector:	None

Source Port

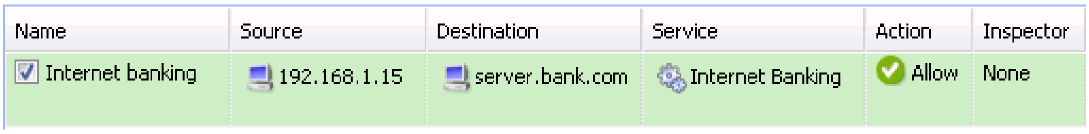
Condition:	Any

Destination Port

Condition:	Equal to
Port number:	2000

Figure 8.22 Service definition without inspector protocol

2. In the *Configuration* → *Traffic Policy* → *Traffic Rules* section, create a rule which will permit this service traffic between the local network and the bank's server. Specify that no protocol inspector will be applied.



Name	Source	Destination	Service	Action	Inspector
☑ Internet banking	192.168.1.15	server.bank.com	Internet Banking	✓ Allow	None

Figure 8.23 This traffic rule allows accessing service without protocol inspection

Warning:
To disable a protocol inspector, it is not sufficient to define a service that would not use the inspector! Protocol inspectors are applied to all traffic performed by corresponding protocols by default. To disable a protocol inspector, special traffic rules must be defined.

8.8 Use of Full cone NAT

However, many applications (especially applications working with multimedia, Voice over IP technologies, etc.) use another traffic method where other clients can (with direct connection established) connect to a port "opened" by an outgoing packet. For these cases, *Kerio Control* includes a special mode of address translation, known as *Full cone NAT*. In this mode, opened port can be accessed from any IP address and the traffic is always redirected to a corresponding client in the local network.

Use of *Full cone NAT* may bring certain security risk. Each connection established in this mode opens a possible passage from the Internet to the local network. To keep the security as high as possible, it is therefore necessary to enable *Full cone NAT* for particular clients and services only. The following example refers to an IP telephone with the SIP protocol.

Note: For details on traffic rules definition, refer to chapter 8.3.

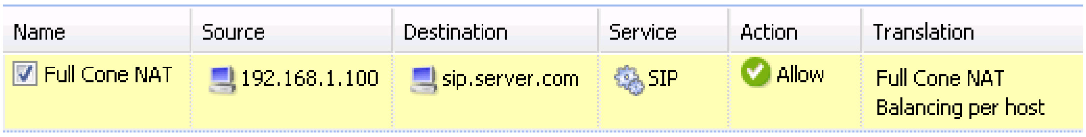
Example: SIP telephone in local network

In the local network, there is an IP telephone registered to an SIP server in the Internet. The parameters may be as follows:

- IP address of the phone: `192.168.1.100`
- Public IP address of the firewall: `195.192.33.1`
- SIP server: `sip.server.com`

Since the firewall performs IP address translation, the telephone is registered on the SIP server with the firewall's public address (`195.192.33.1`). If there is a call from another telephone to this telephone, the connection will go through the firewall's address (`195.192.33.1`) and the corresponding port. Under normal conditions, such connection can be established only directly from the SIP server (to which the original outgoing connection for the registration was established). However, use of *Full cone NAT* allows such connection for any client calling to the SIP telephone in the local network.

Full cone NAT will be enabled by an extremely restrictive traffic rule (to keep the security level as high as possible):



Name	Source	Destination	Service	Action	Translation
☑ Full Cone NAT	192.168.1.100	sip.server.com	SIP	✓ Allow	Full Cone NAT Balancing per host

Figure 8.24 Definition of a Full cone NAT traffic rule

- *Source* — IP address of an SIP telephone in the local network.
- *Destination* — name or IP address of an SIP server in the Internet. *Full cone NAT* will apply only to connection with this server.
- *Service* — *SIP* service (for an SIP telephone). *Full cone NAT* will not apply to any other services.
- *Action* — traffic must be allowed.
- *Translation* — select a source NAT method (see chapter 8.3) and enable the *Allow returning packets from any host (Full cone NAT)* option.

Rule for *Full cone NAT* must precede the general rule with NAT allowing traffic from the local network to the Internet.

8.9 Media hairpinning

Kerio Control allows to "arrange" traffic between two clients in the LAN which "know each other" only from behind the firewall's public IP address. This feature of the firewall is called *hairpinning* (with the *hairpin* root suggesting the packet's "U-turn" back to the local network). Used especially for transmission of voice or visual data, it is also known as *media hairpinning*.

Example: Two SIP telephones in the LAN

Let us suppose two SIP telephones are located in the LAN. These telephones authenticate at a SIP server in the Internet. The parameters may be as follows:

- IP addresses of the phones: `192.168.1.100` and `192.168.1.101`
- Public IP address of the firewall: `195.192.33.1`
- SIP server: `sip.server.com`

For the telephones, define corresponding traffic rules — see chapter 8.8 (as apparent from figure8.24, simply specify *Source* of the *Full cone NAT* traffic rule by IP address of the other telephone).

Both telephones will be registered on SIP server under the firewall's public IP address (`195.192.33.1`). If these telephones establish mutual connection, data packets (for voice transmission) from both telephones will be sent to the firewall's public IP address (and to the port of the other telephone). Under normal conditions, such packets would be dropped. However, *Kerio Control* is capable of using a corresponding record in the NAT table to recognize that a packet is addressed to a client in the local network. Then it translates the destination IP address and sends the packet back to the local network (as well as in case of port mapping). This ensures that traffic between the two phones will work correctly.

Note:

1. Hairpinning requires traffic between the local network and the Internet being allowed (before processed by the firewall, packets use a local source address and an Internet destination address — i.e. this is an outgoing traffic from the local network to the Internet). In default traffic rules created by the wizard (see chapter 8.1), this condition is met by the *NAT* rule.
2. In principle, hairpinning does not require that *Full cone NAT* is allowed (see chapter 8.8). However, in our example, *Full cone NAT* is required for correct functioning of the *SIP* protocol.

Chapter 9

Firewall and Intrusion Prevention System

9.1 Network intrusion prevention system (IPS)

Kerio Control integrates *Snort*, an intrusion detection and prevention system (IDS/IPS) protecting the firewall and the local network from known network intrusions. In *Kerio Control*, the system name is simplified for *Intrusion Prevention* (the name includes meaning of both functions — no prevention measures can be taken without detection).

What the intrusion prevention system is for and how it works

Network intrusion is undesirable network traffic impacting on functionality or security of the victim-host. Its purpose is mostly to get illegitimate access or/and to exploit fragile data. A typical attribute of such intrusions is their apparent legitimacy and it is difficult to uncover such traffic and filter it simply out by traffic rules. Let us use *DoS* intrusion (*Denial of Service*) as an example. In this type of intrusion, too many connections are established on a port to use up the system resources of the server application so that no other users can connect there. However, the firewall considers this act only as an access to an allowed port.

Therefore, sophisticated analysis of network traffic is needed here to detect network intrusions. Network intrusion detection systems use databases of known intrusions (this is similar to antivirus programs using databases of known viruses). Thanks to regular update of the database, new intrusion types are also recognized.

In the current version of *Kerio Control*, the intrusion prevention system works on all network interfaces included in the *Internet interfaces* group (see chapter 6). This implies that it detects and blocks network intrusions coming from the Internet, not from hosts in local networks or VPN clients (these hosts are considered as trusted).

For correct functionality of the intrusion prevention system, use of NAT is required (for details on NAT, see chapter 8.3). It can therefore be used for all typical configurations where *Kerio Control* is used for protection of local network. If *Kerio Control* is implemented as so called neutral router (without IP address translation), the intrusion prevention system will not work correctly.

Intrusion detection is performed before application of traffic rules (see chapter 8) which avoids intervention of traffic rules with the detection process.

Intrusion prevention configuration in Kerio Control

The intrusion prevention system can be configured under *Configuration* → *Traffic Policy* → *Intrusion Prevention*.

Detection of known intrusion types

Kerio Control distinguishes three levels of intrusion severity:

- *High severity* — activity where probability that it is an intrusion attempt is very high (e.g. Trojan horse network activity).
- *Medium severity* — activities considered as suspicious and possibly harmful where there is a certain chance the traffic may be legitimate (e.g. traffic by a non-standard protocol on the standard port of another protocol).
- *Low severity* — suspicious network activities which do not indicate immediate security threat (e.g. port scanning).

For each severity level, one of the following actions can be set:

- *Log and drop* — information about the detected activity will be recorded in the *Security* log (see chapter 23.11) and the particular network traffic will be blocked.
- *Log* — detected activity will be only recorded in the *Security* log,
- *No action* — the detected activity will be ignored.

Default and recommended settings for individual intrusion severity levels:

- *High severity* → *Log and drop*,
- *Medium severity* → *Log*,
- *Low severity* → *No action* (in case that there is a suspicion of too many false alarm cases, see also *Advanced settings*).

Functionality of the intrusion prevention system can be tested by clicking on the link on a special web page on one of the *Kerio Technologies* servers. Upon startup of the test, three fake harmless intrusions of high, middle and low severity will be sent to the client's address (i.e. to the IP address of your firewall). The test script then evaluates whether the firewall let the intrusion attempts in or blocked them. The *Security* log will also include three corresponding records informing of whether the firewall blocked, only logged or ignored the intrusions (for details, see chapter 23.11).

Note: This test is designed only for purposes of the intrusion prevention system built in *Kerio Control*. It cannot be used for testing of other IDS/IPS.

Use of known intruders databases (blacklists)

In addition to detection of known intrusion types, it is also possible to detect and block traffic from IP addresses listed in web databases of known intruders (so called *blacklists*). In this case, all traffic from the IP address is logged and possibly blocked. Such method of detection and blocking of intruders is much faster and also less demanding than detection of individual intrusion types. However, there are also some disadvantages of this method. Blacklists cannot include IP addresses of all possible intruders as the intruders often use fake addresses. Blacklist also may include IP addresses of legitimate clients or servers. Therefore, it is possible to set the same actions for blacklists as for detected intrusions:

- *Log and drop* — information about the detected traffic and blocked IP address will be recorded in the *Security* log and any network traffic from that IP address will be blocked.
- *Log* — information about the detected traffic and blocked IP address will be only recorded in the *Security* log,
- *No action* — the detected blacklisted IP address will not be considered as an intruder.

Note: Kerio Control does not include the option of custom blacklist adding.

Update of intrusions and known intruders databases

For correct functionality of the intrusion detection system, it is necessary to update databases of known intrusions and intruder IP addresses regularly. *Kerio Control* allows to set an interval for regular automatic updates (the default value is *24 hours*) and it is also possible to perform an immediate update if needed (e.g. after a longer electricity supply outage). Under usual circumstances there is no reason to disable automatic updates — non-updated databases decrease effectivity of the intrusion prevention system.

> ***Warning:***
> For update of the databases, a valid *Kerio Control* license or a registered trial version is required. For details see chapter 5.

Advanced Options

Kerio Control allows to set advanced parameters for the intrusion prevention system. These parameters can increase effectivity of the intrusion prevention system and help avoid so called *false positives*. However, it is recommended not to change these parameters unless you are absolutely sure about the values!

Ignored intrusions

In some cases, legitimate traffic may be detected as an intrusion. If this happens frequently or even regularly, it may be helpful to define an exception for the particular intrusion. Exceptions are defined by adding the rule ID number in the list. Identifier of the rule can be found in the *Security* log (see chapter 23.11), or in the *Snort* system documentation (http://www.snort.org/).

Note: Exceptions are helpful only in cases where legitimate traffic is detected as an intrusion repeatedly or even better — regularly. It may be harmful to define exceptions after the first time such a problem is detected.

Protocol-specific intrusions

Some intrusions may target security weaknesses in specific application protocols. Therefore, it is usually not helpful to detect these intrusions in traffic of other application protocols. For individual protocols recognized by the intrusion detection system, lists of standard and frequently used ports are predefined. The lists may include individual port numbers separated by commas or port ranges (initial and final port separated by a dash, non-spaced).

If an application is available from the Internet that uses any of the listed protocols on a non-standard port (e.g. *HTTP* on port *10000*), it can be helpful to add this port in list of ports on which *HTTP*-specific intrusions will be detected.
If, on the other hand, an application using a different protocol is used on a listed port (e.g. VPN server on port *8000*), it is recommended to remove this port from the list of ports for the particular protocol — it is meaningless to perform detection on the port, the detection process would be a redundant load for the firewall and false positives might also occur.

9.2 MAC address filtering

Besides *Traffic Rules* that filter network traffic by using IP addresses, protocols and ports (see chapter 8), *Kerio Control* also allows "low-level" filtering by hardware addresses (so called MAC addresses) of individual computers and network devices. Filtering of physical address helps for example prevent users from undesirable connections to the network or get around the firewall traffic policy by changing IP address of their device.

Note: The MAC address filter works on lower level than the firewall's traffic rules (see chapter 8) and it is therefore applied earlier than traffic rules.

MAC address filtering can be configured under *Configuration* → *Traffic Policy* → *Security Options*.

Network interfaces

The MAC address filter can be applied on any network *Ethernet* or *Wi-Fi* interface of the firewall. However, it is recommended to select only such interface on which network traffic should be filtered. If you want to block unwanted devices in local network, there is no reason to use filtering of MAC addresses on web interfaces. This might mean a redundant load on the firewall and it can also cause blocking of Internet traffic.

Filtering mode

The MAC address filter works in two modes:

- Blocking of computers with listed MAC addresses.
  The filter will block only traffic of computers (devices) with MAC addresses included on the list. Traffic will be allowed for any other computers. This mode can be used for quick blocking of certain MAC addresses but it does not protect from connection of new, unknown devices. Another deficit is that many systems and devices allow change of their network adapter's MAC address.
- Allowing of traffic of computers with listed MAC addresses.
  The filter allows only traffic of computers with MAC addresses included on the list, any other traffic will be blocked. This filtering mode is very effective as all unknown MAC addresses are blocked (in one physical network cannot include more than one device with an identical MAC address — misuse of allowed MAC address is very difficult or even impossible).

However, for this purpose, it is necessary to create and maintain a complete list of MAC addresses of all devices with traffic allowed. This can be quite demanding in case of larger networks.

MAC address list

This list includes MAC addresses of computers with either filtered (blocked) or allowed traffic — depending on the mode.

MAC addresses are defined as six bytes (hexadecimal numbers) separated by colons (e.g.: `a0:de:bf:33:ce:12`) or dashes (e.g.: `a0-de-bf-33-ce-12`) or in a compact format without separators (`a0debf33ce12`).

For better reference, each MAC address can be optionally accompanied by a description of the particular device. It is highly recommended to use these descriptions thoroughly — the MAC address itself provides no helpful reference information.

9.3 Special Security Settings

Kerio Control provides several additional options for traffic filtering that cannot be defined by traffic rules. These options can be set in the *Miscellaneous* tab of the *Configuration* → *Traffic Policy* → *Security Settings* section.

Anti-Spoofing

Anti-Spoofing checks whether only packets with allowed source IP addresses are received at individual interfaces of the *Kerio Control* host. This function protects *Kerio Control* host from attacks from the internal network that use false IP addresses (so called *spoofing*).

For each interface, any source IP address belonging to any network connected to the interface is correct (either directly or using other routers). For any interface connected to the Internet (so called external interface), any IP address which is not allowed at any other interface is correct.

Detailed information on networks connected to individual interfaces is acquired in the routing table.

The *Anti-Spoofing* function can be configured in the

Anti-Spoofing folder in *Configuration* → *Advanced Options*.

Enable Anti-Spoofing

This option activates *Anti-Spoofing*.

Log

If this option is on, all packets that have not passed the anti-spoofing rules will be logged in the *Security* log (for details see chapter 23.11).

Connection Limit

This security function defines a limit for the maximum number of network connections which can be established from one local host (workstation) to the Internet or from the Internet to the local server via a mapped port.

Incoming and outgoing connections are monitored separately. If number of all connections established from/to a single local host in any direction reaches the specified value, *Kerio Control* block any further connections in the particular direction.

These restrictions protects firewall (*Kerio Control* host) from overload and may also help protect it from attacks to the target server, reduce activity and impact of a worm or Trojan horse.

Count limit for outgoing connections is useful for example when a local client host is attacked by a worm or Trojan horse which attempts to establish connections to larger number of various servers. Limiting of number of incoming connections can for example prevent the target from so called *SYN flood* attacks (flooding the server by opening too many concurrent connections without any data transferred).

Filtering traffic via the IPv6 protocol

Kerio Control supports blocking of traffic by IPv6. In newer operating systems (such as *Windows Vista* and *Windows 7*), this protocol is enabled by default and the computer has an automatically generated IPv6 address. This can cause a security hazard.

Kerio Control allows:

- *Block native IPv6* — *Kerio Control* is connected to the network with the IPv6 protocol.

  This option is available only in the *Windows* edition. In editions *Software Appliance* and *Box*, any native IPv6 traffic is blocked by default.

- *Block tunelled IPv6* — to ease the transition to IPv6, some protocol can encapsulate IPv6 packets into IPv4 and thus communicate via network without IPv6 support.

  You can define exceptions for tunelled IPv6 traffic — tunelled traffic of computers with certain IPv4 addresses will not be blocked. The exceptions are defined by IPv4 address groups (see chapter16.1). The selected group may include both local or Internet IPv4 addresses.

For these security reasons, all IPv6 traffic is disabled by default.

Note: No *Kerio Control* traffic rules or other functions can be applied to traffic via the IPv6 protocol.

9.4 P2P Eliminator

Peer-to-Peer (*P2P*) networks are world-wide distributed systems, where each node can represent both a client and a server. These networks are used for sharing of big volumes of data (this sharing is mostly illegal). *DirectConnect* and *Kazaa* are the most popular ones.

In addition to illegal data distribution, utilization of *P2P* networks overload lines via which users are connected to the Internet. Such users may limit connections of other users in the same network and may increase costs for the line (for example when volume of transmitted data is limited for the line).

Kerio Control provides the *P2P Eliminator* module which detects connections to *P2P* networks and applies specific restrictions. Since there is a large variety of *P2P* networks and parameters at individual nodes (servers, number of connections, etc.) can be changed, it is hardly possible to detect all *P2P* connections.[5]. However, using various methods (such as known ports, established connections, etc.), the *P2P Eliminator* is able to detect whether a user connects to one or multiple *P2P* networks.

The following restrictions can be applied to users of *P2P* networks (i.e. to hosts on which clients of such networks are run):

- *Block all traffic* — the host will not be allowed to access the Internet,
- *Allow only secure traffic* — only such traffic of the particular host is allowed that is for sure not using P2P networks (e.g. web, email, etc.).

P2P Eliminator Configuration

P2P networks are detected automatically (the *P2P Eliminator* module keeps running). To set the *P2P Eliminator* module's parameters, go to the *P2P Eliminator* tab in the *Configuration → Advanced Options* section.

As implied by the previous description, it is not possible to block connections to particular *P2P* networks. *P2P Eliminator* allows to block all traffic (i.e. access to the Internet from the particular host) or to permit only such services where it is guaranteed that they do not use P2P networks. The settings will be applied to all clients of *P2P* networks detected by *P2P Eliminator*.

Check the *Inform user by email* option if you wish that users at whose hosts *P2P* networks are detected will be warned and informed about actions to be taken (blocking of all traffic / allowance of only certain services and length of the period for which restrictions will be applied). The email is sent only if a valid email address (see chapter 17.1) is specified in the particular user account. This option does not apply to unauthenticated users.

The *Traffic will be blocked for* value defines time when the restriction for the particular host will be applied. The *P2P Eliminator* module enables traffic for this user automatically when

[5] According to thorough tests, the detection is highly reliable (probability of failure is very low).

the specified time expires. The time of disconnection should be long enough to make the user consider consequences and to stop trying to connect to *P2P* networks.

Note:

1. If a user who is allowed to use *P2P* networks (see chapter 17.1) is connected to the firewall from a certain host, no *P2P* restrictions are applied to this host. Settings in the *P2P Eliminator* tab are always applied to unauthorized users.
2. Information about *P2P* detection and blocked traffic can be viewed in the *Status → Hosts / users* section (for details, refer to chapter 20.1).
3. If you wish to notify also another person when a *P2P* network is detected (e.g. the firewall administrator), define the alert on the *Alerts Settings* tab of the *Configuration → Accounting* section. For details, see chapter 20.4.

Parameters for detection of P2P networks

Click *Advanced* to set parameters for *P2P* detection.

Ports of P2P networks

List of ports which are exclusively used by *P2P* networks. These ports are usually ports for control connections — ports (port ranges) for data sharing can be set by users themselves.

Ports in the list can be defined by port numbers or by port ranges. Individual values are separated by commas while dash is used for definition of ranges.

Number of suspicious connections

Big volume of connections established from the client host is a typical feature of *P2P* networks (usually one connection for each file). The *Number of connections* value defines maximal number of client's network connections that must be reached to consider the traffic as suspicious.

The optimum value depends on circumstances (type of user's work, frequently used network applications, etc.) and it must be tested. If the value is too low, the system can be unreliable (users who do not use *P2P* networks might be suspected). If the value is too high, reliability of the detection is decreased (less *P2P* networks are detected).

Safe services

Certain "legitimate" services may also show characteristics of traffic in *P2P* networks (e.g. big number of concurrent connections). To ensure that traffic is not detected incorrectly and users of these services are not persecuted by mistake, it is possible to define list of so called secure services. These services will be excluded from detection of *P2P* traffic.

The *Define services...* button opens a dialog where services can be define that will not be treated as traffic in *P2P* network. All services defined in *Configuration → Definitions → Services* are available (for details, refer to chapter sect-services"/>).

Warning:

Default values of parameters of *P2P* detection were set with respect to long-term testing. As already mentioned, it is not always possible to say that a particular user really uses *P2P* networks or not which results only in certain level of probability. Change of detection parameters may affect its results crucially. Therefore, it is recommended to change parameters of *P2P* networks detection only in legitimate cases (e.g. if a new port number is detected which is used only by a *P2P* network and by no legitimate application or if it is found that a legitimate service is repeatedly detected as a *P2P* network).

Chapter 10

Configuration of network services

This chapter provides guidelines for setting of basic services in *Kerio Control* helpful for easy configuration and smooth access to the Internet:

- *DNS* module — this service is used as a simple DNS server for the LAN,
- *DHCP server* — provides fully automated configuration of LAN hosts,
- *DDNS* client — provides automatic update of firewall logs in public dynamic DNS,
- *Proxy server* — enables access to the Internet for clients which cannot or do not want to use the option of direct access,
- *HTTP cache* — this service accelerates access to repeatedly visited web pages (for direct connections with proxy server).

10.1 DNS module

In *Kerio Control*, the *DNS Forwarder* module can be used to enable easier configuration for DNS hosts within local networks or to speed up responses to repeated DNS queries. At local hosts, DNS can be defined by taking the following actions:

- use IP address of the primary or the back-up DNS server. This solution has the risk of slow DNS responses. All requests from each computer in the local network will be sent to the Internet.
- use the DNS server within the local network (if available). The DNS server must be allowed to access the Internet in order to be able to respond even to queries sent from outside of the local domain.
- use the *DNS* module in *Kerio Control*. It can be also used as a basic DNS server for the local domain or/and as a forwarder for the existing server.

If possible, it is recommended to use the *DNS* module as a primary DNS server for LAN hosts (the last option). The *DNS* module provides fast processing of DNS requests and their correct routing in more complex network configurations. The *DNS* module can answer directly to repeated requests and to requests for local DNS names, without the need of contacting DNS servers in the Internet.

If the *DNS* module cannot answer any DNS request on its own, it forwards it to a DNS server set for the Internet link through which the request is sent. For details addressing configuration of the firewall's network interfaces, see chapter 6, more information on Internet connection options, refer to chapter 7.

The DNS module configuration

By default, DNS server (the *DNS forwarder* service), cache (for faster responses to repeated requests) and simple DNS names resolver are enabled in *Kerio Control*.

The configuration can be fine-tuned in *Configuration* → *DNS*.

Enable DNS forwarder

This option enables DNS server in *Kerio Control*. Without other configuration, any DNS requests are forwarded to DNS servers on the corresponding Internet interface.
If the *DNS forwarder* service is disabled, the *DNS* module is used only as a *Kerio Control's* DNS resolver.

> ***Warning:***
> If *DNS forwarder* is not used for your network configuration, it can be switched off. If you want to run another DNS server on the same host, *DNS forwarder must* be disabled, otherwise collision might occur at the DNS service's port (`53/UDP`).

Enable cache for faster response of repeated queries

If this option is on, all responses will be stored in local *DNS* cache. Responses to repeated queries will be much faster (the same query sent by various clients is also considered as a repeated query).
Physically, the DNS cache is kept in RAM. However, all DNS records are also saved in the `DnsCache.cfg` file (see chapter 26.2). This means that records in DNS cache are kept even after *Kerio Control Engine* is stopped or the firewall is closed.
Note:

1. Time period for keeping DNS logs in the cache is specified individually in each log (usually 24 hours).
2. Use of DNS also speeds up activity of the *Kerio Control's* non-transparent proxy server (see chapter 10.5).

Clear cache

Clear-out of all records from the *DNS* cache (regardless of their lifetime). This feature can be helpful e.g. for configuration changes, dial-up testing, error detection, etc.

Use custom forwarding

Use this option to enable settings for forwarding certain DNS queries to other DNS servers (see below).

Simple DNS resolution

The *DNS* module can answer some DNS requests on its own, typically requests regarding local host names. In local network, no other DNS server is required, neither it is necessary to save information about local hosts in the public DNS. For hosts configured automatically by the DHCP protocol (see chapter 10.2), the response will always include the current IP address.

Note: The *DNS* module in *Kerio Control* cannot respond to so called reverse DNS queries (i.e. to resolve hostnames from IP addresses). These queries are always forwarded to another DNS server.

Before forwarding a query...

These options allow setting of where the *DNS* module would search for the name or IP address before the query is forwarded to another DNS server.

- *Hostname table* — table defined by *Kerio Control* administrator. Each row of this table includes host IP addresses and a list of appropriate DNS names.
- *DHCP lease table*— if the hosts within local network are configured by the DHCP server in *Kerio Control* (see chapter 10.2), the DHCP server knows what IP address was defined for each host. After starting the system, the host sends a request for IP address definition including the name of the host.
  The *DNS* module can use DHCP server databases to find out which IP address has been assigned to the host name. If asked to inform about the local name of the host, *DNS Forwarder* will always respond with the current IP address. Actually, this is a method of dynamical DNS update.

Note: If both options are disabled, the *DNS* forwards all queries to other DNS servers.

Local DNS domain

In the *When resolving name from the hostname table or lease table combine it with DNS domain below* entry, specify name of the local DNS domain.

If a host or a network device sends a request for an IP address, it uses the name only (it has not found out the domain yet). Therefore, only host names without domain are saved in the table of addresses leased by DHCP server. The *DNS* module needs to know the name of the local domain to answer queries on fully qualified local DNS names (names including the domain).

Note: If the local domain is specified in the *DNS* module, local names with or without the domain can be recorded in the hostname table.

The problem can be better understood through the following example.

Example:
The local domain's name is `company.com`. The host called `john` is configured so as to obtain an IP address from the DHCP server. After the operating system is started the host sends to the DHCP server a query with the information about its name (`john`). The DHCP server assigns the host IP address `192.168.1.56`. The DHCP server then keeps the information that the IP address is assigned to the `john` host.
Another host that wants to start communication with the host will send a query on the `john.company.com` name (the `john` host in the `company.com` domain). If the local domain name would not have been known by the *DNS* module, the forwarder would pass the query to another DNS server as it would not recognize that it is a local host. However, as *DNS Forwarder* knows the local domain name, the `company.com` name will be separated and the `john` host with the appropriate IP address will be easily looked up in the DHCP table.

Hostname table

Hostname table includes a list of IP addresses and corresponding DNS hostnames. *Kerio Control* uses this table to detect IP address of hostname-specified local hosts.

Each table row includes one IP address. DNS names can be specified with or without domain — for lookup, the ebove-mentioned combination with local domain is applied.

Each IP address can have multiple DNS names assigned. This can be defined in the following ways:

- To write all information in a single record and separate individual names with semicolons. Example:

  ```
  192.168.1.10 server;mail
  ```

  The main advantage of this method is space-saving. First name written is always considered as primary (so called canonical name) and the other names are used as its aliases.

- Create an individual record for each name. Example:

  ```
  192.168.1.10 server
  ```

  ```
  192.168.1.10 mail
  ```

  In case of this method, primary name can be set as needed. To move records, use arrow buttons on the right side of the window. The name written as first at the IP address will be used as primary (canonical).

It is recommended to choose one from the provided record-layout methods. If these methods are combined, the table can be confusing.

Each DNS name can have multiple IP addresses assigned (e.g. a computer with multiple network adapters). In that case, a record must be added to the table for each IP address, while DNS name will be identical in all these records.

Warning:
Hostname table content is saved in the `hosts` system file. Therefore, it is not recommended to edit this file manually on the *Kerio Control* server!

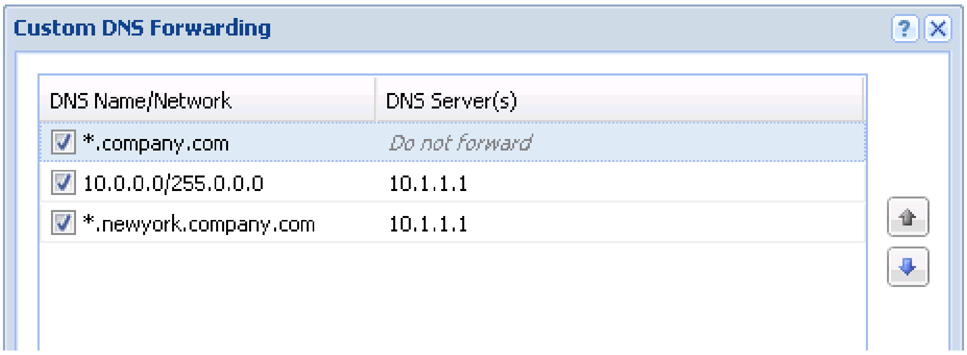
Enable DNS forwarding

The *DNS* module allows forwarding of certain DNS requests to specific DNS servers. This feature can be helpful for example when we intend to use a local DNS server for the local domain (the other DNS queries will be forwarded to the Internet directly — this will speed up the response). DNS forwarder's settings also play role in configuration of private networks where it is necessary to provide correct forwarding of requests for names in domains of remote subnets (for details, check chapter 24).

Request forwarding is defined by rules for DNS names or subnets. Rules are ordered in a list which is processed from the top. If a DNS name or a subnet in a request matches a rule, the request is forwarded to the corresponding DNS server. Queries which do not match any rule are forwarded to the "default" DNS servers (see above).

Note: If the *Simple DNS resolution* is enabled (see below), the forwarding rules are applied only if the *DNS* module is not able to respond by using the information in the hostname table and/or by the DHCP lease table.

Clicking on the *Define* button in the *DNS* module configuration opens a dialog for setting of rules concerning forwarding of DNS queries.



DNS Name/Network	DNS Server(s)
☑ *.company.com	*Do not forward*
☑ 10.0.0.0/255.0.0.0	10.1.1.1
☑ *.newyork.company.com	10.1.1.1

Figure 10.1 Specific settings of DNS forwarding

The rule can be defined for:

- DNS name — queries requiring names of computers will be forwarded to this DNS server (so called `A` queries),
- a subnet — queries requiring IP addresses of the particular domain will be forwarded to the DNS server (reverse domain — `PTR` queries).

Rules can be reordered by arrow buttons. This enables creating of more complex combinations of rules — e.g. exceptions for certain workstations or subdomains. As the rule list is processed from the top downwards, rules should be ordered starting by the most specific one (e.g. name of a particular computer) and with the most general one at the bottom (e.g. the main domain of the company). Similarly to this, rules for reversed DNS queries should be ordered by subnet mask length (e.g. with `255.255.255.0` at the top and `255.0.0.0` at the bottom). Rules for queries concerning names and reversed queries are independent from each other. For better reference, it is recommended to start with all rules concerning queries for names and continue with all rules for reversed queries, or vice versa.

Click on the *Add* or the *Edit* button to open a dialog where custom DNS forwarding rules can be defined.

- The *Name DNS query* option allows specification of a rule for name queries. Use the *If the queried name matches* entry to specify a corresponding DNS name (name of a host in the domain).

  It is usually desirable to forward queries to entire domains rather than to specific names. Specification of a domain name may therefore contain `*` wildcard symbol (asterisk — substitutes any number of characters) and/or `?` (question mark — substitutes a single character). The rule will be applied to all names matching with the string (hosts, domains, etc.).

  > ***Example::***
  > DNS name will be represented by the string `?erio.c*`. The rule will be applied to all names in domains `kerio.com`, `cerio.com`, `aerio.c` etc., such as on `www.kerio.com`, `secure.kerio.com`, `www.aerio.c`, etc.

  > ***Warning:***
  > In rules for DNS requests, it is necessary to enter an expression matching the full DNS name! If, for example, the `kerio.c*` expression is introduced, only names `kerio.cz`, `kerio.com` etc. would match the rule and host names included in these domains (such as `www.kerio.cz` and `secure.kerio.com`) would not!

- Use the *Reverse DNS query* alternative to specify rule for DNS queries on IP addresses in a particular subnet. Subnet is specified by a network address and a corresponding mask (i.e. `192.168.1.0 / 255.255.255.0`).

- Use the *Then forward query to DNS Server(s)* field to specify IP address(es) of one or more DNS server(s) to which queries will be forwarded.

  If multiple DNS servers are specified, they are considered as primary, secondary, etc.

  If the *Do not forward* option is checked, DNS queries will not be forwarded to any other DNS server — *Kerio Control* will search only in the hostname table or in the DHCP server table (see below). If requested name or IP address is not found, non-existence of the name/address is reported to the client.

  Note: Using of the *Do not forward* option is meaningless for reverse DNS queries as the *DNS* module in *Kerio Control* cannot respond to them by itself.

10.2 DHCP server

The DHCP protocol (*Dynamic Host Configuration Protocol*) is used for easy TCP/IP configuration of hosts within the network. Upon an operation system start-up, the client host sends a configuration request that is detected by the DHCP server. The DHCP server selects appropriate configuration parameters (IP address with appropriate subnet mask and other optional parameters, such as IP address of the default gateway, addresses of DNS servers, domain name, etc.) for the client stations. All client parameters can be set at the server only — at individual hosts, enable the option that TCP/IP parameters are configured automatically from the DHCP server. For most operating systems (e.g. *Windows*, *Linux*, etc.), this option is set by default — it is not necessary to perform any additional settings at client hosts.

The DHCP server assigns clients IP addresses within a predefined scope for a certain period (*lease time*). If an IP address is to be kept, the client must request an extension on the period of time before the lease expires. If the client has not required an extension on the lease time, the IP address is considered free and can be assigned to another client. This is performed automatically and transparently.

So called reservations can be also defined on the DHCP server — certain clients will have their own IP addresses reserved. Addresses can be reserved for a hardware address (MAC) or a host name. These clients will have fixed IP address. These addresses are configured automatically.

Using DHCP brings two main benefits. First, the administration is much easier than with the other protocols as all settings may be done at the server (it is not necessary to configure individual workstations). Second, many network conflicts are eliminated (i.e. one IP address cannot be assigned to more than one workstation, etc.).

Kerio Control also allows automatic configuration of the DHCP server. This option involves automatic creation and updates of IP address ranges and parameters in accordance with network interfaces included in group *Trusted /Local* (see chapter 6). This implies that the only thing to do is actually to run the DHCP server. If the automatic configuration is not suitable enough, it is possible to use the option of manual configuration.

DHCP Server Configuration

To configure the DHCP server in *Kerio Control* go to

Configuration → *DHCP Server*. Here you can define IP scopes, reservations or optional parameters, and view information about occupied IP addresses or statistics of the DHCP server.

The DHCP server can be enabled/disabled using the *DHCP Server enabled* option (at the top). Configuration can be modified even when the DHCP server is disabled.

Automatic configuration of IP scopes

By default, the DHCP server works in the mode of automatic configuration of IP scopes. In this mode, *Kerio Control* detects parameters of network interfaces included in group *Trusted /Local* and uses them to generate and update IP scopes for the corresponding subnets. Whenever an interface is changed in group *Trusted /Local*, the DHCP server's configuration will be updated automatically.

For each interface's subnet, a scope of the following parameters will be created:

- *Range* — by IP address of the interface and the corresponding subnet mask.

  The range should cover the particular subnet with free resources for assigned static addresses (e.g. for mask `255.255.255.0`, the range from `x.x.x.11` to `x.x.x.254` will be created). If an interface's address is covered by a range, then an exception is automatically defined for it.

- *Subnet mask* — according to the particular interface.

- *Default gateway* — IP address of the particular interface.

- *DNS server* — IP address of the particular interface.

Some other parameters that are available at the interface can also be set (DNS domain, WINS server address). This depends on the firewall's operating system as well as on the configuration of the particular interface.

Manual Definition of Scopes and Reservations

If you do not want to use the automatic configuration of IP ranges, you can switch to the manual mode. However, bear in mind that changes of interfaces in group *Trusted /Local* (e.g. adding of a new interface, change of IP address, etc.) require manual update of address scopes defined in the DHCP server!

Only one scope can be defined for each IP subnet.

Note: In the *Kerio Control Administration* interface, it is also possible to use a scope template where parameters are already predefined in accordance with the particular firewall's interface. For details, see above, section *Automatic configuration of IP scopes*.

Definition of IP scopes:

Description
Comment on the new address scope (just as information for *Kerio Control* administrator).

First address, Last address
First and last address of the new scope.
Note: If possible, we recommend you to define the scope larger than it would be defined for the real number of users within the subnet.

Subnet mask
Mask of the appropriate subnet. It is assigned to clients together with the IP address.
Note: The administration interface monitors whether first and last address belong to the subnet defined by the mask. If this requirement is not met, an error will be reported after the confirmation with the *OK* button.

Lease time
Time for which an IP address is assigned to clients. This IP address will be automatically considered free by expiration of this time (it can be assigned to another client) unless the client requests lease time extension.

Exclusions
Kerio Control enables the administrator to define only one scope in within each subnet. To create more individual scopes, follow these instructions:

- create address scope covering all desired scopes
- define so called exclusions that will not be assigned

> ***Example:***
> In `192.168.1.0` subnet you intend to create two scopes: from `192.168.1.10` to `192.168.1.49` and from `192.168.1.61` to `192.168.1.100`. Addresses from `192.168.1.50` to `192.168.1.60` will be left free and can be used for other purposes.
> Create the scope from `192.168.1.10` to `192.168.1.100` and click on the *Exclusions* button to define the scope from `192.168.1.50` to `192.168.1.60`. These addresses will not be assigned by the DHCP server.

DHCP parameters
In the *Address Scope* dialog, basic DHCP parameters of the addresses assigned with IP address can be defined: For correct functionality of TCP/IP on client hosts, the following parameters need to be assigned:

- *Default Gateway* — IP address of the router that will be used as the default gateway for the subnet from which IP addresses are assigned. IP address of the interface the network is connected to. Default gateway of another network would be useless (not available to clients).

- *DNS server* — any DNS server (or more DNS servers separated with semicolons). However, it is recommended to use the *Kerio Control* host's IP address as the primary DNS server (i.e. at the top). The *DNS* module can cooperate with DHCP server (see chapter 10.1) so that it will always use correct IP addresses to response to requests on local host names.
- *Domain* — local Internet domain. Do not specify this parameter if there is no local domain.
  This parameter is not used for specification of the name of *Windows NT* domain!

Leases and Reservations

IP scopes can be viewed in the *Leases* tab. These scopes are displayed in the form of trees. All current leases within the appropriate subnet are displayed in these trees.

Note: Icons marked with R represent reserved addresses.

Columns in this section show the following information:

- *Leased Address* — leased IP address
- *Name* — reservation name / description (blank at dynamically assigned addresses),
- *Manufacturer* — name of the manufacturer of the client's network adapter (detected from the MAC address),
- *Lease Expiration* — date and time specifying expiration of the appropriate lease
- *MAC Address* — hardware address of the host that the IP address is assigned to (including name of the network adapter manufacturer).
- *Hostname* — name of the host that the IP address is assigned to (only if the DHCP client at this host sends it to the DHCP server).
- *Status* — status of the appropriate IP address; *Leased* (leased addresses), *Expired* (addresses with expired lease — the client has not asked for the lease to be extended yet), *Declined* (the lease was declined by the client) or *Released* (the address has been released by the client).

  Note: Data about expired and released addresses are kept by the DHCP server and can be used later if the same client demands a lease. If free IP addresses are lacked, these addresses can be leased to other clients.
- *User* — name of the user which is connected from the particular host to the firewall
- *Last Request Time* — date and time when the recent request for a lease or lease extension was sent by a client.
- *Lease Remaining Time* — time remaining until the appropriate *Lease Expiration*

Using the *Remove* button you can release the selected IP address and/or cancel IP address reservation on the spot. *DHCPRELEASE* control message will be sent to the corresponding client.

Lease Reservations

DHCP server enables the administrator to book an IP address for any host. Reservations can be set in both scope configuration modes, manual and automatic. The act of adding a reservation in the automatic mode does not switch to manual mode.

You can use the *Add* button to:

- Create a new reservation with the predefined parameters.
- Reserve a dynamically assigned IP address.

Any IP address included in a defined subnet can be reserved. This address can but does not have to belong to the scope of addresses dynamically leased, and it can also belong to any scope used for exceptions.

IP addresses can be reserved for:

- hardware (MAC) address of the host — it is defined by hexadecimal numbers separated by colons — for example:

  `00:bc:a5:f2:1e:50`

  or by dashes— for example:

  `00-bc-a5-f2-1e-50`

  The MAC address of a network adapter can be detected with operating system tools (i.e. with the `ipconfig` command) or with a special application provided by the network adapter manufacturer.

- host name — DHCP requests of most DHCP clients include host names (i.e. all *Windows* operating systems), or the client can be set to send a host name (e.g. the *Linux* operating system).

For assigning of IP address, DHCP parameters of the configuration will be automatically used int he given scope. In the *Lease Reservation* dialog window, additional parameters can be specified or/and new values can be entered for parameters yet existing.

Note: When reserving dynamically assigned address it is possible to change IP address. This actually creates a new reservation but without the need to specify MAC address manually.

10.3 Dynamic DNS for public IP address of the firewall

Kerio Control provides (among others) services for remote access from the Internet to the local network (*VPN server* — see chapter 24 and the *Clientless SSL-VPN* interface — see chapter 25). Also other services can be accessible from the Internet — e.g. the *Kerio StaR* interface (see chapter 22), administration of *Kerio Control* (see chapter 4) or any other service (e.g. web server in local network — see chapter 8.4). These services are available at the firewall's public IP address. If this IP address is static and there exists a corresponding DNS record for it, a corresponding name can be used for access to a given service (e.g. `server.company.com`). If there is no corresponding DNS record, it is necessary to remember the firewall's IP address and use it for access to all services. If the public IP address is dynamic (i.e. it changes), it is extremely difficult or even impossible to connect to these services from the Internet.

This problem is solved by *Kerio Control's* support for dynamic DNS. Dynamic DNS provides DNS record for a specific name of a server which will always keep the current IP address. This method thus allows making mapped services always available under the same server name, regardless of the fact if IP address changes and how often.

How cooperation with dynamic DNS works

Dynamic DNS (*DDNS*) is a service providing automatic update of IP address in DNS record for the particular host name. Typically, two versions of DDNS are available:

- free — user can choose from several second level domains (e.g. `no-ip.org`, `ddns.info`, etc.) and select a free host name for the domain (e.g. `company.ddns.info`).
- paid service — user registers their own domain (e.g. `company.com`) and the service provider then provides DNS server for this domain with the option of automatic update of records.

User of the service gets an account which is used for access authentication (this will guarantee that only authorized users can update DNS records. Update is performed via secured connection (typically HTTPS) to make sure that the traffic cannot be tapped. Dynamic DNS records can be updated either manually by the user or (mostly) by a specialized software — *Kerio Control* in this case.

If *Kerio Control* enables cooperation with dynamic DNS, a request for update of the IP address in dynamic DNS is sent upon any change of the Internet interface's IP address (including switching between primary and secondary Internet connection — see chapter 7.4). This keeps DNS record for the particular IP address up-to-date and mapped services may be accessed by the corresponding host name.

Note:

1. Usage of DDNS follows conditions of the particular provider.
2. Dynamic DNS records use very short time-to-live (TTL) and, therefore, they are kept in cache of other DNS servers or forwarders for a very short time. Probability that the client receives DNS response with an invalid (old) IP address is, therefore, very low.

3. Some DDNS servers also allow concurrent update of more records. Wildcards are used for this purpose.
   Example: In DDNS there exist two host names, both linked to the public IP address of the firewall: `fw.company.com` and `server.company.com`. If the IP address is changed, it is therefore possible to send a single request for update of DNS records with name `*.company.com`. This requests starts update of DNS records of both names.

Kerio Control DDNS configuration

To set cooperation with the dynamic DNS server, go to the *Dynamic DNS* folder in *Configuration → Advanced Options*.

As already mentioned, the first step is to make an account (i.e. required dynamic DNS record with appropriate access rights) at a DDNS provider. *Kerio Control* now supports these DDNS providers:

- *ChangeIP* (http://www.changeip.com/),
- *DynDNS* (http://www.dyndns.org/),
- *No-IP* (http://www.no-ip.com/).

On the *Dynamic DNS* tab, select a DDNS provider, enter DNS name for which dynamic record will be kept updated and set user name and password for access to updates of the dynamic record. If DDNS supports wildcards, they can be used in the host name.

Once this information is defined, it is recommended to test update of dynamic DNS record by clicking on *Update now*. This verifies that automatic update works well (the server is available, set data is correct, etc.) and also updates the corresponding DNS record (IP address of the firewall could have changed since the registration or the last manual update).

If an error occurs while attempting to update DNS record, an error is reported on the *Dynamic DNS* tab providing closer specification of the error (e.g. DDNS server is not available, user authentication failed, etc.). This report is also recorded in the *error* log.

10.4 HTTP cache

Using cache to access Web pages that are opened repeatedly reduces Internet traffic (in case of line where traffic is counted, it is also remarkable that using of cache decreases total volume of transferred data). Downloaded files are saved to the hard drive of the *Kerio Control* host so that it is not necessary to download them from the web server again later.

Note: For technical reasons, HTTP cache is not available on *Kerio Control Box*.

All objects are stored in cache for a certain time only (*Time To Live — TTL*). This time defines whether checks for the most recent versions of the particular objects will be performed upon a new request of the page. The required object will be found in cache unless the *TTL* timeout has expired. If it has expired, a check for a new update of the object will be performed. This ensures continuous update of objects that are stored in the cache.

The cache can be used either for direct access or for access via the proxy server. If you use direct access, the HTTP protocol inspector must be applied to the traffic. In the default configuration of *Kerio Control*, this condition is met for the HTTP protocol at the default port 80 (for details, see chapters 8.3 and 16.3).

To set HTTP cache parameters go to the *Cache* tab in *Configuration* → *Content Filtering* → *HTTP Policy*.

Enable cache on transparent proxy

This option enables cache for HTTP traffic that uses the HTTP protocol inspector (direct access to the Internet).

Enable cache on proxy server

Enables the cache for HTTP traffic via *Kerio Control's* proxy server (see chapter 10.5).

Cache size

Size of the cache file on the disk.
Maximal cache size allowed is *2 GB* (*2047 MB*). However tests in field prove that with size larger than *1 GB* (*1024 MB*), the speed of object search and thus the efficiency of the cache decreases significantly. Therefore, it is not recommended to create cache larger than *1 GB*.
The cache is located in the `cache` subdirectory of the *Kerio Control's* head directory, i.e.:

- in *Windows* edition typically:

  `C:\Program Files\Kerio\WinRoute\Firewall\cache`

- in *Appliance* edition, always:

  `/opt/kerio/winroute/cache`

It is necessary that there is enough free space on the particular drive or to change cache size according to the free disk space.
Note:

1. If 98 percent of the cache is full, a so called cleaning will be run — this function will remove all objects with expired TTL. If no objects are deleted successfully, no other objects can be stored into the cache unless there is more free space on the disk (made by further cleaning or by manual removal).
2. If the maximum cache size set is larger than the free space on the corresponding disk, the cache is not initialized and the following error is recorded in the *Error* log (see chapter 23.8).

Note: Clients can always require a check for updates from the Web server (regardless of the cache settings). Use combination of the *Ctrl* and the *F5* keys to do this using either the *Internet Explorer* or the *Firefox/SeaMonkey* browser. You can set browsers so that they will check for updates automatically whenever a certain page is opened (then you will only refresh the particular page).

Cache status and administration

Kerio Control allows monitoring of the HTTP cache status as well as manipulation with objects in the cache (viewing and removing).

At the bottom of the *Cache* tab, basic status information is provided such as the current cache size occupied and efficiency of the cache. The efficiency status stands for number of objects kept in the cache (it is not necessary to download these objects from the server) in proportion to the total number of queries (since the startup of the *Kerio Control Engine*). The efficiency of the cache depends especially on user behavior and habits (if users visit certain webpages regularly, if any websites are accessed by multiple users, etc.) and, in a manner, it can be also affected by the configuration parameters described above. If the efficiency of the cache is permanently low (less than 5 percent), it is recommended to change the cache configuration.

The *Clear cache* button deletes all objects saved in cache.

10.5 Proxy server

Even though the NAT technology used in *Kerio Control* enables direct access to the Internet from all local hosts, it contains a standard HTTP proxy server. Under certain conditions the direct access cannot be used or it is inconvenient . The following list describes the most common situations:

1. To connect from the *Kerio Control* host it is necessary to use the proxy server of your ISP.

   Proxy server included in *Kerio Control* can forward all queries to so called *parent proxy server*).

2. Internet connection is performed via a dial-up and access to certain Web pages is blocked (refer to chapter 14.2). If a direct connection is used, the line will be dialed before the HTTP query could be detected (line is dialed upon a DNS query or upon a client's request demanding connection to a Web server). If a user connects to a forbidden web page, *Kerio Control* dials the line and blocks access to the page — the line is dialed but the page is not opened.

   Proxy server can receive and process clients' queries locally. The line will not be dialed if access to the requested page is forbidden.

3. *Kerio Control* is deployed within a network with many hosts where proxy server has been used. It would be too complex and time-consuming to re-configure all the hosts.

   The Internet connection functionality is kept if proxy server is used — it is not necessary to edit configuration of individual hosts (or only some hosts should be re-configured).

The *Kerio Control's* proxy server can be used for HTTP, HTTPS and FTP protocols. Proxy server does not support the SOCKS protocol (a special protocol used for communication between the client and the proxy server).

Note: For detailed information on using FTP on the *Kerio Control's* proxy server, refer to chapter 26.4.

Proxy Server Configuration

To configure proxy server parameters open the *Proxy server* tab in *Configuration → Content Filtering → HTTP Policy*.

Enable non-transparent proxy server

This option enables the HTTP proxy server in *Kerio Control* on the port inserted in the *Port* entry (3128 port is set by the default).

> ***Warning:***
> If you use a port number that is already used by another service or application, *Kerio Control* will accept this port, however, the proxy server will not be able to run and the following report will be logged into the *Error* log (refer to chapter 23.8):

```
failed to bind to port 3128:  another application is using this port
```

If you are not sure that the port you intend to use is free, click on the *Apply* button and check the *Error* log (check whether the report has or has not been logged) immediately.

Enable tunneled connections to any TCP port

This security option enables to allow or block so called tunneling of other application protocols (than HTTP, HTTPS and FTP) via the proxy server (secured HTTPS connection). If this option is disabled, the proxy server allows to establish HTTPS connection only to the standard HTTPS port 443) — it is supposed that secured web pages are being opened. If the option is enabled, the proxy server can establish connection to any port. It can be a non-standard HTTPS port or tunneling of another application protocol.
Note: This option does not affect the non-secured traffic performed by HTTP and/or FTP. In *Kerio Control*, HTTP traffic is controlled by a protocol inspectors which allows only valid HTTP and FTP queries.

Forward to parent proxy server

Tick this option for *Kerio Control* to forward all queries to the parent proxy server which will be specified by the following data:

- *Server* — DNS name or IP address of parent proxy server and the port on which the server is running (3128 port is used by the default).
- *Parent proxy server requires authentication* — enable this option if authentication by username and password is required by the parent proxy server. Specify the *Username* and *Password* login data.
  Note: The name and password for authentication to the parent proxy server is sent with each HTTP request. Only *Basic* authentication is supported.

The *Forward to parent proxy server* option specifies how *Kerio Control* will connect to the Internet (for update checks, downloads of *Sophos* updates and for connecting to the online *Kerio Web Filter* databases).

Set automatic proxy configuration script to...

If a proxy server is used, Web browsers on client hosts must be configured correctly. Most common web browsers (e.g. *Internet Explorer*, *Firefox/SeaMonkey*, *Google Chromea*, etc.) enable automatic configuration of corresponding parameters by using a script downloaded from a corresponding website specified by URL.

In the case of *Kerio Control's* proxy server, the configuration script is saved at

`http://192.168.1.1:3128/pac/proxy.pac,`

where `192.168.1.1` is the IP address of the *Kerio Control* host and number `3128` represents the port of the proxy server (see above).

The *Allow browsers to use configuration script automatically...* option adjusts the configuration script in accord with the current *Kerio Control* configuration and the settings of the local network:

- *Direct access* — no proxy server will be used by browsers
- *Kerio Control proxy server* — IP address of the *Kerio Control* host and the port on which the proxy server is running will be used by the browser (see above).

Note: The configuration script requires that the proxy server is always available (even if the *Direct access* option is used).

Allow browsers to use configuration script automatically...

It is possible to let *Internet Explorer* be configured automatically by the DHCP server. To set this, enable the *Automatically detect settings* option.

Kerio Control's DHCP server must be running (see chapter 10.2), otherwise the function will not work. TCP/IP parameters at the host can be static — *Internet Explorer* sends a special DHCP query when started.

> ***Hint:***
> This method enables to configure all *Internet Explorer* browsers at all local hosts by a single click.

Chapter 11

Bandwidth Management and QoS

The main problem of shared Internet connection is when one or more users download or upload big volume of data and occupy great part of the line connected to the Internet (so called bandwidth). The other users are ten limited by slower Internet connection or also may be affected by failures of certain services (e.g. if the maximal response time is exceeded).

The gravest problems arise when the line is overloaded so much that certain network services (such as mailserver, web server or VoIP) must be limited or blocked. This means that, by data downloads or uploads, even a single user may endanger functionality of the entire network.

Data transmission speed (thoughput, capacity) of Internet link is known as *bandwidth*. Kerio Control includes module *Bandwidth Management* which allows optimization and balancing of an Internet link use so that the connection does not get congested and essential network services have enough recources to function properly.

11.1 How bandwidth management works

The *Bandwidth Management* module provides two basic functions:

Limiting bandwidth for data transfers

This feature allows to cut down especially non-productive traffic that consume too large part of the bandwidth at the expense of other services (download and upload of large data volumes, video streaming, etc.).

Reserving bandwidth for specific services

It is possible to reserve bandwidth for services crucial for the company's basic operations (email, IP telephony, etc.). This bandwidth will be always available, regardless of the current traffic load on the link. This guarantees that user cannot take any actions to jeopardize crucial network services and compeny's operation at any rate. Reservation of bandwidth for particular service is known as *QoS* (*Quality of Service*).

11.2 Internet Links Speed

For correct management of the bandwidth, it is necessary to set link speed, i.e. speed of links used for Internet connection correctly (at the page bottom).

Link speed can be set in selected format, it is not necessary to convert units. Lowercase *b* stands for bits, uppercase *B* stands for bytes (*1B = 8b*).

The more precisely the link speed is set, the better the bandwidth management works. Real speed of a link is usually around 80 percent of the speed claimed by the ISP.

Example: For ASDL line with declared *8192/512 kbit/s*, set download speed to *6.4 Mbit/s* and upload speed to *410 kbit/s*.

11.3 Bandwidth Management Rules

Bandwidth management is defined by ordered rules. Each rule describes certain traffic type and defines limiting and/or reservation of bandwidth for the particular traffic.

Traffic type

Traffic which bandwidth reservation or limit will be applied to can be described as follows:

- Predefined traffic type — web, email, FTP, multimedia, etc.,
- Traffic of selected users,
- Traffic of all users who have already exceeded any of their transmitted data quota.
- Large data transfers,
- Packets matching selected traffic rule (see chapter 8),
- Traffic of selected network service (see chapter 16.3),
- Packets with a particular *DSCP* value.
  The *DSCP* value in *Kerio Control* can be set by using traffic rules, but it can also be set by other routers on the way, the client or/and the server.

Download, Upload

In each traffic direction it is possible to limit maximum transfer speed or reserve minimal bandwidth. If desirable, it is also possible to combine these two rules to set reservation in a way which would not consume bandwidth reserved for other services.

Interface

In some cases, it can be desirable to define various rules for individual interfaces / links. For example, traffic does not need to be limited on the fast primary link for Internet connection failover but on slow failover connection link it is necessary to define restrictions so that the link does not get congested.

Bandwidth management rule can be applied either to all Internet interfaces or to one particular interface. If you need to define restrictions for multiple but not all interfaces, it is necessary to define a separate rule for each interface.

Valid in

Each bandwidth managament rule can be valid in certain time range only — e.g. stricter resctrictions are usually applied within working hours. In a nutshell, time intervals (see chapter 16.2) allow to define any time-related condition.

Internet Traffic Chart

Timeline for Internet traffic matching the rule can be viewed under *Status* → *Traffic Charts* (up to 24 hours back). The chart shows how much the particular traffic loads the Internet link and helps you optimize bandwidth management rules (e.g. if you have reserved or limited too large bandwidth for certain service, you can make corresponding changes). Local traffic is not recorded.

11.4 How detection of large data transfer connections works

This chapter provides description of the method used by the *Bandwidth Management* module to detect connections where large data volumes are transmitted. This description is an extra information which is not necessary for usage of the bandwidth management module.

Network traffic is different for individual services. For example, web browsers usually access sites by opening one or more connections and using them to transfer certain amount of data (objects included at the page) and then closes the connections. Terminal services (e.g. *Telnet*, *SSH*, etc.) typically use an open connection to transfer small data volumes in longer intervals. Large data volume transfers typically uses the method where the data flow continuously with minimal intervals between the transfer impulses.

Two basic parameters are tested in each connection: volume of transferred data and duration of the longest idle interval. If the specified data volume is reached without the idleness interval having been thresholded, the connection is considered as a transfer of large data volume and corresponding limits are applied.

If the idle time exceeds the defined value, the transferred data counter is set to zero and the process starts anew. This implies that each connection that *once* reaches the defined values is considered as a large data volume transfer.

Boundary value of transfer data volume and minimal idle time are optimized in accordance with results of long-term testing.

Examples:

The detection of connections transferring large data volumes will be better understood through the following examples. The default configuration of the detection is as follows: at least *200 KB* of data must be transferred while there is no interruption for *5 sec* or more.

1. The connection at figure 11.1 is considered as a transmission of large data volume after transfer of the third load of data. At this point, the connection has transferred 200 KB of data while the longest idleness interval has been only 3 sec.

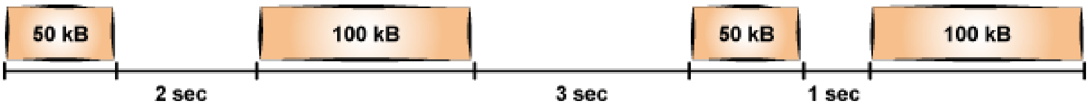


Figure 11.1 Connection example — short idleness intervals

2. Connection at figure 11.2 is not considered as a large data volume transfer, since after 150 KB of data have been transferred before an only 5 sec long idleness interval and then, only other 150 KB of data have been transmitted within the connection.

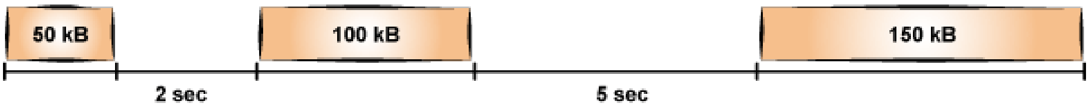


Figure 11.2 Connection example — long idleness interval

3. The connection shown at figure 11.3 transfers 100 KB of data before a 6 sec idleness interval. For this reason, the counter of transferred data is set to zero. Other three blocks of data of 100 KB are then transmitted. When the third block of data is transferred, only 200 KB of transmitted data are recorded at the counter (since the last long idleness interval). Since there is only a 3 sec idleness interval between transmission of the second and the third block of data, the connection is considered as a large data volume transfer.

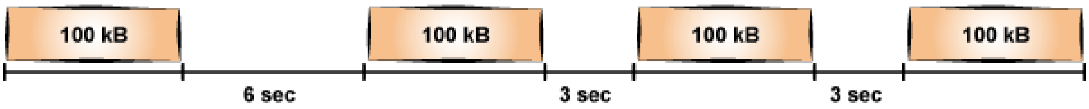


Figure 11.3 Connection example — long idleness interval at the beginning of the transfer

Chapter 12

User Authentication

Kerio Control allows administrators to monitor connections (packet, connection, web pages or FTP objects and command filtering) related to each user. The username in each filtering rule represents the IP address of the host(s) from which the user is connected (i.e. all hosts the user is currently connected from). This implies that a user group represents all IP addresses its members are currently connected from.

Besides access restrictions, user authentication can be used also for monitoring of their activities in the *Kerio StaR* interface (see chapter 22), in logs (see chapter 23), in the list of opened connections (see chapter 20.2) and in the overview of hosts and users (see chapter 20.1). If there is no user connected from a certain host, only the IP address of the host will be displayed in the logs and statistics. In statistics, this host's traffic will be included in the group of *not logged in* users.

12.1 Firewall User Authentication

Any user with their own account in *Kerio Control* can authenticate at the firewall (regardless their access rights). Users can connect:

- Manually — by opening the *Kerio Control* web interface in their browser

  `https://server:4081/` or `http://server:4080/`

  (the name of the server is only an example — see chapter 13).

  It is also possible to authenticate for viewing of the web statistics (see chapter 22) at

  `https://server:4081/star` or `http://server:4080/star`

  Note: Login to the *Administration* interface at
  `https://server:4081/admin` or `http://server:4080/admin`
  is not equal to user authentication at the firewall (i.e. the user does not get authenticated at the firewall by the login)!

- Automatically — IP addresses of hosts from which they will be authenticated automatically can be associated with individual users. This actually means that whenever traffic coming from the particular host is detected, *Kerio Control* assumes that it is currently used by the particular user , and the user is considered being authenticated from the IP address. However, users may authenticate from other hosts (using the methods described above).

  IP addresses for automatic authentication can be set during definition of user account (see chapter 17.1).

This authentication method is not recommended for cases where hosts are used by multiple users (user's identity might be misused easily).

- Redirection — when accessing any website (unless access to this page is explicitly allowed to unauthenticated users — see chapter 14.2).

  Login by re-direction is performed in the following way: user enters URL pages that he/she intends to open in the browser. *Kerio Control* detects whether the user has already authenticated. If not, *Kerio Control* will re-direct the user to the login page automatically. After a successful login, the user is automatically re-directed to the requested page or to the page including the information where the access was denied.

- Using NTLM — if *Internet Explorer* or *Firefox/SeaMonkey* is used and the user is authenticated in a *Windows NT* domain or *Active Directory*, the user can be authenticated automatically (the login page will not be displayed). For details, see chapter 26.3.

User authentication advanced options

Login/logout parameters can be set on the *Authentication Options* tab under *Users and Groups* → *Users*.

Redirection to the authentication page

If the *Always require users to be authenticated when accessing web pages* option is enabled, user authentication will be required for access to any website (unless the user is already authenticated). The method of the authentication request depends on the method used by the particular browser to connect to the Internet:

- *Direct access* — the browser will be automatically redirected to the authentication page of the *Kerio Control's* web interface (see chapter 13.2) and, if the authentication is successful, to the solicited web page.
- *Kerio Control proxy server* — the browser displays the authentication dialog and then, if the authentication is successful, it opens the solicited web page.

If the *Always require users to be authenticated when accessing web pages* option is disabled, user authentication will be required only for Web pages which are not available (are denied by URL rules) to unauthenticated users (refer to chapter 14.2).

Note: User authentication is used both for accessing a Web page (or/and other services) and for monitoring of activities of individual users (the Internet is not anonymous).

Force non-transparent proxy server authentication

Under usual circumstances, a user connected to the firewall from a particular computer is considered as authenticated by the IP address of the host until the moment when they log out manually or are logged out automatically for inactivity. However, if the client station allows multiple users connected to the computer at a moment (e.g. *Microsoft Terminal Services*, *Citrix Presentation Server* or*Fast user switching* on *Windows XP*, *Windows Server 2003*, *Windows Vista* and *Windows Server 2008*), the firewall requires authentication only from the user who starts to work on the host as the first. The other users will be authenticated as this user.

In case of *HTTP* and *HTTPS*, this technical obstruction can be passed by. In web browsers of all clients of the multi-user system, set connection to the Internet via the *Kerio Control's* proxy server (for details, see chapter 10.5), and enable the *Enable non-transparent proxy server* option in *Kerio Control*. The proxy server will require authentication for each new session of the particular browser.[6].

Forcing user authentication on the proxy server for initiation of each session may bother users working on "single-user" hosts. Therefore, it is desirable to force such authentication only for hosts used by multiple users. For this purpose, you can use the *Apply only for these IP addresses* option.

Automatic authentication (NTLM)

If the *Enable user authentication automatically...* option is checked and *Internet Explorer* or *Firefox/SeaMonkey* is used, it is possible to authenticate the user automatically using the NTLM method.

This means that the browser does not require username and password and simply uses the identity of the first user connected to *Windows*. However, the NTLM method is not available for other operating systems.

For details, refer to chapter 26.3.

Automatically logout users when they are inactive

Timeout is a time interval (in minutes) of allowed user inactivity. When this period expires, the user is automatically logged out from the firewall. The default timeout value is 120 minutes (2 hours).

This situation often comes up when a user forgets to logout from the firewall. Therefore, it is not recommended to disable this option, otherwise login data of a user who forgot to logout might be misused by an unauthorized user.

[6] *Session* is every single period during which a browser is running. For example, in case of *Internet Explorer*, *Firefox* and *Google Chrome*, a session is terminated whenever all windows and tabs of the browser are closed, while in case of *SeaMonkey*, a session is not closed unless the *Quick Launch* program is stopped (an icon is displayed in the toolbar's notification area when the program is running).

Chapter 13

Web Interface

Kerio Control includes a special web server which provides an interface where statistics can be viewed (*Kerio StaR*), as well as for firewall administration via web browser (the *Kerio Control Administration* interface) and for setting of some user account parameters. Access to the web interaced is secured by SSL so that the network communication cannot be tapped and fragile data such as user password and other cannot be misused.

Use the following URL (`server` refers to the name or IP of the *Kerio Control* host, `4081` represents a web interface port) to open the firewall's web interface.

`https://server:4081/`

It is also possible to use the unsecured version of the administration web interface on port `4080`:

`https://server:4080/`

By default, the unsecured web interface is available only on the firewall's local loopback address (`localhost`, typically `127.0.0.1`). Connections to port `4080` from outside computers will be redirected to the secured web interface automatically (`https://server:4081/`). This behavior can be changed in *Configuration* → *Advanced options*, on the *Web Interface* tab (see chapter 13.1).

Web interface ports cannot be changed.

This chapter addresses the web interface configuration in the *Kerio Control's* administration program. *Kerio StaR* and user web interface are addressed in detail in the *Kerio Control — User's Guide*.

13.1 Web interface and certificate settings information

To configure*Kerio Control* web interface, go to the *Web Interface* folder in *Configuration* → *Advanced Options*.

In the upper section you can find links to unsecured versions of the firewall's web interface and the administration interface (*Kerio Control Administration*). Lower you can get information about the SSL certificate used for the secured version of the web interface and an option to change the certificate if desirable.

By disabling option *Force SSL secured connection* it is possible to allow access to the unsecured web interface (including the administration interface) from any computer. However, for security reasons, it is recommended to keep this option enabled and always use the secure web interface.

SSL Certificate for the Web Interface

The principle of an encrypted *Kerio Control* web interface is based on the fact that all communication between the client and server is encrypted to protect it from wiretapping and misuse of the transmitted data. The SSL protocol uses an asymmetric encryption first to facilitate exchange of the symmetric encryption key which will be later used to encrypt the transmitted data.

The asymmetric cipher uses two keys: a public one for encrypting and a private one for decrypting. As their names suggest, the public (encrypting) key is available to anyone wishing to establish a connection with the server, whereas the private (decrypting) key is available only to the server and must remain secret. The client, however, also needs to be able to identify the server (to find out if it is truly the server and not an impostor). For this purpose there is a certificate, which contains the public server key, the server name, expiration date and other details. To ensure the authenticity of the certificate it must be certified and signed by a third party, the certification authority.

Communication between the client and server then follows this scheme: the client generates a symmetric encryption key for and encrypts it with the public server key (obtained from the server certificate). The server decrypts it with its private key (kept solely by the server). Thus the symmetric key is known only to the server and client. This key is then used for encryption and decipher any other traffic.

Generate or Import Certificate

During *Kerio Control* installation, a testing certificate for the SSL-secured Web interface is created automatically (it is stored in the `sslcert` subdirectory under the *Kerio Control's* installation directory, in the `server.crt` file; the private key for the certificate is saved as `server.key`). The certificate created is unique. However, it is issued against a non-existing server name and it is not issued by a trustworthy certificate authority. This certificate is intended to ensure functionality of the secured Web interface (usually for testing purposes) until a new certificate is created or a certificate issued by a public certificate authority is imported.

Click on the *Change SSL certificate* (in the dialog for advanced settings for the Web interface) to view the dialog with the current server certificate. By selecting the *Field* (certificate entry) option you can view information either about the certificate issuer or about the subject represented by your server.

You can obtain your own certificate, which verifies your server's identity, by two means.

You can create your own self-signed certificate. Click *Generate Certificate* in the dialog where current server status is displayed. Insert required data about the server and your company into the dialog entries. Only entries marked with an asterisk (*) are required.

Click on the *OK* button to view the *Server SSL certificate* dialog. The certificate will be started automatically (you will not need to restart your operating system). When created, the certificate is saved as `server.crt` and the corresponding private key as `server.key`.

A new (*self-signed*) certificate is unique. It is created by your company, addressed to your company and based on the name of your server. Unlike the testing version of the certificate, this certificate ensures your clients security, as it is unique and the identity of your server is guaranteed by it. Clients will be warned only about the fact that the certificate was not issued by a trustworthy certification authority. However, they can install the certificate in the browser without worrying since they are aware of who and why created the certificate. Secure communication is then ensured for them and no warning will be displayed again because your certificate has all it needs.

Another option is to purchase a full certificate from a public certification authority (e.g. *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode*, etc.).

To import a certificate, open the certificate file (`*.crt`) and the file including the corresponding private key (`*.key`). These files are stored in `sslcert` under the *Kerio Control's* installation directory.

The process of certification is quite complex and requires a certain expertise. For detailed instructions contact Kerio technical support.

13.2 User authentication at the web interface

User authentication is required for access to the *Kerio Control's* web interface. Any user with their own account in *Kerio Control* can authenticate to the web interface. Depending on the right to view statistics (see chapter 17.2), either *Kerio StaR* is opened or a page with status information and personal preferences is displayed upon logon.

If more than one domain are used (see chapter"/>sect-domains"/>), the following rules apply to the user name:

- *Local user account* — the name must be specified without the domain (e.g. `admin`),
- *Primary domain* — missing domain is acceptable in the name specification (e.g. `jsmith`), but it is also possible to include the domain (e.g. `jsmith@company.com`),
- *Other domains* — the name specified must include the domain

  (e.g. `drdolittle@usoffice.company.com`).

If none or just one domain is mapped, all users can authenticate by their usernames without the domain specified.

Note: Authentication at the web interface is a basic user authentication method at the firewall. Other authentication methods are described in chapter 12.1.

Chapter 14

HTTP and FTP filtering

Kerio Control provides a wide range of features to filter traffic using HTTP and FTP protocols. These protocols are the most spread and the most used in the Internet.

Here are the main purposes of HTTP and FTP content filtering:

- to block access to undesirable Web sites (i.e. pages that do not relate to employees' work)
- to block certain types of files (i.e. illegal content)
- to block or to limit viruses, worms and Trojan horses

Let's focus on filtering options featured by *Kerio Control*. For their detailed description, read the following chapters.

HTTP protocol — web pages filtering:

- access limitations according to URL (substrings contained in URL addresses)
- blocking of certain HTML items (i.e. scripts, *ActiveX* objects, etc.)
- filtering based on classification by the *Kerio Web Filter* module (worldwide website classification database)
- limitations based on occurrence of denied words (strings)
- antivirus control of downloaded objects

FTP protocol — control of access to FTP servers:

- access to certain FTP servers is denied
- limitations based on or file names
- transfer of files is limited to one direction only (i.e. download only)
- certain FTP commands are blocked
- antivirus control of transferred files

Note: Kerio Control provides only tools for filtering and access limitations. Decisions on which websites and files will be blocked must be made by the administrator (or another qualified person).

14.1 Conditions for HTTP and FTP filtering

For HTTP and FTP content filtering, the following conditions must be met:

1. Traffic must be controlled by an appropriate protocol inspector.

An appropriate protocol inspector is activated automatically unless its use is denied by traffic rules. For details, refer to chapter 8.3.

2. Connections must not be encrypted. SSL encrypted traffic (HTTPS and FTPS protocols) cannot be monitored. In this case you can block access to certain servers using traffic rules (see chapter 8.3).

3. FTP protocols cannot be filtered if the secured authentication (*SASO*) is used.

4. Both HTTP and FTP rules are applied also when the *Kerio Control's* proxy server is used (then, condition 1 is irrelevant). However, FTP protocol cannot be filtered if the parent proxy server is used (for details, see chapter 10.5). In such a case, FTP rules are not applied.

5. If the proxy server is used (see chapter 10.5), It is also possible to filter HTTPS servers (e.g. `https://secure.kerio.com/`). However, it is not possible to filter individual objects at these servers.

14.2 URL Rules

These rules allow the administrator to limit access to Web pages with URLs that meet certain criteria. They include other functions, such as filtering of web pages by occurrence forbidden words, blocking of specific items (scripts, active objects, etc.) and antivirus switch for certain pages.

To define URL rules, go to the *URL Rules* tab in *Configuration* → *Content Filtering* → *HTTP Policy*.

Rules in this section are tested from the top of the list downwards (you can order the list entries using the arrow buttons at the right side of the dialog window). If a requested URL passes through all rules without any match, access to the site is allowed. All URLs are allowed by default (unless denied by a URL rule).

Note: URLs which do not match with any URL rule are available for any authenticated user (any traffic permitted by default). To allow accessing only a specific web page group and block access to other web pages, a rule denying access to any URL must be placed at the end of the rule list.

The following items (columns) can be available in the *URL Rules* tab:

- *Description* — description of a particular rule (for reference only). You can use the checking box next to the description to enable/disable the rule (for example, for a certain time).

- *Action* — action which will be performed if all conditions of the rule are met (*Permit* — access to the page will be allowed, *Deny* — connection to the page will be denied and denial information will be displayed, *Drop* — access will be denied and a blank page will be opened, *Redirect* — user will be redirected to the page specified in the rule).

- *Condition* — condition which must be met to apply the rule (e.g. URL matches certain criteria, page is included in a particular category of the *Kerio Web Filter* database, etc.).
- *Properties* — advanced options for the rule (e.g. anti-virus check, content filtering, etc.).
- *IP Groups* — IP group to which the rule is applied. The IP groups include addresses of clients (workstations of users who connect to the Internet through *Kerio Control*).
- *Valid Time* — time interval during which the rule is applied.
- *Users List* — list of users and user groups to which the rule applies.

Note: The default *Kerio Control* configuration includes a set of predefined rules for URL traffic. These rules are disabled by default. These rules are available to the firewall administrators.

URL Rules Definition

To create a new rule, select a rule after which the new rule will be added, and click *Add*. You can later use the arrow buttons to reorder the rule list.

You can double-click on individual items (columns) to set rule parameters.

Name

Rule name (for better reference).

Action, Properties

Actions applied on pages matching the rule and additional settings for the particular action:

- *Allow* — traffic allowed, user does not even notice anything happening.
  The following additional actions can be set for allowed pages:
  - *Filter out HTML Java applets* (filtering of all `<applet>` elements),
  - *Filter out HTML ActiveX objects* (filtering of all `<embed>` elements),
  - *Filter out HTML Script tags* (filtering of all `<script>` elements),
  - *Filter out HTML JavaScript pop-up windows* (so called pop-up blocker),
  - *Filter out cross-domain referer* (referers are often used for monitoring from which page the visitor came to the particular page),
  - *Deny web pages containing forbidden words in HTML code* (see chapter 14.4),
  - *Skip anti-virus scanning* (this option may speed up access to trusted pages; however, it is recommended to perform antivirus check).
- *Deny* — user will be redirected to the firewall page with informing that access is denied.
  It is useful to add information about the reason for the denial. Users with corresponding rights (see chapter 17.2) can be allowed to “unlock” the page. All unlocked pages are logged in the *Security* log (see chapter 23.11).

- *Drop* — access is denied and the user will see the page as unavailable.
- *Redirect* — user will be automatically redirected to the specified URL (required parameter).

URL

URL to which the rule applies:

- *URL beginning with* — any URL starting with the specified string. It is possible to use wildcards * (asterisk) and ? (question mark).
  Example: `*.kerio.com`
- *URL from the group* — any URL belonging to the selected URL group.
- *URL rated by Kerio Web Filter rating system* — all pages sorted in the selected categories by the *Kerio Web Filter* module.
- *any URL where server is specified by an IP address* (experienced users may use this method to get through URL rules).

MIME type

MIME type of objects (downloaded files) to which the rule applies. It is possible to use wildcard * (asterisk). A stand-alone asterisk stands for any MIME type.

Source

IP address group to which the rule applies.
Setting the value to *Any* annuls IP address restrictions.

Valid in

Time interval within which the rule will be valid.

Log

Enables/disables logging of all HTTP queries matching this rule in the *Filter* log (see chapter 23.9).

HTTP Inspection Advanced Options

Use the *Apply filtering rules also for local server* to specify whether content filtering rules will be applied to local WWW servers which are available from the Internet (see chapter 8). This option is disabled by default — the protocol inspector only scans HTTP protocol syntax and performs logging of queries (web pages) according to the settings.

14.3 Content Rating System (Kerio Web Filter)

The *Kerio Web Filter* module enables *Kerio Control* to rate web page content. Each page is sorted into predefined categories. Access to the page will be either permitted or denied according to this classification.

Kerio Web Filter uses a dynamic worldwide database which includes URLs and classification of web pages. This database is maintained by special servers that perform page ratings. Whenever a user attempts to access a web page, *Kerio Control* sends a request on the page rating. According to the classification of the page the user will be either allowed or denied to access the page. To speed up URL rating the data that have been once acquired can be stored in the cache and kept for a certain period.

Note: A special license is bound with *Kerio Web Filter*. Unless *Kerio Control* includes this module, the module behaves as a trial version only (this means that it is automatically disabled after 30 days from the *Kerio Control* installation and options in the *Kerio Web Filter* tab will not be available). For detailed information about the licensing policy, read chapter 55.

Kerio Web Filter configuration

The *Kerio Web Filter* module can be set and configured through the *Kerio Web Filter* tab in *Configuration → Content Filtering → HTTP Policy*.

Enable Kerio Web Filter

use this option to enable/disable the *Kerio Web Filter* module for classification of websites.
If *Kerio Web Filter* is disabled:

- the other options in the *Kerio Web Filter* tab are not available,
- all URL rules which use the *Kerio Web Filter* classification are disabled (for details, refer to chapter 14.2).

Categorize each page regardless of HTTP rules...

If this option is enabled, *Kerio Web Filter* categorization will be applied to any web pages (i.e. to all HTTP requests processed by the *HTTP* protocol inspector).
Categorization of all pages is necessary for statistics of the categories of visited web pages (see chapter 22). If you do not intend to keep these statistics, it is recommended disable this option (categorization of all web pages might be demanding and it might decrease *Kerio Control* performance).

Servers (Web sites) not to be rated by the module can be specified in *Kerio Web Filter white list*. Use the *Add* button to open a dialog where a new item (server or a Web page) can be added.

Server

Use the *Server* item to specify web sites not to be classified by the *Kerio Web Filter*. The following items can be specified:

- server name (e.g. `www.kerio.com`). Server name represents any URL at a corresponding server,
- address of a particular webpage without protocol specification (`http://`) — e.g. `www.kerio.com/index.html`,
- URL using wildcard matching (e.g. `*.ker?o.*`). An asterisk stands for any number of characters (even zero), a`*.ker?o.*` question-mark represents just one symbol.

Description

Comments for the items defined. For reference only.

Kerio Web Filter use

To enable classification of Websites by the *Kerio Web Filter* module, this module must be running and all corresponding parameters must be set.

Whenever *Kerio Control* processes a URL rule that requires classification of pages, the *Kerio Web Filter* module is activated. The usage will be better understood through the following example that describes a rule denying all users to access pages containing job offers.

Under *Configuration* → *Content Filter* → *HTTP Policy* on the *URL Rules* tab, enable the predefined rule *Deny sites rated in Kerio Web Filter Categories* (see chapter 14.2).

Double-click o the *URL* column and use the *Select Rating* button to open a dialog where *Kerio Web Filter* rating categories can be chosen. Select the *Job Search / Job offers* rating category (pages including job offers).

Note:

1. You can define multiple URL rules that will use the *Kerio Web Filter* rating technology. Multiple categories may be used for each rule.
2. We recommend you to unlock rules that use the *Kerio Web Filter* rating system (the *Users can Unlock this rule* option in the *Advanced* tab). This option will allow users to unlock pages blocked for incorrect classification. All unlock queries are logged into the *Filter* log — here you can monitor whether unlock queries were appropriate or not.

14.4 Web content filtering by word occurrence

Kerio Control can also filter web pages that include undesirable words.

This is the filtering principle: Denied words are matched with values, called weight (represented by a whole positive integer). Weights of these words contained in a required page are summed (weight of each word is counted only once regardless of how many times the word is included in the page). If the total weight exceeds the defined limit (so called threshold value), the page is blocked.

So called forbidden words are used to filter out web pages containing undesirable words. URL rules (see chapter 14.2) define how pages including forbidden content will be handled.

Warning:
Definition of forbidden words and threshold value is ineffective unless corresponding URL rules are set!

Definition of rules filtering by word occurrence

First, suppose that some forbidden words have been already defined and a threshold value has been set (for details, see below).

On the *URL Rules* tab under *Configuration* → *Content Filtering* → *HTTP Policy*, create a rule (or a set of rules) to allow access to the group of web pages which will be filtered by forbidden words. Double-click on the *Properties* column and enable option *Deny web pages containing forbidden words in HTML code.*

Word groups

To define word groups go to the *Word Groups* tab in *Configuration* → *Content Filtering* → *HTTP Policy*, the *Forbidden Words* tab. Words are sorted into groups. This feature only makes *Kerio Control* easier to follow. All groups have the same priority and all of them are always tested.

Individual groups and words included in them are displayed in form of trees. To enable filtering of particular words use checkboxes located next to them. Unchecked words will be ignored. Due to this function it is not necessary to remove rules and define them again later.

Note: The following word groups are predefined in the default *Kerio Control* installation:

- *Pornography* — words that typically appear on pages with erotic themes,
- *Warez / Cracks* — words that typically appear on pages offering downloads of illegal software, license key generators etc.

All key words in predefined groups are disabled by default. The firewall administrator can enable filtering of the particular words and modify the weight for each word.

Threshold value for Web page filtering

The value specified in *Deny pages with weight over* represents so called threshold weight value for each page (i.e. total weight of all forbidden words found at the page). If the total weight of the tested page exceeds this limit, access to the page will be denied (each word is counted only once, regardless of the count of individual words).

Definition of forbidden words

Use the *Add* button to add a new word into a group or to create a new group.

Group

Selection of a group to which the word will be included. You can also add a new name to create a new group.

Keyword

Forbidden word that is to be scanned for. This word can be in any language and it should follow the exact form in which it is used on websites (including diacritics and other special symbols and characters). If the word has various forms (declension, conjugation, etc.), it is necessary to define separate words for each word in the group. It is also possible to set various weight of words.

Weight

Word weight the level of how the word affects possible blocking or allowing of access to websites. The weight should respect frequency of the particular word in the language (the more common word, the lower weight) so that legitimate webpages are not blocked.

Description

A comment on the word or group.

14.5 FTP Policy

To define rules for access to FTP servers go to *Configuration* → *Content Filtering* → *FTP Rules*.

Rules in this section are tested from the top of the list downwards (you can order the list entries using the arrow buttons at the right side of the dialog window). Testing is stopped when the first convenient rule is met. If the query does not match any rule, access to the FTP server is implicitly allowed.

Note: The default *Kerio Control* configuration includes a set of predefined rules for FTP traffic. These rules are disabled by default. These rules are available to the firewall administrators:

- *Forbid resume due to antivirus scanning* — blocking of download resumption after interruption (so called *resume* — FTP command REST).
  This rule can increase effectivity of the antivirus control (each file will be checked as a whole). However, if larger files are transferred, it can be counterproductive — the probability that a virus code is right at the spot where the interruption took place is very low and repeating of the whole tranfer would burden Internet connection redundantly.
  For details on antivirus scan of FTP protocol, refer to chapter 15.3.
- *Forbid upload* — blocking of uploading files to FTP servers. This is one of the methods that can be used to avoid leak of fragile information from the local network.
- Two rules that block audio and video files downloads — these files are usually large and their download burdens Internet connection. Besides that, such activity is usually quite unproductive.

FTP Rules Definition

To create a new rule, select a rule after which the new rule will be added, and click *Add*. You can later use the arrow buttons to reorder the rule list.

Note: FTP traffic which does not match any FTP rule is allowed (any traffic permitted by default). To allow accessing only a specific group of FTP servers and block access to other web pages, a rule denying access to all FTP servers must be placed at the end of the rule list.

Individual rule parameters can be set upon double-clicking on the particular item (column):

Name

Rule name (for better reference).
Checking the box next to the rule name can be used to “disable” the rule. Rules can be disabled temporarily so that it is not necessary to remove rules and create identical ones later.

Action

Action applied to the traffic.

Features

Additional settings for the selected action:

- Allow — optionally it is possible to disable antivirus check of transferred files (it is recommend to use this option only if there is a good reason and only for trustworthy FTP servers!).
- Deny — no additional settings are available.

Server

FTP servers to which the rule applies:

- Any FTP server,
- Specific FTP server — the server can be defined either by a DNS name or an IP address,
- All FTP servers belonging to the selected IP address group (see chapter 16.1).

Condition

Condition of the rule:

- *Anything* — the rule is applied to any FTP traffic matching all the other defined parameters (*Server*,
  Users, *Source*, *Valid Time*).
- *Upload* — applied to upload of specified files to an FTP server. The name can include wildcards * (asterisk) and ? (question mark). A standalone asterisk stands for any file.
- *Download* — applied to download of specified files from an FTP server.
- *Download /Upload* — applied to download/upload of specified files from/to an FTP server.
- *FTP Command* — the rule is applied to specific FTP commands. Commands can be selected from the list or it is possible to define new commands upon clicking on *Add*.

Users

Selection of users or/and groups which the rule will be applied to.

Source

IP address group to which the rule applies (see chapter 16.1).

Setting the value to *Any* annuls IP address restrictions.

Valid in

Time interval to which the rule applies (see chapter 16.2).

Log

Enables/disables logging of all FTP operations matching this rule in the *Filter* log (see chapter 23.9).

Go to the *Advanced* tab to define other conditions that must be met for the rule to be applied and to set advanced options for FTP communication.

Valid at time interval

Selection of the time interval during which the rule will be valid (apart from this interval the rule will be ignored). Use the *Edit* button to edit time intervals (for details see chapter 16.2).

Valid for IP address group

Selection of IP address group on which the rule will be applied. Client (source) addresses are considered. Use the *Any* option to make the rule independent of clients.
Click on the *Edit* button to edit IP groups (for details see chapter 16.1).

Content

Advanced options for FTP traffic content.
Use the *Type* option to set a filtering method:

- *Download*, *Upload*, *Download / Upload* — transport of files in one or both directions.
  If any of these options is chosen, you can specify names of files on which the rule will be applied using the *File name* entry. Wildcard matching can be used to specify a file name (i.e. `*.exe` for executables).
- *FTP command* — selection of commands for the FTP server on which the rule will be applied
- *Any* — denies all traffic (any connection or command use)

Scan content for viruses according to scanning rules

Use this option to enable/disable scanning for viruses for FTP traffic which meet this rule. This option is available only for allowing rules — it is meaningless to apply antivirus check to denied traffic.

Chapter 15

Antivirus control

Kerio Control provides antivirus check of objects (files) transmitted by HTTP, FTP, SMTP and POP3 protocols. In case of HTTP and FTP protocols, the firewall administrator can specify which types of objects will be scanned.

Kerio Control is also distributed in a special version which includes integrated *Sophos* antivirus. Besides the integrated module, *Kerio Control* also supports many external antiviruses of third parties. The antivirus license must meet the conditions of the producer (usually the same or higher number of users of the licensed version of *Kerio Control* or a special server license).

Kerio Control allows to use both the integrated *Sophos* antivirus and a selected external antivirus. In such a case, transferred files are checked by both antiviruses (so called dual antivirus control). This feature reduces the risk of letting in a harmful file.

However, using of two antiviruses at a time also decreases the speed of firewall's performance. It is therefore highly recommended to consider thoroughly which method of antivirus check should be used and to which protocols it should be applied and, if possible and desired, to try the configuration in the trial version of *Kerio Control* before purchasing a license.

Note:

1. However, supported external antiviruses as well as versions and license policy of individual programs may change as the time flows. For up-to-date information please refer to (http://www.kerio.com/control).
2. External *Sophos* antivirus is not supported by *Kerio Control*.

15.1 Conditions and limitations of antivirus scan

Antivirus check of objects transferred by a particular protocol can be applied only to traffic where a corresponding protocol inspector which supports the antivirus is used (see chapter 16.3). This implies that the antivirus check is limited by the following factors:

- Antivirus check cannot be used if the traffic is transferred by a secured channel (SSL/TLS). In such a case, it is not possible to decipher traffic and separate transferred objects.

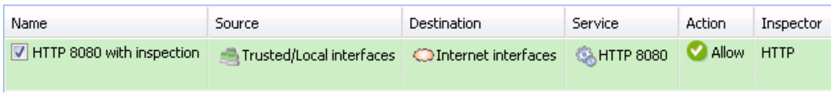
- Within email antivirus scanning (SMTP and POP3 protocols), the firewall only removes infected attachments — it is not possible to drop entire email messages. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Check of outgoing traffic causes problems with temporarily undeliverable email.

For details, see chapter 15.4.

- Object transferred by other than HTTP, FTP, SMTP and POP3 protocols cannot be checked by an antivirus.
- If a substandard port is used for the traffic, corresponding protocol inspector will not be applied automatically. In that case, simply define a traffic rule which will allow this traffic using a corresponding protocol inspector (for details, see chapter 8.3).

  Example: You want to perform antivirus checks of the HTTP protocol at port 8080.

  1. Define the *HTTP 8080* service (TCP protocol, port 8080).
  2. Create a traffic rule which will allow this service applying a corresponding protocol inspector.



Name	Source	Destination	Service	Action	Inspector
☑ HTTP 8080 with inspection	Trusted/Local interfaces	Internet interfaces	HTTP 8080	✓ Allow	HTTP

Figure 15.1 Traffic rule for HTTP protocol inspection at non-standard ports

Add the new rule before the rule allowing access to any service in the Internet (if such a rule exists). If the NAT (source address translation) technology is used for Internet connection, address translation must be set for this rule as well.

Note: A corresponding protocol inspector can be also specified within the service definition, or both definition methods can be used. Both methods yield the same result, however, the corresponding traffic rule is more transparent when the protocol inspector is defined in it.

15.2 How to choose and setup antiviruses

To select antiviruses and set their parameters, open the *Antivirus* tab in *Configuration* → *Content Filtering* → *Antivirus*. Ob this tab, you can select the integrated *Sophos* module, an external antivirus, or both.

If both antiviruses are used, each transferred object (downloaded file, an email attachment, etc.) will be first checked by the integrated *Sophos* antivirus module and then by the other antivirus (a selected external antivirus).

Integrated Sophos antivirus engine

To enable the integrated *Sophos* antivirus, enable *Use integrated Sophos antivirus engine* in the *Antivirus* tab. This option is not available unless the license key for *Kerio Control* includes a license for the *Sophos* antivirus or in trial versions. For detailed information about the licensing policy, read chapter 55.

Use the *Integrated antivirus engine* section in the *Antivirus* tab to set update parameters for *Sophos*.

Check for update every ... hours

Time interval of checks for new updates of the virus database and the antivirus engine (in hours).

If any new update is available, it will be downloaded automatically by *Kerio Control*.

If the update attempt fails (i.e. the server is not available), detailed information about the attempt will be logged into the *Error* log (refer to chapter 23.8).

Each download (update) attempt sets the *Last update check performed* value to zero.

> ***Warning:***
> To make the antivirus control as mighty as possible, it is necessary that the antivirus module is always equipped by the most recent version of the virus database. Therefore, it is recommended to keep automatic updates running and not to set too long intervals between update checks (update checks should be performed at least twice a day).

Current virus database is ...

Information regarding the age of the current database.

Note: If the value is too high, this may indicate that updates of the database have failed several times. In such cases, we recommend you to perform a manual update check by the *Update now* button and view the *Error* log.

Last update check performed ... ago

Time that has passed since the last update check.

Virus database version

Database version that is currently used.

Scanning engine version

Sophos scanning engine version used by *Kerio Control*.

Update now

Use this button for immediate update of the virus database and of the scanning engine.

After you run the update check using the *Update now...* button, an informational window displaying the update check process will be opened. You can use the *OK* button to close it — it is not necessary to wait until the update is finished.

If updated successfully, the version number of the new virus database or/and the new antivirus version(s), as well as information regarding the age of the current virus database will be displayed. If the update check fails (i.e. the server is not available), an error will be reported and detailed information about the update attempt will be logged into the *Error* log.

Each download (update) attempt sets the *Last update check performed* value to zero.

External antivirus

For external antivirus, enable the *Use external antivirus* option in the *Antivirus* tab and select an antivirus to be employed from the combo box. This menu provides all external antivirus programs supported in *Kerio Control* by special *plugins*.

> ***Warning:***
> External antivirus must be installed before it is set in *Kerio Control*, otherwise it is not available in the combo box. It is recommended to stop the *Kerio Control Engine* service before an antivirus installation.

Use the *Options* button to set advanced parameters for the selected antivirus. Dialogs for individual antiviruses differ (some antivirus programs may not require any additional settings). For detailed information on installation and configuration of individual antivirus programs, refer to http://www.kerio.com/control/third-party.

Click *Apply* to test the selected antivirus. If the test is passed successfully, the antivirus will be used from the moment on. If not, an error is reported and no antivirus will be set. Detailed information about the failure will be reported in the *Error* log (see chapter 23.8).

Antivirus settings

Check items in the *Settings* section of the *Antivirus* tab to enable antivirus check for individual application protocols. By default, antivirus check is enabled for all supported modules.

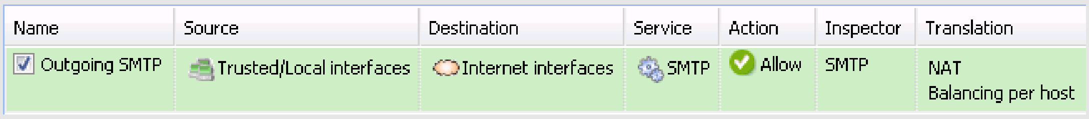
In *Settings*, maximum size of files to be scanned for viruses at the firewall can be set. Scanning of large files are demanding for time, the processor and free disk space, which might affect the firewall's functionality dramatically. It might happen that the connection over which the file is transferred is interrupted when the time limit is exceeded.

The optimal value of the file size depends on particular conditions (the server's performance, load on the network, type of the data transmitted, antivirus type, etc.). *Caution! We strongly discourage administrators from changing the default value for file size limit. In any case, do not set the value to more than 4 MB.*

Parameters for HTTP and FTP scanning can be set in the *HTTP and FTP scanning* (refer to chapter 15.3), while SMTP and POP3 scanning can be configured in the *Email scanning* tab (see chapter 15.4).

Warning:

1. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Checks of outgoing SMTP traffic (from the local network to the Internet) might cause problems with temporarily undeliverable email — for example in cases where the destination SMTP server uses so called *greylisting*.
   To perform smooth checks of outgoing traffic, define a corresponding traffic rule using the SMTP protocol inspector. Such rule may be useful for example if clients in the local network send their email via an SMTP server located in the Internet. Checking of outgoing SMTP traffic is not apt for local SMTP servers sending email to the Internet.
   An example of a traffic rule for checking of outgoing SMTP traffic is shown at figure 15.2.



Name	Source	Destination	Service	Action	Inspector	Translation
☑ Outgoing SMTP	Trusted/Local interfaces	Internet interfaces	SMTP	✓ Allow	SMTP	NAT Balancing per host

Figure 15.2 An example of a traffic rule for outgoing SMTP traffic check

2. Substandard extensions of the SMTP protocol can be used in case of communication of two *Microsoft Exchange* mailservers. Under certain conditions, email messages are transmitted in form of binary data. In such a case, *Kerio Control* cannot perform antivirus check of individual attachments.
   In such cases, it is recommended to use an antivirus which supports *Microsoft Exchange* and not to perform antivirus check of SMTP traffic of a particular server in *Kerio Control*. To achieve this, disable antivirus check for SMTP protocol or define a corresponding traffic rule where no protocol inspector will be applied (see chapter 8.7).

15.3 HTTP and FTP scanning

As for HTTP and FTP traffic, objects (files) of selected types are scanned.

The file just transmitted is saved in a temporary file on the local disk of the firewall. *Kerio Control* caches the last part of the transmitted file (segment of the data transferred) and performs an antivirus scan of the temporary file. If a virus is detected in the file, the last segment of the data is dropped. This means that the client receives an incomplete (damaged) file which cannot be executed so that the virus cannot be activated. If no virus is found, *Kerio Control* sends the client the rest of the file and the transmission is completed successfully.

Optionally, a warning message informing about a virus detected can be sent to the user who tried to download the file (see the *Notify user by email* option).

Warning:

1. The purpose of the antivirus check is only to detect infected files, it is not possible to heal them!
2. If the antivirus check is disabled in HTTP and FTP filtering rules, objects and files matching corresponding rules are not checked. For details, refer to chapters 14.2 and 14.5).
3. Full functionality of HTTP scanning is not guaranteed if any non-standard extensions to web browsers (e.g. download managers, accelerators, etc.) are used!

To set parameters of HTTP and FTP antivirus check, open the *HTTP, FTP scanning* tab in *Configuration → Content Filtering → Antivirus*.

Use the *If a virus is found...* entry to specify actions to be taken whenever a virus is detected in a transmitted file:

- *Move the file to quarantine* — the file will be saved in a special directory on the firewall. *Kerio Control* administrators can later try to heal the file using an antivirus program and if the file is recovered successfully, the administrator can provide it to the user who attempted to download it.

  The `quarantine` subdirectory under the *Kerio Control* installation directory is used for the quarantine

  On Windows: `C:\Program Files\Kerio\WinRoute Firewall\quarantine`

  In other editions: `/opt/kerio/winroute/quarantine`

  Infected files (files which are suspected of being infected) are saved into this directory with names which are generated automatically. Name of each file includes information about protocol, date, time and connection number used for the transmission.

  > ***Warning:***
  > When handling files in the `quarantine` directory, please consider carefully each action you take, otherwise a virus might be activated and the *Kerio Control* host could be attacked by the virus!

- *Alert the client* — *Kerio Control* alerts the user who attempted to download the file by an email message warning that a virus was detected and download was stopped for security reasons.

  Kerio Control sends alert messages under the following circumstances: The user is authenticated and connected to the firewall, a valid email address is set in a corresponding user account (see chapter 17.1) and the SMTP server used for mail sending is configured correctly (refer to chapter 19.3).

Note: Regardless of the fact whether the *Alert the client* option is used, alerts can be sent to specified addresses (e.g. addresses of network administrators) whenever a virus is detected. For details, refer to chapter 20.4.

In the *If the transferred file cannot be scanned* section, actions to be taken when the antivirus check cannot be applied to a file (e.g. the file is compressed and password-protected, damaged, etc.):

- *Deny transmission of the file* — *Kerio Control* will consider these files as infected and deny their transmission.

  > ***Hint:***
  > It is recommended to combine this option with the *Move the file to quarantine* function — the firewall administrator can extract the file and perform manual antivirus check in response to user requests.

- *Allow the file to be transferred* — *Kerio Control* will treat compressed password-protected files and damaged files as trustful (not infected).

  Generally, use of this option is not secure. However, it can be helpful for example when users attempt to transmit big volume of compressed password-protected files and the antivirus is installed on the workstations.

HTTP and FTP scanning rules

These rules specify when antivirus check will be applied. By default (if no rule is defined), all objects transmitted by HTTP and FTP are scanned.

Kerio Control contains a set of predefined rules for HTTP and FTP scanning. By default, all executable files as well as all *Microsoft Office* files are scanned. The firewall administrator can change the default configuration.

Scanning rules are ordered in a list and processed from the top. Arrow buttons on the right can be used to change the order. When a rule which matches the object is found, the appropriate action is taken and rule processing is stopped.

New rules can be created in the dialog box which is opened after clicking the *Add* button.

Description

Comment on the rule (for use of the firewall administrator).

Condition

Condition of the rule:

- *HTTP/FTP filename*

— this option filters out certain filenames (not entire URLs) transmitted by FTP or HTTP (e.g. `*.exe`, `*.zip`, etc.).

If only an asterisk is used for the specification, the rule will apply to any file transmitted by HTTP or FTP.

The other two conditions can be applied only to HTTP:

- *MIME type*
  — MIME types can be specified either by complete expressions (e.g. `image/jpeg`) or using a wildcard matching (e.g. `application/*`).
- *URL* — URL of the object (e.g. `www.kerio.com/img/logo.gif`), a string specified by a wildcard matching (e.g. `*.exe`) or a server name (e.g. `www.kerio.com`). Server names represent any URL at a corresponding server (`www.kerio.com/*`).

If a MIME type or a URL is specified only by an asterisk, the rule will apply to any HTTP object.

Action

Settings in this section define whether or not the object will be scanned.

If the *Do not scan* alternative is selected, antivirus control will not apply to transmission of this object.

The new rule will be added after the rule which had been selected before

Add was clicked. You can use the arrow buttons on the right to move the rule within the list.

Checking the box next to the rule can be used to disable the rule. Rules can be disabled temporarily so that it is not necessary to remove rules and create identical ones later.

If the object does not match with any rule, it will be scanned automatically. If only selected object types are to be scanned, a rule disabling scanning of any URL or MIME type must be added to the end of the list (the *Skip all other files* rule is predefined for this purpose).

15.4 Email scanning

SMTP and POP3 protocols scanning settings are defined through this tab. If scanning is enabled for at least one of these protocols, all attachments of transmitted messages are scanned.

Individual attachments of transmitted messages are saved in a temporary directory on the local disk. When downloaded completely, the files are scanned for viruses. If no virus is found, the attachment is added to the message again. If a virus is detected, the attachment is replaced by a notice informing about the virus found.

Note: Warning messages can also be sent to specified email addresses (e.g. to network administrators) when a virus is detected. For details, refer to chapter 20.4.

Warning:

1. Email antivirus control can only detect and block infected attachments. Attached files cannot be healed by this control!

2. Within antivirus scanning, it is possible to remove only infected attachments, entire email messages cannot be dropped. This is caused by the fact that the firewall cannot handle email messages like mailservers do. It only maintains network traffic coming through. In most cases, removal of an entire message would lead to a failure in communication with the server and the client might attempt to send/download the message once again. Thus, one infected message might block sending/reception of any other (legitimate) mail.

3. In case of SMTP protocol, only incoming traffic is checked (i.e. traffic from the Internet to the local network — incoming email at the local SMTP server). Checks of outgoing SMTP traffic (i.e. from the local network to the Internet) might cause problems with temporarily undeliverable email (for example in cases where the destination SMTP server uses so called *greylisting*).
   To check also outgoing traffic (e.g. when local clients connect to an SMTP server without the local network), define a corresponding traffic rule using the SMTP protocol inspector. For details, see chapter 15.2.

Advanced parameters and actions that will be taken when a virus is detected can be set in the *Email scanning* tab.

In the *Specify an action which will be taken with attachments...* section, the following actions can be set for messages considered by the antivirus as infected:

- *Save message to quarantine* — untrustworthy messages will be moved to a special directory on the *Kerio Control* host. The *Kerio Control* administrator can try to heal infected files and later send them to their original addressees.

  The `quarantine` subdirectory under the *Kerio Control* installation directory is used for the quarantine

  On Windows: `C:\Program Files\Kerio\WinRoute Firewall\quarantine`

  In other editions: `/opt/kerio/winroute/quarantine`

  Messages with untrustworthy attachments are saved to this directory under names which are generated automatically by *Kerio Control*. Each filename includes information about protocol, date, time and the connection number used for transmission of the message.

- *Prepend subject message with text* — use this option to specify a text to be attached before the subject of each email message where at least one infected attachment is found. This text informs the recipient of the message and it can be also used for automatic message filtering.

Note: Regardless of what action is set to be taken, the attachment is always removed and a warning message is attached instead.

Use the *TLS connections* section to set firewall behavior for cases where both mail client and the server support TLS-secured SMTP or POP3 traffic.

In case that TLS protocol is used, unencrypted connection is established first. Then, client and server agree on switching to the secure mode (encrypted connection). If the client or the server does not support TLS, encrypted connection is not used and the traffic is performed in a non-secured way.

If the connection is encrypted, firewall cannot analyze it and perform antivirus check for transmitted messages. The firewall administrator can select one of the following alternatives:

- Enable TLS. This alternative is suitable for such cases where protection from wiretapping is prior to antivirus check of email.

  Hint:
  In such cases, it is recommended to install an antivirus engine at individual hosts that would perform local antivirus check.

- Disable TLS. Secure mode will not be available. Clients will automatically assume that the server does not support TLS and messages will be transmitted through an unencrypted connection. Firewall will perform antivirus check for all transmitted mail.

The *If an attachment cannot be scanned* section defines actions to be taken if one or multiple files attached to a message cannot be scanned for any reason (e.g. password-protected archives, damaged files, etc.):

- *Reject the attachment — Kerio Control* reacts in the same way as when a virus was detected (including all the actions described above).

- *Allow delivery of the attachment — Kerio Control* behaves as if password-protected or damaged files were not infected.

  Generally, this option is not secure. However, it can be helpful for example when users attempt to transmit big volume of compressed password-protected files (typically password-protected archives) and the antivirus is installed on the workstations.

15.5 Scanning of files transferred via Clientless SSL-VPN (Windows)

If *Kerio Control* is installed on *Windows*, the antivirus check is performed also for transfers of files between the local network and a remote client via *Clientless SSL-VPN* (see chapter 25). The *SSL-VPN Scanning*tab allows to set advanced parameters for scanning of files transferred via this interface. In *Kerio Control* administration in editions *Appliance* and *Box*, the *SSL-VPN Scanning* option is not available.

Transfer directions

Use the top section of the *SSL-VPN Scanning* tab to set to which transfer direction the antivirus check will be applied. By default, only files downloaded from a remote client to a local host are scanned to avoid slowdown (local network is treated as trustworthy).

If the antivirus check fails

Options in the lower section of the tab specify an action which will be performed if a file cannot be scanned for any reason (encrypted or corrupted files, etc.). By default, transfer of such files is denied.

Chapter 16

Definitions

16.1 IP Address Groups

IP groups are used for simple access to certain services (e.g. *Kerio Control's* remote administration, Web server located in the local network available from the Internet, etc.). When setting access rights a group name is used. The group itself can contain any combination of computers (IP addresses), IP address ranges, subnets or other groups.

Creating and Editing IP Address Groups

You can define IP address groups in *Configuration* → *Definitions* → *IP Address Groups* section.

Click on *Add* to add a new group (or an item to an existing group) and use *Edit* or *Delete* to edit or delete a selected group or item.

The following dialog window is displayed when you click on the *Add* button:

Name

The name of the group. Add a new name to create a new group. Insert the group name to add a new item to an existent group.

Type

Type of the new item:

- *Host* (IP address or DNS name of a particular host),
- *Network / Mask* (subnet with a corresponding mask),
- *IP range* (an interval of IP addresses defined by starting and end IP address including the both limit values),
- *Address group* (another group of IP addresses — groups can be cascaded),
- *Firewall* (a special group including all the firewall's IP addresses, see also chapter 8.3).

IP address, Mask...

Parameters of the new item (related to the selected type).

Description

Commentary for the IP address group. This helps guide the administrator.

Note: Each IP group must include at least one item. Groups with no item will be removed automatically.

16.2 Time Ranges

Time ranges in *Kerio Control* are closely related to traffic policy rules (see chapter 8). The firewall allows its administrator to set a time period where each rule will be applied. These time ranges are actually not a single time interval, but groups that can consist of any number of various intervals and/or single actions.

Using time ranges you can also set dial-up parameters — see chapter 6.

To define time ranges go to *Configuration* → *Definitions* → *Time Ranges*.

Time range types

When defining a time interval three types of time ranges (subintervals) can be used:

Absolute

The time interval is defined with the initial and expiration date and it is not repeated

Weekly

This interval is repeated weekly (according to the day schedule)

Daily

It is repeated daily (according to the hour schedule)

Defining Time Ranges

Time ranges can created, edited and removed in *Configuration* → *Definitions* → *Time Ranges*.

Clicking on the *Add* button will display the following dialog window:

Name

Name (identification) of the time interval. Insert a new name to create a new time range. Insert the name of an existent time range to add a new item to this range.

Description

Time ranges description, for the administrator only

Time Range Type

Time range type: *Daily*, *Weekly* or *Absolute*. The last type refers to the user defined initial and terminal date.

From, To

The beginning and the end of the time range. Beginning and end hours, days or dates can be defined according to the selected time range type

Valid on

Defines days when the interval will be valid. You can either select particular weekdays (*Selected days*) or use one of the predefined options (*All Days*, *Weekday* — from Monday to Friday, *Weekend* — Saturday and Sunday).

16.3 Services

Kerio Control services enable the administrator to define communication rules easily (by permitting or denying access to the Internet from the local network or by allowing access to the local network from the Internet). Services are defined by a communication protocol and by a port number (e.g. the *HTTP* service uses the TCP protocol with the port number 80). You can also match so-called protocol inspector with certain service types (for details see below).

Services can be defined in *Configurations* → *Definitions* → *Services*. Some standard services, such as HTTP, FTP, DNS etc., are already predefined in the default *Kerio Control* installation.

Clicking on the *Add* or the *Edit* button will open a dialog for service definition.

Name

Service identification within *Kerio Control*. It is strongly recommended to use a concise name to keep the program easy to follow.

Description

Comments for the service defined. It is strongly recommended describing each definition, especially with non-standard services so that there will be minimum confusion when referring to the service at a later time.

Protocol

The communication protocol used by the service.
Most standard services uses the *TCP* or the *UDP* protocol, or both when they can be defined as one service with the *TCP/UDP* option. Other options available are *ICMP* and *other*.
The *other* options allows protocol specification by the number in the IP packet header. Any protocol carried in IP (e.g. GRE — protocol number is 47) can be defined this way.

Protocol inspector

Kerio Control protocol inspector (see below) that will be used for this service.

> ***Warning:***
> Each inspector should be used for the appropriate service only. Functionality of the service might be affected by using an inappropriate inspector.

Source Port and Destination Port

If the TCP or UDP communication protocol is used, the service is defined with its port number. In case of standard client-server types, a server is listening for connections on a particular port (the number relates to the service), whereas clients do not know their port in advance (port are assigned to clients during connection attempts). This means that source ports are usually not specified, while destination ports are usually known in case of standard services.
Note: Specification of the source port may be important, for example during the definition of communication filter rules. For details, refer to chapter 8.3.
Source and destination ports can be specified as:

- *Any* — all the ports available (1-65535)
- *Equal to* —a particular port (e.g.80)
- *Greater than*, *Less than* — all ports with a number that is either greater or less than the number defined
- *Not equal to* — all ports that are not equal to the one defined
- *In range* — all ports that fit to the range defined (including the initial and the terminal ones)
- *List* — list of the ports divided by commas (e.g. 80,8000,8080)

Protocol Inspectors

Kerio Control includes special subroutines that monitor all traffic using application protocols, such as HTTP, FTP or others. The modules can be used to modify (filter) the communication or adapt the firewall's behavior according to the protocol type. Benefits of protocol inspectors can be better understood through the two following examples:

1. *HTTP protocol inspector* monitors traffic between clients (browsers) and Web servers. It can be used to block connections to particular pages or downloads of particular objects (i.e. images, pop-ups, etc.).

2. With active FTP, the server opens a data connection to the client. Under certain conditions this connection type cannot be made through firewalls, therefore FTP can only be used in passive mode. The *FTP protocol inspector* distinguishes that the FTP is active, opens the appropriate port and redirects the connection to the appropriate client in the local network. Due to this fact, users in the local network are not limited by the firewall and they can use both FTP modes (active/passive).

The protocol inspector is enabled if it is set in the service definition and if the corresponding traffic is allowed. Each protocol inspector applies to a specific protocol and service. In the default *Kerio Control* configuration, all available protocol inspectors are used in definitions of corresponding services (so they will be applied to corresponding traffic automatically), except protocol inspectors for *SIP*

and *H.323* (*SIP* and *H.323* are complex protocols and protocol inspectors may work incorrectly in some configurations).

To apply a protocol inspector explicitly to another traffic, it is necessary to define a new service where this inspector will be used or to set the protocol inspector directly in the corresponding traffic rule.

Example:
You want to perform inspection of the HTTP protocol at port 8080. Define a new service: TCP protocol, port 8080, HTTP protocol inspector. This ensures that *HTTP* protocol inspector will be automatically applied to any *TCP* traffic at port 8080 and passing through *Kerio Control*.

Note:

1. Generally, protocol inspectors cannot be applied to secured traffic (SSL/TLS). In this case, *Kerio Control* "perceives" the traffic as binary data only. This implies that such traffic cannot be deciphered.
2. Under certain circumstances, appliance of a protocol inspector is not desirable. Therefore, it is possible to disable a corresponding inspector temporarily. For details, refer to chapter 8.7.

16.4 URL Groups

URL Groups enable the administrator to define HTTP rules easily (see chapter 14.2). For example, to disable access to a group of web pages, you can simply define a URL group and assign permissions to the URL group, rather than defining permissions to each individual URL rule. A URL group rule is processed significantly faster than a greater number of separate rules for individual URLs. It is also possible to cascade URL groups.

URL groups can be defined in *Configuration* → *Definitions* → *URL Groups*.

The default *Kerio Control* installation already includes predefined URL groups:

- *Ads/Banners* — common URLs of pages that contain advertisements, banners, etc.
- *Search engines* — top Internet search engines.
- *Windows Updates* — URL of pages requested for automatic updates of Windows.

These URL groups are used in predefined URL rules (see chapter 14.2). The firewall administrator can use predefined groups in their custom rules or/and edit them if needed.

Matching fields next to each item of the group can be either checked to activate or unchecked to disable the item. This way you can deactivate items with no need to remove them and to define them again.

Click on the *Add* button to display a dialog where a new group can be created or a new item can be added to existing groups.

Name

Name of the group in which the new item will be added. Options of the *Name* entry are as follows:

- select a group to which the URL will be added,
- add a name to create a new group where the item will be included.

Type

Type of the item — URL or URL group (groups can be cascaded).

URL / URL Group

URL or URL group that will be added to the group (depending on the item type).
URL can be specified as follows:

- full address of a server, a document or a web page without protocol specification (http://)
- use substrings with the special * and ? characters. An asterisk stands for any number of characters, a question-mark represents one character.

Examples::

- www.kerio.com/index.html — a particular page
- www.* — all URL addresses starting with www.
- www.kerio.com — all URLs at the www.kerio.com server (this string is equal to the www.kerio.com/* string)
- *sex* — all URL addresses containing the sex string
- *sex??.cz* — all URL addresses containing such strings as sexxx.cz, sex99.cz, etc.

Description

The item's description (comments and notes for the administrator).

Chapter 17

User Accounts and Groups

User accounts in *Kerio Control* improve control of user access to the Internet from the local network. User account can also be used for access to the *Kerio Control* administration.

Kerio Control supports several methods of user accounts and groups saving, combining them with various types of authentication, as follows:

Internal user database

User accounts and groups and their passwords are saved in *Kerio Control*. During authentication, usernames are compared to the data in the internal database.

This method of saving accounts and user authentication is particularly adequate for networks without a proper domain, as well as for special administrator accounts (user can authenticate locally even if the network communication fails).

On the other hand, in case of networks with proper domains (*Windows NT*, *Active Directory* or *Open Directory*), local accounts in *Kerio Control* may cause increased demands on administration since accounts and passwords must be maintained twice (at the domain and in *Kerio Control*).

Internal user database with authentication within the domain

User accounts are stored in the *Kerio Control* database. However, users are authenticated at the domain (i.e. password is not stored in the user account in *Kerio Control*). Obviously, usernames in *Kerio Control* must match with the usernames in the domain.

This method is less demanding than local accounts as far as the administration is concerned. When, for example, a user wants to change the password, it can be simply done at the domain and the change will be automatically applied to the account in *Kerio Control*. In addition to this, it is not necessary to create user accounts in *Kerio Control* by hand, as they can be imported from a corresponding domain (*Windows NT* or *Active Directory*).

Transparent cooperation with directory service (domain mapping)

Kerio Control can use accounts and groups stored in *Active Directory* or *Open Directory* directly — no import to the local database is performed. Specific *Kerio Control* parameters are added by the template of the corresponding account. These parameters can also be edited individually.

This type is the least demanding from the administrator's point of view (all user accounts and groups are managed in directory service) and it is the only one that allows using accounts from multiple domains.

Note: In cases when users are authenticated at the domain (i.e. the second and third method), it is recommended to create at least one local account in *Kerio Control* that has both read and write rights, or keep the original `Admin` account. This account provides connection to the *Kerio Control* administration in case of the network or domain server failure.

17.1 Viewing and definitions of user accounts

To define local user accounts, import accounts to the local database or/and configure accounts mapped from the domain, go to the *User Accounts* tab in the *Users and Groups* → *Users* section.

Domain

Use the *Domain* option to select a domain for which user accounts as well as other parameters will be defined. This item provides a list of mapped domains (see chapter"/>sect-domains"/>) and the local (internal) user database.

Search

In upper part of the window, you can enter a user search filter.

The filter is interactive — each symbol typed or deleted defines the string which is evaluated immediately and all accounts including the string in either *Name*, *Full name* or *Description* are viewed. The icon next to the entry can be clicked to clear the filtering string and display all user accounts in the selected domain (if the *Filter* entry is blank, the icon is hidden).

The searching is helpful especially when the domain includes too many accounts which might make it difficult to look up particular items.

Hiding / showing disabled accounts

It is possible to disable accounts in *Kerio Control*. Check the *Hide disabled user accounts* to show only active (enabled) accounts.

Account template

Parameters shared by the most accounts can be defined by a template. Templates simplify administration of user accounts — shared parameters are set just once, when defining the template. It is also possible to configure some accounts (such as administrator accounts) separately, without using the template.

Templates apply to specific domains (or to the local user database). Each template includes parameters of user rights, data transfer quota and rules for content rules (for detailed description of all these parameters, refer to chapter 17.2).

Local user accounts

If the *Local user database* is selected in the *Domain* item, user accounts in *Kerio Control* are listed (complete information on these accounts are stored in the *Kerio Control* configuration database). The following options are available for accounts in the local database:

Add, Edit, Remove

Click *Add*, *Edit* or *Remove* to create, modify or delete local user accounts (for details, see chapter 17.2). It is also possible to select more than one account by using the `Ctrl` and `Shift` keys to perform mass changes of parameters for all selected accounts.

Importing accounts from a domain

Accounts can be imported to the local database from the *Windows NT* domain or from *Active Directory*. Actually, this process includes automatic copying of domain accounts (account authenticating at the particular domain) to newly created local accounts. For detailed information about import of user accounts, refer to chapter 17.3.

Import of accounts is recommended in case of the *Windows NT* domain. If *Active Directory* or *Open Directory* domain is used, it is recommended to use the transparent cooperation (so called domain mapping — see chapter 17.4).

Accounts mapped from Active Directory or Open Directory

If any of the mmaped domains is selected as *Domain*, user accounts in this domain are listed.

Edit User

For mapped accounts, specific *Kerio Control* parameters can be set (refer to chapter 17.2). These settings are stored in the *Kerio Control's* configuration database. Information stored in directory service (username, full name, email address) and authentication method cannot be edited.

Note: It is also possible to select more than one account by using the `Ctrl` and `Shift` keys to perform mass changes of parameters for all selected accounts.

In mapped domains, it is not allowed to create or/and remove user accounts. Such actions need to be taken directly on the particular domain server. It is also not possible to import user accounts — such an action would take no effect in case of a mapped domain.

17.2 Local user accounts

Local accounts are accounts created in the *Kerio Control* or imported from a domain. These accounts are stored in the *Kerio Control* configuration database (see chapter 26.2). These accounts can be useful especially in domainless environments or for special purposes (typically for the firewall's administration).

Regardless on the method used for creation of the account, each user can be authenticated through the *Kerio Control's* internal database, *Active Directory* or *Windows NT* domain.

The basic administrator account (`Admin`) is created during the *Kerio Control* installation process. This account has full administration rights.

Warning:

1. All passwords should be kept safe and secret, otherwise they might be misused by an unauthorized person.
2. If all accounts with full administration rights are removed and you logout from the *Kerio Control* administration, it is not possible to connect to the *Kerio Control* administration any longer. Under these conditions, a local user account (`Admin` with a blank password) will be created automatically upon the next start of the *Kerio Control Engine*.
3. Provided that you forget your administration password, contact the *Kerio Technologies* technical support (see chapter 27).

Creating a local user account

Open the *User Accounts* tab in the *User and groups* → *Users* section. In the *Domain* combo box, select *Local User Database*. Click on the *Add* button to open a dialog to create a new user account.

General — basic information

Name

Username used for login to the account.

> ***Warning:***
> The user name is not case-sensitive. We recommend not to use special characters (non-English languages) which might cause problems when authenticating at the firewall's web interfaces.

Full name

A full name of the user (usually first name and surname).

Description

User description (e.g. a position in a company).

The *Full Name* and the *Description* items have informative values only. Any type of information can be included or the field can be left empty.

Email address

Email address of the user that alerts (see chapter 20.4) and other information (e.g. alert if a limit for data transmission is exceeded, etc.) will be sent to. A valid email address should be set for each user, otherwise some of the *Kerio Control* features may not be used efficiently.

Note: A relay server must be set in *Kerio Control* for each user, otherwise sending of alert messages to users will not function. For details, refer to chapter 19.3.

Authentication

User authentication (see below)

Account is disabled

Temporary blocking of the account so that you do not have to remove it.
Note: For example, this option can be used to create a user account for a user that will not be used immediately (e.g. an account for a new employee who has not taken up yet).

Domain template

Define parameters for the corresponding user account (access rights, data transfer quotas and content rules). These parameters can be defined by the template of the domain (see chapter 17.1) or they can be set especially for the corresponding account.
Using a template is suitable for common accounts in the domain (common user accounts). Definition of accounts is simpler and faster, if a template is used.
Individual configuration is recommended especially for accounts with special rights (e.g. *Kerio Control* administration accounts). Usually, there are not many such accounts which means their configuration comfortable.

Authentication options:

Internal user database

Users are only authenticated within *Kerio Control*. In such a case, specify the *Password* and *Confirm password* items (later, the password can be edited in the web interface — see the *Kerio Control — User's Guide*).

> ***Warning:***
>
> 1. Passwords may contain printable symbols only (letters, numbers, punctuation marks). Password is case-sensitive. We recommend not to use special characters (non-English languages) which might cause problems when authenticating via the Web interface.
> 2. NTLM authentication cannot be used for automatic authentication method by NTLM (refer to chapter 26.3).. These accounts also cannot be used for authentication to the *Clientless SSL-VPN* interface (see chapter 25).

Directory Service

User will be authenticated in *Active Directory* or *Open Directory* service domain, or in the *Windows NT* domain which the firewall belongs to.
Note: If domain is not set correctly, user accounts with authentication in the domain are inactive.. For details, see chapter 17.3.

Groups

Groups into which the user will be included can be added or removed with the *Add* or the *Remove* button within this dialog (to create new groups go to *User and Groups → Groups* — see chapter 17.5). Follow the same guidelines to add users to groups during group definition. It is not important whether groups or users are defined first.

> ***Hint:***
> While adding new groups you can mark more than one group by holding either the *Ctrl* or the*Shift* key.

Access rights

Each user must be assigned one of the following three levels of access rights.

No access to administration

These users do not have any access to *Kerio Control* administration. This setting is commonly used for the majority of users.

Read only access to administration

These users can connect to *Kerio Control* administration but they can only view the logs and settings; they cannot make any changes.

Full access to administration

The user can read or edit all the records and settings and his or her rights are equal to the administrator rights (`Admin`). If there is at least one user with the full access to the administration, the default `Admin` account can be removed.

Additional rights:

User can override WWW content rules

This rule affects web elements filtering rules use (for details, see *Step 5*):

- If there *exists* a URL rule (see chapter 14.2) and the user *does not have* this right, settings of the particular URL rule will be applied and user account settings will be ignored.
- If there *exists* a URL rule for the particular page and the user *has* this right, the user account settings will be used and the particular URL rule settings will be ignored.
- If there *exists no* URL rule for the particular page, user account settings will be applied and the rule is not important.

User can unlock URL rules

The user with this right is allowed to bypass the rule denying access to the requested website — at the page providing information about the denial, the *Unlock* button is displayed. The unlock feature must also be enabled in the corresponding URL rule (for details, refer to chapter 14.2).

User can dial RAS connection

If the Internet connection uses dial-up lines, users with this right will be allowed to dial and hang up these lines in the web interface (see chapter 13).

User can connect using VPN

The user is allowed to connect through *Kerio Control's* VPN server (using *Kerio VPN Client*). For detailed information, see chapter 24.

User can use Clientless SSL-VPN

The user will be allowed to access shared files and folders in the local network via the *Clientless SSL-VPN* web interface.

The *Clientless SSL-VPN* interface and the corresponding user right in *Kerio Control* is available for *Windows* only. For details, see chapter 25.

User is allowed to use P2P networks

Traffic of this user will not be blocked if *P2P* (*Peer-to-Peer*) networks are detected. For details, see chapter 9.4.

User is allowed to view statistics

This user will be allowed to view firewall statistics in the web interface (see chapter 13).

Hint:
Access rights can also be defined by a user account template.

Transfer quota

Daily and monthly limit for volume of data transferred by a user, as well as actions to be taken when the quota is exceeded, can be set in this section.

Transfer quota

Setting of daily, weekly and monthly limit of volume of transferred data for the user.

Use the *Direction* combo box to select which transfer direction will be controlled (*download* — incoming data, *upload* — outgoing data, *all traffic* — both incoming and outgoing data).

The limit can be set in the *Quota* entry using megabytes or gigabytes.

Quota exceed action

Set actions which will be taken whenever a quota is exceeded:

- *Block any further traffic* — the user will be allowed to continue using the opened connections, however, will not be allowed to establish new connections (i.e. to connect to another server, download a file through FTP, etc.)
- *Don't block further traffic (Only limit bandwidth...)* — Internet connection speed (so called bandwidth) will be limited for the user. Traffic will not be blocked but the user will notice that the Internet connection is slower than usual (this should make such users to reduce their network activities). For detailed information, see chapter 11.

Check the *Notify user by email when quota is exceeded* option to enable sending of warning messages to the user in case that a quota is exceeded. It is necessary that the user has a valid email address set (see
Step 1 of this wizard). SMTP Relay must be set in *Kerio Control* (see chapter 19.3).
If you wish that your *Kerio Control* administrator is also notified when a quota is almost exceeded, set the alert parameters in *Configuration* → *Accounting*. For details, refer to chapter 20.4.
Note:

1. If a quota is exceeded and the traffic is blocked in result, the restrictions will continue being applied until the end of the quota period (day or month). To cancel these restrictions before the end of a corresponding period, the following actions can be taken:
    - disable temporarily a corresponding limit, raise its value or switch to the *Don't block further traffic* mode
    - resetting of the data volume counter of the user (see chapter 21.1).
2. Actions for quota-exceeding are not applied if the user is authenticated at the firewall. This would block all firewall traffic as well as all local users. However, transferred data is included in the quota!

> ***Hint:***
> Data transfer quota and actions applied in response can also be set by a user account template.

Preferences — web content rules and language preferences

Within this step special objects filter rules settings for individual users can be defined. By default, all elements are allowed.

Application of these rules depends on the rule *User can override WWW content rules* and of the fact whether there exists a URL rule for the particular web page or not. For details see *Step 3* (user rights).

Kerio Control allows to block the following web elements:

ActiveX objects

Active objects at web pages. This option allows/blocks `<object>` and `<embed>` HTML tags.

<Script> HTML tags

The executive code in *JavaScript*, *VBScript*, etc.

Pop-up windows

Automatic opening of new browser windows — usually pop-up windows with advertisements.
This option will allow / block the *window.open()* method in *JavaScript*.

<Applet> HTML tags

Applets in *Java*.

Cross-domain referers

This option allows / blocks the `Referer` item included in an *HTTP* header.

The `Referer` item includes pages that have been viewed prior to the current page. This option allows to block `Referer` in case that it includes a server name different from the one defined in the particular HTTP request.

The *Cross-domain referer* function protects users' privacy (the `Referer` item can be monitored to see which pages are opened by each user).

The *Language options* section allows setting of preferred language of the *Kerio Control's* web interface (including the *Kerio StaR* interface). The *browser detected* option sets preferred language in accordance with settings in user's web browser and uses the language with the highest preference rate available. English will be used if none of other preferred languages is available.

Preferred language also applies to email alerts sent by the firewall (notices of reaching of data transfer quota, detected viruses, detected P2P networks, etc.). If language is detected and set by using user's web browser preferences, language set as preferred for the previous user's login to the web interface will be used. If the user has not logged into the web interface before, alerts will be in English.

Note: These settings can be customized at a corresponding page of the *Kerio Control's* web interface (see *Kerio Control — User's Guide*).

> ***Hint:***
> Content rules can also be defined by a user account template.

User IP addresses

If a user works at a reserved workstation (i.e. this computer is not by any other user) with a fixed IP address (static or reserved at the DHCP server), the user can use automatic login from the particular IP address. This implies that whenever a connection attempt from this IP address is detected, *Kerio Control* assumes that the connection is performed by the particular user and it does not require authentication. The user is logged-in automatically and all functions are available as if connected against the username and password.

This implies that only one user can be automatically authenticated from a particular IP address. When a user account is being created, *Kerio Control* automatically detects whether the specified IP address is used for automatic login or not.

Automatic login can be set for the firewall (i.e. for the *Kerio Control* host) or/and for any other host(s) (i.e. when the user connects also from an additional workstation, such as notebooks, etc.). An IP address group can be used for specification of multiple hosts (refer to chapter 16.1).

Warning:
Automatic login decreases user's security. If an unauthorized user works on the computer for which automatic login is enabled, he/she uses the identity of the host's user who is authenticated automatically. Therefore, automatic login should be accompanied by another security feature, such as by user login to the operating system.

IP address which will be always assigned to the VPN client of the particular user can be specified under

VPN client address. Using this method, a fixed IP address can be assigned to a user when he/she connects to the local network via the *Kerio VPN Client*. It is possible to add this IP to the list of IP addresses from which the user will be authenticated automatically.

For detailed information on the *Kerio Technologies'* proprietary VPN solution, refer to chapter 24.

Editing User Account

The *Edit* button opens a dialog window where you can edit the parameters of the user account. This dialog window contains all of the components of the account creation guide described above, divided into tabs in one window.

17.3 Local user database: external authentication and import of accounts

User in the local database can be authenticated either at the *Active Directory* domain or at the *Windows NT* domain (see chapter 17.2, step one). To apply these authentication methods, the *Kerio Control* host must belong to the corresponding domain.

If *Kerio Control* is installed on *Windows*, the host can be added to the domain or domain membership can be changed only in the operating system (in the computer properties).

In editions *Appliance* and *Box* it is possible to set domain membership directly in the firewall's administration, under *Domains and User Login*, on the *Directory Services* tab. *Kerio Control* in this edition can be connected only to the *Active Directory* domain, never to the *Windows NT* domain.

Importing user accounts

It is also possible to import special accounts to the local database from *Active Directory* or *Windows NT* domain . Import from *Windows NT* domain is available only in *Kerio Control* on *Windows*. It is not possible to import accounts from *Open Directory* domain.

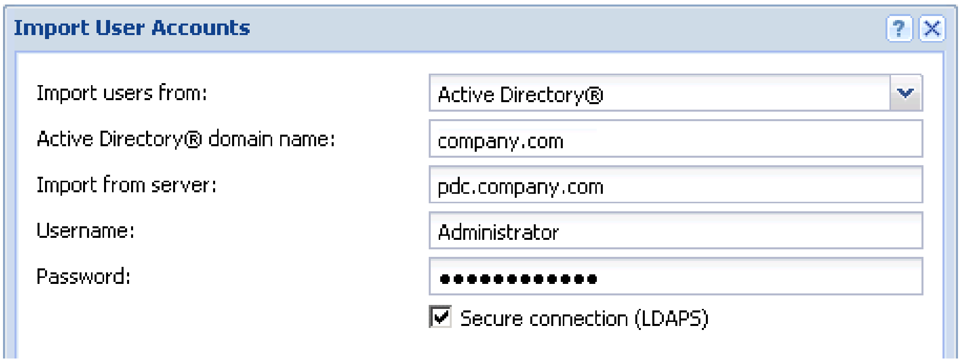
Each import of a user account covers creating of a local account with the identical name and the same domain authentication parameters. Specific *Kerio Control* parameters (such as access rights, content rules, data transfer quotas, etc.) can be set by using the template for the local user database (see chapter 17.1) or/and they can be defined individually for special accounts. The *Directory Service* authentication type is set for all accounts imported.

Note: This method of user accounts import is recommended especially when *Windows NT* domain is used (domain server with the *Windows NT Server* operating system). If *Active Directory* domain is used, it is easier and recommended to use domain mapping — see chapter 17.4.

Click *Import* to start importing user accounts (in the *Domain* entry, the *Local user database* must be selected, otherwise this button is inactive).

In the import dialog, select the type of the domain from which accounts will be imported and, with respect to the domain type, specify the following parameters:

- *Active Directory* — for import of accounts, *Active Directory* domain name, DNS name or IP address of the domain server as well as login data for user database reading (any account belonging to the domain) are required.



Import User Accounts

Import users from: Active Directory®

Active Directory® domain name: company.com

Import from server: pdc.company.com

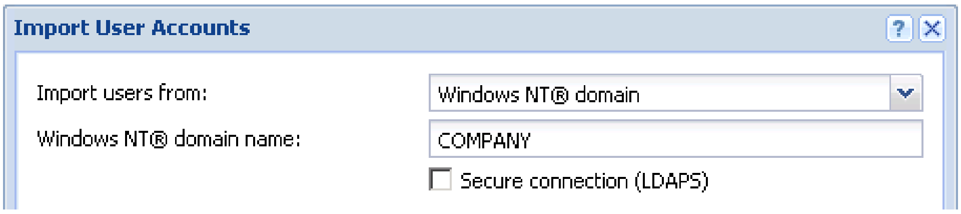
Username: Administrator

Password: ●●●●●●●●●●●●

☑ Secure connection (LDAPS)

Figure 17.1 Import of accounts from Active Directory

- *NT domain* — domain name is required for import. The *Kerio Control* host must be a member of this domain.



Import User Accounts

Import users from: Windows NT® domain

Windows NT® domain name: COMPANY

□ Secure connection (LDAPS)

Figure 17.2 Importing accounts from the Windows NT domain

Note: Import of user accounts from *Windows NT* is available only in *Kerio Control* on *Windows*.

When connection with the corresponding domain server is established successfully, all accounts in the selected domain are listed. When accounts are selected and the selection is confirmed, the accounts are imported to the local user database.

17.4 User accounts in directory services — domain mapping

In *Kerio Control*, it is possible to directly use user accounts from one or more *Active Directory* or *Open Directory* domain(s). This feature is called domain mapping. The main benefit of this feature is that the entire administration of all user accounts and groups is maintained in directory service only (using standard system tools). In *Kerio Control* a template can be defined for each domain that will be used to set specific *Kerio Control* parameters for user accounts (access rights, data transfer quotas, content rules — see chapter 17.1). If needed, these parameters can also be set individually for any accounts.

Note: The *Windows NT* domain cannot be mapped as described. In case of the *Windows NT* domain, it is recommended to import user accounts to the local user database (refer to 17.3)

Domain mapping settings

Domain mapping can be set under *Users and Groups* → *Domains and User Login*, on the *Directory Services* tab.

Conditions for mapping from Active Directory domains

The following conditions must be met to enable smooth functionality of user authentication through *Active Directory* domains:

- For mapping of one domain:

  1. The *Kerio Control* host must be a member of the corresponding *Active Directory* domain.

  2. Hosts in the local network (user workstations) should use the *Kerio Control's DNS* module as the primary DNS server, because it can process queries for *Active Directory* and forward them to the corresponding domain server. If another DNS server is used, user authentication in the *Active Directory* may not work correctly.

- For mapping of multiple domains:

  1. The *Kerio Control* host must be a member of one of the mapped domains. This domain will be set as primary.

  2. It is necessary that the primary domain trusts any other domains mapped in *Kerio Control* (for details, see the documentation regarding the operating system on the corresponding domain server).

  3. For DNS configuration, the same rules as in mapping of a single domain are applied (the *Kerio Control's DNS* module is the best option).

Connecting the firewall to Active Directory domain (editions Appliance and Box)

The upper part of the *Directory Services* tab displays information about membership of the firewall host in the domain and allows to add the firewall to *Active Directory* domain, change the membership or remove it from domain.

First it is necessary to select *Active Directory* service and enter the full domain name (e.g. `company.com`).

Click on *Join domain* to run a simple wizard where it is necessary to specify the name of the host (firewall) and password of a user with privileges to add hosts to domains.

If *Kerio Control* cannot find the domain server of the specified domain automatically, it requires specification of its IP address in the next step. Then the user gets informed about the result of the attempt to add the firewall to the domain.

Primary domain mapping

To set mapping of the primary domain (the domain of which the firewall host is a member), use option *Use domain user database*. For connection to the domain server, it is required to enter username and password of an account with read rights for the user database (any user account of the domain can be used, unless it is blocked).

Advanced Options

Method of cooperation between *Kerio Control* and directory services can be customized by some advanced options.

Secured connection to the domain server

For higher security (to prevent from tapping of traffic and exploiting user passwords), connection to the directory server can be encrypted. Enabling of encrypted connection requires corresponding settings on the particular domain server (or on all servers of the particular domain if automatic detection is used).

Active Directory: Domain mapping vs domain user authentication

The recommended method of cooperation with the *Active Directory* is domain mapping (user accounts are saved and managed only in the *Active Directory*). However, this can be undesirable under certain circumstances. For example if the *Active Directory* is implemented in a network where the *Windows NT* domain or no domain has been used, user accounts are already created in the *Kerio Control's* local database. In such case, the best solution is to keep the local accounts and set only authentication in the *Active Directory* (so that users can use the same password both for the domain and the firewall). If *Kerio Control* is installed on *Windows*, it is possible to allow authentication compatible with older systems (i.e. authentication via the *Windows NT* domain). This option is required if the domain server uses *Windows NT* or if any of the clients in the local network uses *Windows* of older edition than *Windows 2000*. In editions *Appliance* and *Box*, this option is not available (authentication in *Windows NT* domain is not supported).

Then, the settings include an option of automatic import of user accounts from the *Active Directory* to the local database (upon the first logon of user to the firewall by their domain name and password, an account with the same name will be created in the local database automatically). This option is helpful only for compatibility of older versions of *Kerio Control* (*Kerio WinRoute Firewall*). In new installations it is strongly recommended to use domain mapping — administration of users is much more simple and much less time consuming. For details, see the *Administrator's Guide* for older versions of *Kerio WinRoute Firewall* (versions *6.7.0* or lower).

Mapping of other domains

To map user accounts from multiple domains, add domains in advanced settings available on the *Other Mapping* tab.

Users of other domains must login by username including the domain (e.g. `drdolittle@usoffice.company.com`). User accounts with no domain specified (e.g. `wsmith`), will be searched in the primary domain or in the local database.

Use buttons *Add* or *Edit* to open a dialog for a new domain definition and enter parameters of the mapped domain. For details, see above (Primary domain mapping and Advanced options).

Collision of directory service with the local database and conversion of accounts

During directory service domain mapping, collision with the local user database may occur if a user account with an identical name exists both in the domain and in the local database. If multiple domains are mapped, a collision may occur only between the local database and the primary domain (accounts from other domains must include domain names which make the name unique).

If a collision occurs, a warning is displayed at the bottom of the *User Accounts* tab. Click on the link in the warning to convert selected user accounts (to replace local accounts by corresponding directory service accounts).

The following operations will be performed automatically within each conversion:

- substitution of any appearance of the local account in the *Kerio Control* configuration (in traffic rules, URL rules, FTP rules, etc.) by a corresponding account from the directory service domain,
- removal of the account from the local user database.

Accounts not selected for the conversion are kept in the local database (the collision is still reported). Colliding accounts can be used — the accounts are considered as two independent accounts. However, under these circumstances, directory service accounts must be always specified including the domain (even though it belongs to the primary domain); username without the domain specified represents an account belonging to the local database. However, as long as possible, it is recommended to remove all collisions by the conversion.

Note: In case of user groups, collisions do not occur as local groups are always independent from the directory service (even if the name of the local group is identical with the name of the group in the particular domain).

17.5 User groups

User accounts can be sorted into groups. Creating user groups provides the following benefits:

- Specific access rights can be assigned to a group of users. These rights complement rights of individual users.
- Each group can be used when traffic and access rules are defined. This simplifies the definition process so that you will not need to define the same rule for each user.

User groups Definitions

User groups can be defined in *User and Groups* → *Groups*.

Domain

Use the *Domain* option to select a domain for which user accounts or other parameters will be defined. This item provides a list of mapped domains (see chapter 17.4) and the local user database.
In *Kerio Control*, it is possible to create groups only in the local user database. It is not possible to create groups in mapped domains. Neither it is possible to import groups from domain to local database.
In case of groups in mapped domains, it is possible to set only access rules (see below — step 3 of the user group definition wizard).

Search

In upper part of the window, you can enter a user group search filter.
The filter is interactive — each symbol typed or deleted defines the string which is evaluated immediately and all groups including the string in either *Name* or *Description* are viewed. The icon next to the entry can be clicked to clear the filtering string and display all groups in the selected domain (if the *Filter* entry is blank, the icon is hidden).
The searching is helpful especially when the domain includes too many groups which might make it difficult to look up particular items.

Creating a new local user group

In the *Domain* combo box in *Groups*, select Local User Database.

Click on *Add* to start a dialog where a new user group can be created.

General — group name and description

Name

Group name (group identification).

Description

Group description. It has an informative purpose only and may contain any information or the field can be left empty.

Group members

Using the *Add* and *Remove* buttons you can add or remove users to/from the group. If user accounts have not been created yet, the group can be left empty and users can be added during the account definition (see chapter 17.1).

> ***Hint:***
> When adding new users you can select multiple user accounts by holding either the *Ctrl* or the *Shift* key.

Rights — user rights of group members

The group must be assigned one of the following three levels of access rights:

No access to administration

Users in this group have no access to *Kerio Control* administration.

Read only access

Users in this group can log in to *Kerio Control* administration but they can only view the logs and settings. They cannot alter any settings.

Full access to administration

Users in this group have full access rights.

Additional rights:

Users can override WWW content rules

This option specifies application of ruled for web page elements for pages matching an existing URL rule. For details on this right, refer to chapter 17.2.

User can unlock URL rules

This option allows its members one-shot bypassing of denial rules for blocked websites (if allowed by the corresponding URL rule — see chapter 14.2). All performed unlock actions are traced in the *Security* log.

Users can dial RAS connection

If the Internet connection uses dial-up lines, users of this group will be allowed to dial and hang up these lines in the Web interface (see chapter 13).

Users can connect using VPN

Members of the group can connect to the local network via the Internet using the *Kerio VPN Client* (for details, see chapter 24).

User can use Clientless SSL-VPN

Members of this group will be allowed to access shared files and folders in the local network via the *Clientless SSL-VPN* web interface.

The *Clientless SSL-VPN* interface and the corresponding user right in *Kerio Control* is available for *Windows* only. For details, see chapter 25.

Users are allowed to use P2P networks

The *P2P Eliminator* module (detection and blocking of *Peer-to-Peer* networks — see chapter 9.4) will not be applied to members of this group.

Users are allowed to view statistics

Users in this group will be allowed to view firewall statistics in the web interface (see chapter 13).

Group access rights are combined with user access rights. This means that current user rights are defined by actual rights of the user and by rights of all groups in which the user is included.

Chapter 18

Administrative settings

18.1 System Configuration (editions Appliance and Box)

In editions *Appliance* and *Box*, the *Kerio Control* administration console allows setting of a few basic parameters of the firewall's operating system. These settings are necessary for correct functionality of the firewall and they can be found in *Configuration / Advanced options*, on the *System Configuration* tab.

Server name

Name is important both for some *Kerio Control* services (e.g. secured web interface) and for the firewall's operating system's services.

The *DNS* module in *Kerio Control* sets IP addresses of all the firewall's interfaces for the name automatically. If another DNS server is used in the local network, it is necessary to set corresponding DNS records on it.

Date, time and time zone

Many *Kerio Control* features (user authentication, logs, statistics, etc.) require correct setting of date, time and time zone on the firewall.

Date and time can be set automatically but it is more useful to use an NTP server which provides information about the current time and allows automatic management of the firewall's system time. The time zone also includes information about daylight saving time settings.

Kerio Technologies offers the following free NTP servers for this purpose: `0.kerio.pool.ntp.org`, `1.kerio.pool.ntp.org`, `2.kerio.pool.ntp.org` and `3.kerio.pool.ntp.org`.

18.2 Update Checking

Kerio Control enables automatic check for new versions at the *Kerio Technologies* website. Update checker acts differently in dependence on the firewall's platform:

- in the *Windows* edition, only links to sources with more information and to installation package download are provided,
- in editions *Appliance* and *Box*, the firewall may download a new image of the drive and perform update of the entire appliance automatically.

may offer download and installation.

Open the *Update Checker* tab in the *Configuration* → *Advanced Options* section to view information on a new version and to set parameters for automatic checks for new versions.

Check for new versions regularly

Use this option to enable/disable automatic checks for new versions. Checks are performed:

- 2 minutes after each startup of the *Kerio Control Engine*,
- and then every 24 hours.

Results of each attempted update check (successful or not) is logged into the *Debug* log (see chapter 23.6).

Check also for beta versions

Enable this option if you want *Kerio Control* to perform also update checks for beta and *Release Candidate* versions of *Kerio Control*.

If you wish to participate in testing of *Kerio Control* beta versions, enable this option. In case that you use *Kerio Control* in operations in your company (i.e. at the Internet gateway of your company), we recommend you not to use this option (beta versions are not tested yet and they could endanger functionality of your networks, etc.).

Download new versions automatically

This option is available only in editions *Appliance* and *Box*. If this option is enabled, once a new version of the product is detected, the corresponding update package is downloaded immediately and the firewall can be updated directly from the administration interface.

Last update check performed ... ago

Information on how much time ago the last update check was performed.

If the time is too long (several days) this may indicate that the automatic update checks fail for some reason (i.e. access to the update server is blocked by a traffic rule). In such cases we recommend you to perform a check by hand (by clicking on the *Check now* button), view results in the *Debug* log (see chapter 23.6) and take appropriate actions.

Check

Click on this button to check for updates immediately.

Any time a new version of the product is detected, then:

- In the *Windows* edition, a link is displayed referring to a page with detailed information and another one to the installation package download page.

- In editions *Appliance* and *Box*, a button for download of the update package is displayed (or for immediate start of the update in case that the automatic updates are enabled). Update of the firewall takes up to several minutes. Once it is finished, you will be informed that the firewall would be restarted. Upon the restart (in approximately 1 minute), the firewall will be fully available again.

For detailed information on *Kerio Control* installation, refer to chapter 2.4.

Note: Whenever a newer version is available, this information is displayed as a link in the welcome page of the administration window (an image providing information about the application and the license). Clicking on the link will take you to section *Configuration* → *Advanced Options*, the *Updates* tab.

Chapter 19

Other settings

19.1 Routing table

In the *Kerio Control Administration* interface you can view or edit the system routing table of the host where *Kerio Control* is running. This can be useful especially to resolve routing problems remotely (it is not necessary to use applications for terminal access, remote desktop, etc.).

To view or modify the routing table go to *Configuration* → *Routing Table*. This section provides up-to-date version of the routing table of the operating system including so called *persistent routes* on Windows (routes added by the `route -p` command).

Note:

1. In the Internet connection failover mode (see chapter 7.4), only the current default route is shown (depending on which Internet interface is currently active).
2. In case of multiple Internet links in the network load balancing mode (see chapter 7.3), only a single default route will be displayed which is routed through the link with the highest proposed speed.

Dynamic and static routes can be added and/or removed in section *Routing table*. Dynamic routes are valid only until the operating system is restarted or until removed by the `route` system command. Static routes are saved in *Kerio Control* and they are restored upon each restart of the operating system.

Note: Changes in the routing table might interrupt the connection between the *Kerio Control Engine* and the *Kerio Control Administration* interface (immediately upon clicking on *Apply*). We recommend to check the routing table thoroughly before clicking the *Apply* button!

Route Types

The following route types are used in the *Kerio Control* routing table:

- *System routes* — routes downloaded from the operating system's routing table (including so called persistent routes). These routes cannot be edited some of them can be removed — see the *Removing routes from the Routing Table* section).

- *Static routes* — manually defined routes managed by *Kerio Control* (see below). These routes can be added, modified and/or removed.

  The checking boxes can be used to disable routes temporarily —such routes are provided in the list of inactive routes. Static routes are marked with an *S* icon.

- *VPN routes* — routes to VPN clients and to networks at remote endpoints of VPN tunnels (for details, see chapter 24). These routes are created and removed dynamically upon connecting and disconnecting of VPN clients or upon creating and removing of VPN tunnels. VPN routes cannot be created, modified nor removed by hand.

- *Inactive routes* — routes which are currently inactive are showed in a separate section. These can be static routes that are temporarily disabled, static routes via an interfaces which has been disconnected or removed from the system, etc.

Static routes

Kerio Control includes a special system for creation and management of static routes in the routing table. All static routes defined in *Kerio Control* are saved into the configuration file and upon each startup of the *Kerio Control Engine* they are added to the system routing table. In addition to this, these routes are monitored and managed all the time *Kerio Control* is running. This means that whenever any of these routes is removed by the `route` command, it is automatically added again.

Note:
1. The operating system's persistent routes are not used for implementation of static routes (for management of these routes, *Kerio Control* uses a proprietary method).
2. If a static connection uses a dial-up, any UDP or TCP packet with the *SYN* flag dials the line. For detailed information, see chapter 7.5.

Definitions of Dynamic and Static Rules

Click on the *Add* (or *Edit* when a particular route is selected) button to display a dialog for route definition.

Network, Network Mask

IP address and mask of the destination network.

Interface

Selection of an interface through which the specific packet should be forwarded.

Gateway

IP address of the gateway (router) which can route to the destination network. The IP address of the gateway must be in the same IP subnet as the selected interface.

Metric

"Distance" of the destination network. The number stands for the number of routers that a packet must pass through to reach the destination network.
Metric is used to find the best route to the desired network. The lower the metric value, the "shorter" the route is.

Note: Metric in the routing table may differ from the real network topology. It may be modified according to the priority of each line, etc.

Create a static route

Enable this option to make this route static. Such route will be restored automatically by *Kerio Control* (see above). A brief description providing various information (why the route was created, etc.) about the route can be attached.

If this option is not enabled, the route will be valid only until the operating system is restarted or until removed manually in the *Kerio Control Administration* interface or using the `route` command.

Removing routes from the Routing Table

Using the *Remove* button, records can be removed from the routing table. The following rules are used for route removal:

- Static routes in the *Static Routes* folder are managed by *Kerio Control*. Removal of any of the static routes would remove the route from the system routing table immediately and permanently (after clicking on the *Apply* button).
- Dynamic (system) route will be removed as well, regardless whether it was added in the *Kerio Control Administration* interface or by using the `route` command. However, it is not possible to remove any route to a network which is connected to an interface.
- Persistent route of the operating system will be removed from the routing table only after restart of the operating system. Upon reboot of the operating system, it will be restored automatically. There are many methods that can be used to create persistent routes (the methods vary according to operating system — in some systems, the `route -p` or the `route` command called from an execution script can be used, etc.). It is not possible to find out how a particular persistent route was created and how it might be removed for good.

19.2 Universal Plug-and-Play (UPnP)

Kerio Control supports UPnP protocol (*Universal Plug-and-Play*). This protocol enables client applications (i.e. *Microsoft MSN Messenger*) to detect the firewall and make a request for mapping of appropriate ports from the Internet for the particular host in the local network. Such mapping is always temporary — it is either applied until ports are released by the application (using UPnP messages) or until expiration of the certain timeout.

The required port must not collide with any existing mapped port or any traffic rule allowing access to the firewall from the Internet. Otherwise, the UPnP port mapping request will be denied.

Configuration of the UPnP support

UPnP can be enabled under *Configuration* → *Traffic Policy* → *Security Settings*, the *Miscellaneous* tab.

Enable UPnP

This option enables UPnP.

Log packets

If this option is enabled, all packets passing through ports mapped with UPnP will be recorded in the *Filter* log (see chapter 23.9)).

Log connections

If this option is enabled, all packets passing through ports mapped with UPnP will be recorded in the *Connection* log (see chapter 23.5).

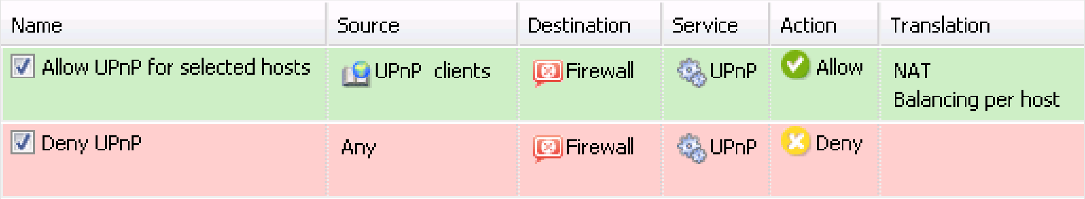
Warning:

1. If *Kerio Control* is running on *Windows XP*, *Windows Server 2003*, *Windows Vista* or *Windows Server 2008*, check that the following system services are not running before you start the *UPnP* function:

    - *SSDP Discovery Service*
    - *Universal Plug and Play Device Host*

    If any of these services is running, close it and deny its automatic startup. In *Kerio Control*, these services work with the UPnP protocol in *Windows*, and therefore they cannot be used together with *UPnP*.
    Note: The *Kerio Control* installation program detects the services and offers their stopping and denial.

2. Apart from the fact that UPnP is a useful feature, it may also endanger network security, especially in case of networks with many users where the firewall could be controlled by too many users. The firewall administrator should consider carefully whether to prefer security or functionality of applications that require UPnP.
    Using traffic policy (see chapter 8.3) you can limit usage of UPnP and enable it to certain IP addresses or certain users only.
    Example:



Name	Source	Destination	Service	Action	Translation
☑ Allow UPnP for selected hosts	UPnP clients	Firewall	UPnP	✓ Allow	NAT Balancing per host
☑ Deny UPnP	Any	Firewall	UPnP	✗ Deny	

Figure 19.1 Traffic rules allowing UPnP for specific hosts

The first rule allows UPnP only from *UPnP Clients* IP group. The second rule denies UPnP from other hosts (IP addresses).

19.3 Relay SMTP server

Kerio Control provides a function which enables notification to users or/and administrators by email alerts. These alert messages can be sent upon various events, for example when a virus is detected (see chapter 15.3), when a *Peer-to-Peer* network is detected (refer to chapter 9.4), when an alert function is set for certain events (details in chapter 17.1) or upon reception of an alert (see chapter 20.4).

For this purpose, *Kerio Control* needs an SMTP Relay Server. This server is used for forwarding of infected messages to a specified address.

Note: Kerio Control does not provided any built-in SMTP server.

To configure an SMTP server, go to the *SMTP server* tab in *Configuration → Advanced Options*.

Server

Name or IP address of the server.
Note: If available, we recommend you to use an SMTP server within the local network (messages sent by *Kerio Control* are often addressed to local users).

SMTP requires authentication

Enable this option to require authentication through username and password at the specified SMTP server.

Specify sender email address in "From" header

In this option you can specify a sender's email address (i.e. the value for the `From` header) for email sent from *Kerio Control* (email or SMS alerts sent to users). Preset `From` header does not apply to messages forwarded during antivirus check (refer to chapter 15.4).
This item must be preset especially if the SMTP server strictly checks the header (messages without or with an invalid `From` header are considered as spams). The item can also be used for reference in recipient's mail client or for email classification. This is why it is always recommended to specify sender's email address in *Kerio Control*.

Connection test

Click *Test* to test functionality of sending of email via the specified SMTP server. *Kerio Control* sends a testing email message to the specified email address.

Warning:

1. If SMTP is specified by a DNS name, it cannot be used until *Kerio Control* resolves a corresponding IP address (by a DNS query). The *IP address of specified SMTP server cannot be resolved* warning message is displayed in the *SMTP Relay* tab until the IP address is not found. If the warning is still displayed, this implies that an invalid (non-existent) DNS name is specified or the DNS server does not respond.
   If the warning on the *SMTP server* tab is still displayed, it means that an invalid DNS name was specified or that an error occurred in the communication (DNS server is not responding). Therefore, we recommend you to specify SMTP server by an IP address if possible.

2. Communication with the SMTP server must not be blocked by any rule, otherwise the *Connection to SMTP server is blocked by traffic rules* error is reported upon clicking the *Apply* button.
   For detailed information about traffic rules, refer to chapter 8.

Chapter 20

Status Information

Kerio Control activities can be well monitored by the administrator (or by other users with appropriate rights). There are three types of information — status monitoring, statistics and logs.

- Communication of each computer, users connected or all connections using *Kerio Control* can be monitored.

  Note:

  1. *Kerio Control* monitors only traffic between the local network and the Internet. The traffic within the local network is not monitored.
  2. Only traffic allowed by traffic rules (see chapter 8) can be viewed. If a traffic attempt which should have been denied is detected, the rules are not well defined.

- Statistics provide information on users and network traffic for a certain time period. Statistics are viewed in the form of charts and tables. For details see chapter 21.

- Logs are files where information about certain activity is reported (e.g. error or warning reports, debug information etc.). Each item is represented by one row starting with a timestamp (date and time of the event). Events reported are in English only (they are generated by the *Kerio Control Engine*). For details, refer to chapter 23.

The following chapters describe what information can be viewed and how its viewing can be changed to accommodate the user's needs.

20.1 Active hosts and connected users

In *Status* → *Active Hosts*, the hosts within the local network or active users using *Kerio Control* for communication with the Internet will be displayed.

Note: For more details about the firewall user's logon, see chapter 12.1.

Look at the upper window to view information on individual hosts, connected users, data size/speed, etc.

The following information can be found in the *Active Hosts* window:

Hostname

DNS name of a host. In case that no corresponding DNS record is found, IP address is displayed instead.

User

Name of the user which is connected from a particular host. If no user is connected, the item is empty.

Currently Rx, Currently Tx

Monitors current traffic speed (kilobytes per second) in both directions (from and to the host — *Rx* values represent incoming data, *Tx* values represent outgoing data)

The following columns are hidden by default. To view these columns select the *Modify columns* option in the context menu (see below).

IP address

IP address of the host from which the user is connecting from (i.e. which communicates with the Internet via *Kerio Control*).

Login time

Date and time of the recent user login to the firewall

Login duration

Monitors length of the connection. This information is derived from the current time status and the time when the user logged on

Inactivity time

Duration of the time with zero data traffic. You can set the firewall to logout users automatically after the inactivity exceeds allowed inactivity time (for more details see chapter 13.1)

Start time

Date and time when the host was first acknowledged by *Kerio Control*. This information is kept in the operating system until the *Kerio Control Engine* disconnected.

Total received, Total transmitted

Total size of the data (in kilobytes) received and transmitted since the
Start time

Connections

Total number of connections to and from the host. Details can be displayed in the context menu (see below)

Authentication method

Authentication method used for the recent user connection:

- *plaintext* — user is connected through an insecure login site *plaintext*
- *SSL* — user is connected through a login site protected by SSL security system *SSL*
- *proxy* — a *Kerio Control* proxy server is used for authentication and for connection to websites
- *NTLM* — user was automatically authenticated in the NT domain by NTLM (works with *Internet Explorer* or *Firefox/SeaMonkey*),
- *VPN client* — user has connected to the local network using the *Kerio VPN Client* (for details, see chapter 24).

Note: Connections are not displayed and the volume of transmitted data is not monitored for VPN clients.

For more details about connecting and user authentication see chapter 12.1.

Information displayed in the *Active Hosts* window can be refreshed by clicking on the *Refresh*button.

Use the *Show / Hide details* to open the bottom window providing detailed information on a user, host and open connections.

Active Hosts dialog options

Clicking the right mouse button in the *Active Hosts* window (or on the record selected) will display a context menu that provides the following options:

User quota

Use this option to show quota of the particular user (the *Kerio Control Administration* interface switches to the *User Quota* tab in *Status* → *User Statistics* and selects the particular user automatically).

The *User quota* option is available in the context menu only for hosts from which a user is connected to the firewall.

Refresh

This option refreshes information in the *Active Hosts* window immediately (this function is equal to the *Refresh* button displayed at the bottom of the window).

Auto refresh

Settings for automatic refreshing of the information in the *Active Hosts* window. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Logout user

Immediate logout of a selected user.

Logout all users

Immediate logout of all firewall users.

Manage Columns

By choosing this option you can select which columns will be displayed in the *Active Hosts* window.

Detailed information on a selected host and user

Detailed information on a selected host and connected user are provided in the bottom window of the *Active Hosts* section.

Open the *General* tab to view information on user's login, size/speed of transmitted data and information on activities of a particular user.

Login information

Information on logged-in users:

- *User* — name of a user, DNS name (if available) and IP address of the host from which the user is connected
- *Login time* — date and time when a user logged-in, authentication method that was used and inactivity time (idle).

If no user is connected from a particular host, detailed information on the host are provided instead of login information.

- *Host* — DNS name (if available) and IP address of the host
- *Idle time* — time for which no network activity performed by the host has been detected

Traffic information

Information on size of data received (*Download*) and sent (*Upload*) by the particular user (or host) and on current speed of traffic in both directions.

Overview of detected activities of the particular user (host) are given in the main section of this window:

Activity Time

Time (in minutes and seconds) when the activity was detected.

Activity Event

Type of detected activity (network communication). *Kerio Control* distinguishes between the following activities: *SMTP*, *POP3*, *WWW* (HTTP traffic), *FTP*, *Streams* (real-time transmission of audio and video streams) and *P2P* (use of Peer-to-Peer networks).
Note: Kerio Control is not able to recognize which type of *P2P* network is used. According to results of certain testing it can only "guess" that it is possible that the client is connected to such network. For details, refer to chapter 9.4.

Activity Description

Detailed information on a particular activity:

- *WWW* — title of a Web page to which the user is connected (if no title is available, URL will be displayed instead). Page title is a hypertext link — click on this link to open a corresponding page in the browser which is set as default in the operating system.
  Note: For better transparency, only the first visited page of each web server to which the user connected is displayed. For detailed information about all visited pages, refer to *Kerio StaR* (see chapter 22).
- *SMTP, POP3* — DNS name or IP address of the server, size of downloaded/uploaded data.
- *FTP* — DNS name or IP address of the server, size of downloaded/saved data, information on currently downloaded/saved file (name of the file including the path, size of data downloaded/uploaded from/to this file).
- *Multimedia* (real time transmission of video and audio data) — DNS name or IP address of the server, type of used protocol (*MMS*, *RTSP*, *RealAudio*, etc.) and volume of downloaded data.
- *P2P* — information that the client is probably using Peer-To-Peer network.

Information about connections from/to the Internet

On the *Connections* tab, you can view detailed information about connections established from the selected host to the Internet and in the other direction (e.g. by mapped ports, *UPnP*, etc.). The list of connections provides an overview of services used by the selected user. Undesirable connections can be terminated immediately.

Information about connections:

Traffic rule
Name of the *Kerio Control* traffic rule (see chapter 8) by which the connection was allowed.

Service
Name of the service. For non-standard services, port numbers and protocols are displayed.

Source, Destination
Source and destination IP address (or name of the host in case that the *Show DNS names* option is enabled —see below).

Bandwidth Management Rule
Bandwidth limiting or reservation rule applied to this connection (empty column means that no rule has been applied).

Load Balancing
If the firewall works in the load balancing mode, the interface over which the connection is directed is displayed here (for connections to/from the Internet).

Source port, Destination port
Source and destination port (only for TCP and UDP protocols).

Protocol
Protocol used for the transmission (TCP, UDP, etc.).

Timeout
Time left before the connection will be removed from the table of *Kerio Control* connections.
Each new packet within this connection sets timeout to the initial value. If no data is transmitted via a particular connection, *Kerio Control* removes the connection from the table upon the timeout expiration — the connection is closed and no other data can be transmitted through it.

Rx, Tx
Volume of incoming (*Rx*) and outgoing (Tx) data transmitted through a particular connection (in KB).

Info
Additional information (such as a method and URL in case of HTTP protocol).

Use the *Show DNS names* option to enable/disable showing of DNS names instead of IP addresses in the *Source* and *Destination* columns. If a DNS name for an IP address cannot be resolved, the IP address is displayed.

You can click on the *Colors* button to open a dialog where colors used in this table can be set.

Note:

1. Upon right-clicking on a connection, the context menu extended by the *Kill connection* option is displayed. This option can be used to kill the particular connection between the LAN and the Internet immediately.
2. The selected host's overview of connections lists only connections established from the particular host to the Internet and vice versa. Local connections established between the particular host and the firewall can be viewed only in *Status* → *Connections* (see chapter 20.2). Connections between hosts within the LAN are not routed through *Kerio Control*, and therefore they cannot be viewed there.

Histogram

The *Histogram* tab provides information on data volume transferred from and to the selected host in a selected time period. The chart provides information on the load of this host's traffic on the Internet line through the day.

Select an item from the *Time interval* combo box to specify a time period which the chart will refer to (2 hours or 1 day). The x axis of the chart represents time and the y axis represents traffic speed. The x axis is measured accordingly to a selected time period, while measurement of the y axis depends on the maximal value of the time interval and is set automatically (bytes per second is the basic measure unit — *B/s*).

This chart includes volume of transferred data in the selected direction in certain time intervals (depending on the selected period). The green curve represents volume of incoming data (download) in a selected time period, while the area below the curve represents the total volume of data transferred in the period. The red curve and area provide the same information for outgoing data (upload). Below the chart, basic statistic information, such as volume of data currently transferred (in the last interval) and the average and maximum data volume per an interval, is provided.

Select an option for *Picture size* to set a fixed format of the chart or to make it fit the screen.

20.2 Network connections overview

In *Status* → *Connections*, all the network connections which can be detected by *Kerio Control* include the following:

- client connections to the Internet through *Kerio Control*
- connections from the host on which *Kerio Control* is running

- connections from other hosts to services provided by the host with *Kerio Control*
- connections performed by clients within the Internet that are mapped to services running in LAN

Kerio Control administrators are allowed to close any of the active connections.

Note:

1. Connections among local clients will not be detected nor displayed by *Kerio Control*.
2. UDP protocol is also called connectionless protocol. This protocol does not perform any connection. The communication is performed through individual messages (so-called datagrams). Periodic data exchange is monitored in this case.

One connection is represented by each line of the *Connections* window. These are network connections, not user connections (each client program can occupy more than one connection at a given moment). Lines are highlighted: green color marks outgoing connections, while red color marks incoming connections.

The columns contain the following information:

Traffic rule

Name of the *Kerio Control* traffic rule (see chapter 8) by which the connection was allowed.

Service

Name of transmitted service (if such service is defined in *Kerio Control* — see chapter 16.3). If the service is not defined in *Kerio Control*, the corresponding port number and protocol will be displayed instead (e.g. *5004/UDP*).

Source, Destination

IP address of the source (the connection initiator) and of the destination.

Bandwidth Management Rule

Bandwidth limiting or reservation rule applied to this connection (empty column means that no rule has been applied).

Load Balancing

If the firewall works in the load balancing mode (see chapter 7.3), the interface over which the connection is directed is displayed here (for connections to/from the Internet).

Source port, Destination port

Ports used for the particular connection.

Protocol

Communication protocol (*TCP* or *UDP*)

Timeout

Time left until automatic disconnection. The countdown starts when data traffic stops. Each new data packet sets the counter to zero.

Age

Time for which the connection has been established.

Rx, Tx

Total size of data received (*Rx*) or transmitted (*Tx*) during the connection (in kilobytes). Received data means the data transferred from *Source* to *Destination*, transmitted data means the opposite.

Info

An informational text describing the connection (e.g. about the protocol inspector applied to the connection).

Type

Connection direction — either incoming or outgoing.

Information in *Connections* can be refreshed automatically within a user defined interval or the *Refresh* button can be used for manual refreshing.

Options of the Connections Dialog

The following options are available below the list of connections:

- *Hide local connections* — connections from or/and to the *Kerio Control* host will not be displayed in the *Connections* window.

  This option only makes the list better-arranged (especially if we are curious only about connections between hosts in the local network and the Internet).

- *Show DNS names* — this option displays DNS names instead of IP addresses. If a DNS name is not resolved for a certain connection, the IP address will be displayed.

Right-click on the *Connections* window (on the connection selected) to view a context menu including the following options:

Kill connection

Use this option to finish selected connection immediately (in case of UDP connections all following datagrams will be dropped).
Note: This option is active only if the context menu has been called by right-clicking on a particular connection. If called up by right-clicking in the *Connections* window (with no connection selected), the option is inactive.

Refresh

This option will refresh the information in the *Connections* window immediately. This function is equal to the function of the *Refresh* button at the bottom of the window.

Auto refresh

Settings for automatic refreshing of the information in the *Connections* window. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Manage Columns

By choosing this option you can select which columns will be displayed in the *Connections* window.

Color Settings

Clicking on the *Colors* button displays the color settings dialog to define colors for each connection:

For each item either a color or the *Default* option can be chosen. Default colors are set in the operating system (the common setting for default colors is black font and white background).

Font Color

- *Active connections* — connections with currently active data traffic
- *Inactive connections* — TCP connections which have been closed but 2 minutes after they were killed they are still kept active — to avoid repeated packet mishandling)

Background Color

- *Local connections* — connections where an IP address of the host with *Kerio Control* is either source or destination
- *Inbound connections* — connections from the Internet to the local network (allowed by firewall)
- *Outbound connections* — connections from the local network to the Internet

Note: Incoming and outgoing connections are distinguished by detection of direction of IP addresses — "out" (*SNAT*) or "in" (*DNAT*). For details, refer to chapter 8.

20.3 List of connected VPN clients

In *Status* → *VPN clients*, you can see an overview of VPN clients currently connected to the *Kerio Control's* VPN server.

The information provided is as follows:

- Username used for authentication to the firewall. VPN traffic is reflected in statistics of this user.
- The operating system on which the user have the *Kerio VPN Client* installed.
- DNS name of the host which the user connects from. If *Kerio Control* cannot resolve the corresponding hostname from the DNS, its (public) IP address is displayed instead.
- IP address assigned to the client by the VPN server. This IP address "represents" the client in the local network.
- Session duration.

- *Kerio VPN Client* version, including build number.
- IP address — public IP address of the host which the client connects from (see the *Hostname* column above).
- Client status — *connecting*, *authenticating* (*Kerio Control* verifies username and password), *authenticated* (username and password correct, client configuration in progress), *connected* (the configuration has been completed, the client can now communicate with hosts within the local network).

  Note: Disconnected clients are removed from the list automatically.

20.4 Alerts

Kerio Control enables automatic sending of messages informing the administrator about important events. This makes the firewall administration more comfortable, since it is not necessary to connect to the firewall too frequently to view all status information and logs (however, it is definitely worthy to do this occasionally).

Kerio Control generates alert messages upon detection of any specific event for which alerts are preset. All alert messages are recorded into the *Alert* log (see chapter 23.3). The firewall administrator can specify which alerts will be sent to whom, as well as a format of the alerts. Sent alerts can be viewed in *Status → Alerts*.

Note: SMTP relay must be set in *Kerio Control* (see chapter 19.3), otherwise alerting will not work.

Alerts Settings

Alerts settings can be configured in the *Alerts settings* tab under *Configuration → Accounting*.

This tab provides list of "rules" for alert sending. Use checking boxes to enable/disable individual rules.

Use the *Add* or the *Edit* button to (re)define an alert rule.

Alert

Type of the event upon which the alert will be sent:

- *Virus detected* — antivirus engine has detected a virus in a file transmitted by HTTP, FTP, SMTP or POP3 (refer to chapter 15).
- *Host connection limit reached* — a host in the local network has reached the connection limit (see chapter 9.3). This may indicate deployment of an undesirable network application (e.g. Trojan horse or a spyware) on a corresponding host.
- *Low free disk space warning* — this alert warns the administrator that the free space of the *Kerio Control* host is low (under 11 percent of the total disk capacity). *Kerio Control* needs enough disk space for saving of logs, statistics, configuration settings, temporary files (e.g. an installation archive of a new version or

a file which is currently scanned by an antivirus engine) and other information. Whenever the *Kerio Control* administrator receives such alert message, adequate actions should be performed immediately.

- *New version available* — a new version of *Kerio Control* has been detected at the server of Kerio Technologies during an update check.
- *User transfer quota exceeded* — a user has reached daily, weekly or monthly user transfer quota and *Kerio Control* has responded by taking an appropriate action. For details, see chapter 17.1.
- *Connection failover event* — the Internet connection has failed and the system was switched to a secondary line, or vice versa (it was switched back to the primary line). For details, refer to chapter 7.4.
- *License expiration* — expiration date for the corresponding license or *Kerio Control* Software Maintenance or license of any module integrated in *Kerio Control* (such as *Kerio Web Filter*, the *Sophos* antivirus, etc.) is getting closer. The administrator should check the expiration dates and prolong a corresponding license or Software Maintenance (for details, refer to chapter 5).
- *Dial / Hang-up of RAS line* *Kerio Control* is dialing or hanging-up a RAS line (see chapter 6). The alert message provides detailed information on this event: line name, reason of the dialing, username and IP address of the host from which the request was sent.

Action

Method of how the user will be informed:

- *Send email* — information will be sent by an email message,
- *Send SMS (shortened email)* — short text message will be sent to the user's cell phone.
  Note: SMS messages are also sent as email. User of the corresponding cell phone must use an appropriate email address (e.g. `number@provider.com`). Sending of SMS to telephone numbers (for example via GSM gateways connected to the *Kerio Control* host) is not supported.

To

Email address of the recipient or of his/her cell phone (related to the *Action* settings). Recipients can be selected from the list of users (email addresses) used for other alerts or new email addresses can be added by hand.

Valid at time interval

Select a time interval in which the alert will be sent. Click *Edit* to edit the interval or to create a new one (details in chapter 16.2).

Alert Templates

Formats of alert messages (email or/and SMS) are defined by templates. Individual formats can be viewed in the *Status* → *Alerts* section of the administration interface. Templates are predefined messages which include certain information (e.g. username, IP address, number of connections, virus information, etc.) defined through specific variables. *Kerio Control* substitutes variables by corresponding values automatically. The *Kerio Control* administrator can customize these templates.

Templates are stored in the `templates` subdirectory of the installation directory of *Kerio Control*.

(the typical path is `C:\Program Files\Kerio\WinRoute Firewall\templates`):

- the `console` subdirectory — messages displayed in the left-positioned part of the section *Status → Alerts* (overview),
- the `console\details` subdirectory — messages displayed at the right part of the section *Status → Alerts* (details),
- the `email` subdirectory — messages sent by email (each template contains a message in the plain text and HTML formats),
- the `sms` subdirectory — SMS messages sent to a cell phone.

Each subdirectory includes a set of templates in all languages supported by *Kerio Control*. In the *Kerio Control Administration* interface, alerts are displayed in the currently set language. Email and SMS alerts sent are always in English.

Alerts overview in the administration interface

Section *Status → Alerts* displays all alerts sent to users since startup of *Kerio Control*. Alerts are displayed in the language of the *Administration Console*.

Note: Email sending of individual alerts can be set under *Configuration → Accounting*, on the *Alerts* tab (see above).

On the left side of the *Alerts* section, all sent alerts (sorted by dates and times) are listed.

Each line provides information on one alert:

- *Date* — date and time of the event,
- *Alert* — event type.

Click an event to view detailed information on the item including a text description (defined by templates under `console\details` — see above) in the right-side section of the window.

Note: Details can be optionally hidden or showed by clicking the *Hide/Show details* button (details are displayed by default).

Alert Log

The *Alert* log gathers records about all alerts generated by *Kerio Control* (no matter if they were or were not sent by email to user/administrator). For details, see chapter 23.3.

20.5 System Health (editions Appliance and Box)

The *System Health* section shows current usage of CPU, RAM and the disk space of the computer or device where *Kerio Control* is running.

Time interval

Selection of time period for which CPU load and RAM usage is displayed (2 hours or 1 day).

CPU

Timeline of the computer's (device's) CPU load. Short time peak load rates ("peaks" of the chart) are not unusual and can be caused for example by the network activity.

RAM

RAM usage timeline.

Disk space

Currently used and free space on the disk space or a memory card.

Tasks

Restart of the system or shutdown of the device (available only in editions *Appliance* and *Box*).

Lack of system resources may seriously affect functionality of *Kerio Control.* If these resources are permanently overloaded, it is recommended to check other applications and services running on the system. In case of editions *Appliance* and *Box* it is recommended to restart *Kerio Control* and then check system resources usage once again.

If storage space is missing, it is possible to click on *Manage* and delete some files created by running *Kerio Control* (logs, statistics data, etc.) and set limits which prevent possible running out of storage space.

Storage space management

To get enough free space on the disk, you can use the following methods:

- Free disk space by deleting old or unnecessary files (logs, statistics, etc.),
- Set size limits for files created by *Kerio Control* appropriately.

The dialog shows only such components data of which occupy at least a certain amount of space (MB).

Chapter 21

Basic statistics

Statistical information about users (volume of transmitted data, used services, categorization of web pages) as well as of network interfaces of the *Kerio Control* host (volume of transmitted data, load on individual lines) can be viewed in *Kerio Control*.

In the *Kerio Control Administration* interface, it is possible to view basic quota information for individual users (volume of transferred data and quota usage information) and statistics of network interfaces (transferred data, traffic charts). Detailed statistics of users, web pages and volume of transferred data are available in the firewall's web interface (*Kerio StaR* — see chapter 22).

21.1 Volume of transferred data and quota usage

The *User Statistics* of the *Status* → *Statistics* section provides detailed statistics on volume of data transmitted by individual users during various time periods (today, this week, this month and total).

The *Quota* column provides usage of transfer quota by a particular user in percents (see chapter 17.1). Colors are used for better reference:

- green — 0%–74% of the quota is used
- yellow — 75%–99% of the quota is used
- red — 100% (limit reached)

Note:

1. User quota consists of three limits: daily, weekly and monthly. The *Quota* column provides the highest value of the three percentual values (if the daily usage is 50% of the daily quota, the weekly usage is 90% and the monthly usage is 70%, yellowed *90%* value is displayed in the *Quota* column).
2. Monthly quota is reset automatically at the beginning of an accounting period. This period may differ from a civil month (see chapter 22.2).

The *all users* line provides total volume of data transmitted by all users in the table (even of the unrecognized ones). The *unrecognized users* item includes all users who are currently not authenticated at the firewall. These lines do not include quota usage information.

Note:

1. Optionally, other columns providing information on volume of data transmitted in individual time periods in both directions can be displayed. Direction of data transmission

is related to the user (the *IN* direction stands for data received by the user, while *OUT* represents data sent by the user).

2. Information of volume of data transferred by individual users is saved in the `stats.cfg` file in the *Kerio Control* directory. This implies that this data will be saved the next time the *Kerio Control Engine* will be started.

User Quota dialog options

Right-click on the table (or on an item of a selected user) to open the context menu with the following options:

Delete User Traffic Counters

Removal of the selected line with data referring to a particular user. This option is helpful for reference purposes only (e.g. to exclude blocked user accounts from the list, etc.). Removed accounts will be added to the overview automatically when data in the particular account is changed (e.g. when we unblocked an account and its user connects and starts to communicate again).

> ***Warning:***
> Be aware that using this option for the *all users* item resets counters of all users, including unrecognized ones!

Note: Values of volumes of transferred data are also used to check user traffic quota (see chapter 17.1). Reset of user statistics also unblocks traffic of the particular user in case that the traffic has been blocked for quota reasons.

View host...

This option is not available unless the selected user is connected to the firewall. The *View host* option switches to the *Status* → *Active Hosts* section of the host the particular user is connected from.

If the user is connected from multiple hosts, the *View host* option opens a submenu with a list of all hosts which the particular user is connected from.

Refresh

This option will refresh the information on the *User Statistics* tab immediately. This function is equal to the function of the *Refresh* button at the bottom of the window.

Auto refresh

Settings for automatic refreshing of the information on the *User Statistics* tab. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Manage Columns

Use this option to select and unselect items (columns) which will (not) be displayed in the table.

21.2 Traffic Charts

!!! The *Interface statistics* tab in *Status* → *Statistics* provides detailed information on volume of data transmitted in both directions through individual interfaces of the firewall in selected time intervals (today, this week, this month, total).

Interfaces can be represented by network adapters, dial-ups or VPN tunnels. *VPN server* is a special interface — communication of all VPN clients is represented by this item in *Interface statistics*.

Optionally, other columns providing information on volume of data transmitted in individual time periods in both directions can be displayed. Direction of data transmission is related to the interface (the *IN* direction stands for data received by the interface, while *OUT* represents data sent from the interface).

Example:
The firewall connects to the Internet through the *Public* interface and the local network is connected to the
LAN interface. A local user downloads 10 MB of data from the Internet. This data will be counted as follows:

- *IN* at the *Public* interface is counted as an *IN* item (data from the Internet was received through this interface),
- at the *LAN* interface as *OUT* (data was sent to the local network through this interface).

Note: Interface statistics are saved into the `stats.cfg` configuration file in the *Kerio Control* installation directory. This implies that they are not reset when the *Kerio Control Engine* is closed.

Interface Statistics menu

A context menu providing the following options will be opened upon right-clicking anywhere in the table (or on a specific interface):

Reset interface statistics

This option resets statistics of the selected interface. It is available only if the mouse pointer is hovering an interface at the moment when the context menu is opened.

Refresh

This option will refresh the information on the *Interface Statistics* tab immediately. This function is equal to the function of the *Refresh* button at the bottom of the window.

Auto refresh

Settings for automatic refreshing of the information on the *Interface Statistics* tab. Information can be refreshed in the interval from 5 seconds up to 1 minute or the auto refresh function can be switched off (*No refresh*).

Manage Columns

Use this option to select and unselect items (columns) which will (not) be displayed in the table.

Remove interface statistics

This option removes the selected interface from the statistics. Only inactive interfaces (i.e. disconnected network adapters, hung-up dial-ups, disconnected VPN tunnels or VPN servers which no client is currently connected to) can be removed. Whenever a removed interface is activated again (upon connection of the VPN tunnel, etc.), it is added to the statistics automatically.

Graphical view of interface load

The traffic processes for a selected interface (transfer speed in *B/s*) and a specific time period can be viewed in the chart provided in the bottom window of the *Interface statistics* tab. Use the *Show details / Hide details* button to show or hide this chart (the show mode is set by default).

The period (*2 hours* or *1 day*) can be selected in the *Time interval* box. The selected time range is always understood as the time until now ("last 2 hours" or "last 24 hours").

The x axis of the chart represents time and the y axis represents traffic speed. The x axis is measured accordingly to a selected time period, while measurement of the y axis depends on the maximal value of the time interval and is set automatically (bytes per second is the basic measure unit — *B/s*).

The legend above the graph shows the sampling interval (i.e. the time for which a sum of connections or messages is counted and is displayed in the graph).

> ***Example:***
> Suppose the *1 day* interval is selected. Then, an impulse unit is represented by 5 minutes. This means that every 5 minutes an average traffic speed for the last 5 minutes is recorded in the chart.

Chapter 22

Kerio StaR - statistics and reporting

The *Kerio Control's* web interface provides detailed statistics on users, volume of transferred data, visited websites and web categories. This information may help figure out browsing activities and habits of individual users.

The statistics monitor the traffic between the local network and the Internet. Volumes of data transferred between local hosts and visited web pages located on local servers are not included in the statistics (also for technical reasons).

One of the benefits of web statistics and reports is their high availability. The user (usually an office manager) does not need rights for *Kerio Control* administration (special rights are used for statistics). Statistics viewed in web browsers can also be easily printed or saved on the disk as web pages.

Notes:

1. The firewall administrator should inform users that their browsing activities are monitored by the firewall.

2. Statistics and reports in *Kerio Control* should be used for reference only. It is highly unrecommended to use them for example to figure out exact numbers of Internet connection costs per user.

3. For correct functionality of the *Kerio StaR* interface, it is necessary that the firewall host's operating system supports all languages that would be used in the *Kerio StaR* interface. Some languages (Chinese, Japanese, etc.) may require installation of supportive files. For details, refer to documents regarding the corresponding operating system.

This chapter addresses setting of parameters in the *Kerio Control* administration. The *Kerio StaR* interface is described thoroughly in the *Kerio Control — User's Guide*.

22.1 Monitoring and storage of statistic data

Diverse data is needed to be gathered for the statistics. Statistic data is stored in the database (the `star\data` subdirectory of the *Kerio Control's* installation directory — for details, see chapter 26.1). Total period length for which *Kerio Control* keeps the statistics can be set in the *Accounting* section (see chapter 22.2). By default, this time is set to *24 months* (i.e. 2 years).

For technical reasons, the *Kerio Control Engine* stores gathered statistic data in the cache (the `star\cache` subdirectory) and data is recorded in the database once per hour. The cache is represented by several files on the disk. This implies that any data is kept in the cache even if the *Kerio Control Engine* is stopped or another problem occurs (failure of power supply, etc.) though not having been stored in the database yet.

The statistics use data from the main database. This implies that current traffic of individual users is not included in the statistics immediately but when the started period expires and the data is written in the database.

Note: Data in the database used for statistics cannot be removed manually (such action would be meaningless). In statistics, it is possible to switch into another view mode where data is related only to a period we need to be informed about. If you do not wish to keep older data, it is possible to change the statistics storage period (see above).

Requirements of the statistics

The following conditions must be met for correct function of all statistics:

- The firewall should always require user authentication. The statistics by individual users would not match the true state if unauthenticated users are allowed to access the Internet. For details see chapter 12.

- For statistics on visited websites, it is necessary that a corresponding protocol inspector is applied to any *HTTP* traffic. This condition is met by default unless special traffic rules disabling the particular protocol inspector are applied (see chapter 8.7).

  If the *Kerio Control* proxy server is used, visited pages are monitored by the proxy server itself (see chapter 10.5).

  Note: HTTPS traffic is encrypted and, therefore, it is impossible to monitor visited sites and categories. Only volume of transferred data is included in the statistics for such traffic.

- For monitoring of web categories of visited websites, the *Kerio Web Filter* module must be enabled. In its configuration, the *Categorize each page regardless of HTTP rules* option should be enabled, otherwise web categories statistics would be unreliable. For details, see chapter 14.3.

Gathering of statistical information and mapped services

Connections from the Internet to mapped services on local hosts (or to services on the firewall available from the Internet — see chapter 8.3) are also included in user statistics. If a user is connected to the firewall from the particular host, access to the mapped service is considered as an activity of this user. Otherwise, such connection is included in activity of unknown users (users who are not logged in).

The following example helps recognize importance of this feature. User *jsmith* is authenticated at the firewall and connected to it from a local workstation. The *RDP* service for this host is mapped on the firewall, allowing the user to work remotely on the workstation. If user *jsmith* connects from the Internet to the remote desktop on the workstation, this connection (and data transferred within the connection) will be correctly included in the user's statistics and quota.

The following example addresses case of a mapped web server accessible from the Internet. Any (anonymous) user in the Internet can connect to the server. However, web servers are usually located on a special machine which is not used by any user. Therefore, all traffic of this server will be accounted for users who are "not logged in".

However, if any user is connected to the firewall from the server, any traffic between clients in the Internet and the web server is accounted as an activity of this user. If this user also reaches their data volume quota, corresponding restrictions will be applied to this web server (see chapters 17.2 and 11.3).

22.2 Settings for statistics and quota

Under certain circumstances (too many connected users, great volume of transmitted data, low capacity of the *Kerio Control* host, etc.), viewing of statistics may slow the firewall and data transmission (Internet connection) down. Be aware of this fact while opening the statistics. Therefore, *Kerio Control* allows such configuration of statistics that is customized so that only useful data is gathered and useful statistics created. It is also possible to disable creation of statistics if desirable. This would save operation space of *Kerio Control* as well as the disk space of its host.

Statistics settings also affect monitoring of volume of transferred data against user quota (refer to chapters 17.1 and 21).

Use the *Statistics / Quota* tab in *Configuration → Accounting* to set gathering of statistical data and accounting periods for quota and statistics.

Enable/disable gathering of statistic data

The *Gather Internet Usage statistics* option enables/disables all statistics (i.e. stops gathering of data for statistics).

The *Monitor user browsing behavior* option enables monitoring and logging of browsing activity of individual users. If is not necessary to gather these statistics, it is recommended to disable this option (this reduces demands to the firewall and saves the server's disk space).

You can use the *Keep at most...* parameter to specify a time period for which the data will be kept (i.e. the age of the oldest data that will be available). This option affects disk space needed for the statistics remarkably. To save disk space, it is therefore recommended to keep the statistics only for a necessary period.

Advanced settings for statistics

The *Advanced* button opens a dialog where parameters can be set for viewing of statistics in the *Kerio StaR* interface (see chapter 21).

The *Show user names in statistics by...* option enables select a mode of how users and their names will be displayed in individual user statistics. Full names can be displayed as *first name second name* or *second name, first name*. Optionally, it is also possible to view full names followed by username without or with domain (if domain mapping is used).

Statistics and quota accounting periods

Accounting period is a time period within which information of transferred data volume and other information is gathered. Statistics enable generating of weekly and monthly overviews. In *Accounting Periods*, it is possible to define starting days for weekly and monthly periods (for example, in statistics, a month can start on day 15 of the civil month and end on day 14 of the following civil month).

The parameter of first day of monthly period also sets when the monthly transferred data counter of individual users will be set to zero (for monthly quota details, see chapter 17.2).

Note: Setting of accounting period does not affect log rotation (see chapter 23.2).

Statistics and quota exceptions

On the *Exceptions* tab, it is possible to define exceptions for statistics and for transferred data quota.

This feature helps avoid gathering of irrelevant information. Thus, statistics are kept transparent and gathering and storage of needless data is avoided.

Usage of individual exceptions:

Time interval

Define a time period when information will be gathered and included in statistics and quota (e.g. only in working hours). Without this period, no traffic will be included in the statistics and in the quota neither.

For details on time intervals, see chapter 16.2.

IP addresses

Define IP addresses of hosts which will be excluded from the statistics and to which quota will not be applied.

The selected group may include both local or Internet IP addresses. If any of these IP addresses belongs to the local network, bear in mind that no traffic of the host will be included in the statistics or the quota. In case of addresses of Internet servers, traffic of local users with the server will not be accounted in the statistics or any user quota.

For details on IP groups, see chapter 16.1.

Users and groups

Select users and/or user groups which will be excluded from the statistics and no quota will be applied to them. This setting has the highest priority and overrules any other quota settings in user or group preferences.

For details on users and groups, see chapter 17.

Web Pages

Define a URL group. Connections to web sites with these URLs will not be accounted. Such exception can be used for example to exclude the own corporate web servers from the statistics (connection to corporate websites is usually considered a work-related activity) or to exclude ads connection to certain pages may download advertisements

automatically, it is not the user's request. For this purpose, you can use the predefined URL group *Ads/banners* (see chapter 16.4).
Wildcards can be used in URL groups items. This implies that it is possible to define exceptions for particular pages or for all pages on a particular server, all web servers in a domain, etc. For details on URL groups, refer to chapter 16.1.
URL exceptions can be applied only to unsecured web pages (the *HTTP* protocol). Connections to secured pages (the *HTTPS* protocol) are encrypted and URL of such pages cannot be detected.
Note: Unlike in case of exceptions described above, data transferred within connections to such web pages will be included in the quota.

22.3 Connection to StaR and viewing statistics

To view statistics, user must authenticate at the *Kerio Control's* web interface first. User (or the group the user belongs to) needs rights for statistics viewing — see chapter 17.1. *StaR* can be accessed by several methods, depending on whether connecting from the *Kerio Control* host (locally) or from another host (remotely).

Note: For details on the *Kerio Control's* web interface, see chapter 13.2.

Accessing the statistics from the Kerio Control host

On the *Kerio Control* host, the *StaR* may be opened as follows:

- By using the *Internet Usage Statistics* link available in the *Kerio Control Engine Monitor* context menu (opened by the corresponding icon in the notification area — see chapter 3.1).
- By using the *Internet Usage Statistics* link under *Start* → *Programs* → *Kerio* → *Kerio Control*.

Both links open the unsecured *StaR* interface directly on the local host (`http://localhost:4080/star`) using the default web browser.

Note: Within local systems, secured traffic would be useless and the browser would bother user with needless alerts.

Remote access to the statistics

It is also possible to access the statistics remotely, i.e. from any host which is allowed to connect to the *Kerio Control* host and the web interface's ports, by using the following methods:

- If you are currently logged on to the *Kerio Control* administration, the *Internet Usage Statistics* link available in section *Status* → *Statistics* can be used. This link opens the secured *StaR* interface for statistics in the default web browser.

Note: URL for this link consists of the name of the server and of the port of the secured web interface see chapter 13.1). This guarantees function of the link from the *Kerio Control* host and from the local network. To make *Internet Usage Statistics* link work also for remote administration over the Internet, name of the particular server must be defined in the public DNS (with the IP address of the particular firewall) and traffic rules must allow access to the port of the secured Web interface(`4081` by default).

- At `https://server:4081/star` or `http://server:4080/star` This URL works for the *StaR* only. If the user has not appropriate rights to view statistics, an error is reported.

- At `https://server:4081/` or `http://server:4080/`. This is the primary URL of the *Kerio Control's* web interface. If the user possesses appropriate rights for stats viewing, the *StaR* welcome page providing overall statistics (see below) is displayed. Otherwise, the *My Account* page is opened (this page is available to any user).

Warning:
In case of access via the Internet (i.e. from a remote host) it is recommended to use only the secured version of the web interface. The other option would be too risky.

Updating data in StaR

First of all, the *StaR* interface is used for gathering of statistics and creating of reviews for certain periods. To *Kerio Control*, gathering and evaluation of information for *StaR* means processing of large data volumes. To reduce load on the firewall, data for *StaR* is updated approximately once in an hour. The top right corner of each *StaR* page displays information about when the last update of the data was performed.

For these reasons, the *StaR* interface is not useful for real-time monitoring of user activity. For these purposes, you can use the *Active Hosts* section in the *Kerio Control Administration* interface (see chapter 20.1).

Chapter 23

Logs

Logs keep information records of selected events occurred in *Kerio Control* or detected by *Kerio Control*. Each log is displayed in a window in the *Logs* section.

Each event is represented by one record line. Each line starts with a time mark in brackets (date and time when the event took place, in seconds). This mark is followed by an information, depending on the log type. If the record includes a URL, it is displayed as a hypertext link. Follow the link to open the page in your default browser.

Optionally, records of each log may be recorded in files on the local disk[7] and/or on the *Syslog* server.

Locally, the logs are saved in the files under the `logs` subdirectory where *Kerio Control* is installed. The file names have this pattern:

`file_name.log`

(e.g. `debug.log`). Each log includes an `.idx` file, i.e. an indexing file allowing faster access to the log when displayed in the *Kerio Control Administration* interface.

Individual logs can be rotated — after a certain time period or when a threshold of the file size is reached, log files are stored and new events are logged to a new (empty) file.

Kerio Control allows to save a selected log (or its part) in a file as plaintext or in HTML. The log saved can be analyzed by various tools, published on web servers, etc.

23.1 Logs Context Menu

When you right-click inside any log window, a context menu will be displayed where you can choose several functions or change the log's parameters (view, logged information).

Copy

This action makes a copy of the selected text from the log and keeps it in the clipboard. Text selection and copying through the context menu is supported only in *Internet Explorer* where it is necessary to allow access to the clipboard.
For this operation it is recommended to use shortcut `Ctrl+C` (or `Apple+C` on Mac). This method is compatible throughout operating systems.

[7] The local disk is a drive of the host where *Kerio Control* is installed, not a disk of the host you perform the administration on!

Save log

This option saves the log or selected text in a file as plaintext or in HTML.

> ***Hint:***
> This function provides more comfortable operations with log files than a direct access to log files on the disk of the computer where *Kerio Control* is installed. Logs can be saved even if *Kerio Control* is administered remotely.

The *Save log* option opens a dialog box where the following optional parameters can be set:

- *Target file* — name of the file where the log will be saved. By default, a name derived from the file name is set. The file extension is set automatically in accordance with the format selected.
- *Format* — logs can be saved as plaintext or in HTML. If the HTML format is used, colors will be saved for the lines background (see section *Highlighting*) and all URLs will be saved as hypertext links.
- *Source* — either the entire log or only a part of the text selected can be saved. Bear in mind that in case of remote administration, saving of an entire log may take some time.

Highlighting

Highlighting may be set for logs meeting certain criteria (for details, see below).

Log Settings

A dialog where log parameters such as log file name and path, rotation and *Syslog* parameters can be set. For details, see chapter 23.2.

Clear log

Removes entire log. All information of will be removed from the log forever (not only the information saved in the selected window).

> ***Warning:***
> Removed logs cannot be refreshed anymore.

Note: Only users with read and write rights are allowed to change log settings or remove logs.

Log highlighting

For better reference, it is possible to set highlighting for logs meeting certain criteria. Highlighting is defined by special rules shared by all logs. Seven colors are available (plus the background color of unhighlighted lines), however, number of rules is not limited.

Use the *Highlighting* option in the context pop-up menu of the corresponding log to set highlighting parameters.

Highlighting rules are ordered in a list. The list is processed from the top. The first rule meeting the criteria stops other processing and the found rule is highlighted by the particular color. Thanks to these features, it is possible to create even more complex combinations of rules, exceptions, etc. In addition to this, each rule can be “disabled” or “enabled” for as long as necessary.

Use the *Add* or the *Edit* button to (re)define a highlighting rule.

Each highlighting rule consists of a condition and a color which will be used to highlight lines meeting the condition. Condition can be specified by a substring (all lines containing the string will be highlighted) or by a so called regular expression (all lines containing one or multiple strings matching the regular expression will be highlighted).

The *Description* item is used for reference only. It is recommended to describe all created rules well (it is recommended to mention also the name of the log to which the rule applies).

Note: Regular expression is such expression which allows special symbols for string definition. *Kerio Control* accepts all regular expressions in accordance with the POSIX standard.
For detailed instructions contact Kerio technical support. For detailed information, refer for example to
http://www.gnu.org/software/grep/

23.2 Log settings

Option In *Log settings* in the log context menu, you can select options for saving the log and sending messages to the *Syslog* server. These parameters are saved separatelly for each log.

File Logging

Use the *File Logging*tab to define file name and rotation parameters.

Enable logging to file

This option enables/disables saving to a file. The file inherits the log’s name plus the `.log` extension. If log rotation is enabled, older logs are saved in files of the particular names including date and time of rotation.
All log files are stored in the `logs` subfolder of the *Kerio Control* head directory, i.e.:

- in *Windows* edition typically:

  `C:\Program Files\Kerio\WinRoute\Firewall\logs`

- in editions *Appliance* and *Box*, always:

  `/opt/kerio/winroute/logs`

Note: If the log is not saved in a file on the disk, only records generated since the last login to *Kerio Control Engine* will be shown. After logout (or closing of the window with the administration interface), the records will be lost.

Rotate regularly

Set intervals in which the log will be rotated regularly. The file will be stored and a new log file will be started in selected intervals.
Weekly rotation takes effect on Sunday nights. Monthly rotation is performed at the end of the month (in the night when one month ends and another starts).

Rotate when file exceeds size

Set a maximal size for each file. Whenever the threshold is reached, the file will be rotated. Maximal size is specified in megabytes (MB).

Keep at most ... log file(s)

Maximal count of log files that will be stored. Whenever the threshold is reached, the oldest file will be deleted.

Note:

1. If both *Rotate regularly* and the *Rotate when file exceeds size* are enabled, the particular file will be rotated whenever one of these conditions is met.
2. Setting of statistics and quotas accounting period does not affect log rotation (see chapter 22.2). Rotation follows the rules described above.

Syslog Logging

Tab *External log* allows sending of individual log records to the *Syslog* server. Simply enter the DNS name or the IP address of the *Syslog* server.

The *Syslog* server distinguishes logs by *Facility* and *Severity*. These values are fixed for each log (current values for individual logs can be found *External log*).

In *Kerio Control*, for all logs *Facility* is set to *16: Local use 0*. *Severity* values are provided in table 23.1.

Log	Severity
Alert	1: Alert
Config	6: Informational
Connection	6: Informational
Debug log	7: Debug
Dial	5: Notice
Error	3: Error
Filter	6: Informational
Http	6: Informational
Security	5: Notice
Sslvpn	5: Notice
Warning	4: Warning
Web	6: Informational

Table 23.1 Severity of Kerio Control logs

23.3 Alert Log

The *Alert* log provides a complete history of alerts generated by *Kerio Control* (e.g. alerts upon virus detection, dialing and hanging-up, reached quotas, detection of P2P networks, etc.).

Each event in the *Alert* log includes a time stamp (date and time when the event was logged) and information about an alert type (in capitals). The other items depend on an alert type.

Hint:
Email and SMS alerts can be set under *Configuration* → *Accounting*. All sent alerts can be viewed in the *Status* → *Alert messages* section (for details, see chapter 20.4).

23.4 Config Log

The *Config* log stores the complete history of communication between the administration interface and *Kerio Control Engine*. It is possible to determine what administration tasks were performed by a specific user.

The *Config* window contains three log types:

1. *Information about logging in to Kerio Control administration*

   Example:

   ```
   [18/Apr/2011 10:25:02] james - session opened
   for host 192.168.32.100
   [18/Apr/2011 10:32:56] james - session closed
   for host 192.168.32.100
   ```

   - `[18/Apr/2011 10:25:02]` — date and time when the record was written to the log
   - `winston` — the name of the user logged in for *Kerio Control* administration.
   - `session opened for host 192.168.32.100` — information about the beginning of the communication and the IP address of the computer from which the user connected
   - `session closed for host 192.168.32.100` — information about the end of the communication with the particular computer (user logged out or the administration closed)

2. *Configuration database changes*

   Changes performed in the administration interface. A simplified form of the SQL language is used when communicating with the database.

Example:

```
[18/Apr/2011 10:27:46] james - insert StaticRoutes
set Enabled='1', Description='VPN',
Net='192.168.76.0', Mask='255.255.255.0',
Gateway='192.168.1.16', Interface='LAN', Metric='1'
```

- `[18/Apr/2011 10:27:46]` — date and time when the record was written
- `winston` — the name of the user logged in for *Kerio Control* administration.
- `insert StaticRoutes ...` — the particular command used to modify the *Kerio Control's* configuration database (in this case, a static route was added to the routing table)

3. *Other changes in configuration*

A typical example of this record type is the change of traffic rules. When the user hits *Apply* in *Configuration* → *Traffic Policy* → *Traffic Rules*, a complete list of current traffic rules is written to the *Config* log.

Example:

```
[18/Apr/2011 12:06:03] Admin - New traffic policy set:
[18/Apr/2011 12:06:03] Admin - 1:  name=(ICMP traffic)
src=(any) dst=(any) service=("Ping")
snat=(any) dnat=(any) action=(Permit)
time_range=(always) inspector=(default)
```

- `[18/Apr/2011 12:06:03]` — date and time of the change
- `Admin` — login name of the user who did the change
- `1:` — traffic rule number (rules are numbered top to bottom according to their position in the table, the numbering starts from 1)
- `name=(ICMP Traffic) ...` — traffic rule definition (name, source, destination, service etc.)

Note: The default rule (see chapter 8.1) is marked with `default` instead of the positional number.

23.5 Connection Log

The *Connection* log gathers information about traffic matching traffic rules with the *Log matching connections* enabled (see chapter 8) or meeting certain conditions (e.g. log of *UPnP* traffic — see chapter 19.2).

How to read the Connection Log?

```
[18/Apr/2011 10:22:47] [ID] 613181 [Rule] NAT
[Service] HTTP [User] james
[Connection] TCP 192.168.1.140:1193 -> hit.google.com:80
[Duration] 121 sec [Bytes] 1575/1290/2865 [Packets] 5/9/14
```

- `[18/Apr/2011 10:22:47]` — date and time when the event was logged (Note: Connection logs are saved immediately after a disconnection)
- `[ID] 613181` — *Kerio Control* connection identification number
- `[Rule] NAT` — name of the traffic rule which has been used (a rule by which the traffic was allowed or denied).
- `[Service] HTTP` — name of a corresponding application layer service (recognized by destination port).

  If the corresponding service is not defined in *Kerio Control* (refer to chapter 16.3), the `[Service]` item is missing in the log.
- `[User] james` name of the user connected to the firewall from a host which participates in the traffic.

  If no user is currently connected from the corresponding host, the `[User]` item is missing in the log.
- `[Connection] TCP 192.168.1.140:1193 -> hit.top.com:80` — protocol, source IP address and port, destination IP address and port. If an appropriate log is found in the *DNS* module cache (see chapter 10.1), the host's DNS name is displayed instead of its IP address. If the log is not found in the cache, the name is not detected (such DNS requests would slow *Kerio Control* down).
- `[Duration] 121 sec` — duration of the connection (in seconds)
- `[Bytes] 1575/1290/2865` — number of bytes transferred during this connection (transmitted /accepted /total).
- `[Packets] 5/9/14` — number of packets transferred through this connection (transmitted/accepted/total)

23.6 Debug Log

Debug (debug information) is a special log which can be used to monitor certain kinds of information, especially for problem-solving. Too much information could be confusing and impractical if displayed all at the same time. Usually, you only need to display information relating to a particular service or function. In addition, displaying too much information slows *Kerio Control's* performance. Therefore, it is strongly recommended to monitor an essential part of information and during the shortest possible period only.

Selection of information monitored by the Debug log

The window's context menu for the *Debug* log includes (see chapter 23.1) further options for advanced settings of the log and for an on-click one-time view of status information.

These options are available only to users with full administration rights for *Kerio Control* (see chapter 17.1)..

Format of logged packets

For logging network traffic a template is used which defines which information will be recorded and what format will be used for the log. This helps make the log more transparent and reduce demands on disk space.
Detailed help is available in the dialog for template definition.

IP Traffic

This function enables monitoring of packets according to the user defined log expression. The expression must be defined with special symbols. After clicking on the *Help* button, a brief description of possible conditions and examples of their use will be displayed.
Logging of IP traffic can be cancelled by leaving or setting the *Expression* entry blank.

Show status

A single overview of status information regarding certain *Kerio Control* components. This information can be helpful especially when solving problems with *Kerio Technologies* technical support.

Messages

This feature allows advanced monitoring of functioning of individual *Kerio Control* modules. This information may be helpful when solving issues regarding *Kerio Control* components and/or certain network services.

- *WAN / Dial-up messages* information about dialed lines (request dialing, auto disconnection down-counter),
- *Filtering* — logs proving information on filtering of traffic passing through *Kerio Control* (antivirus control, website classification, detection and elimination of *P2P* networks, intrusion detection and prevention, dropped packets, etc.),
- *Accounting* — user authentication and monitoring of their activities (protocol recognition, statistics and reporting, etc.),
- *Kerio Control services* — protocols processed by *Kerio Control* services (*DHCP server*, the *DNS* module, web interface, and *UPnP* support),

- *Decoded protocols* — logs of specific protocols (*HTTP* and *DNS*),
- *Miscellaneous* — additional data (e.g. packet processing *Bandwidth Management*, switching between primary and secondary Internet connection, HTTP cache, license use, update checker, dynamic DNS, system configuration in editions *Appliance* and *Box*, etc.),
- *Protocol inspection* — reports from individual *Kerio Control's* protocol inspectors (sorted by protocol),
- *Kerio VPN* — detailed information on traffic within *Kerio VPN* VPN tunnels, VPN clients, encryptions, exchange of routing information, web server for *Clientless SSL-VPN*, etc.

23.7 Dial Log

Data about dialing and hanging up the dial-up lines, and about time spent on-line.

The following items (events) can be reported in the *Dial* log:

1. Manual connection (from the *Kerio Control Administration* interface — see chapter 6 or directly in the operating system)

   ```
   [15/Mar/2011 15:09:27] Line "Connection" dialing,
   console 127.0.0.1 - Admin
   ```

   ```
   [15/Mar/2011 15:09:39] Line "Connection" successfully connected
   ```

   The first log item is reported upon initialization of dialing. The log always includes *Kerio Control* name of the dialed line (see chapter 6). If the line is dialed from the administration interface, the log provides this additional information

   - where the line was dialed from (`console` — the administration interface, `system` — operating system),
   - IP address of the client (i.e. the host from which administration is performed),
   - login name of the user who sent the dial request.

   Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

2. Line disconnection (manual or automatic, performed after a certain period of idleness)

   ```
   [15/Mar/2011 15:29:18] Line "Connection" hang-up,
   console 127.0.0.1 - Admin
   ```

   ```
   [15/Mar/2011 15:29:20] Line "Connection" disconnected,
   connection time 00:15:53, 1142391 bytes received,
   250404 bytes transmitted
   ```

   The first log item is recorded upon reception of a hang-up request. The log provides information about interface name, client type, IP address and username.

The second event is logged upon a successful hang-up. The log provides information about interface name, time of connection (`connection time`), volume of incoming and outgoing data in bytes (`bytes received` and `bytes transmitted`).

3. Disconnection caused by an error (connection is dropped)

   ```
   [15/Mar/2011 15:42:51] Line "Connection" dropped,
   connection time 00:17:07, 1519 bytes received,
   2504 bytes transmitted
   ```

   The items are the same as in the previous case (the second item — the `disconnected` report).

4. Requested dialing (as a response to a DNS query)

   ```
   [15/Mar/2011 15:51:27] DNS query for "www.microcom.com"
   (packet UDP 192.168.1.2:4567 -> 195.146.100.100:53)
   initiated dialing of line "Connection"
   ```

   ```
   [15/Mar/2011 15:51:38] Line "Connection" successfully connected
   ```

   The first log item is recorded upon reception of a DNS request (the

   DNS module has not found requested DNS record in its cache). The log provides:

   - DNS name from which IP address is being resolved,
   - description of the packet with the corresponding DNS query (protocol, source IP address, source port, destination IP address, destination port),
   - name of the line to be dialed.

   Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

5. Dial of the link on demand (responding to a packet from the local network — only in *Windows* edition)

   ```
   [15/Mar/2011 15:53:42] Packet
   TCP 192.168.1.3:8580 -> 212.20.100.40:80
   initiated dialing of line "Connection"
   ```

   ```
   [15/Mar/2011 15:53:53] Line "Connection" successfully connected
   ```

   The first record is logged when *Kerio Control* finds out that the route of the packet does not exist in the routing table. The log provides:

   - description of the packet (protocol, source IP address, destination port, destination IP address, destination port),
   - name of the line to be dialed.

Another event is logged upon a successful connection (i.e. when the line is dialed, upon authentication on a remote server, etc.).

6. Connection error (e.g. error at the modem was detected, dial-up was disconnected, etc.)

```
[15/Mar/2011 15:59:08] DNS query for "www.microsoft.com"
(packet UDP 192.168.1.2:4579 -> 195.146.100.100:53)
initiated dialing of line "Connection"
```

```
[15/Mar/2011 15:59:12] Line "Connection" disconnected
```

The first record represents a DNS record sent from the local network, from that the line is to be dialed (see above).

The second log item (immediately after the first one) informs that the line has been hung-up. Unlike in case of a regular disconnection, time of connection and volume of transmitted data are not provided (because the line has not been connected).

23.8 Error Log

The *Error* log displays information about serious errors that affect the functionality of the entire firewall. The *Kerio Control* administrator should check this log regularly and try to eliminate problems found here. Otherwise, users might have problems with some services or/and serious security problems might arise.

Pattern of Error logs:

```
[15/Apr/2011 15:00:51] (6) Automatic update error:  Update failed.
```

- `[15/Apr/2011 15:00:51]` — timestamp (date and exact time when the error occurred),
- `(6)` — associated system error code (only for some errors),
- `Automatic update error:  Update failed.` — error description (failure of the automatic update in this case).

Categories of logs recorded in the *Error* log:

- An issue associated with system resources (insufficient memory, memory allocation error, etc.),
- License issues (the license has expired, will expire soon, invalid license, etc.),
- Internal errors (unable to read routing table or interface IP addresses, etc.),
- License issues (the number of users would break license limit, unable to find license file, Software Maintenance expiration, etc.),

- Configuration errors (unable to read configuration file, detected a loop in the configuration of the *DNS* module or the *Proxy server*, etc.),
- Network (socket) errors,
- Errors while starting or stopping the *Kerio Control Engine* (problems with low-level driver, problems when initializing system libraries, services, configuration databases, etc.),
- File system errors (cannot open/save/delete file),
- SSL errors (problems with keys and certificates, etc.),
- *Kerio Web Filter* errors (failed to activate the license, etc.),
- *Kerio VPN* errors,
- HTTP cache errors (errors when reading/writing cache files, not enough space for cache, etc.),
- *Kerio Web Filter* errors,
- Checking subsystem errors,
- Anti-virus module errors (anti-virus test not successful, problems when storing temporary files, etc.),
- Dial-up errors (unable to read defined dial-up connections, line configuration error, etc.),
- LDAP errors (server not found, login failed, etc.),
- Errors in automatic update and product registration,
- Dynamic DNS errors (unable to connect to the server, failed to update the record, etc.),
- *Bandwidth Management* errors,
- Errors of the web interface,
- Crashdumps after failure of the application,
- NTP client errors (synchronization of time with the server),
- The *Kerio Control Administration* web interface errors,
- Intrusion prevention system errors.

Note: If you are not able to correct an error (or figure out what it is caused by) which is repeatedly reported in the *Error* log, do not hesitate to contact our technical support. For detailed information, refer to chapter 27 or to http://www.kerio.com/.

23.9 Filter Log

This log gathers information on web pages and objects blocked/allowed by the HTTP and FTP filters (see chapters 14.2 and 14.5) and on packets matching traffic rules with the *Log matching packets* option enabled (see chapter 8) or meeting other conditions (e.g. logging of *UPnP* traffic — see chapter 19.2).

Each log line includes the following information depending on the component which generated the log:

- When an HTTP or FTP rule is applied: rule name, user, IP address of the host which sent the request and object's URL.
- When a traffic rule is applied: detailed information about the packet that matches the rule (rule name, source and destination address, ports, size, etc.). Format of the logged packets is defined by template which can be edited through the *Filter* log context menu. Detailed help is available in the dialog for template definition.

Example of a URL rule log message:

```
[18/Apr/2011 13:39:45] ALLOW URL 'Sophos update'
192.168.64.142 james HTTP GET
http://update.kerio.com/nai-antivirus/datfiles/4.x/dat-4258.zip
```

- `[18/Apr/2011 13:39:45]` — date and time when the event was logged
- `ALLOW` — action that was executed (`ALLOW` = access allowed, `DENY` = access denied)
- `URL` — rule type (for URL or FTP)
- `'Sophos update'` — rule name
- `192.168.64.142` — IP address of the client
- `jsmith` — name of the user authenticated on the firewall (no name is listed unless at least one user is logged in from the particular host)
- `HTTP GET` — HTTP method used in the request
- `http:// ...` — requested URL

Packet log example:

```
[16/Apr/2011 10:51:00] PERMIT 'Local traffic' packet to LAN,
proto:TCP, len:47, ip/port:195.39.55.4:41272 ->
192.168.1.11:3663, flags:  ACK PSH, seq:1099972190
ack:3795090926, win:64036, tcplen:7
```

- `[16/Apr/2011 10:51:00]` — date and time when the event was logged
- `PERMIT` — action that was executed with the packet (`PERMIT`, `DENY` or `DROP`)
- `Local traffic` — the name of the traffic rule that was matched by the packet
- `packet to` — packet direction (either `to` or `from` a particular interface)
- `LAN` — interface name (see chapter 6 for details)
- `proto:` — transport protocol (TCP, UDP, etc.)
- `len:` — packet size in bytes (including the headers) in bytes
- `ip/port:` — source IP address, source port, destination IP address and destination port
- `flags:` — TCP flags
- `seq:` — sequence number of the packet (TCP only)
- `ack:` — acknowledgement sequence number (TCP only)
- `win:` — size of the receive window in bytes (it is used for data flow control — TCP only)
- `tcplen:` — TCP payload size (i.e. size of the data part of the packet) in bytes (TCP only)

23.10 Http log

This log contains all HTTP requests that were processed by the HTTP inspection module (see section 16.3) or by the built-in proxy server (see section 10.5).

Http log has the standard format of either the *Apache* WWW server (see http://www.apache.org/) or of the *Squid* proxy server (see http://www.squid-cache.org/). Format of the log can be set through the context menu. The change will take effect with the next new log record (it is not possible convert existing records).

Note:

1. Only accesses to allowed pages are recorded in the *HTTP* log. Request that were blocked by HTTP rules are logged to the *Filter* log (see chapter 23.9), if the *Log* option is enabled in the particular rule (see section 14.2).
2. The *Http* log is intended to be processes by external analytical tools. The *Web* log (see bellow) is better suited to be viewed by the *Kerio Control* administrator.

An example of an HTTP log record in the Apache format:

```
192.168.64.64 - jflyaway
[18/Apr/2011:15:07:17 +0200]
"GET http://www.kerio.com/ HTTP/1.1" 304 0 +4
```

- `192.168.64.64` — IP address of the client host
- `rgabriel` — name of the user authenticated through the firewall (a dash is displayed if no user is authenticated through the client)
- `[18/Apr/2011:15:07:17 +0200]` — date and time of the HTTP request. The +0200 value represents time difference from the UTC standard (+2 hours are used in this example — CET).
- `GET` — used HTTP method
- `http://www.kerio.com` — requested URL
- `HTTP/1.1` — version of the HTTP protocol
- `304` — return code of the HTTP protocol
- `0` — size of the transferred object (file) in bytes
- `+4` — count of HTTP requests transferred through the connection

An example of Http log record in the Squid format:

```
1058444114.733 0 192.168.64.64 TCP_MISS/304 0
GET http://www.squid-cache.org/ - DIRECT/206.168.0.9
```

- `1058444114.733` — timestamp (seconds and milliseconds since January 1st, 1970)
- `0` — download duration (not measured in *Kerio Control*, always set to zero)
- `192.168.64.64` — IP address of the client (i.e. of the host from which the client is connected to the website)
- `TCP_MISS` — the TCP protocol was used and the particular object was not found in the cache ("missed"). *Kerio Control* always uses this value for this field.
- `304` — return code of the HTTP protocol
- `0` — transferred data amount in bytes (HTTP object size)
- `GET http://www.squid-cache.org/` — the HTTP request (HTTP method and URL of the object)
- `DIRECT` — the WWW server access method (*Kerio Control* always uses direct access)
- `206.168.0.9` — IP address of the WWW server

23.11 Security Log

A log for security-related messages. Records of the following types may appear in the log:

1. *Intrusion prevention system logs*

   Records of detected intrusions or traffic from IP addresses included in web databases of known intruders (blacklists) — for details, see chapter 9.1.

Example:

```
[02/Mar/2011 08:54:38] IPS: Packet drop, severity:  High,
Rule ID: 1:2010575 ET TROJAN ASProtect/ASPack Packed Binary
proto:TCP, ip/port:95.211.98.71:80(hosted-by.example.com)
-> 192.168.48.131:49960(wsmith-pc.company.com,user:smith)
```

- `IPS: Packet drop` — the particular intrusion had the action set for *Log and drop* (in case of the *Log* action, `IPS: Alert` is displayed in the log)
- `severity:  High` — severity level
- `Rule ID: 1:2010575` — number identifier of the intrusion (this number can be used for definition of exceptions from the intrusion detection system, i.e. in the system's advanced settings)
- `ET TROJAN ASProtect/ASPack...` — intrusion name and description (only available for some intrusions)
- `proto:TCP` — traffic protocol used
- `ip/port:95.211.98.71:80(hosted-by.example.com)` — source IP address and port of the detected packet; the brackets provide information of the DNS name of the particular computer, in case that it is identifiable
- `-> 192.168.48.131:49960(wsmith-pc.company.com,user:wsmith)` — destination IP address and port in the detected packet; the brackets provide DNS name of the particular host (if identifiable) or name of the user connected to the firewall from the particular local host

2. *Anti-spoofing log records*

   Messages about packets that where captured by the *Anti-spoofing* module (packets with invalid source IP address) — see section 9.3 for details.

Example:

```
[17/Jul/2011 11:46:38] Anti-Spoofing:
Packet from LAN, proto:TCP, len:48,
ip/port:61.173.81.166:1864 -> 195.39.55.10:445,
flags:  SYN, seq:3819654104 ack:0, win:16384, tcplen:0
```

- `packet from` — packet direction (either `from`, i.e. sent via the interface, or `to`, i.e. received via the interface)
- `LAN` — interface name (see chapter 6 for details)
- `proto:` — transport protocol (TCP, UDP, etc.)
- `len:` — packet size in bytes (including the headers) in bytes
- `ip/port:` — source IP address, source port, destination IP address and destination port
- `flags:` — TCP flags
- `seq:` — sequence number of the packet (TCP only)
- `ack:` — acknowledgement sequence number (TCP only)
- `win:` — size of the receive window in bytes (it is used for data flow control — TCP only)
- `tcplen:` — TCP payload size (i.e. size of the data part of the packet) in bytes (TCP only)

3. *FTP protocol parser log records*

Example 1:

```
[17/Jul/2011 11:55:14] FTP: Bounce attack attempt:
client:  1.2.3.4, server:  5.6.7.8,
command:  PORT 10,11,12,13,14,15
```

(attack attempt detected — a foreign IP address in the `PORT` command)

Example 2:

```
[17/Jul/2011 11:56:27] FTP: Malicious server reply:
client:  1.2.3.4, server:  5.6.7.8,
response:  227 Entering Passive Mode (10,11,12,13,14,15)
```

(suspicious server reply with a foreign IP address)

4. *Failed user authentication log records*

   Message format:

   ```
   Authentication: <service>: Client: <IP address>: <reason>
   ```

   - `<service>` — the *Kerio Control* service to which the client connects (`WebAdmin` = web administration interface, `WebAdmin SSL` = secured version of the web administration interface, `Proxy` = user authentication on the proxy server)
   - `<IP address>` — IP address of the computer from which the user attempted to authenticate
   - `<reason>` — reason of the authentication failure (nonexistent user / wrong password)

   Note: For detailed information on user quotas, refer to chapters 17.1 and 12.1.

5. *Information about the start and shutdown of the Kerio Control Engine*

   a) Engine Startup:

   ```
   [17/Dec/2011 12:11:33] Engine: Startup.
   ```

   b) Engine Shutdown:

   ```
   [17/Dec/2011 12:22:43] Engine: Shutdown.
   ```

23.12 Sslvpn Log

In this log, operations performed in the *Clientless SSL-VPN* interface are recorded. Each log line provides information about an operation type, name of the user who performed it and file associated with the operation.

Example:

```
[17/Mar/2011 08:01:51] Copy File: User: jsmith@company.com
File: '\\server\data\www\index.html'
```

The *Clientless SSL-VPN* interface and the corresponding log is available in *Kerio Control* for *Windows* only.

23.13 Warning Log

The *Warning* log displays warning messages about errors of little significance. Warnings can display for example reports about invalid user login (invalid username or password), error in communication of the server and Web administration interface, etc.

Events causing display of warning messages in this log do not greatly affect *Kerio Control's* operation. They can, however, indicate certain (or possible) problems. The *Warning* log can help if for example a user is complaining that certain services are not working.

Categories of warnings recorded in the *Warning* log:

- System warnings (e.g. an application found that is known as conflicting),
- *Kerio Control* configuration issues (invalid values retrieved from the configuration file),
- Warnings of *Kerio Control Engine* operations (e.g. DHCP, DNS, anti-virus check, user authentication, etc.),
- License warnings (Software Maintenance expiration, forthcoming expiration of the *Kerio Control* license, *Kerio Web Filter* license, or the anti-virus license),

  Note: License expiration (end of functionality of the product) is considered to be an error and it is logged into the *Error* log.
- *Bandwidth Management* warnings,
- *Kerio Web Filter* warnings,
- Crashdumps after failure of the application.

Examples of Warning logs:

```
[15/Apr/2011 15:00:51] Authentication subsystem warning:
Kerberos 5 auth:  user james@company.com not authenticated
[15/Apr/2011 15:00:51] Authentication subsystem warning:
Invalid password for user admin
[16/Apr/2011 10:53:20] Authentication subsystem warning:
User jflyaway doesn't exist
```

- The first log informs that authentication of user `jsmith` by the *Kerberos* system in the `company.com` domain failed
- The second log informs on a failed authentication attempt by user `admin` (invalid password)
- The third log informs on an authentication attempt by a user which does not exist (`johnblue`)

Note: With the above three examples, the relevant records will also appear in the `Security` log.

23.14 Web Log

This log contains all HTTP requests that were processed by the HTTP inspection module (see section 16.3) or by the built-in proxy server (see section 10.5). Unlike in the *HTTP* log, the log displays only queries to text pages, not including objects within these pages. In addition to each URL, name of the page is provided for better reference.

For administrators, the *Web* log is easy to read and it provides the possibility to monitor which Websites were opened by each user.

How to read the Web *Log?*

```
[24/Apr/2011 10:29:51] 192.168.44.128 james
"Kerio Technologies" http://www.kerio.com/
```

- `[24/Apr/2011 10:29:51]` — date and time when the event was logged
- `192.168.44.128` — IP address of the client host
- `james` — name of authenticated user (if no user is authenticated through the client host, the name is substituted by a dash)
- `"Kerio Technologies"` — page title

  (content of the `<title>` HTML element)

  Note: If the page title cannot be identified (i.e. for its content is compressed), the `"Encoded content"` will be reported.
- `http://www.kerio.com/` — URL pages

Chapter 24

Kerio VPN

Kerio Control enables secure interconnection of remote private networks using an encrypted tunnel and it provides clients secure access to their local networks via the Internet. This method of interconnection of networks (and of access of remote clients to local networks) is called virtual private network (*VPN*). *Kerio Control* includes a proprietary implementation of VPN, called "*Kerio VPN*".

VPN *Kerio Control* is designed so that it can be used simultaneously with the firewall and with NAT (even along with multiple translations) on any side. Creation of an encrypted tunnel between networks and setting remote access of clients at the server is very easy.

Kerio VPN enables creation of any number of encrypted *server-to-server* connections (i.e. tunnels to remote private networks). Tunnels are created between two *Kerio Control* firewalls (typically at Internet gateways of corresponding networks). Individual servers (endpoints of the tunnels) verify each other using SSL certificates — this ensures that tunnels will be created between trustworthy servers only.

Individual hosts can also connect to the VPN server in *Kerio Control* (secured *client-to-server* connections). Identities of individual clients are authenticated against a username and password (transmitted also by secured connection), so that unauthorized clients cannot connect to local networks.

Remote connections of clients are performed through *Kerio VPN Client*, included in *Kerio Control* (for a detailed description, view the stand-alone *Kerio VPN Client — User Guide* document).

Note: For deployment of the *Kerio VPN*, it is supposed that *Kerio Control* is installed at a host which is used as an Internet gateway. If this condition is not met, *Kerio VPN* can also be used, but the configuration can be quite complicated.

Benefits of Kerio VPN

In comparison with other products providing secure interconnection of networks via the Internet, the *Kerio VPN* solution provides several benefits and additional features.

- Easy configuration (only a few basic parameters are required for creation of tunnels and for configuration of servers which clients will connect to).
- No additional software is required for creation of new tunnels (*Kerio VPN Client* must be installed at remote clients — installation file of the application is 8 MB).
- No collisions arise while encrypted channels through the firewall are being created. It is supposed that one or multiple firewalls (with or without NAT) are used between connected networks (or between remote clients and local networks).

- No special user accounts must be created for VPN clients. User accounts in *Kerio Control* (or domain accounts if *Active Directory* or *Open Directory* is used — see chapter 12.1) are used for authentication.

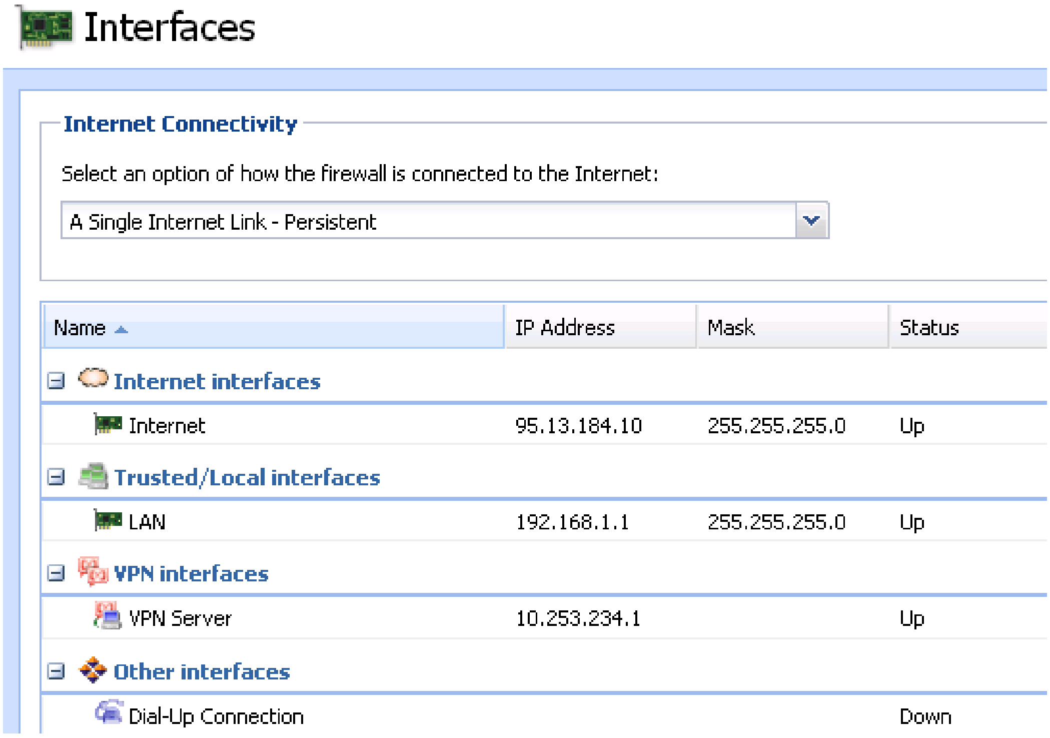
- Statistics about VPN tunnels and VPN clients can be viewed in *Kerio Control* (refer to chapter 21.2).

24.1 VPN Server Configuration

VPN server is used for connection of remote endpoints of VPN tunnels and of remote clients using *Kerio VPN Client*.

Note: Connection to the VPN server from the Internet must be first allowed by traffic rules. For details, refer to chapters 24.2 and 24.3.

VPN server is available in the *Interfaces* tab of the *Configuration* → *Interfaces* section as a special interface.



Interfaces

Internet Connectivity

Select an option of how the firewall is connected to the Internet:

A Single Internet Link - Persistent

Name	IP Address	Mask	Status
⊟ Internet interfaces			
Internet	95.13.184.10	255.255.255.0	Up
⊟ Trusted/Local interfaces			
LAN	192.168.1.1	255.255.255.0	Up
⊟ VPN interfaces			
VPN Server	10.253.234.1		Up
⊟ Other interfaces			
Dial-Up Connection			Down

Figure 24.1 Viewing VPN server in the table of interfaces

Double-click on the *VPN server* interface (or select the alternative and press *Edit*, or select *Edit* from the context menu) to open a dialog where parameters of the VPN server can be set.

VPN subnet and SSL certificate

Enable VPN server

Use this option to enable /disable VPN server. VPN server uses TCP and UDP protocols, port 4090 is used as default (the port can be changed in advanced options, however, it is usually not necessary to change it). If the VPN server is not used, it is recommended to disable it.
The action will be applied upon clicking the *Apply* button in the *Interfaces* tab.

IP address assignment

Specification of a subnet (i.e. IP address and a corresponding network mask) from which IP addresses will be assigned to VPN clients and to remote endpoints of VPN tunnels which connect to the server (all clients will be connected through this subnet).
By default (upon the first start-up after installation), *Kerio Control* automatically selects a free subnet which will be used for VPN. Under usual circumstances, it is not necessary to change the default subnet. After the first change in VPN server settings, the recently used network is used (the automatic detection is not performed again).

> ***Warning:***
> Make sure that the subnet for VPN clients does not collide with any local subnet! *Kerio Control* can detect a collision of the VPN subnet with local subnets. The collision may arise when configuration of a local network is changed (change of IP addresses, addition of a new subnet, etc.), or when a subnet for VPN is not selected carefully. If the VPN subnet collides with a local network, a warning message is displayed upon saving of the settings (by clicking *Apply* in the *Interfaces* tab). In such cases, redefine the VPN subnet.
> It is recommended to check whether IP collision is not reported after each change in configuration of the local network or/and of the VPN!

Notes:

1. Under certain circumstances, collision with the local network might also arise when a VPN subnet is set automatically (if configuration of the local network is changed later).
2. Regarding two VPN tunnels, it is also examined when establishing a connection whether the VPN subnet does not collide with IP ranges at the other end of the tunnel (remote endpoint).
   If a collision with an IP range is reported upon startup of the VPN server (upon clicking *Apply* in the *Interfaces* tab), the VPN subnet must be set by hand. Select a network which is not used by any of the local networks participating in the connection. VPN subnets at each end of the tunnel must not be identical (two free subnets must be selected).
3. VPN clients can also be assigned IP addresses according to login usernames. For details, see chapter 17.1.

SSL certificate

Information about the current VPN server certificate. This certificate is used for verification of the server's identity during creation of a VPN tunnel (for details, refer to chapter 24.3). The VPN server in *Kerio Control* uses the standard SSL certificate.

When defining a VPN tunnel, it is necessary to send the local endpoint's certificate fingerprint to the remote endpoint and vice versa (mutual verification of identity — see chapter 24.3).

> ***Hint:***
> Certificate fingerprint can be saved to the clipboard and pasted to a text file, email message, etc.

Click *Change SSL Certificate* to set parameters for the certificate of the VPN server. For the VPN server, you can either create a custom (self-subscribed) certificate or import a certificate created by a certification authority. The certificate created is saved in the `sslcert` subdirectory of the *Kerio Control* installation directory as `vpn.crt` and the particular private key is saved at the same location as `vpn.key`.

Methods used for creation and import of SSL certificates are described thoroughly in chapter 13.1.

Note: If you already have a certificate created by a certification authority especially for your server (e.g. for secured Web interface), it is also possible to use it for the VPN server — it is not necessary to apply for a new certificate.

DNS configuration for VPN clients

To allow VPN clients to access to local hosts using the hostnames, they need at least one local DNS server.

The *Kerio Control's* VPN server allows for the following options of DNS server configuration:

- *Use Kerio Control as DNS server* — IP address of a corresponding interface of *Kerio Control* host will be used as a DNS server for VPN clients (VPN clients will use the *DNS* module; see chapter 10.1). This is the default option in case that the *DNS* module is enabled in *Kerio Control*.

  If the *DNS* module is already used as a DNS server for local hosts, it is recommended to use it also for VPN clients. The *DNS* module provides the fastest responses to client DNS requests and possible collision (inconsistency) of DNS records will be avoided.

- *Specific DNS servers* — primary and optionally also secondary DNS server will be set for VPN clients.

  If another DNS server than the *DNS* module in *Kerio Control* is used in the local network, use this option.

DNS domain extension is also assigned to VPN clients. Domain extension specifies local domain. If the VPN client's extension matches a local domain of the networks it connects to, it can use hostnames within this network (e.g. `server`). Otherwise, full name of the host including domain is required (e.g. `server.company.local`).

DNS extension can be also resolved automatically or set manually:

- Automatic resolution can be used in case that the host belongs to the *Active Directory* domain and/or in case that firewall users are authenticated in this domain (see chapter 17.1).
- DNS domain must be specified in case that it is a *Open Directory* domain, *Windows NT* domain or a network without a domain, or in case that another domain extension is desirable (e.g. when multiple domains are mapped).

Note: DNS servers assigned by the VPN server will be used as primary/secondary DNS server(s) on the client host. This implies that *all* DNS queries from the client host will be sent to these servers. However, in most cases this kind of “redirection” has no side effects. Upon closing of the VPN connection, the original DNS configuration will be recovered.

WINS configuration for VPN clients

The WINS service is used for resolution of hostnames to IP addresses within *Microsoft Windows* networks. Assigning of a WINS server address then allows VPN clients browse in LAN hosts (*Network Neighborhood / My Network Places*).

Kerio Control can detect WINS servers either automatically (using its host configuration) or use specified addresses of primary or/and secondary WINS server(s). Automatic configuration can be used if you are sure that WINS servers on the *Kerio Control* host are set correctly.

Advanced Options

Listen on port

The port on which the VPN server listens for incoming connections (both TCP and UDP protocols are used). The port 4090 is set as default (under usual circumstances it is not necessary to switch to another port).
Note:

1. If the VPN server is already running, all VPN clients will be automatically disconnected during the port change.
2. If it is not possible to run the VPN server at the specified port (the port is used by another service), the following error will be reported in the *Error* log (see chapter 23.8) upon clicking on the *Apply* button:

```
(4103:10048) Socket error:  Unable to bind socket
for service to port 4090.

(5002) Failed to start service "VPN"
bound to address 192.168.1.1.
```

To make sure that the specified port is really free, view the *Error* log to see whether an error of this type has not been reported.

Custom Routes

Other networks to which a VPN route will be set for the client can be specified in this section. By default, routes to all local subnets at the VPN server's side are defined — see chapter 24.4).

> ***Hint:***
> Use the `255.255.255.255` network mask to define a route to a certain host. This can be helpful for example when a route to a host in the demilitarized zone at the VPN server's side is being added.

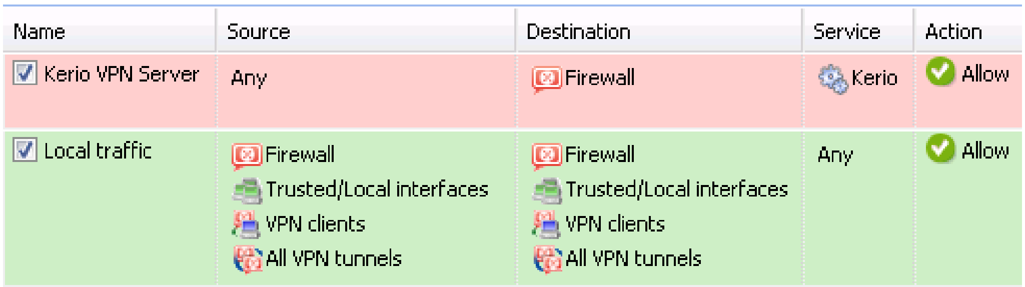
24.2 Configuration of VPN clients

The following conditions must be met to enable connection of remote clients to local networks via encrypted channels:

- The *Kerio VPN Client* must be installed at remote clients (for detailed description, refer to a stand-alone document, *Kerio VPN Client — User Guide*).
- Users whose accounts are used for authentication to *Kerio VPN Client* must possess rights enabling them connect to the VPN server in *Kerio Control* (see chapter 17.117.1).
- Connection to the VPN server from the Internet as well as communication between VPN clients must be allowed by traffic rules.

> ***Hint::***
> VPN clients correctly connected to the firewall can be overviewed in the administration interface, section *Status* → *VPN clients*. For details, see chapter 20.3.

Basic configuration of traffic rules for VPN clients



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	✓ Allow

Figure 24.2 Common traffic rules for VPN clients

- The first rule allows connection to the VPN server in *Kerio Control* from the Internet.

  To restrict the number of IP addresses from which connection to the VPN server will be allowed, edit the *Source* entry.

  By default, the *Kerio VPN* service is defined for TCP and UDP protocols, port 4090. If the VPN server is running at another port, this service must be redefined.

- The second rule allows communication between the firewall, local network and VPN clients.

If the rules are set like this, all VPN clients can access local networks and vice versa (all local hosts can communicate with all VPN clients). To restrict the type of network access available to VPN clients, special rules must be defined. A few alternatives of the restrictions settings within *Kerio VPN* are focused in chapter 24.5.

Note:

1. If you create traffic rules in the *Traffic Policy Wizard*, the rules described above may be created automatically. To achieve this, in the wizard simply enable option *Kerio VPN server* (allows connection of the VPN server from the Internet). For details, see chapter 8.1.
2. For access to the Internet, VPN clients use their current Internet connections. VPN clients are not allowed to connect to the Internet via *Kerio Control* (configuration of default gateway of clients cannot be defined).
3. For detailed information about traffic rules, refer to chapter 8.

24.3 Interconnection of two private networks via the Internet (VPN tunnel)

Kerio Control with support for VPN (VPN support is included in the typical installation) must be installed in both networks to enable creation of an encrypted tunnel between a local and a remote network via the Internet ("VPN tunnel").

Note: Each installation of *Kerio Control* requires its own license (see chapter 5).

Setting up VPN servers

First, the VPN server must be allowed by the traffic policy and enabled at both ends of the tunnel. For detailed description on configuration of VPN servers, refer to chapter 24.1.

Definition of a tunnel to a remote server

VPN tunnel to the server on the other side must be defined at both ends. Use the *Add → VPN tunnel* option in the *Interfaces* section to create a new tunnel.

Name of the tunnel

Each VPN tunnel must have a unique name. This name will be used in the table of interfaces, in traffic rules (see chapter 8.3) and interface statistics (details in chapter 21.2).

Configuration

Selection of a mode for the local end of the tunnel:

- *Active* — this side of the tunnel will automatically attempt to establish and maintain a connection to the remote VPN server.

  The remote VPN server specification is required through the *Remote hostname or IP address* entry. If the remote VPN server does not use the port 4090, a corresponding port number separated by a colon must be specified (e.g. `server.company.com:4100` or `85.17.210.230:9000`).

  This mode is available if the IP address or DNS name of the other side of the tunnel is known and the remote endpoint is allowed to accept incoming connections (i.e. the communication is not blocked by a firewall at the remote end of the tunnel).
- *Passive* — this end of the tunnel will only listen for an incoming connection from the remote (active) side.

  The passive mode is only useful when the local end of the tunnel has a fixed IP address and when it is allowed to accept incoming connections.

At least one end of each VPN tunnel must be switched to the active mode (passive servers cannot initialize connection).

Configuration of a remote end of the tunnel

When a VPN tunnel is being created, identity of the remote endpoint is authenticated through the fingerprint of its SSL certificate. If the fingerprint does not match with the fingerprint specified in the configuration of the tunnel, the connection will be rejected.

The fingerprint of the local certificate and the entry for specification of the remote fingerprint are provided in the *Settings for remote endpoint* section. Specify the fingerprint for the remote VPN server certificate and vice versa — specify the fingerprint of the local server in the configuration at the remote server.

If the local endpoint is set to the active mode, the certificate of the remote endpoint and its fingerprint can be downloaded by clicking *Detect remote certificate*. Passive endpoint cannot detect remote certificate.

However, this method of fingerprint setting is quite insecure —a counterfeit certificate might be used. If a fingerprint of a false certificate is used for the configuration of the VPN tunnel, it is possible to create a tunnel for the false endpoint (for the attacker). Moreover, a valid certificate would not be accepted from the other side. Therefore, for security reasons, it is recommended to set fingerprints manually.

DNS Settings

DNS must be set properly at both sends of the tunnel so that it is possible to connect to hosts in the remote network using their DNS names. One method is to add DNS records of the hosts (to the hosts file) at each endpoint. However, this method is quite complicated and inflexible.

If the *DNS* module in *Kerio Control* is used as the DNS server at both ends of the tunnel, DNS queries (for DNS rules, refer to chapter 10.1) can be forwarded to hostnames in the corresponding domain of the *DNS* module at the other end of the tunnel. DNS domain (or subdomain) must be used at both sides of the tunnel.

Detailed guidance for the DNS configuration is provided in the example in chapter 24.5.

Routing settings

On the *Advanced* tab, you can set which method will be used to add routes provided by the remote endpoint of the tunnel to the local routing table as well as define custom routes to remote networks.

The *Kerio VPN* routing issue is described in detail in chapter 24.4.

Connection establishment

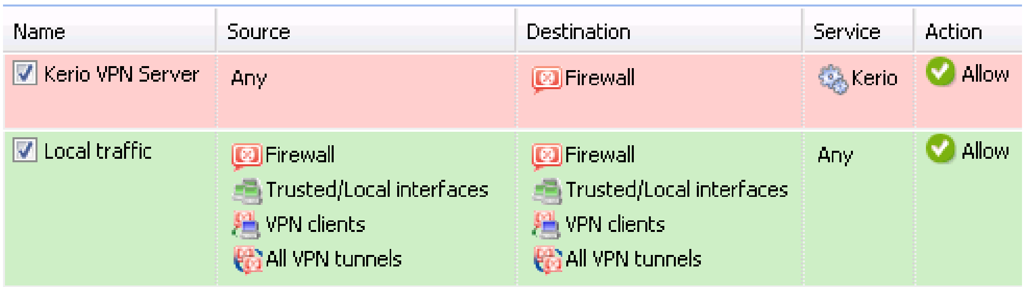
Active endpoints automatically attempt to recover connection whenever they detect that the corresponding tunnel has been disconnected (the first connection establishment is attempted immediately after the tunnel is defined and upon clicking the *Apply* button in *Configuration* → *Interfaces*, i.e. when the corresponding traffic is allowed — see below).

VPN tunnels can be disabled by the *Disable* button. Both endpoints should be disabled while the tunnel is being disabled.

Note: VPN tunnels keeps their connection (by sending special packets in regular time intervals) even if no data is transmitted. This feature protects tunnels from disconnection by other firewalls or network devices between ends of tunnels.

Traffic Rules Settings for VPN

Once the VPN tunnel is created, it is necessary to allow traffic between the LAN and the network connected by the tunnel and to allow outgoing connection for the *Kerio VPN* service (from the firewall to the Internet). If basic traffic rules are created in the wizard (see chapter 24.2), the conditions are met.



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	✓ Allow

Figure 24.3 Traffic Rules Settings for VPN

Note: Traffic rules set by this method allow full IP communication between the local network, remote network and all VPN clients. For access restrictions, define corresponding traffic rules (for local traffic, VPN clients, VPN tunnel, etc.). Examples of traffic rules are provided in chapter 24.5.

24.4 Exchange of routing information

An automatic exchange of routing information (i.e. of data informing about routes to local subnets) is performed between endpoints of any VPN tunnel (or between the VPN server and a VPN client). Thus, routing tables at both sides of the tunnel are always kept up-to-date.

Routing configuration options

Under usual circumstances, it is not necessary to define any custom routes — particular routes will be added to the routing tables automatically when configuration is changed at any side of the tunnel (or at the VPN server). However, if a routing table at any side of the VPN tunnel includes invalid routes (e.g. specified by the administrator), these routes are also interchanged. This might make traffic with some remote subnets impossible and overload VPN tunnel by too many control messages.

A similar problem may occur in case of a VPN client connecting to the *Kerio Control's* VPN server.

To avoid the problems just described, it is possible to go to the VPN tunnel definition dialog (see chapter 24.3) or to the VPN server settings dialog (refer to chapter 24.1) to set which routing data will be used and define custom routes.

Kerio VPN uses the following methods to pass routing information:

- *Routes provided automatically by the remote endpoint* (set as default) — routes to remote networks are set automatically with respect to the information provided by the remote endpoint. If this option is selected, no additional settings are necessary unless problems regarding invalid routes occur (see above).

- *Both automatically provided and custom routes* — routes provided automatically are complemented by custom routes defined at the local endpoint. In case of any collisions, custom routes are used as prior. This option easily solves the problem where a remote endpoint provides one or more invalid route(s).

- *Custom routes only* — all routes to remote networks must be set manually at the local endpoint of the tunnel. This alternative eliminates adding of invalid routes provided by a remote endpoint to the local routing table. However, it is quite demanding from the administrator's point of view (any change in the remote network's configuration requires modification of custom routes).

Routes provided automatically

Unless any custom routes are defined, the following rules apply to the interchange of routing information:

- default routes as well as routes to networks with default gateways are not exchanged (default gateway cannot be changed for remote VPN clients and/or for remote endpoints of a tunnel),
- routes to subnets which are identical for both sides of a tunnel are not exchanged (routing of local and remote networks with identical IP ranges is not allowed).
- other routes (i.e. routes to local subnets at remote ends of VPN tunnels excluding the cases described above, all other VPN and all VPN clients) are exchanged.

Note: As implied from the description provided above, if two VPN tunnels are created, communication between these two networks is possible. The traffic rules can be configured so that connection to the local network will be disabled for both these remote networks.

Update of routing tables

Routing information is exchanged:

- when a VPN tunnel is connected or when a VPN client is connected to the server,
- when information in a routing table at any side of the tunnel (or at the VPN server) is changed,
- periodically, every 10 minutes. The timeout starts upon each update (regardless of the update reason).

24.5 Example of Kerio VPN configuration: company with a filial office

This chapter provides a detailed exemplary description on how to create an encrypted tunnel connecting two private networks using the *Kerio VPN*.

This example can be easily customized. The method described can be used in cases where no redundant routes arise by creating VPN tunnels (i.e. multiple routes between individual private networks). Configuration of VPN with redundant routes (typically in case of a company with two or more filials) is described in chapter 24.6.

This example describes a more complicated pattern of VPN with access restrictions for individual local networks and VPN clients. An example of basic VPN configuration is provided in the *Kerio Control — Step By Step Configuration* document.

Specification

Supposing a company has its headquarters in New York and a branch office in London. We intend to interconnect local networks of the headquarters by a VPN tunnel using the *Kerio VPN*. VPN clients will be allowed to connect to the headquarters network.

The server (default gateway) of the headquarters uses the public IP address `85.17.210.230` (DNS name is `newyork.company.com`), the server of the branch office uses a dynamic IP address assigned by DHCP.

The local network of the headquarters consists of two subnets, `LAN 1` and `LAN 2`. The headquarters uses the `company.com` DNS domain.

The network of the branch office consists of one subnet only (`LAN`). The branch office `filial.company.com`.

Figure 24.4 provides a scheme of the entire system, including IP addresses and the VPN tunnels that will be built.

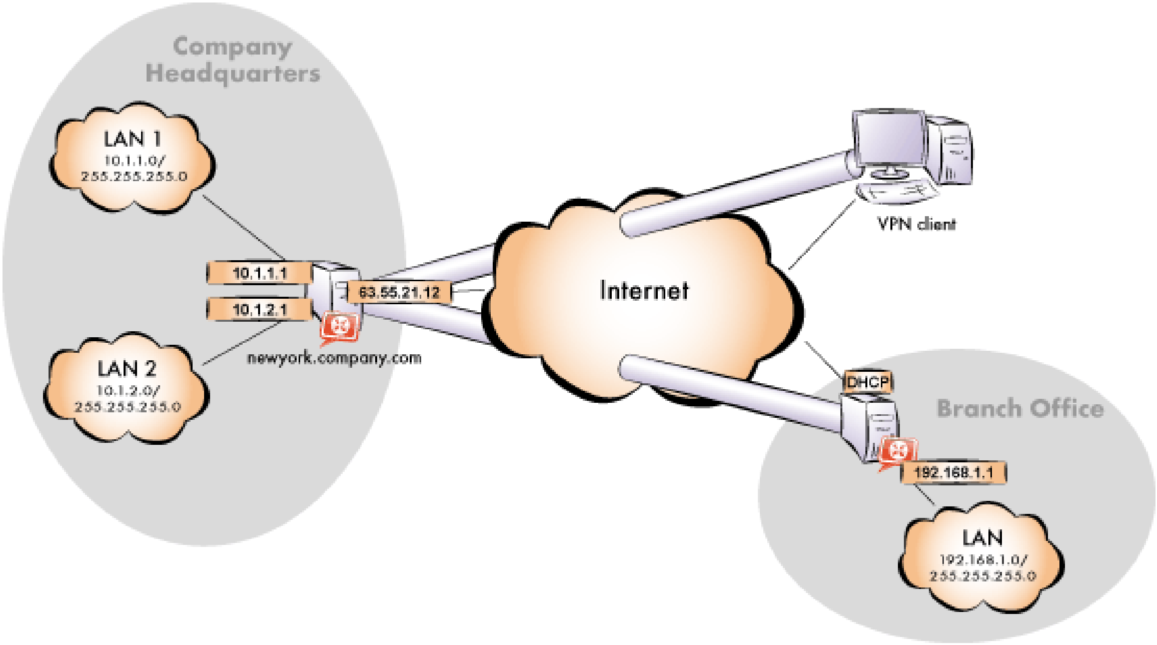


Figure 24.4 Example — interconnection of the headquarter and a filial office by VPN tunnel (connection of VPN clients is possible)

Suppose that both networks are already deployed and set according to the figure and that the Internet connection is available.

Traffic between the network of the headquarters, the network of the branch office and VPN clients will be restricted according to the following rules:

1. VPN clients can connect to the `LAN 1` and to the network of the branch office.

2. Connection to VPN clients is disabled for all networks.

3. Only the LAN 1 network is available from the branch office. In addition to this, only the *WWW*, *FTP* and *Microsoft SQL* services are available.

4. No restrictions are applied for connections from the headquarters to the branch office network.

5. LAN 2 is not available to the branch office network nor to VPN clients.

Common method

The following actions must be taken in both local networks (i.e. in the main office and the filial):

1. *Kerio Control* must be installed on the default gateway of the network.

   For *every* installation of *Kerio Control*, a stand-alone license for the corresponding number of users is required! For details see chapter 5.

2. Configure and test connection of the local network to the Internet. Hosts in the local network must use the *Kerio Control* host's IP address as the default gateway and as the primary DNS server.

   If it is a new (clean) *Kerio Control* installation, it is possible to use the connectivity wizard (refer to chapter 7.1) and the traffic policy wizard (see chapter 8.1).

   For detailed description of basic configuration of *Kerio Control* and of the local network, refer to the *Kerio Control — Step By Step* document.

3. In configuration of the *DNS* module set DNS forwarding rules for the domain in the remote network. This enables to access hosts in the remote network by using their DNS names (otherwise, it is necessary to specify remote hosts by IP addresses).

   For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the hostname table (if they use IP addresses) or enable cooperation of the *DNS* module with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 10.1.

4. In the *Interfaces* section, allow the VPN server and set its SSL certificate if necessary. Note the fingerprint of the server's certificate for later use (it will be required for configuration of the remote endpoint of the VPN tunnel).

   Check whether the automatically selected VPN subnet does not collide with any local subnet either in the headquarters or in the filial and select another free subnet if necessary.

5. Define the VPN tunnel to the remote network. The passive endpoint of the tunnel must be created at a server with fixed public IP address (i.e. at the headquarter's server). Only active endpoints of VPN tunnels can be created at servers with dynamic IP address.

If the remote endpoint of the tunnel has already been defined, check whether the tunnel was created. If not, refer to the *Error* log, check fingerprints of the certificates and also availability of the remote server.

6. In traffic rules, allow traffic between the local network, remote network and VPN clients and set desirable access restrictions. In this network configuration, all desirable restrictions can be set at the headquarter's server. Therefore, only traffic between the local network and the VPN tunnel will be enabled at the filial's server.

7. Test reachability of remote hosts from each local network. To perform the test, use the `ping` and `tracert` (`traceroute`) system commands. Test availability of remote hosts both through IP addresses and DNS names.

   If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

   If an IP address is tested successfully and an error is reported (*Unknown host*) when a corresponding DNS name is tested, then check configuration of the DNS.

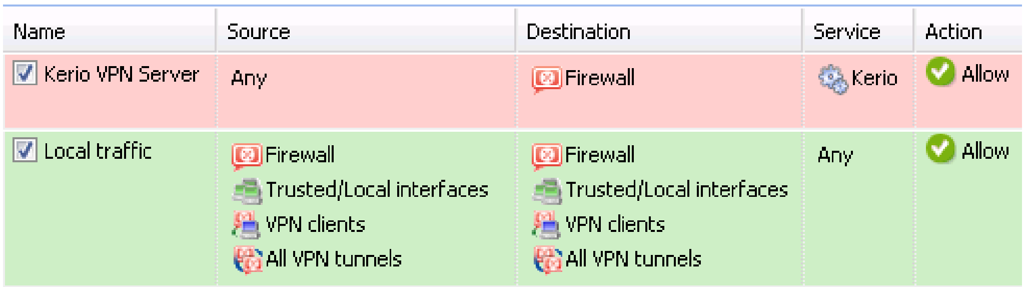
The following sections provide detailed description of the *Kerio VPN* configuration both for the headquarter and the filial offices.

Headquarters configuration

1. On the default gateway of the headquarters (referred as "server" in further text) install *Kerio Control*.

2. Perform basic configuration of *Kerio Control* by using the connectivity wizard (refer to chapter 7.1) and the traffic policy wizard (see chapter 8.1).

   In the traffic policy wizard, allow access to the *Kerio VPN server* service. This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	✓ Allow

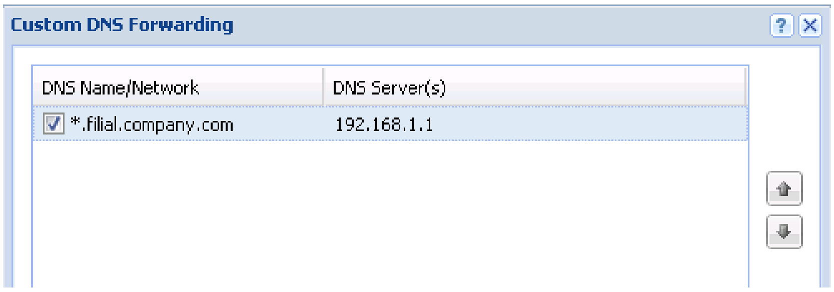
Figure 24.5 Headquarter — default traffic rules for Kerio VPN

Note: To keep the example as simple and transparent as possible, only traffic rules relevant for the *Kerio VPN* configuration are mentioned.

3. Customize DNS configuration as follows:

    - In the *Kerio Control's DNS* module configuration, enable *DNS forwarder* (forwarding of DNS requests to other servers).

    - Enable the *Use custom forwarding* option and define rules for names in the `filial.company.com` domain. Specify the server for DNS forwarding by the IP address of the internal interface of the *Kerio Control* host (i.e. interface connected to the local network at the other end of the tunnel).



Custom DNS Forwarding

DNS Name/Network	DNS Server(s)
☑ *.filial.company.com	192.168.1.1

Figure 24.6 Headquarter — DNS forwarding settings

    - No DNS server will be set on interfaces of the *Kerio Control* host connected to the local networks *LAN 1* and *LAN 2*.

    - On other computers set an IP address as the primary DNS server. This address must match the corresponding default gateway (`10.1.1.1` or `10.1.2.1`). Hosts in the local network can be configured automatically by DHCP protocol.

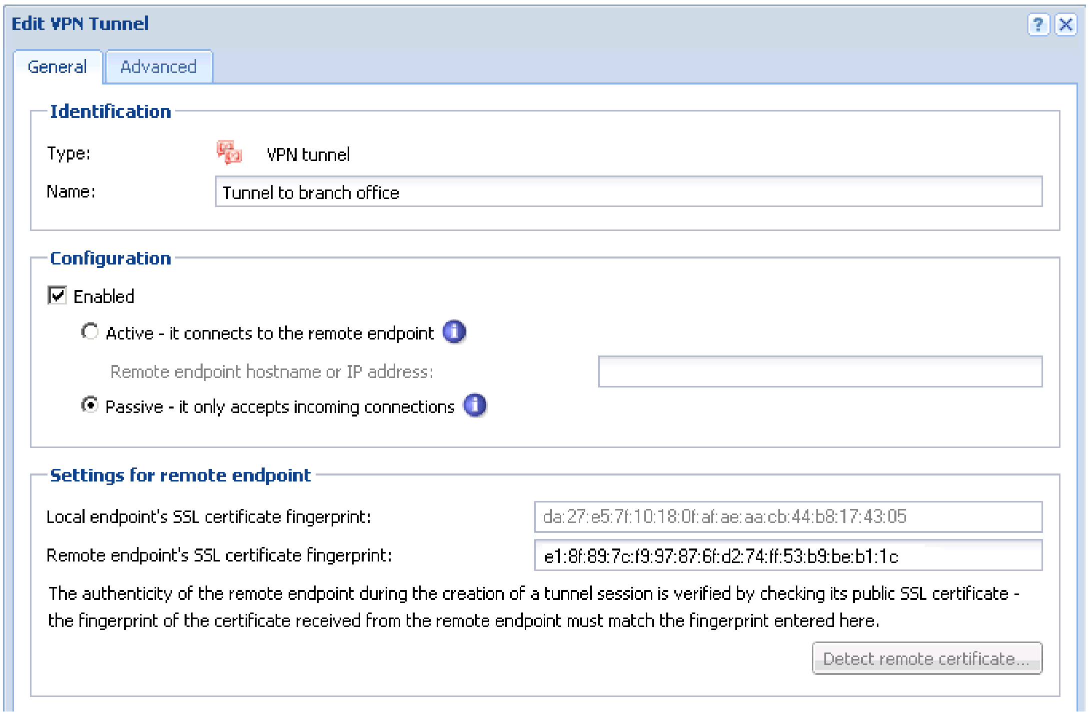
    Note: For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the hostname table (if they use IP addresses) or enable cooperation of the *DNS* module with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 10.1.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

    Note: The *VPN network* and *Mask* entries now include an automatically selected free subnet.

    For a detailed description on the VPN server configuration, refer to chapter 24.1.

5. Create a passive end of the VPN tunnel (the server of the branch office uses a dynamic IP address). Specify the remote endpoint's fingerprint by the fingerprint of the certificate of the branch office VPN server.



Edit VPN Tunnel

Identification

Type: VPN tunnel

Name: Tunnel to branch office

Configuration

☑ Enabled

○ Active - it connects to the remote endpoint

Remote endpoint hostname or IP address:

● Passive - it only accepts incoming connections

Settings for remote endpoint

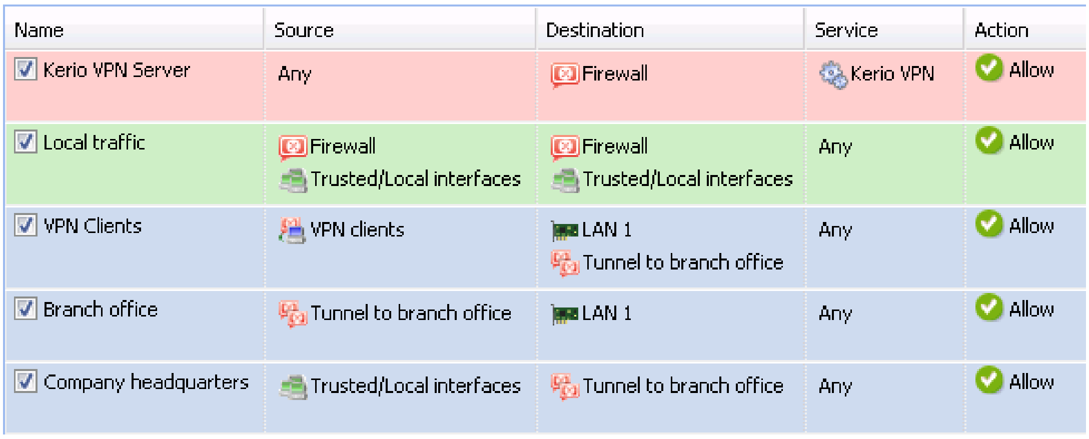
Local endpoint's SSL certificate fingerprint: da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05

Remote endpoint's SSL certificate fingerprint: e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 24.7 Headquarter — definition of VPN tunnel for a filial office

6. Customize traffic rules according to the restriction requirements.



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio VPN	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces	Firewall Trusted/Local interfaces	Any	✓ Allow
☑ VPN Clients	VPN clients	LAN 1 Tunnel to branch office	Any	✓ Allow
☑ Branch office	Tunnel to branch office	LAN 1	Any	✓ Allow
☑ Company headquarters	Trusted/Local interfaces	Tunnel to branch office	Any	✓ Allow

Figure 24.8 Headquarter — final traffic rules

- In the *Local Traffic* rule, remove all items except those belonging to the local network of the company headquarters, i.e. except the firewall and the group of interfaces *Trusted / Local*.
- Define (add) the *VPN clients* rule which will allow VPN clients to connect to *LAN 1* and to the network of the branch office (via the VPN tunnel).
- Create the *Branch office* rule which will allow connections to services in *LAN 1*.
- Add the *Company headquarters* rule allowing connections from the local network to the branch office network.

Rules defined this way meet all the restriction requirements. Traffic which will not match any of these rules will be blocked by the default rule (see chapter 8.3).

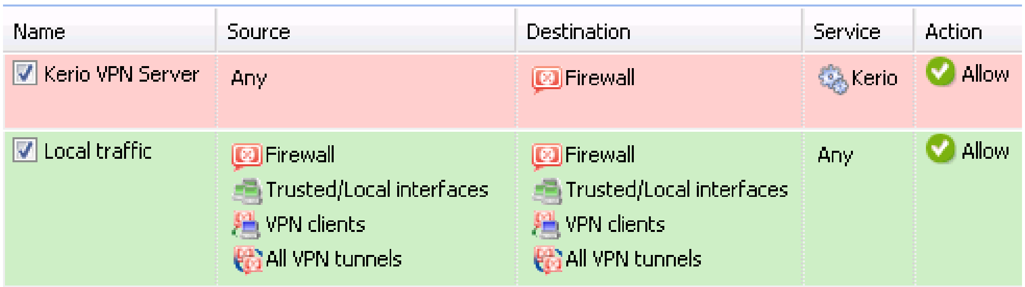
Configuration of a filial office

1. On the default gateway of the filial office (refered as "server" in further text) install *Kerio Control*.

2. Perform basic configuration of *Kerio Control* by using the connectivity wizard (refer to chapter 7.1) and the traffic policy wizard (see chapter 8.1).

   In this case there is no reason to enable the *Kerio VPN server* service (the server uses dynamic public IP address).

   This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	✓ Allow

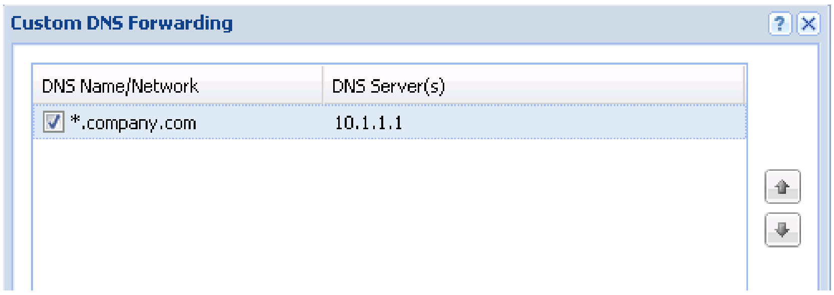
Figure 24.9 Filial office — default traffic rules for Kerio VPN

   When the VPN tunnel is created, customize these rules according to the restriction requirements (Step 6).

3. Customize DNS configuration as follows:

   - In the *Kerio Control's DNS* module configuration, enable *DNS forwarder* (forwarding of DNS requests to other servers).
   - Enable the *Use custom forwarding* option and define rules for names in the `filial.company.com` domain. Specify the server for DNS forwarding by the IP

address of the internal interface of the *Kerio Control* host (i.e. interface connected to the local network at the other end of the tunnel).



Custom DNS Forwarding

DNS Name/Network	DNS Server(s)
☑ *.company.com	10.1.1.1

Figure 24.10 Filial office — DNS forwarding settings

- No DNS server will be set on the interface of the *Kerio Control* host connected to the local network.

- On other computers set an IP address as the primary DNS server. This address must match the corresponding default gateway (`192.168.1.1`). Hosts in the local network can be configured automatically by DHCP protocol.

Note: For proper functionality of DNS, the DNS database must include records for hosts in a corresponding local network. To achieve this, save DNS names and IP addresses of local hosts into the hostname table (if they use IP addresses) or enable cooperation of the *DNS* module with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 10.1.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

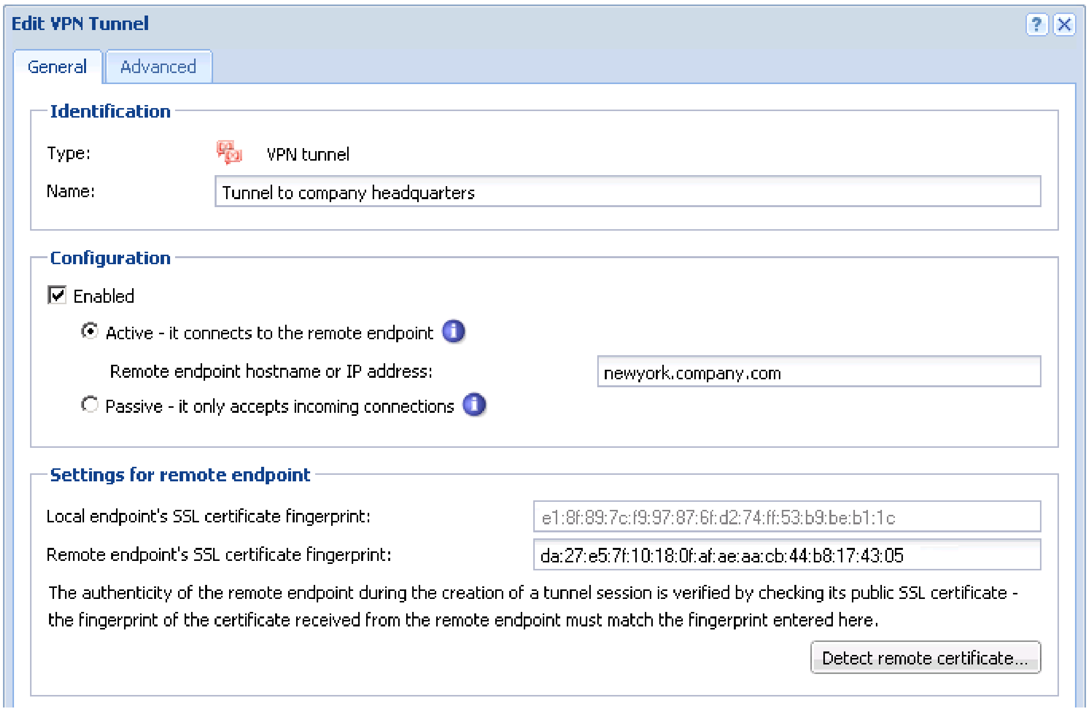
   Note: The *VPN network* and *Mask* entries now include an automatically selected free subnet.

   For a detailed description on the VPN server configuration, refer to chapter 24.1.

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (`newyork.company.com`). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.

   At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the *Connected* status will be reported in the *Adapter info* column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability of the remote server — in our example, the following command can be used at the branch office server:

   ```
   ping newyork.company.com
   ```



Edit VPN Tunnel

General | Advanced

Identification

Type: VPN tunnel

Name: Tunnel to company headquarters

Configuration

☑ Enabled

● Active - it connects to the remote endpoint

Remote endpoint hostname or IP address: newyork.company.com

○ Passive - it only accepts incoming connections

Settings for remote endpoint

Local endpoint's SSL certificate fingerprint: e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c

Remote endpoint's SSL certificate fingerprint: da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05

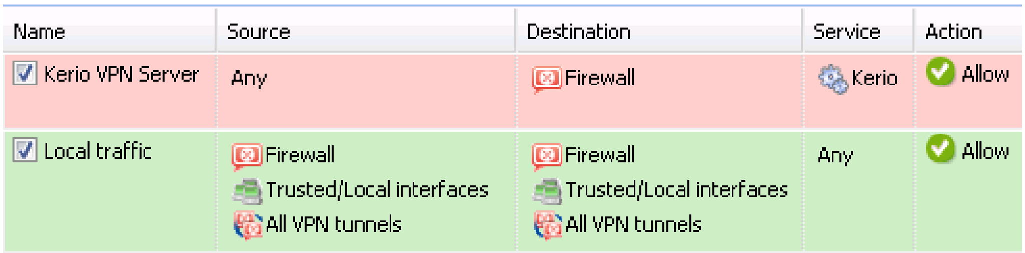
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 24.11 Filial office — definition of VPN tunnel for the headquarters

Note: If a collision of VPN network and the remote network is detected upon creation of the VPN tunnel, select an appropriate free subnet and specify its parameters at the VPN server (see Step 4).

For detailed information on how to create VPN tunnels, see chapter 24.3.

6. The *All VPN Clients* group from the *Local Traffic* rule (no VPN clients will connect to the branch office network).



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces All VPN tunnels	Firewall Trusted/Local interfaces All VPN tunnels	Any	✓ Allow

Figure 24.12 Filial office — final traffic rules

Note: It is not necessary to perform any other customization of traffic rules. The required restrictions should be already set in the traffic policy at the server of the headquarters.

VPN test

Configuration of the VPN tunnel has been completed by now. At this point, it is recommended to test availability of the remote hosts from each end of the tunnel (from both local networks).

For example, the `ping` or/and `tracert` (`traceroute`) operating system commands can be used for this testing. It is recommended to test availability of remote hosts both through IP addresses and DNS names.

If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

If an IP address is tested successfully and an error is reported (*Unknown host*) when a corresponding DNS name is tested, then check configuration of the DNS.

24.6 Example of a more complex Kerio VPN configuration

In this chapter, an example of a more complex VPN configuration is provided where redundant routes arise between interconnected private networks (i.e. multiple routes exist between two networks that can be used for transfer of packets).

The only difference of *Kerio VPN* configuration between this type and VPN with no redundant routes (see chapter 24.5) is setting of routing between endpoints of individual tunnels. In such a case, it is necessary to set routing between individual endpoints of VPN tunnels by hand. Automatic route exchange is inconvenient since *Kerio VPN* uses no routing protocol and the route exchange is based on comparison of routing tables at individual endpoints of the VPN tunnel (see also chapter 24.4). If the automatic exchange is applied, the routing will not be ideal!

For better reference, the configuration is here described by an example of a company with a headquarters and two filial offices with their local private network interconnected by VPN tunnels (so called triangle pattern). This example can be then adapted and applied to any number of interconnected private networks.

The example focuses configuration of VPN tunnels and correct setting of routing between individual private networks (it does not include access restrictions). Access restrictions options within VPN are described by the example in chapter 24.5.

Specification

The network follows the pattern shown in figure 24.13.

The server (default gateway) uses the fixed IP address `85.17.210.230` (DNS name is `gw-newyork.company.com`). The server of one filial uses the IP address `195.39.22.12` (DNS name `gw-london.company.com`), the other filial's server uses a dynamic IP address assigned by the ISP.

The headquarters uses the DNS domain `company.com`, filials use subdomains `santaclara.company.com` and `newyork.company.com`. Configuration of individual local networks and the IP addresses used are shown in the figure.

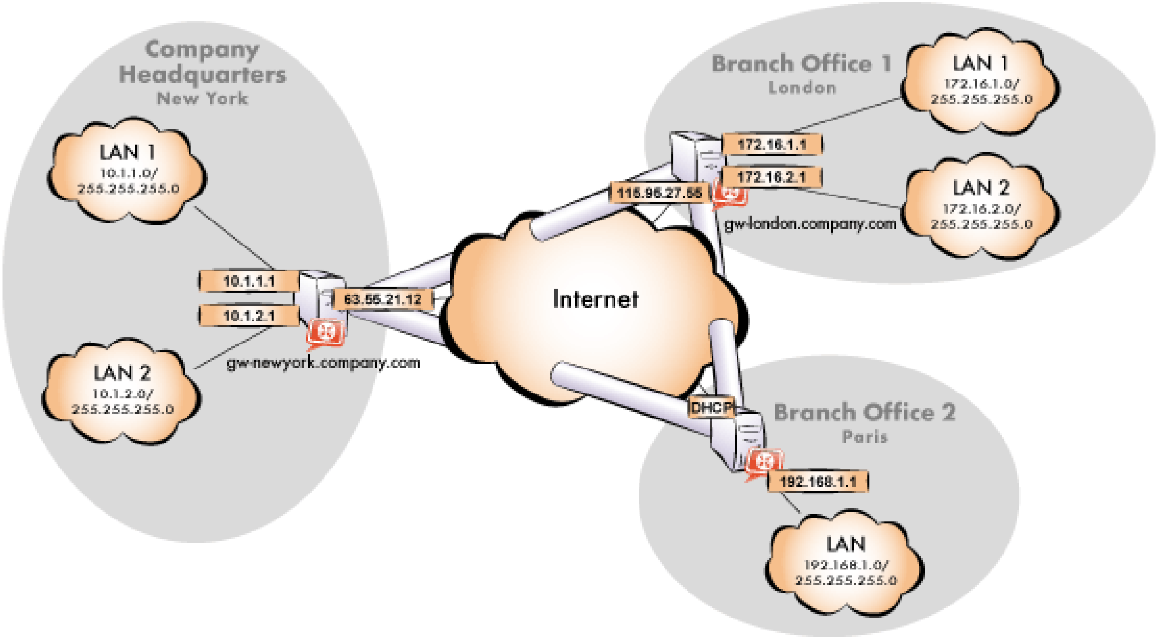


Figure 24.13 Example of a VPN configuration — a company with two filials

Common method

The following actions must be taken in all local networks (i.e. in the main office and both filials):

1. *Kerio Control* must be installed on the default gateway of the network.

   Note: For *every* installation of *Kerio Control*, a stand-alone license for the corresponding number of users is required! For details see chapter 5.

2. Configure and test connection of the local network to the Internet. Hosts in the local network must use the *Kerio Control* host's IP address as the default gateway and as the primary DNS server.

   If it is a new (clean) *Kerio Control* installation, it is possible to use the connectivity wizard (refer to chapter 7.1) and the traffic policy wizard (see chapter 8.1).

   For detailed description of basic configuration of *Kerio Control* and of the local network, refer to the *Kerio Control — Step By Step* document.

3. In configuration of the *DNS* module, set DNS forwarding rules for domains of the other filials. This enables to access hosts in the remote networks by using their DNS names (otherwise, it is necessary to specify remote hosts by IP addresses).

For proper functionality of the DNS, at least one DNS server must be specified to which DNS queries for other domains (typically the DNS server of the ISP).

Note: The DNS database must include records of hosts in the correcponding local network. To achieve this, save DNS names and IP addresses of local hosts into the hostname table (if they use IP addresses) nad/or enable cooperation of the *DNS* module with the DHCP server (in case that IP addresses are assigned dynamically to these hosts). For details, see chapter 10.1.

4. In the *Interfaces* section, allow the VPN server and set its SSL certificate if necessary. Note the fingerprint of the server's certificate for later use (it will be required for configuration of the VPN tunnels in the other filials).

   Check whether the automatically selected VPN subnet does not collide with any local subnet in any filial and select another free subnet if necessary.

   Note: With respect to the complexity of this VPN configuration, it is recommended to reserve three free subnets in advance that can later be assigned to individual VPN servers.

5. Define the VPN tunnel to one of the remote networks. The passive endpoint of the tunnel must be created at a server with fixed public IP address. Only active endpoints of VPN tunnels can be created at servers with dynamic IP address.

   Set routing (define custom routes) for the tunnel. Select the *Use custom routes only* option and specify all subnets of the remote network in the custom routes list.

   If the remote endpoint of the tunnel has already been defined, check whether the tunnel was created. If not, refer to the *Error* log, check fingerprints of the certificates and also availability of the remote server.

6. Follow the same method to define a tunnel and set routing to the other remote network.

7. Allow traffic between the local and the remote networks. To allow any traffic, just add the created VPN tunnels to the *Source* and *Destination* items in the *Local traffic* rule. Access restrictions options within VPN are described by the example in chapter 24.5.

8. Test reachability of remote hosts in both remote networks. To perform the test, use the `ping` and `tracert` (`traceroute`) system commands. Test availability of remote hosts both through IP addresses and DNS names.

   If a remote host is tested through IP address and it does not respond, check configuration of the traffic rules or/and find out whether the subnets do not collide (i.e. whether the same subnet is not used at both ends of the tunnel).

   If an IP address is tested successfully and an error is reported (*Unknown host*) when a corresponding DNS name is tested, then check configuration of the DNS.

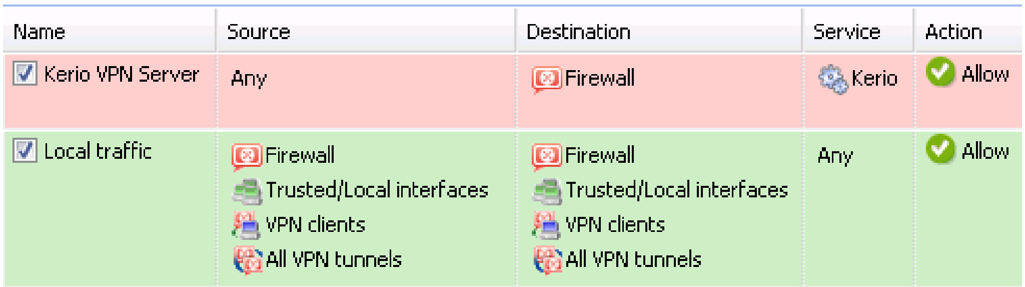
The following sections provide detailed description of the *Kerio VPN* configuration both for the headquarter and the filial offices.

Headquarters configuration

1. *Kerio Control* must be installed on the default gateway of the headquarter's network.
2. In *Kerio Control* set basic traffic rules by using the connectivity wizard (refer to chapter 7.1) and the traffic policy wizard (see chapter 8.1).

   In the traffic policy wizard, allow access to the *Kerio VPN server* service.

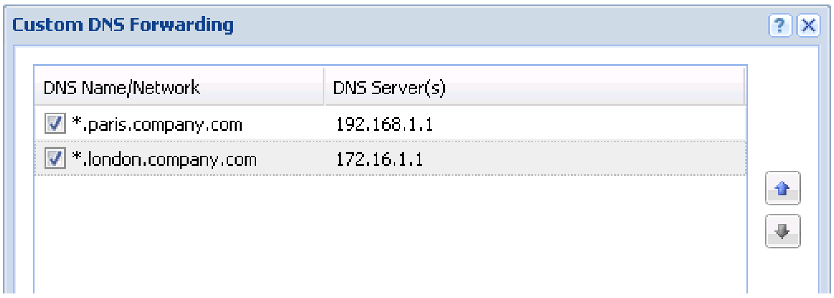
   This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	✓ Allow

Figure 24.14 Headquarter — default traffic rules for Kerio VPN

3. Customize DNS configuration as follows:
   - In the *Kerio Control's DNS* module configuration, enable *DNS forwarder* (forwarding of DNS requests to other servers).
   - Enable the *Use custom forwarding* option and define rules for names in the `filial1.company.com` and `filial2.company.com` domains. To specify the forwarding DNS server, always use the IP address of the *Kerio Control* host's inbound interface connected to the local network at the remote side of the tunnel.



Custom DNS Forwarding

DNS Name/Network	DNS Server(s)
☑ *.paris.company.com	192.168.1.1
☑ *.london.company.com	172.16.1.1

Figure 24.15 Headquarter — DNS forwarding settings

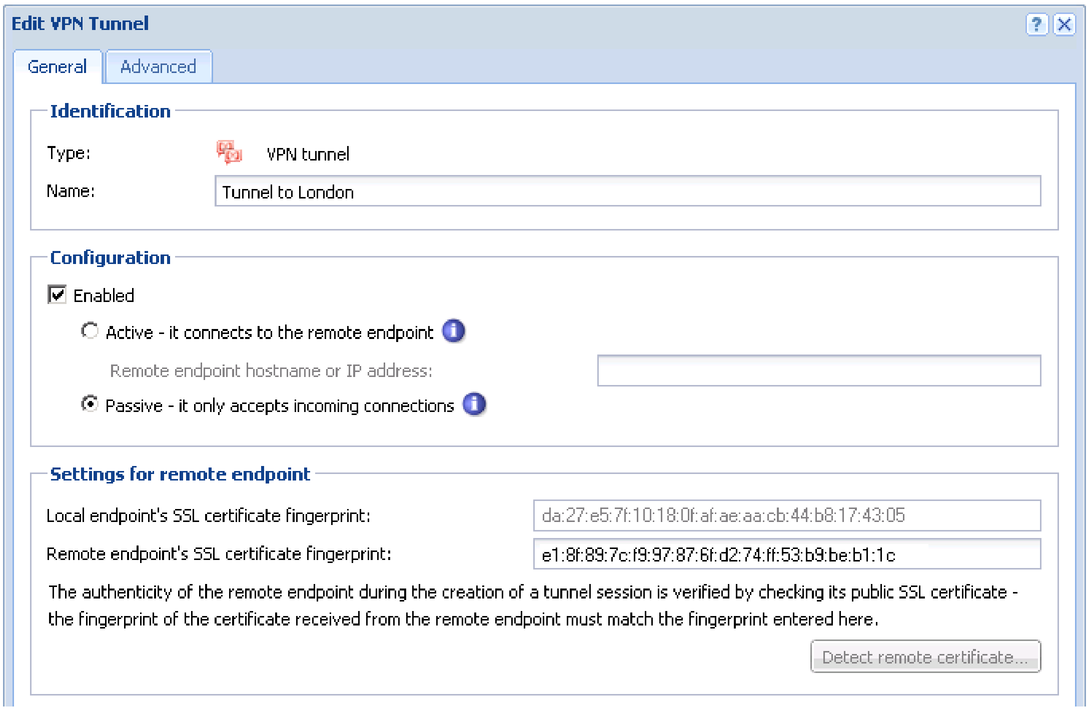
- No DNS server will be set on interfaces of the *Kerio Control* host connected to the local networks *LAN 1* and *LAN 2*.
- On other computers set an IP address as the primary DNS server. This address must match the corresponding default gateway (`10.1.1.1` or `10.1.2.1`). Hosts in the local network can be configured automatically by DHCP protocol.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: The *VPN network* and *Mask* entries now include an automatically selected free subnet. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

   For a detailed description on the VPN server configuration, refer to chapter 24.1.

5. Create a passive endpoint of the VPN tunnel connected to the *London* filial. Use the fingerprint of the VPN server of the *London* filial office as a specification of the fingerprint of the remote SSL certificate.



Edit VPN Tunnel

General | Advanced

Identification

Type: VPN tunnel

Name: Tunnel to London

Configuration

☑ Enabled

○ Active - it connects to the remote endpoint

Remote endpoint hostname or IP address:

● Passive - it only accepts incoming connections

Settings for remote endpoint

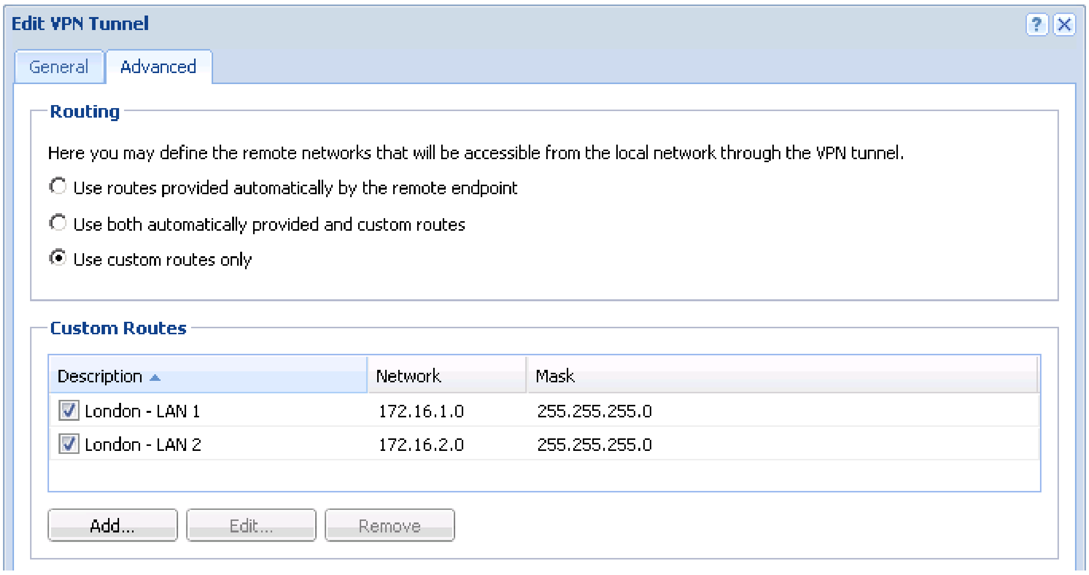
Local endpoint's SSL certificate fingerprint: da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05

Remote endpoint's SSL certificate fingerprint: e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 24.16 Headquarter — definition of VPN tunnel for the London filial

On the *Advanced* tab, select the *Use custom routes only* option and set routes to the subnets at the remote endpoint of the tunnel (i.e. in the *London* filial).



Routing

Here you may define the remote networks that will be accessible from the local network through the VPN tunnel.

○ Use routes provided automatically by the remote endpoint

○ Use both automatically provided and custom routes

● Use custom routes only

Custom Routes

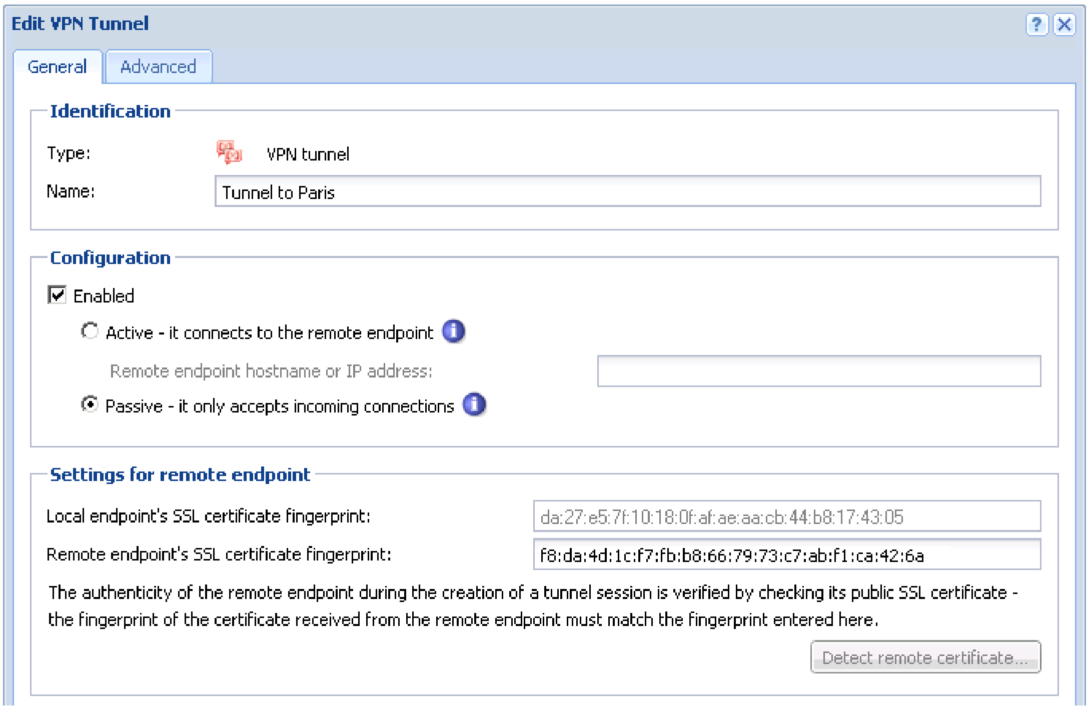
Description ▲	Network	Mask
☑ London - LAN 1	172.16.1.0	255.255.255.0
☑ London - LAN 2	172.16.2.0	255.255.255.0

Figure 24.17 The headquarters — routing configuration for the tunnel connected to the London filial

Warning:
In case that the VPN configuration described here is applied (see figure 24.13), it is *unrecommended* to use automatically provided routes! In case of an automatic exchange of routes, the routing within the VPN is not be ideal (for example, any traffic between the *headquarters* and the *Paris* filial office is routed via the *London* filial whereas the tunnel between the *headquarters* and the *Paris* office stays waste.

6. Use the same method to create a passive endpoint for the tunnel connected to the *Paris* filial.

   On the *Advanced* tab, select the *Use custom routes only* option and set routes to the subnets at the remote endpoint of the tunnel (i.e. in the *Paris* filial).



Edit VPN Tunnel

General | Advanced

Identification

Type: VPN tunnel

Name: Tunnel to Paris

Configuration

☑ Enabled

○ Active - it connects to the remote endpoint

Remote endpoint hostname or IP address:

● Passive - it only accepts incoming connections

Settings for remote endpoint

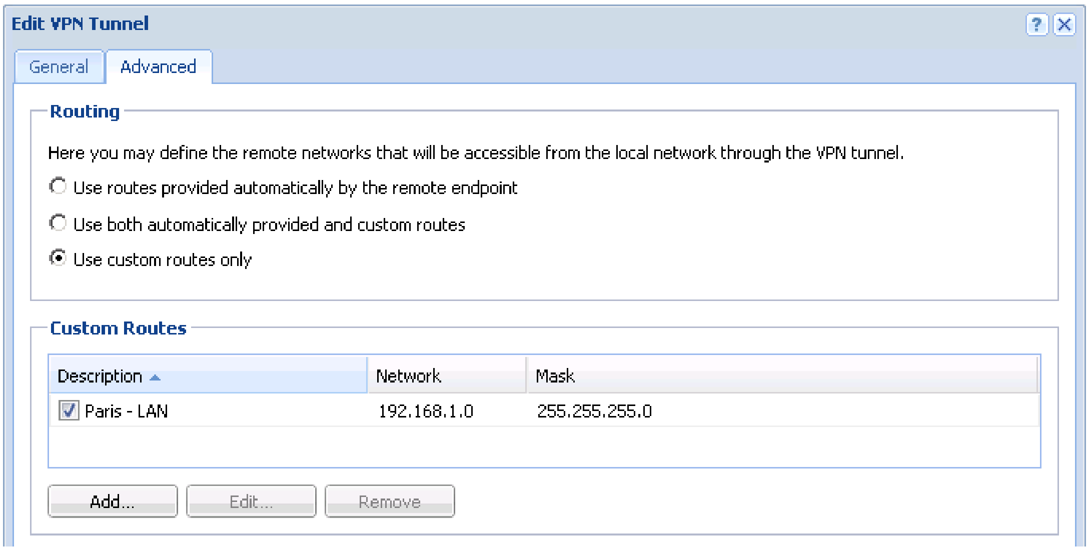
Local endpoint's SSL certificate fingerprint: da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05

Remote endpoint's SSL certificate fingerprint: f8:da:4d:1c:f7:fb:b8:66:79:73:c7:ab:f1:ca:42:6a

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Detect remote certificate...

Figure 24.18 The headquarters — definition of VPN tunnel for the Paris filial



Edit VPN Tunnel

General | Advanced

Routing

Here you may define the remote networks that will be accessible from the local network through the VPN tunnel.

○ Use routes provided automatically by the remote endpoint

○ Use both automatically provided and custom routes

● Use custom routes only

Custom Routes

Description	Network	Mask
☑ Paris - LAN	192.168.1.0	255.255.255.0

Add... | Edit... | Remove

Figure 24.19 The headquarters — routing configuration for the tunnel connected to the Paris filial

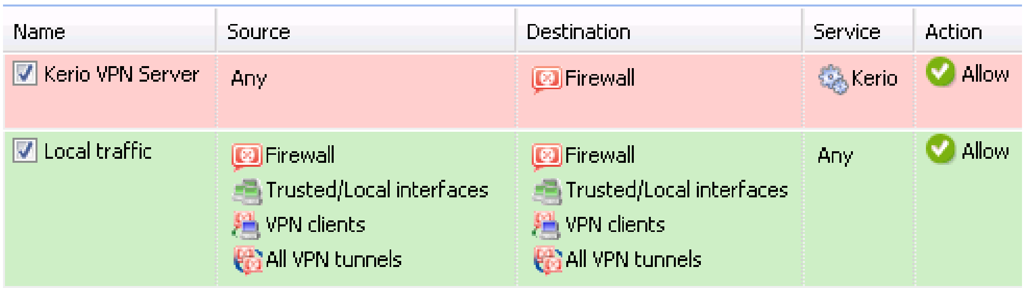
Configuration of the London filial

1. *Kerio Control* must be installed on the default gateway of the filial's network.

2. In *Kerio Control* set basic traffic rules by using the connectivity wizard (refer to chapter 7.1) and the traffic policy wizard (see chapter 8.1).

   In the traffic policy wizard, allow access to the *Kerio VPN server* service.

This step will create rules for connection of the VPN server as well as for communication of VPN clients with the local network (through the firewall).

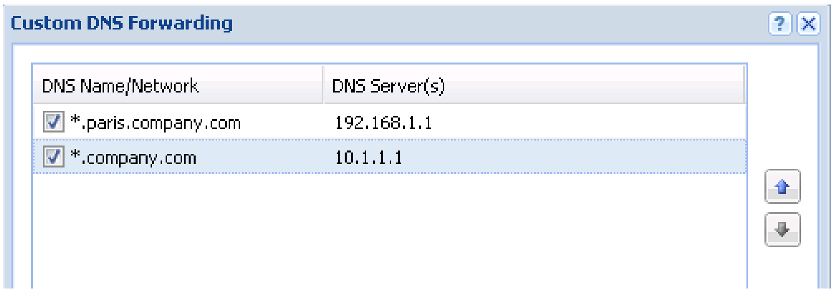


Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Firewall Trusted/Local interfaces VPN clients All VPN tunnels	Any	✓ Allow

Figure 24.20 The London filial office — default traffic rules for Kerio VPN

3. Customize DNS configuration as follows:

   - In the *Kerio Control's DNS* module configuration, enable *DNS forwarder* (forwarding of DNS requests to other servers).
   - Enable the *Use custom forwarding* option and define rules for names in the `company.com` and `filial2.company.com` domains. To specify the forwarding DNS server, always use the IP address of the *Kerio Control* host's inbound interface connected to the local network at the remote side.



Custom DNS Forwarding

DNS Name/Network	DNS Server(s)
☑ *.paris.company.com	192.168.1.1
☑ *.company.com	10.1.1.1

Figure 24.21 The London filial office — DNS forwarding settings

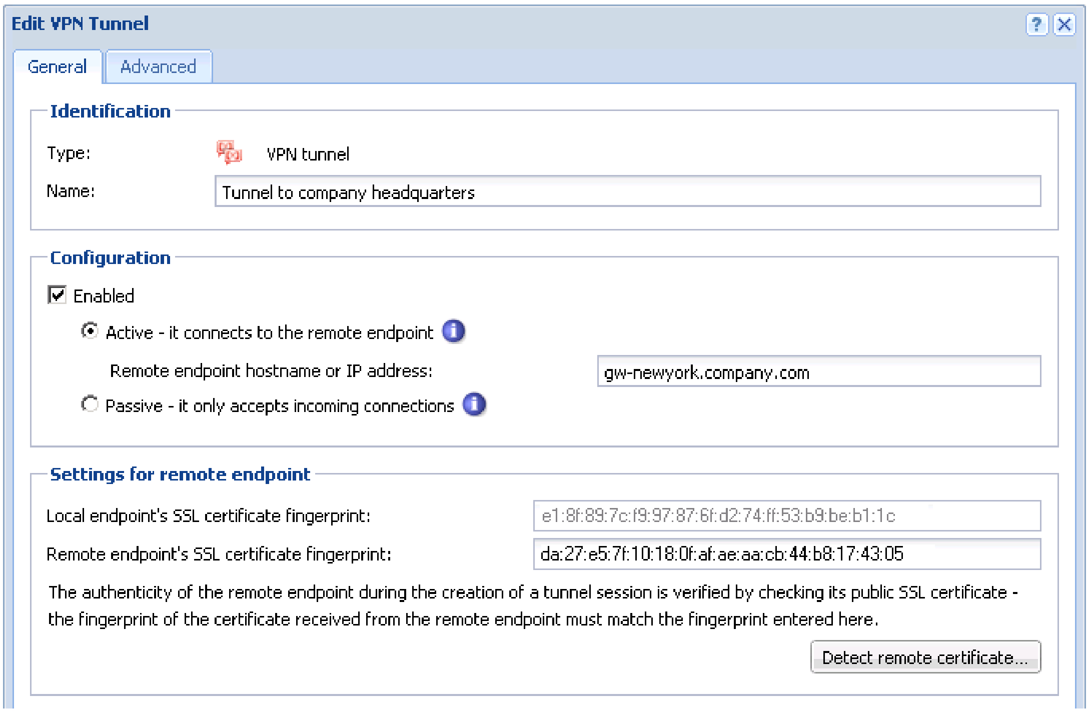
   - No DNS server will be set on interfaces of the *Kerio Control* host connected to the local networks *LAN 1* and *LAN 2*.
   - On other computers set an IP address as the primary DNS server. This address must match the corresponding default gateway (`172.16.1.1` or `172.16.2.1`). Hosts in the local network can be configured automatically by DHCP protocol.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: The *VPN network* and *Mask* entries now include an automatically selected free subnet. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

   For a detailed description on the VPN server configuration, refer to chapter 24.1.

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (`newyork.company.com`). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.



Identification

Type: VPN tunnel

Name: Tunnel to company headquarters

Configuration

☑ Enabled

● Active - it connects to the remote endpoint

Remote endpoint hostname or IP address: gw-newyork.company.com

○ Passive - it only accepts incoming connections

Settings for remote endpoint

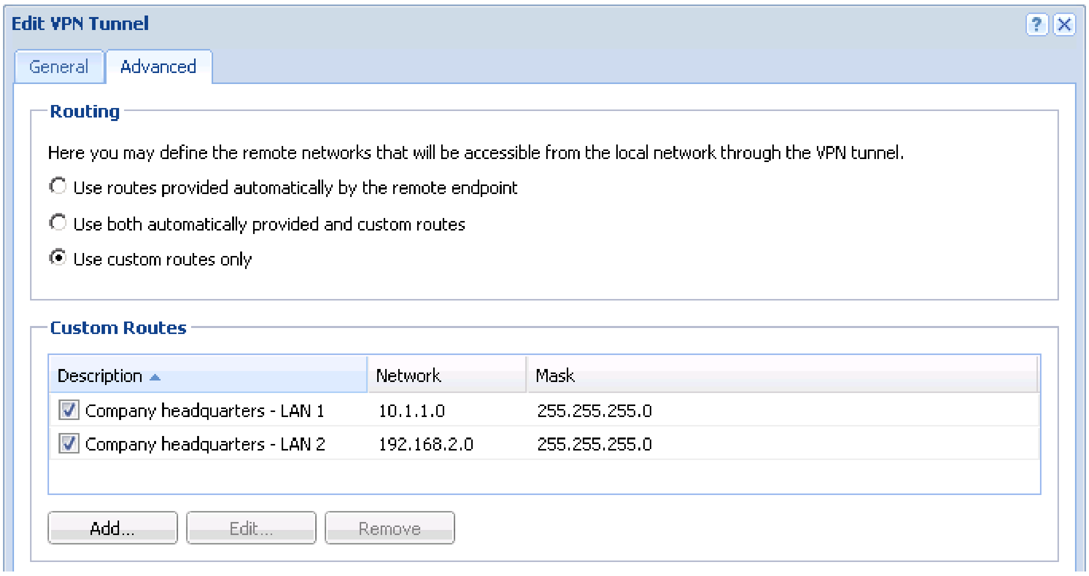
Local endpoint's SSL certificate fingerprint: e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c

Remote endpoint's SSL certificate fingerprint: da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 24.22 The London filial office — definition of VPN tunnel for the headquarters

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *headquarters'* local networks.



Routing

Here you may define the remote networks that will be accessible from the local network through the VPN tunnel.

○ Use routes provided automatically by the remote endpoint

○ Use both automatically provided and custom routes

● Use custom routes only

Custom Routes

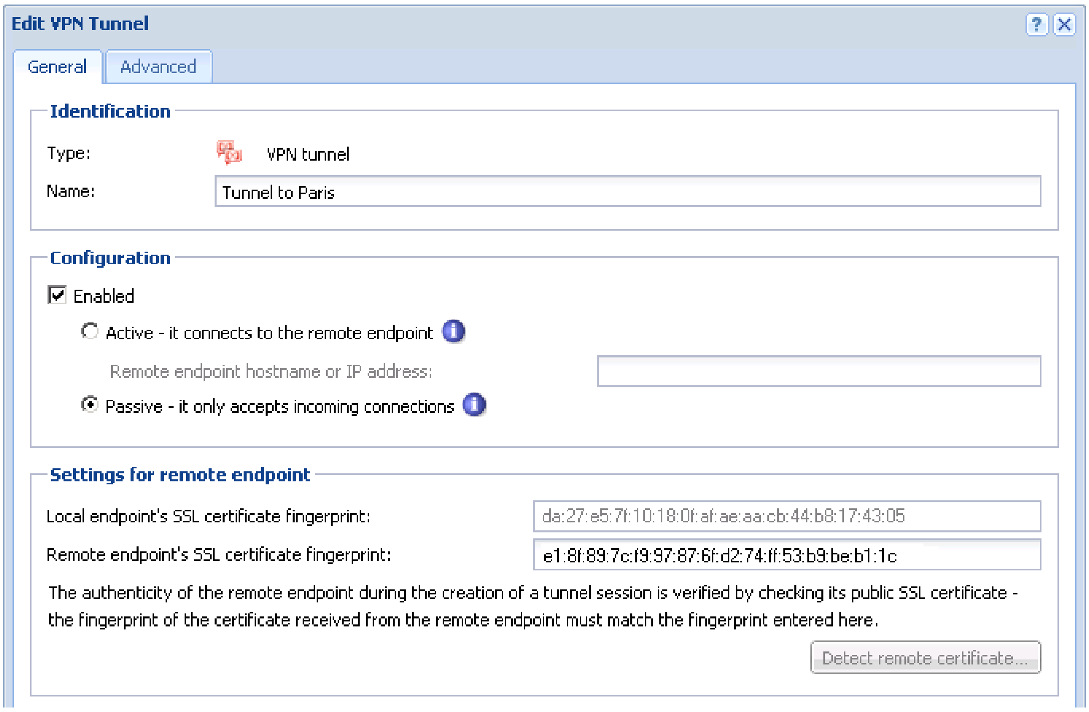
Description	Network	Mask
☑ Company headquarters - LAN 1	10.1.1.0	255.255.255.0
☑ Company headquarters - LAN 2	192.168.2.0	255.255.255.0

Figure 24.23 The London filial — routing configuration for the tunnel connected to the headquarters

At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the *Connected* status will be reported in the *Adapter info* column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability of the remote server — in our example, the following command can be used at the London branch office server:

```
ping gw-newyork.company.com
```

6. Create a passive endpoint of the VPN tunnel connected to the *Paris* filial. Use the fingerprint of the VPN server of the *Paris* filial office as a specification of the fingerprint of the remote SSL certificate.



Edit VPN Tunnel

Identification

Type: VPN tunnel

Name: Tunnel to Paris

Configuration

☑ Enabled

○ Active - it connects to the remote endpoint

Remote endpoint hostname or IP address:

● Passive - it only accepts incoming connections

Settings for remote endpoint

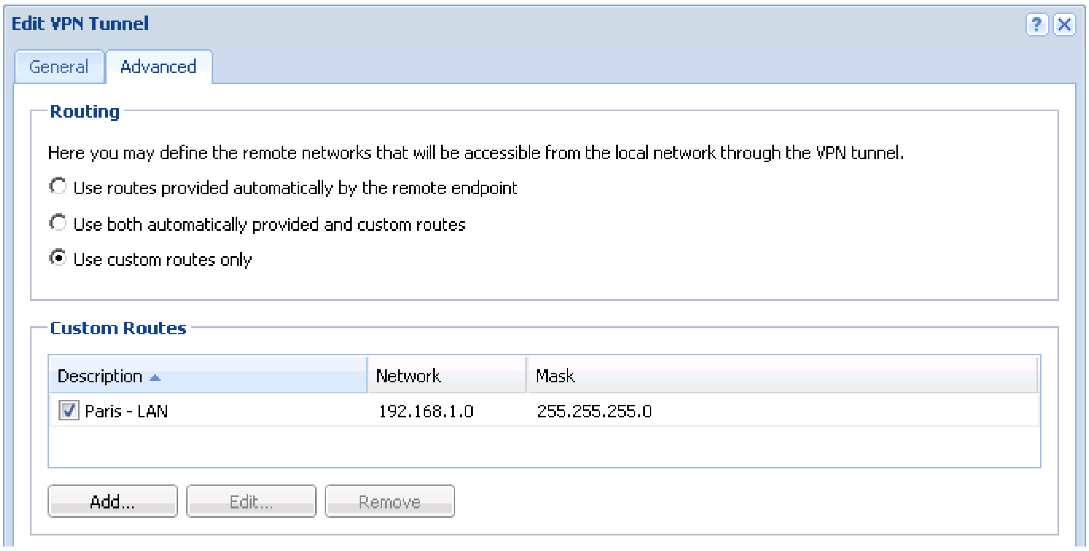
Local endpoint's SSL certificate fingerprint: da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05

Remote endpoint's SSL certificate fingerprint: e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 24.24 The London filial office — definition of VPN tunnel for the Paris filial office

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *Paris'* local networks.



Edit VPN Tunnel

Routing

Here you may define the remote networks that will be accessible from the local network through the VPN tunnel.

○ Use routes provided automatically by the remote endpoint

○ Use both automatically provided and custom routes

● Use custom routes only

Custom Routes

Description ▲	Network	Mask
☑ Paris - LAN	192.168.1.0	255.255.255.0

Figure 24.25 The London filial — routing configuration for the tunnel connected to the Paris branch office

Configuration of the Paris filial

1. *Kerio Control* must be installed on the default gateway of the filial's network.

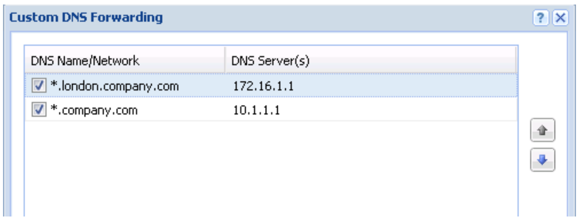
2. In *Kerio Control* set basic traffic rules by using the connectivity wizard (refer to chapter 7.1) and the traffic policy wizard (see chapter 8.1).

   In this case there is no reason to enable the *Kerio VPN server* service (the server uses dynamic public IP address).

3. Customize DNS configuration as follows:

   - In the *Kerio Control's DNS* module configuration, enable *DNS forwarder* (forwarding of DNS requests to other servers).

     - Enable the *Use custom forwarding* option and define rules for names in the `company.com` and `filial1.company.com` domains. Specify the server for DNS forwarding by the IP address of the internal interface of the *Kerio Control* host (i.e. interface connected to the local network at the other end of the tunnel).



Custom DNS Forwarding

DNS Name/Network	DNS Server(s)
☑ *.london.company.com	172.16.1.1
☑ *.company.com	10.1.1.1

Figure 24.26 The Paris filial office — DNS forwarding settings

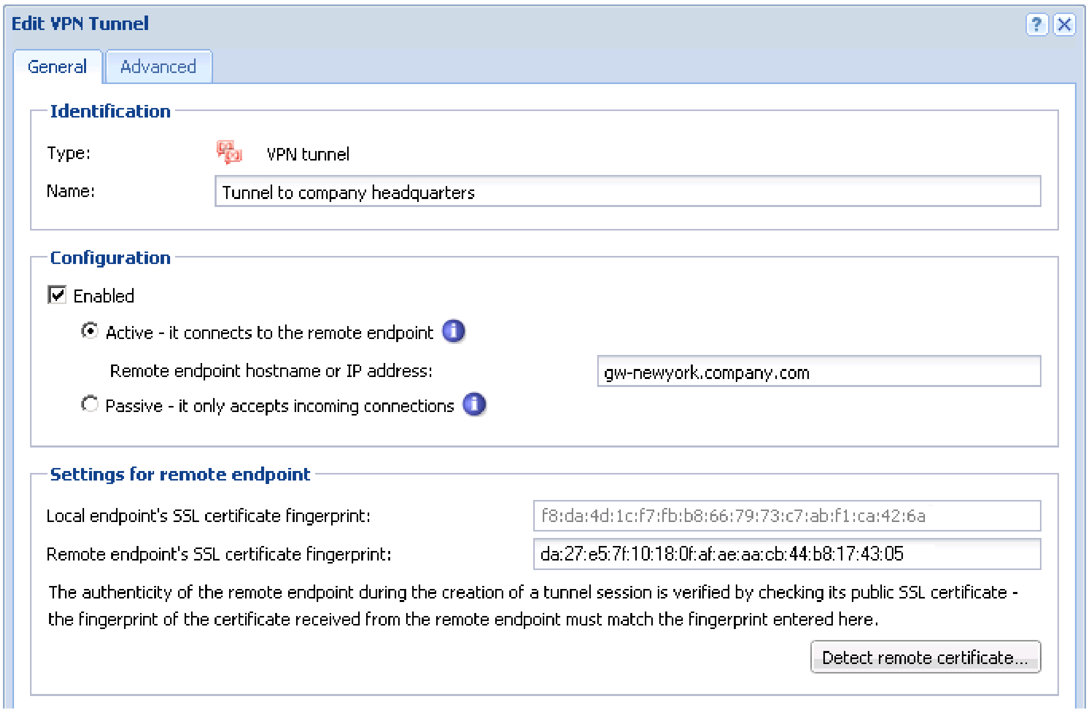
- No DNS server will be set on the interface of the *Kerio Control* host connected to the local network *LAN*.
- Set the IP address `192.168.1.1` as a primary DNS server also for the other hosts.

4. Enable the VPN server and configure its SSL certificate (create a self-signed certificate if no certificate provided by a certification authority is available).

   Note: The *VPN network* and *Mask* entries now include an automatically selected free subnet. Check whether this subnet does not collide with any other subnet in the headquarters or in the filials. If it does, specify a free subnet.

   For a detailed description on the VPN server configuration, refer to chapter 24.1.

5. Create an active endpoint of the VPN tunnel which will connect to the headquarters server (`newyork.company.com`). Use the fingerprint of the VPN server of the headquarters as a specification of the fingerprint of the remote SSL certificate.



Identification

Type: VPN tunnel

Name: Tunnel to company headquarters

Configuration

☑ Enabled

● Active - it connects to the remote endpoint

Remote endpoint hostname or IP address: gw-newyork.company.com

○ Passive - it only accepts incoming connections

Settings for remote endpoint

Local endpoint's SSL certificate fingerprint: f8:da:4d:1c:f7:fb:b8:66:79:73:c7:ab:f1:ca:42:6a

Remote endpoint's SSL certificate fingerprint: da:27:e5:7f:10:18:0f:af:ae:aa:cb:44:b8:17:43:05

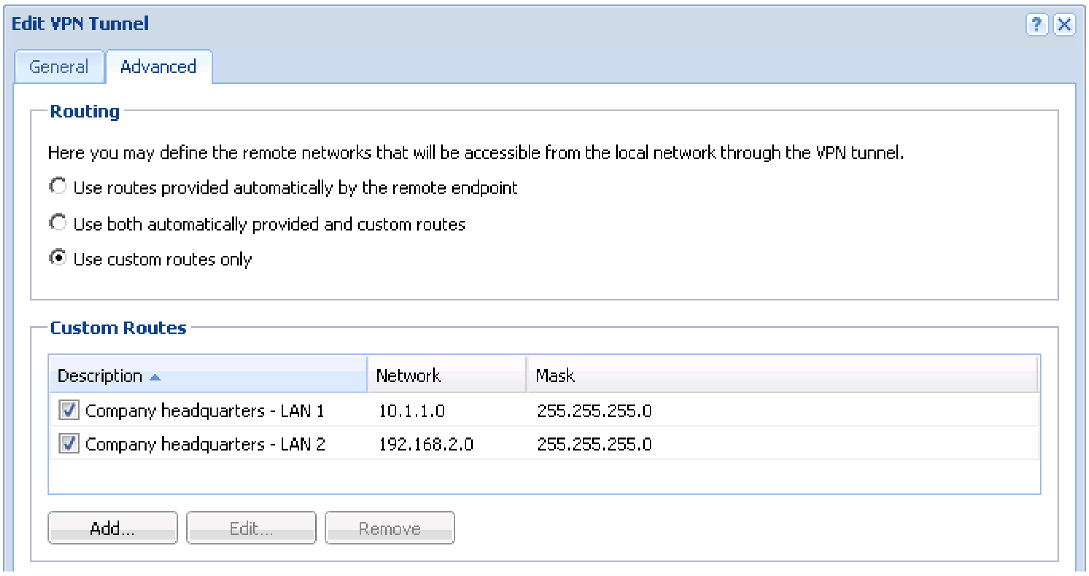
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 24.27 The Paris filial office — definition of VPN tunnel for the headquarters

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *headquarters'* local networks.

At this point, connection should be established (i.e. the tunnel should be created). If connected successfully, the *Connected* status will be reported in the *Adapter info* column for both ends of the tunnel. If the connection cannot be established, we recommend you to check the configuration of the traffic rules and test availability of the remote server — in our example, the following command can be used at the Paris branch office server:

```
ping gw-newyork.company.com
```



Routing

Here you may define the remote networks that will be accessible from the local network through the VPN tunnel.

○ Use routes provided automatically by the remote endpoint

○ Use both automatically provided and custom routes

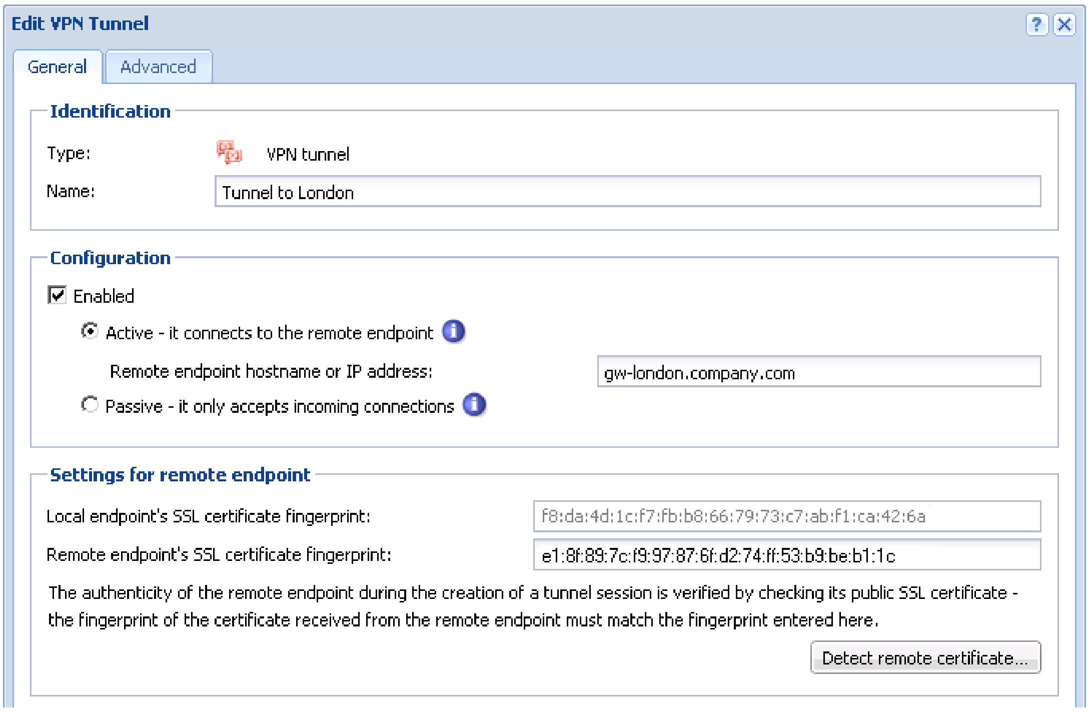
● Use custom routes only

Custom Routes

Description ▲	Network	Mask
☑ Company headquarters - LAN 1	10.1.1.0	255.255.255.0
☑ Company headquarters - LAN 2	192.168.2.0	255.255.255.0

Figure 24.28 The Paris filial — routing configuration for the tunnel connected to the headquarters

6. Create an active endpoint of the tunnel connected to *London* (server `gw-london.company.com`). Use the fingerprint of the VPN server of the *London* filial office as a specification of the fingerprint of the remote SSL certificate.



Identification

Type: VPN tunnel

Name: Tunnel to London

Configuration

☑ Enabled

● Active - it connects to the remote endpoint

Remote endpoint hostname or IP address: gw-london.company.com

○ Passive - it only accepts incoming connections

Settings for remote endpoint

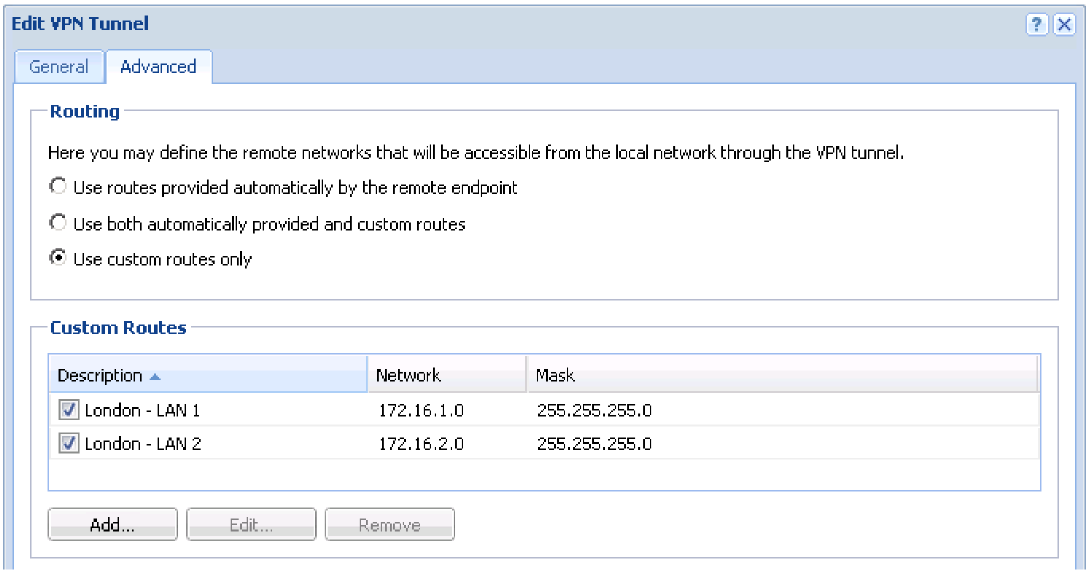
Local endpoint's SSL certificate fingerprint: f8:da:4d:1c:f7:fb:b8:66:79:73:c7:ab:f1:ca:42:6a

Remote endpoint's SSL certificate fingerprint: e1:8f:89:7c:f9:97:87:6f:d2:74:ff:53:b9:be:b1:1c

The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Figure 24.29 The Paris filial office — definition of VPN tunnel for the London filial office

On the *Advanced* tab, select the *Use custom routes only* option and set routes to *London's* local networks.



Edit VPN Tunnel

Routing

Here you may define the remote networks that will be accessible from the local network through the VPN tunnel.

○ Use routes provided automatically by the remote endpoint

○ Use both automatically provided and custom routes

● Use custom routes only

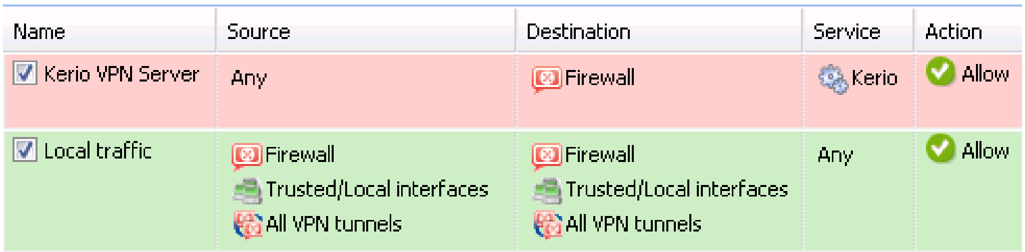
Custom Routes

Description ▲	Network	Mask
☑ London - LAN 1	172.16.1.0	255.255.255.0
☑ London - LAN 2	172.16.2.0	255.255.255.0

Figure 24.30 The Paris filial — routing configuration for the tunnel connected to the London branch office

Like in the previous step, check whether the tunnel has been established successfully, and check reachability of remote private networks (i.e. of local networks in the *London* filial).

7. The *All VPN Clients* group from the *Local Traffic* rule (no VPN clients will connect to this branch office network).



Name	Source	Destination	Service	Action
☑ Kerio VPN Server	Any	Firewall	Kerio	✓ Allow
☑ Local traffic	Firewall Trusted/Local interfaces All VPN tunnels	Firewall Trusted/Local interfaces All VPN tunnels	Any	✓ Allow

Figure 24.31 The Paris filial office — final traffic rules

VPN test

The VPN configuration has been completed by now. At this point, it is recommended to test reachability of the remote hosts in the other remote networks (at remote endpoints of individual tunnels).

For example, the `ping` or/and `tracert` (`traceroute`) operating system commands can be used for this testing.

Chapter 25

Kerio Clientless SSL-VPN (Windows)

Kerio Clientless SSL-VPN (thereinafter “*SSL-VPN*”) is a special interface used for secured remote access to shared items (files and folders) in the network protected by *Kerio Control* via a web browser. This interface is available only in *Kerio Control* on *Windows*.

To a certain extent, the *SSL-VPN* interface is an alternative to *Kerio VPN Client* (see chapter 24). Its main benefit is that it enables an immediate access to a remote network from any location without any special application having been installed and any configuration having been performed (that’s the reason for calling it *clientless*). The main disadvantage of this alternative is that network connections are not transparent. *SSL-VPN* is, in a manner, an alternative to the *My Network Places* system tool) — it does not enable access to web servers or other services in a—remote network.

SSL-VPN is suitable for an immediate access to shared files in remote networks in such environments where it is not possible or useful to use *Kerio VPN Client*.

This chapter addresses configuration details needed for proper functionality of the *SSL-VPN* interface. The *SSL-VPN* interface is described thoroughly in the *Kerio Control — User’s Guide*.

25.1 Kerio Control SSL-VPN configuration

SSL-VPN interface requirements

For proper functionality of the *SSL-VPN* interface, the following conditions must be met:

1. The *Kerio Control* host must be a member of the corresponding domain (*Windows NT* or *Active Directory* domain).

2. User accounts that will be used for connections to *SSL-VPN* must be authenticated at the domain (it is not possible to use local authentication). This implies that the *SSL-VPN* interface cannot be used for accessing shared items in multiple domains or to items at hosts which are not members of any domain.

3. Users who are supposed to be allowed to access the *SSL-VPN* interface needs the right to use *Clientless SSL-VPN* in *Kerio Control* (see chapter 17.2).

4. If *Kerio Control* is installed on the domain server, the corresponding users need to be allowed to log on to the server locally. Local logon can be allowed under *Domain Controller Security Policy*. For details, refer to our Knowledge Base.

SSL-VPN interface configuration

To configure *SSL-VPN*, go to the *SSL-VPN* folder in *Configuration* → *Advanced Settings*.

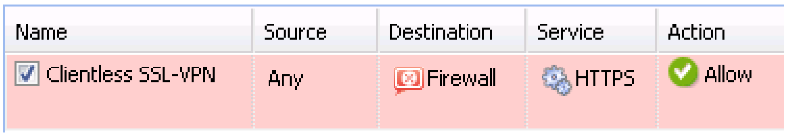
SSL-VPN's default port is port 443 (standard port of the *HTTPS* service).

Click *Change SSL Certificate* to create a new certificate for the *SSL-VPN* service or to import a certificate issued by a trustworthy certification authority. When created, the certificate is saved as `sslvpn.crt` and the corresponding private key as `sslvpn.key`. The process of creating/importing a certificate is identical as the one for *Kerio Control's* interface or the VPN server, addressed in detail in chapter 13.1.

> ***Hint:***
> Certificates for particular server name issued by a trustworthy certification authority can also be used for the Web interface and the VPN server   it is not necessary to use three different certificates.

Allowing access from the Internet

Access to the *SSL-VPN* interface from the Internet must be allowed by defining a traffic rule allowing connection to the firewall's *HTTPS* service. This rule can be generated automatically in case that the *Clientless SSL-VPN* option is enabled in the *Traffic Policy Wizard* (see chapter 8.1) or it can be created manually any time later (see chapter 8.4).



Name	Source	Destination	Service	Action
☑ Clientless SSL-VPN	Any	Firewall	HTTPS	✓ Allow

Figure 25.1 Traffic rule allowing connection to the SSL-VPN interface

Note: If the port for *SSL-VPN* interface is changed, it is also necessary to modify the *Service* item in this rule!

Antivirus control

If at least one antivirus is enabled in *Kerio Control* (see chapter 15), all files transferred by the *SSL-VPN* interface can be scanned for viruses.

In default configuration, only files uploaded to hosts in remote private networks are scanned. For connection speed reasons, files downloaded to local hosts from remote networks are not scanned by antiviruses (files downloaded from private networks are considered as trustworthy). Settings of antivirus check can be changed in antivirus configuration — see chapter 15.5.

25.2 Usage of the SSL-VPN interface

The interface can be accessed from most of common web browsers (see chapter 2.2). Specify URL in the browser in the

`https://server/`

format, where `server` represents the DNS name or IP address of the *Kerio Control* host. If *SSL-VPN* uses another port than the default port for *HTTPS* (`443`), it is necessary to specify the used port in the URL, e.g.

`https://server:12345/`

Upon a connection to the server, the *SSL-VPN* interface's welcome page is displayed localized to the language set in the browser. If the language defined as preferred is not available, the English version will be used.

Chapter 26

Specific settings and troubleshooting

This chapter provides description of advanced features and specific configurations of the firewall. It also includes helpful guidelines for solving of issues which might occur when you use *Kerio Control* in your network.

26.1 Configuration Backup and Transfer

If you need to reinstall the firewall's operating system (e.g. in case of new hardware installation), you can easily back up your *Kerio Control* configuration including local user accounts and possibly also SSL certificates. This backup can be later used for recovery of this configuration in your new installation of *Kerio Control*. This may save significant amount of your time as well as help you avoid solution of problems you have already figured out.

To export or import configuration, login to the administration interface, open the Configuration Assistant and click on the corresponding link.

Configuration export

Configuration is exported to a *.tgz* package (the *tar* archive compressed by *gzip*) which includes all the key *Kerio Control* configuration files. Optionally, it is possible to include the web interface's VPN server's and *SSL-VPN* server's SSL certificates in the package. Exported configuration does not include *Kerio Control* license key.

Configuration import

To import configuration, simply browse for or enter the path to the corresponding file which includes the exported configuration (with the *.tgz* extension).

If network interfaces have been changed since the export took place (e.g. in case of exchange of a defective network adapter) or if the configuration is imported from another computer, *Kerio Control* will attempt to pair the imported network interfaces with the real interfaces on the machine. This pairing can be customized — you can match each network interface from the imported configuration with one interface of the firewall or leave it unpaired.

If network interfaces cannot be simply paired, it is desirable to check and possibly edit interface group settings (see chapter 6) and/or traffic rules (see chapter 8) after completion of the configuration import.

26.2 Configuration files

This chapter provides clear descriptions of *Kerio Control* configuration and status files. This information can be helpful for example when troubleshooting specific issues in cooperation with the *Kerio Technologies* technical support department.

For backup and recovery of your firewall configuration, it is recommended to use configuration export and import tools addressed in chapter 26.1!

Configuration files

All *Kerio Control* configuration data is stored in the following files under the same directory where *Kerio Control* is installed

(the typical path is `C:\Program Files\Kerio\WinRoute Firewall`).

The following files are included:

winroute.cfg
: Chief configuration file

UserDB.cfg
: Information about groups and user accounts.

host.cfg
: Preferences for backs-up of configuration, user accounts data, DHCP server database, etc.

logs.cfg
: Log configurations

Note: The data in these files are saved in XML format so that it can be easily modified by an advanced user or generated automatically using another application.

Files in the following directories are also considered as configuration data:

sslcert
: SSL certificates for all components using SSL for traffic encryption (i.e. the web interface, VPN server and the *Clientless SSL-VPN* interface).

license
: If *Kerio Control* has already been registered, the `license` folder includes a license key file (including registered trial versions). If *Kerio Control* has not been registered yet, the `license` folder is empty.

Status files

In addition, *Kerio Control* generates other files and directories where certain status information is saved:

Files:

dnscache.cfg
: DNS files stored in the *DNS* module's cache (see chapter 10.1).

leases.cfg

IP addresses assigned by the DHCP server.
This file includes all information available in section *Configuration* → *DHCP Server*, the *Leased Addresses* tab (see chapter 10.2).

stats.cfg

Interface statistics (see chapter 21.2) and user statistics (see chapter 21.1) data.

vpnleases.cfg

IP addresses assigned to VPN clients (see chapter 24.2).

Directories:

logs

The `logs` directory stores all *Kerio Control* logs (see chapter 23).

star

The `star` directory includes a complete database for statistics of the *Kerio Control* web interface.

Handling configuration files

We recommend that *Kerio Control Engine* be stopped prior to any manipulation with the configuration files (backups, recoveries, etc.)! Information contained within these files is loaded and saved only upon starting or stopping the engine. All changes to the configuration performed while the *Engine* is running are only stored in memory. All modifications done during *Engine* performance will be overwritten by the configuration in the system memory when the *Engine* is stopped.

26.3 Automatic user authentication using NTLM

Kerio Control supports automatic user authentication by the NTLM method (authentication from web browsers). Users once authenticated for the domain are not asked for username and password.

This chapter provides detailed description on conditions and configuration settings for correct functioning of NTLM.

General conditions

The following conditions are applied to this authentication method:

1. NTLM authentication can be used only in *Kerio Control* on Windows. In editions *Appliance* and *Box*, this authentication method is not supported.

2. *Kerio Control Engine* is running as a service or it is running under a user account with administrator rights to the *Kerio Control* host.

3. The server (i.e. the *Kerio Control* host) belongs to a corresponding *Windows NT* or *Active Directory* (*Windows 2000/2003/2008*) domain.

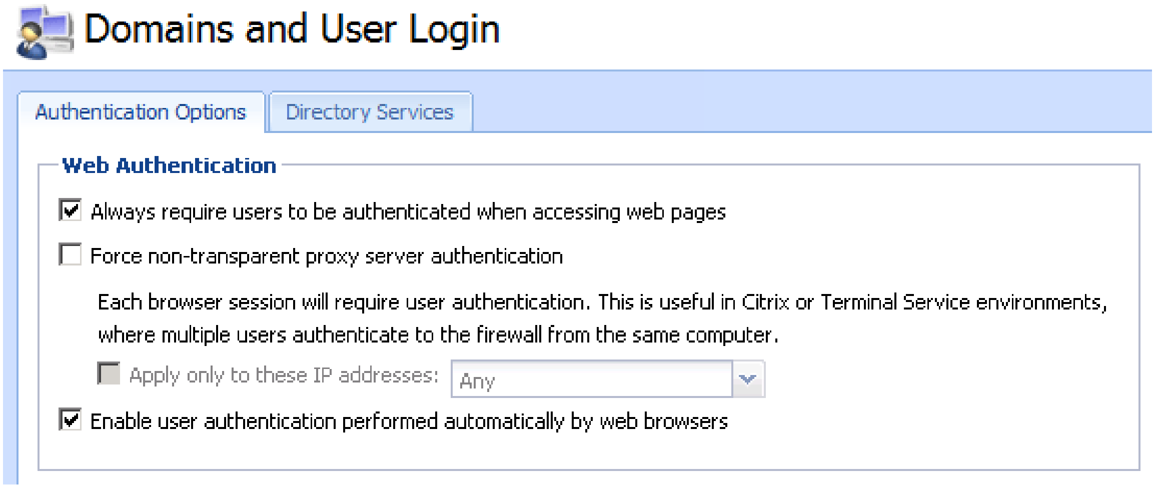
4. Client host belongs to the domain.

5. User at the client host is required to authenticate to this domain (i.e. local user accounts cannot be used for this purpose).

6. The *NT domain* or the *Active Directory* authentication method (see chapter 17.1) must be set for the corresponding user account under *Kerio Control.* NTLM cannot be used for users authenticated only internally inside *Kerio Control.*

Kerio Control configuration

NTLM authentication of users from web browsers must be enabled in *Domains and User Login* → *Authentication Options*. User authentication should be required when attempting to access web pages, otherwise enabling NTLM authentication is meaningless.



Domains and User Login

Web Authentication

☑ Always require users to be authenticated when accessing web pages

☐ Force non-transparent proxy server authentication

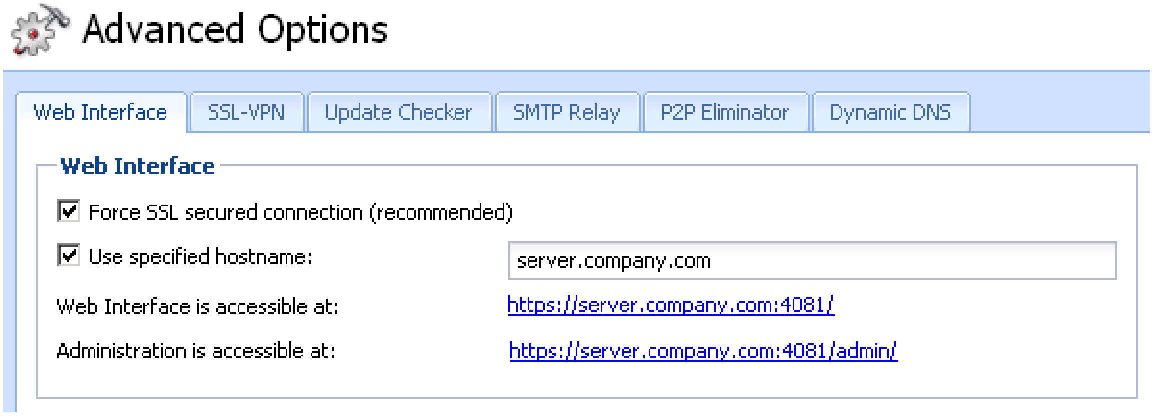
Each browser session will require user authentication. This is useful in Citrix or Terminal Service environments, where multiple users authenticate to the firewall from the same computer.

☐ Apply only to these IP addresses: Any

☑ Enable user authentication performed automatically by web browsers

Figure 26.1 NTLM — user authentication options

The configuration of the *Kerio Control's* web interface must include a valid DNS name of the server on which *Kerio Control* is running (for details, see chapter 13.1).



Web Interface

☑ Force SSL secured connection (recommended)

☑ Use specified hostname: server.company.com

Web Interface is accessible at: https://server.company.com:4081/

Administration is accessible at: https://server.company.com:4081/admin/

Figure 26.2 Kerio Control's Web interface configuration

Note: In editions *Appliance* and *Box*, the server name is set on the *System Configuration* tab (see chapter 18.1).

Web browsers

For proper functioning of NTLM, a browser must be used that supports this method. By now, the following browsers are suitable:

- *Internet Explorer*
- *Firefox or SeaMonkey*

In both cases, *Kerio Control* needs to be added to the list of trusted servers. The NTLM authentication will not be performed on non-trusted servers.

Internet Explorer browser setup

- In the main menu, choose *Tools* → *Internet options*.
- In the *Advanced* tab, the *Security* section, check *Allow Integrated Windows Authentication*. A restart of the browser will be required.
- In the *Security* tab, choose the *Local intranet* zone, press the *Sites* button and the *Advanced* button in the appearing dialog window.
- Add *Kerio Control's* Internet hostname to the list of trusted servers — e.g. `gw.example.com`. For higher security, you can allow secure authentication only — in such a case, enter the server in the form of `https://gw.company.com`. It is not possible to use an IP address instead of server name.

Firefox / SeaMonkey browser setup

- Enter `about:config` into the browser's location bar.
- Use the filter to locate the `network.automatic-ntlm-auth.trusted-uris` configuration option.
- Add *Kerio Control's* Internet hostname to the list of trusted servers — e.g. `gw.example.com`. For higher security, you can allow secure authentication only

— in such a case, enter the server in the form of `https://gw.company.com`. It is not possible to use an IP address instead of server name.

NTLM authentication process

NTLM authentication process differs depending on a browser used.

Internet Explorer

NTLM authentication is performed without user's interaction.

The login dialog is displayed only if NTLM authentication fails (e.g. when user account for user authenticated at the client host does not exist in *Kerio Control*).

> ***Warning:***
> One reason of a NTLM authentication failure can be invalid login username or password saved in the *Password Manager* in *Windows* operating systems (*Control Panels* → *User Accounts* → *Advanced* → *Password Manager*) applying to the corresponding server (i.e. the *Kerio Control* host). In such a case, *Internet Explorer* sends saved login data instead of NTLM authentication of the user currently logged in. Should any problems regarding NTLM authentication arise, it is recommended to remove all usernames/passwords for the server where *Kerio Control* is installed from the *Password Manager*.

Firefox/SeaMonkey

The browser displays the login dialog. For security reasons, automatic user authentication is not used by default in the browser. This behavior of the browser can be changed by modification of configuration parameters — see below.

If authentication fails and direct connection is applied, the firewall's login page is opened automatically (refer to chapter 13.2). The login dialog is displayed if proxy server is used.

Note: If NTLM authentication fails by any reason, details are recorded in the *error* log (see chapter 23.8).

26.4 FTP over Kerio Control proxy server

The *Proxy server* in *Kerio Control* (see chapter 10.5) supports FTP protocol. When using this method of accessing FTP servers, it is necessary to keep in mind specific issues regarding usage of the proxy technology and parameters of *Kerio Control's* proxy server.

1. It is necessary that the FTP client allows configuration of the proxy server. This condition is met for example by web browsers (*Internet Explorer*, *Firefox/SeaMonkey*, *Google Chrome*, etc.), *Total Commander* (originally *Windows Commander*), *CuteFTP*, etc.

   Terminal FTP clients (such as the `ftp` command in *Windows* or *Linux*) do not allow configuration of the proxy server. For this reason, they cannot be used for our purposes.

2. To connect to FTP servers, the proxy server uses the passive FTP mode. If FTP server is protected by a firewall which does not support FTP (this is not a problem of *Kerio Control*), it is not possible to use proxy to connect to the server.

3. Setting of FTP mode in the client is irrelevant for usage of the proxy server. Only one network connection used by the FTP protocol is always established between a client and the proxy server.

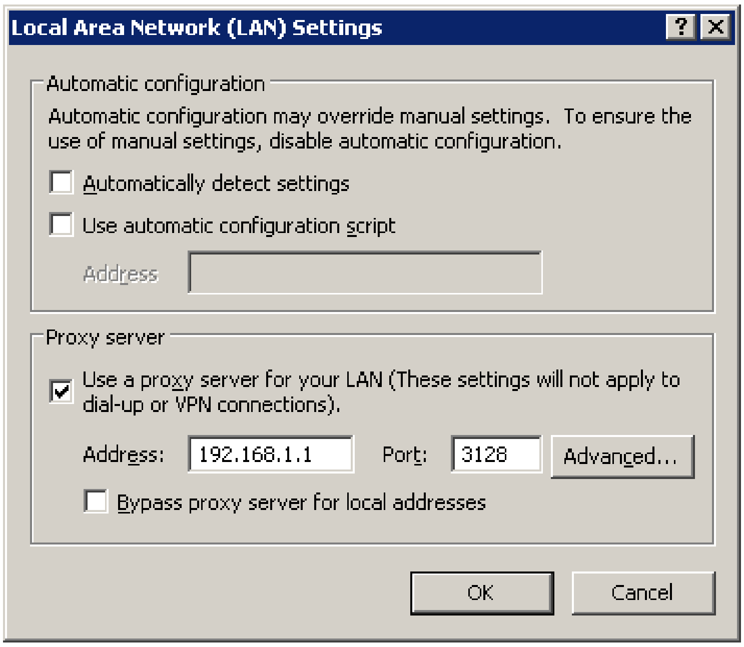
Note: It is recommended to use FTP over proxy server only in cases where it is not possible to connect directly to the Internet (see chapter 10.5).

Example of a client configuration: web browser

Web browsers allow to set the proxy server either globally or for individual protocols. In our example, configuration of *Internet Explorer* focused (configuration of any other browsers is very similar).

1. In the browser's main menu, select *Tools* → *Internet Options*, open the *Connections* tab and click on the *LAN Settings* option.

2. Enable the *Use a proxy server for your LAN* option and enter the IP address and port of the proxy server. IP address of the proxy server is the address of the *Kerio Control's* host interface which is connected to the local network; the default port of the proxy server is `3128` (for details, refer to chapter 10.5). It is also recommended to enable the *Bypass proxy server for local addresses* option — using proxy server for local addresses would slow down traffic and overburden *Kerio Control*.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.1.1 Port: 3128

□ Bypass proxy server for local addresses

Figure 26.3 Configuring proxy server in Internet Explorer

Hint:
To configure web browsers, you can use a configuration script or the automatic detection of configuration. For details, see chapter 10.5.

Note: Web browsers used as FTP clients enable only to download files. Uploads to FTP server via web browsers are not supported.

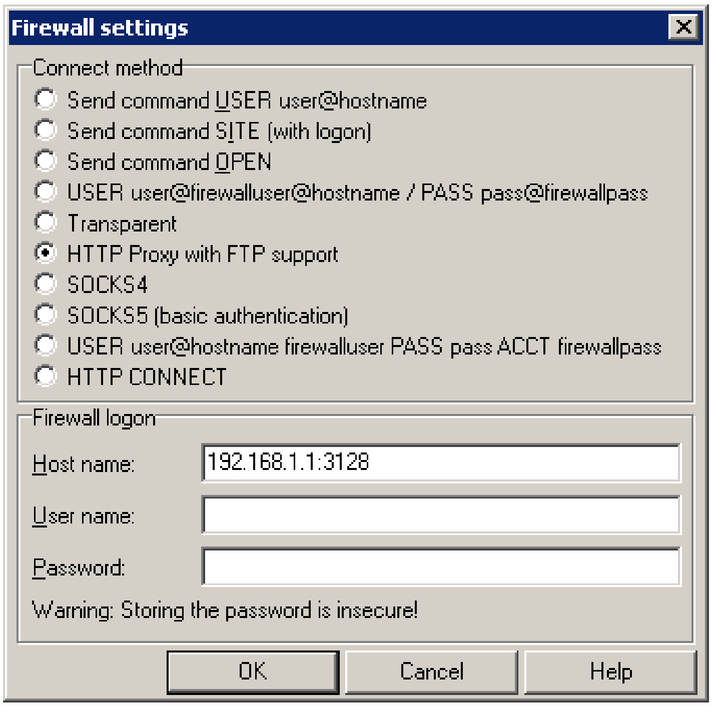
Example of a client configuration: Total Commander

Total Commander allows either single connections to FTP server (by the *Net* → *FTP - New Connection* option available in the main menu) or creating a bookmark for repeated connections (*Net* → *FTP - Connect*). The proxy server must be configured individually for each FTP connection (or for each bookmark).

1. In the *FTP: connection details* dialog, enable the *Use firewall (proxy server)* option and click *Change*.

2. In the *Firewall settings* dialog box, select *HTTP Proxy with FTP support*. In the *Host name* textbox, enter the proxy server's IP address and port (separated by a colon, e.g. `192.168.1.1:3128`). The

   User name and *Password* entries are optional (*Kerio Control* does not use this information).



○ Send command USER user@hostname
○ Send command SITE (with logon)
○ Send command OPEN
○ USER user@firewalluser@hostname / PASS pass@firewallpass
○ Transparent
● HTTP Proxy with FTP support
○ SOCKS4
○ SOCKS5 (basic authentication)
○ USER user@hostname firewalluser PASS pass ACCT firewallpass
○ HTTP CONNECT

Host name: 192.168.1.1:3128
User name:
Password:
Warning: Storing the password is insecure!

Figure 26.4 Setting proxy server for FTP in Total Commander

Hint:
The defined proxy server is indexed and saved to the list of proxy servers automatically. Later, whenever you are creating other FTP connections, you can simply select a corresponding proxy server in the list.

26.5 Internet links dialed on demand

If an on-demand dial-up link is used (see chapter 7.5), consider specific behavior of this connection type. If the network and/or the firewall are not configured correctly, the link may stay hung-up even if the local network sends requests for Internet connection or it may be dialed unintentionally.

Information provided in this chapter should help you understand the principle and behavior of on-demand dial-ups and avoid such problems.

How demand dial works

First, the function of demand dial must be activated within the appropriate line (either permanently or during a defined time period — see chapter 7.5).

Second, there must be no default gateway in the operating system (no default gateway must be defined for any network adapter). This condition does not apply to the dial-up line which is used for the Internet connection — this line will be configured in accordance with information provided by the ISP.

If *Kerio Control* receives a packet from the local network, it will compare it with the system routing table. If the packets goes out to the Internet, no record will be found, since there is no default route in the routing table. Under usual circumstances, the packet would be dropped and a control message informing about unavailability of the target would be sent to the sender. If no default route is available, *Kerio Control* holds the packet in the cache and dials the appropriate line if the demand dial function is enabled. This creates an outgoing route in the routing table via which the packet will be sent.

To avoid undesired dialing of the line, line dialing is allowed by certain packet types only. The line can be dialed only by UDP or TCP packets with the *SYN* flag (connection attempts). Demand dialing is disabled for *Microsoft Network* services (sharing of files and printers, etc.).

Since this moment, the default route exists and other packets directed to the Internet will be routed via a corresponding line. The line may be either disconnected manually or automatically if idle for a certain time period. When the line is hung-up, the default route is removed from the routing table. Any other packet directed to the Internet redials the line.

Note:

1. To ensure correct functionality of demand dialing there must be no default gateway set at network adapters. If there is a default gateway at any interface, packets to the Internet

would be routed via this interface (no matter where it is actually connected to) and *Kerio Control* would not dial the line.

2. Only one link can be set for on-demand dialing in *Kerio Control*. *Kerio Control* does not enable automatic selection of a line to be dialed.
3. Lines can be also dialed if this is defined by a static route in the routing table (refer to chapter 19.1). If a static route via the dial-up is defined, the packet matching this route will dial the line. This line will not be used as the default route — the *Use default gateway on remote network* option in the dial-up definition will be ignored.
4. According to the factors that affect total time since receiving the request until the line is dialed (i.e. line speed, time needed to dial the line, etc.) the client might consider the destination server unavailable (if the timeout expires) before a successful connection attempt. However, *Kerio Control* always finishes dial attempts. In such cases, simply repeat the request, i.e. with the *Refresh* button in your browser.

Technical Peculiarities and Limitations

Demand dialing has its peculiarities and limitations. The limitations should be considered especially within designing and configuration of the network that will use *Kerio Control* for connection and of the dial-up connected to the Internet.

1. Demand dial cannot be performed directly from the host where *Kerio Control* is installed because it is initiated by *Kerio Control* low-lever driver. This driver holds packets and decides whether the line should be dialed or not. If the line is disconnected and a packet is sent from the local host to the Internet, the packet will be dropped by the operating system before the *Kerio Control* driver is able to capture it.

2. Typically the server is represented by the DNS name within traffic between clients and an Internet server. Therefore, the first packet sent by a client is represented by the DNS query that is intended to resolve a host name to an IP address.

   In this example, the DNS server is the *Kerio Control* host (this is very common) and the Internet line is disconnected. A client's request on this DNS server is traffic within the local network and, therefore, it will not result in dialing the line. If the DNS server does not have the appropriate entry in the cache , it must forward the request to another server on the Internet. The packet is forwarded to the Internet by the local DNS client that is run at the *Kerio Control* host. This packet cannot be held and it will not cause dialing of the line. Therefore, the DNS request cannot be answered and the traffic cannot continue.

   For these reasons, the *Kerio Control's DNS* module enables automatic dialing (if the DNS server cannot respond to the request itself). This feature is bound to on-demand dialing.

   Note: If the DNS server is located on another host within the local network or clients within the local network use a DNS server located in the Internet, then the limitation is irrelevant and the dialing will be available. If clients' DNS server is located on the Internet, the line will be dialed upon a client's DNS query. If a local DNS server is used, the line will be dialed upon a query sent by this server to the Internet (the default gateway of the host where the DNS server is running must be set to the IP address of the *Kerio Control* host).

3. It can be easily understood through the last point that if the DNS server is to be running at the *Kerio Control* host, it must be represented by the *DNS* module because it can dial the line if necessary.

   If there is a domain based on *Active Directory* in the LAN (domain server with *Windows Server 2000/2003/2008*), it is necessary to use *Microsoft* DNS server, because communication with *Active Directory* uses special types of DNS request. *Microsoft* DNS server does not support automatic dialing. Moreover, it cannot be used at the same host as the *DNS* module as it would cause collision of ports.

   As understood from the facts above, if the Internet connection is to be available via dial-up, *Kerio Control cannot* be used at the same host where *Windows Server* with *Active Directory* and *Microsoft* DNS are running.

4. If the *DNS* module is used, *Kerio Control* can dial as a response to a client's request if the following conditions are met:

   Destination server must be defined by DNS name so that the application can send aDNS query.

5. The *Proxy server* in *Kerio Control* (see chapter 10.5) also provides direct dial-up connections. A special page providing information on the connection process is opened (the page is refreshed in short periods). Upon a successful connection, the browser is redirected to the specified Website.

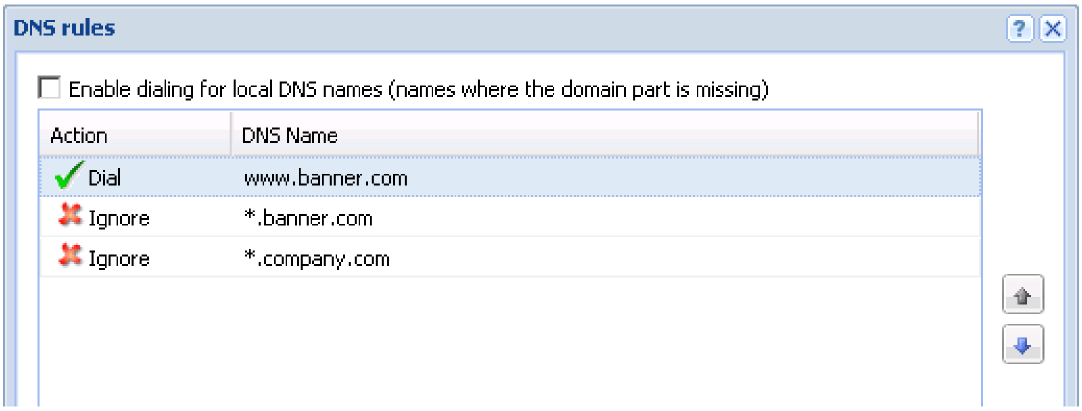
Unintentionally dialed link — application of on-demand dial rules

Demand dial functions may cause unintentional dialing. It's usually caused by DNS requests which cannot be responded by the *DNS* module and so it dials the line instead to forward them to another DNS server. The following causes apply:

- User host generates a DNS query in the absence of the user. This traffic attempt may be an active object at a local HTML page or automatic update of an installed application.
- The *DNS* module performs dialing in response to requests of names of local hosts. Define DNS for the local domain properly (use the hostname table and/or the DHCP server lease table — for details see chapter 10.1).

Note: Undesirable traffic causing unintentional dialing of a link can be blocked by *Kerio Control* traffic rules (see chapter 8.3). However, the best remedy for any pain is always removal of its cause (e.g. perform antivirus check on the corresponding workstation, etc.).

To avoid unintentional dialing based on DNS requests, *Kerio Control* allows definition of rules where DNS names are specified for which the line can be dialed or not. To define these rules, click on *Advanced* in *Configuration→ Interfaces* (in the *A Single Internet Link — Dial on Demand* mode).



DNS rules

☐ Enable dialing for local DNS names (names where the domain part is missing)

Action	DNS Name
✓ Dial	www.banner.com
✗ Ignore	*.banner.com
✗ Ignore	*.company.com

Figure 26.5 Dial on demand rules (for dialing based on DNS queries)

Either full *DNS name* or only its end or beginning completed by an asterisk (*) can be specified in the rule. An asterisk may stand for any number of characters.

Rules are ordered in a list which is processed from the top downwards (rules order can be modified with the arrow buttons at the right side of the window). When the system detects the first rule that meets all requirements, the desired action is executed and the search is stopped. All DNS names missing a suitable rule will be dialed automatically by the *DNS* module when demanded.

In *Actions* for DNS name, you can select either the *Dial* or the *Ignore* option. Use the second option to block dialing of the line in response to a request for this DNS name. The *Dial* action can be used to create complex rule combinations. For example, dial can be permitted for one name within the domain and denied for the others (see figure 26.5).

Dial of local DNS names

Local DNS names are names of hosts within the domain (names that do not include a domain).

> ***Example::***
> The local domain's name is `company.com`. The host is called `pc1`. The full name of the host is `pc1.company.com` whereas local name in this domain is `pc1`.

Local names are generally saved in the local DNS server database (in this sace in the hostname table and the DHCP lease table in *Kerio Control*). Set by default, the *DNS* module does not dial these names as names are considered non-existent unless they can be found in the local DNS database.

If the primary server of the local domain is located outside of the local network, it is necessary that the *DNS* module also dials the line if requests come from these names. Activate the *Enable dialing for local DNS names* option in the *Other settings* tab to enable this (at the top of the *Dial On Demand* dialog window). In other cases, it is recommended to leave the option disabled (again, the line can be dialed undesirably).

Chapter 27

Technical support

Free email and telephone technical support is provided for *Kerio Control*. Contacts and more information can be found at http://www.kerio.com/support. Our technical support staff is ready to help you with any problem you might have.

You can also solve many problems alone (and sometimes even faster). Before you contact our technical support, please take the following steps:

- Try to look up the answer in this manual. Individual chapters describe features and parameters of *Kerio Control* components in detail.
- If you have not found answers here, try to find them at our website, under Technical Support.

If you have not find answers to all your questions and you still intend to contact our technical support, read through the following section which will provide you with a few guidelines.

27.1 Essential Information

To send a request to our technical support, use the contact form at

http://support.kerio.com/.

To be able to help you solve your problems the best and in the shortest possible time our technical support will require your configuration data and as clear information on your problem as possible. Please specify at least the following information:

Description

Clearly describe your problem. Provide as much information on the problem as possible (i.e. whether the issue arose after you had installed a new product version, after an upgrade, etc.).

Error Log Files

In the directory where *Kerio Control* is installed

(the typical path is `C:\Program Files\Kerio\WinRoute Firewall`)

the `logs` subdirectory is created. There you can find files `error.log` and `warning.log`. Attach these two files to your email to our technical support.

License type and license number

Please specify whether you have purchased any *Kerio Control* license or if you use the trial version. Requirements of owners of valid licenses are always preferred.

27.2 Tested in Beta version

As to increase quality of our products, *Kerio Technologies* releases essential versions of our products as so called beta versions. Beta versions are product versions which include all projected new features, however, these functions and the product itself are still under development. Volunteers can test these versions and provide us with feedback to help us improve the product and fix bugs.

The feedback from beta testers is essential for the product's development. Therefore, *Kerio Control* beta versions include extensions and modules helping testers communicate smoothly with *Kerio Technologies*.

For details on beta versions and their testing, refer to http://www.kerio.com/betas.

Appendix A

Legal Notices

Microsoft®, *Windows*®, *Windows NT*®, *Windows Vista*™, *Internet Explorer*®, *ActiveX*®, and *Active Directory*® are registered trademarks or trademarks of *Microsoft Corporation*.

Apple®, *Mac OS*® and *Safari*™ are registered trademarks or trademarks of *Apple Inc.*

Linux® is registered trademark kept by Linus Torvalds.

VMware® is registered trademark of VMware, Inc.

Mozilla® and *Firefox*® are registered trademarks of *Mozilla Foundation*.

Chrome™ is trademark of *Google Inc.*

Kerberos™ is trademark of *Massachusetts Institute of Technology* (*MIT*).

Snort® is registered trademark of *Sourcefire, Inc.*

Sophos® is registered trademark of *Sophos Plc*.

avast!® is registered trademark of *AVAST Software*.

ClamAV™ is trademark held by Tomasz Kojm.

ESET® and *NOD32*® are registered trademarks of *ESET, LLC.*

AVG® is registered trademark of *AVG Technologies*.

Thawte® is registered trademark of *VeriSign, Inc.*

Other names of real companies and products mentioned in this document may be registered trademarks or trademarks of their owners.

Appendix B

Used open source items

Kerio Control contains the following open-source software:

bindlib

Copyright ©1983, 1993 The Regents of the University of California. All rights reserved.
Portions Copyright ©1993 by Digital Equipment Corporation.

bluff

Bluff is a JavaScript port of the *Gruff* graphing library for Ruby. The *Gruff* library is written in Ruby.

Note: For this purpose, *jsclass* (identical author and license) and *excanvas* library are used (see below).

Copyright © 2008-2009 James Coglan.
Original library written in Ruby 2005-2009 Topfunky Corporation.

excanvas

The *ExplorerCanvas* library allows 2D command-based drawing operations in *Internet Explorer*.

Copyright © 2006 Google Inc.

Firebird

This software embeds modified version of *Firebird* database engine distributed under terms of *IPL* and *IDPL* licenses.

All copyright retained by individual contributors — original code Copyright © 2000 *Inprise Corporation*.

The original source code is available at:

http://www.firebirdsql.org/

h323plus

This product includes unmodified version of the *h323plus* library distributed under *Mozilla Public License* (*MPL*).

The original source code is available at:

http://h323plus.org/

KIPF — driver

Kerio IP filter driver for Linux (*Kerio Control's* network interface for Linux):
Copyright © Kerio Technologies s.r.o.
Homepage: http://www.kerio.com/
Kerio IP filter driver for Linux is distributed and licensed under *GNU General Public License* version 2.

The complete source code is available at:

http://download.kerio.com/archive/

KIPF — API

Kerio IP filter driver for Linux API library (API library of the *Kerio Control* network driver for Linux)
Copyright © Kerio Technologies s.r.o.
Homepage: http://www.kerio.com/
Kerio IP filter driver for Linux API library is distributed and licensed under *GNU Lesser General Public License* version 2.
The complete source code is available at:

http://download.kerio.com/archive/

KVNET — driver

Kerio Virtual Network Interface driver for Linux (driver for the *Kerio VPN* virtual network adapter)
Copyright © Kerio Technologies s.r.o.
Homepage: http://www.kerio.com/
Kerio Virtual Network Interface driver for Linux is distributed and licensed under *GNU General Public License* version 2.
The complete source code is available at:

http://download.kerio.com/archive/

KVNET — API

Kerio Virtual Network Interface driver for Linux API library (API library for the driver of the *Kerio VPN* virtual network adapter)
Copyright © Kerio Technologies s.r.o.
Homepage: http://www.kerio.com/
Kerio Virtual Network Interface driver for Linux API library is distributed and licensed under *GNU Lesser General Public License* version 2.
The complete source code is available at:

http://download.kerio.com/archive/

libcurl

Copyright © 1996-2008 Daniel Stenberg.

libiconv

libiconv converts from one character encoding to another through Unicode conversion. *Kerio Control* include a modified version of this library distributed upon the *GNU Lesser General Public License* in version 3.
Copyright ©1999-2003 Free Software Foundation, Inc.
Author: Bruno Haible
Homepage: http://www.gnu.org/software/libiconv/
Complete source code of the customized version of *libiconv* library is available at:

http://download.kerio.com/archive/

libxml2

Copyright © 1998-2003 Daniel Veillard. All Rights Reserved.
Copyright © 2000 Bjorn Reese and Daniel Veillard.
Copyright © 2000 Gary Pennington and Daniel Veillard
Copyright © 1998 Bjorn Reese and Daniel Stenberg.

Netfilter4Win

Netfilter4win is an implementation of the *libnetfilter_queue* interface for *Windows*. It is distributed under *GNU General Public License* version 2.
Copyright © Kerio Technologies s.r.o.
Copyright © 2005 Harald Welte
Distribution package of complete source codes is available at:

http://download.kerio.com/archive/

OpenSSL

This product contains software developed by *OpenSSL Project* designed for *OpenSSL Toolkit* (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young.
This product includes software written by Tim Hudson.

Operating system

Kerio Control in editions *Appliance* and *Box* are based on various open source software. For detailed information on licences of all software used, refer to file

```
/opt/kerio/winroute/doc/Acknowledgements
```

available on the appliance disk.
Distribution package of complete source codes is available at:

http://download.kerio.com/archive/

PHP

Copyright © 1999-2006 The PHP Group. All rights reserved.
This product includes *PHP* software available for free at:

http://www.php.net/software/

Prototype

Framework in JavaScript.
Copyright © Sam Stephenson.
The *Prototype* library is freely distributable under the terms of a *MIT* license.
For details, see the *Prototype* website: http://www.prototypejs.org/

ptlib

This product includes unmodified version of the *ptlib* library distributed under *Mozilla Public License* (*MPL*).
The original source code is available at:

http://h323plus.org/

ScoopyNG

The VMware detection tool.
This product includes software written by Tobias Klein.
Copyright © 2008 Tobias Klein. All Rights Reserved.

Snort

Snort is an open source network intrusion detection and prevention system (*IDS/IPS*). The distribution package includes the *Snort* system and the *pcre* and *pthreads-win32* libraries. The package is distributed under the *GNU General Public License* version 2.
Copyright © Kerio Technologies s.r.o.
Copyright © 2001-2008 Sourcefire Inc.
Copyright © 1998-2001 Martin Roesch
Copyright © 1998 John E. Bossom
Copyright © 1999-2005 The *pthreads-win32* library authors team
Copyright © 1997-2009 University of Cambridge
Copyright © 2007-2008 Google Inc.
Distribution package of complete source codes is available at:

http://download.kerio.com/archive/

zlib

Copyright © Jean-Loup Gailly and Mark Adler.

Glossary of terms

ActiveX

This *Microsoft's* proprietary technology is used for creation of dynamic objects for web pages. This technology provides many features, such as writing to disk or execution of commands at the client (i.e. on the host where the Web page is opened). This technology provides a wide range of features, such as saving to disk and running commands at the client (i.e. at the computer where the Web page is opened). Using *ActiveX*, virus and worms can for example modify telephone number of the dial-up.
ActiveX is supported only by *Internet Explorer* in *Microsoft Windows* operating systems.

Cluster

A group of two or more workstations representing one virtual host (server). Requests to the virtual server are distributed among individual hosts in the cluster, in accordance with a defined algorithm. Clusters empower performance and increase reliability (in case of dropout of one computer in the cluster, the virtual server keeps running).

Connections

A virtual bidirectional communication channel between two hosts.
See also *TCP*

DDNS

DDNS (*Dynamic Domain Name System*) is DNS with the feature of automatic update of records.

Default gateway

A network device or a host where so called default path is located (the path to the Internet). To the address of the default gateway such packets are sent that include destination addresses which do not belong to any network connected directly to the host and to any network which is recorded in the system routing table.
In the system routing table, the default gateway is shown as a path to the destination network *0.0.0.0* with the subnet mask *0.0.0.0*.
Note: Although in *Windows* the default gateway is configured in settings of the network interface, it is used for the entire operating system.

DHCP

DHCP (*Dynamic Host Configuration Protocol*) Serves automatic IP configuration of computers in the network. IP addresses are assigned from a scope. Besides IP addresses, other parameters can be associated with client hosts, such as the default gateway address, DNS server address, local domain name, etc.

DMZ

DMZ (demilitarized zone) is a reserved network area where services available both from the Internet and from the LAN are run (e.g. a company's public web server). DMZ provides an area, where servers accessible for public are be located separately, so they cannot be misused for cracking into the LAN.
More information can be found for example at Wikipedia.

DNS

DNS (*Domain Name System*) A worldwide distributed database of Internet hostnames and their associated IP address. Computers use Domain Name Servers to resolve host names to IP addresses. Names are sorted in hierarchized domains.

Firewall

Software or hardware device that protects a computer or computer network against attacks from external sources (typically from the Internet).
In this guide, the word *firewall* represents the *Kerio Control* host.

FTP

File Transfer Protocol. The FTP protocol uses two types of TCP connection: control and data. The control connection is always established by a client. Two FTP modes are distinguished according to a method how connection is established:

- *active mode* — data connection is established from the server to a client (to the port specified by the client). This mode is suitable for cases where the firewall is at the server's side, however, it is not supported by some clients (e.g. by web browsers).
- *passive mode* — data connection is established also by the client (to the port required by the server). This mode is suitable for cases where the firewall is at the client's side. It should be supported by any FTP client.

Note: Kerio Control includes special support (protocol inspector) for FTP protocol. Therefore, both FTP modes can be used on LAN hosts.

Gateway

Network device or a computer connecting two different subnets. If traffic to all the other (not specified) networks is routed through a gateway, it is called the default gateway.
See also *default gateway.*

Greylisting

A method of protection of *SMTP* servers from spam. If an email message sent by an unknown sender is delivered to the server, the server rejects it for the first time (so called temporary delivery error). Legitimate senders attempt resend the message after some time. SMTP server lets the message in and considers the sender as trustworthy since then, not blocking their messages any longer. Most spam senders try to send as great volume in as short time as possible and stay anonymous. Therefore, they usually do not repeat sending the message and focus on another SMTP server.
More information (in English) can be found for example at Wikipedia.

Ident

The *Ident* protocol is used for identification of user who established certain TCP connection from a particular (multi-user) system. The *Ident* service is used for example by IRC servers, FTP servers and other services.
More information (in English) can be found for example at Wikipedia.

IDS/IPS

IDS/IPS (*Intrusion Detection System / Intrusion Prevention System*) is a system of detection and prevention of network intrusions. It can be used for protection of a particular computer or implemented on the Internet gateway for protection of the entire local network which uses this gateway for Internet connection.
The *IDS/IPS* system analyzes all network traffic, detecting and blocking possible known intrusions (e.g. *portscanning*, *DoS*, etc.), and also analyzes suspicious activities, thus attempting to prevent even from unknown intrusion types.

IMAP

Internet Message Access Protocol (IMAP) enables clients to manage messages stored on a mail server without downloading them to a local computer. This architecture allows the user to access his/her mail from multiple locations (messages downloaded to a local host disk would not be available from other locations).

IP

IP (*Internet Protocol*) is a data protocol used for transfering data via packet networks. This is the basic Internet protocol.

IP address

IP address is a unique number used to identify the host in the Internet. Each packet contains information about where it was sent from (source IP address) and to which address it is to be delivered (destination IP address). The current IP versions are:

- IP address version 4 (or *IPv4 address* or *IP address*) — are 4 bytes in decimal numeral system (`0-255`) divided by a full stop — for example, `195.129.33.1`.
- IP address version 6 (or *IPv6 address*) — are 8 hexadecimal numbers (`0-255`) divided by colons — for example, `2001:ad5e:012f:0184:0000:0000:0000:0001`. It is possible to leave out the zeros: `2001:ad5e:12f:184::1`.

IPSec

IPSec (*IP Security Protocol*) is an extended IP protocol which enables secure data transfer. It provides services similar to SSL/TLS, however, these services are provided on a network layer. IPSec can be used for creation of encrypted tunnels between networks (VPN) — so called tunnel mode, or for encryption of traffic between two hosts— so called transport mode.

Kerberos

Kerberos is a system used for secure user authentication in network environments. It was developed at the *MIT* university and it is a standard protocol used for user authentication under *Windows 2000/2003/2008*. Users use their passwords to authenticate to the central server (*KDC, Key Distribution Center*) and the server sends them encrypted tickets which can be used to authenticate to various services in the network. In case of the *Windows 2000/2003/2008* domains, function of *KDC* is provided by the particular domain server.

LDAP

LDAP (Lightweight Directory Access Protocol) is an Internet protocol used to access directory services (such as *Microsoft Active Directory* or *Apple Open Directory*). Information about user accounts and user rights, about hosts included in the network, etc. are stored in the directories.

MAC address

MAC address (*MAC = Media Access Control*, also known as physical or hardware address) is a unique identifier of network adapters. In case of *Ethernet* and *Wi-Fi* it has 48 bits (6 bytes) and it is recorded as a six of hexadecimal numbers separated by colons or dashes. The *Kerio Control* administration interface uses the format with colons — e.g.: `00:1a:cd:22:6b:5f`.

NAT

NAT (*Network Address Translation*) stands for substitution of IP addresses in packets passing through the firewall:

- source address translation (*Source NAT, SNAT*) — in packets going from local networks to the Internet source (private) IP addresses are substituted with the external (public) firewall address. Each packet sent from the local network is recorded in the NAT table. If any packet incoming from the Internet matches with a record included in this table, its destination IP address will be substituted by the IP address of the appropriate host within the local network and the packet will be redirected to this host. Packets that do not match with any record in the NAT table will be dropped.
- destination address translation (*Destination NAT, DNAT*, it is also called port mapping) — is used to enable services in the local network from the Internet. If any packet incoming from the Internet meets certain requirements, its IP address will be substituted by the IP address of the local host where the service is running and the packet is sent to this host.

The *NAT* technology enables connection from local networks to the Internet using a single IP address. All hosts within the local network can access the Internet directly as if they were on a public network (certain limitations are applied). Services running on local hosts can be mapped to the public IP address.
Detailed description (in English) can be found for example at Wikipedia.

Network adapter

The equipment that connects hosts to a traffic medium. It can be represented by an Ethernet adapter, Wi-Fi adapter, by a modem, etc. Network adapters are used by hosts to send and receive packets. They are also referred to throughout this document as a network interface.

P2P network

Peer-to-Peer (*P2P*) networks are world-wide distributed systems, where each node can represent both a client and a server. These networks are used for sharing of big volumes of data (this sharing is mostly illegal). *DirectConnect* and *Kazaa* are the most popular ones.

Packet

Basic data unit transmitted via computer networks. Packets consist of a header which include essential data (i.e. source and destination IP address, protocol type, etc.) and of the data body,. Data transmitted via networks is divided into small segments, or packets. If an error is detected in any packet or a packet is lost, it is not necessary to repeat the entire transmission process, only the particular packet will be re-sent.

Policy routing

Advanced routing technology using additional information apart from IP addresses, such as source IP address, protocols etc.

See also *routing table.*

POP3

Post Office Protocol is an email accessing protocol that allows users to download messages from a server to a local disk. It is suitable for clients who don't have a permanent connection to the Internet.

Port

16-bit number (1–65535) used by TCP and UDP for application (services) identification on a given computer. More than one application can be run at a host simultaneously (e.g. WWW server, mail client, FTP client, etc.). Each application is identified by a port number. Ports 1–1023 are reserved and used by well known services (e.g. 80 = WWW). Ports above 1023 can be freely used by any application.

PPTP

Microsoft's proprietary protocol used for design of virtual private networks.

See chapters and sections concerning *VPN.*

Private IP addresses

Local networks which do not belong to the Internet (private networks) use reserved ranges of IP addresses (private addresses). These addresses cannot be used in the Internet. This implies that IP ranges for local networks cannot collide with IP addresses used in the Internet.

The following IP ranges are reserved for private networks:

- 10.0.0.0/255.0.0.0
- 172.16.0.0/255.240.0.0
- 192.168.0.0/255.255.0.0

Protocol inspector

Kerio Control's subroutine, which is able to monitor communication using application protocols (e.g. HTTP, FTP, MMS, etc.). Protocol inspection is used to check proper syntax of corresponding protocols (mistakes might indicate an intrusion attempt), to ensure its proper functionality while passing through the firewall (e.g. FTP in the active mode, when data connection to a client is established by a server) and to filter traffic by the corresponding protocol (e.g. limited access to Web pages classified by URLs, anti-virus check of downloaded objects, etc.).

Unless traffic rules are set to follow a different policy, each protocol inspector is automatically applied to all connections of the relevant protocol that are processed through *Kerio Control.*

Proxy server

Older, but still wide-spread method of Internet connection sharing. Proxy servers connect clients and destination servers.

A proxy server works as an application and it is adapted for several particular application protocols (i.e. HTTP, FTP, Gopher, etc.). It requires also support in the corresponding client application (e.g. web browser). Compared to NAT, the range of featured offered is not so wide.

Router

A computer or device with one or more network interfaces between which it handles packets by following specific rules (so called routes). The router's goal is to forward packets only to the destination network, i.e. to the network which will use another router which would handle it on. This saves other networks from being overloaded by packets targeting another network. See also *routing table*.

Routing table

The information used by routers when making packet forwarding decisions (so called routes). Packets are routed according to the packet's destination IP address. On *Windows*, routing table can be printed by the `route print` command, while on *Unix* systems (*Linux*, *Mac OS X*, etc.) by the `route` command.

Script

A code that is run on the Web page by a client (Web browser). Scripts are used for generating of dynamic elements on Web pages. However, they can be misused for ads, exploiting of user information, etc. Modern Web browsers usually support several script languages, such as *JavaScript* and *Visual Basic Script (VBScript)*.

SMTP

Simple Mail Transfer Protocol is used for sending email between mail servers. The SMTP envelope identifies the sender/recipient of an email.

Spam

Undesirable email message, usually containing advertisements.

Spoofing

Spoofing means using false IP addresses in packets. This method is used by attackers to make recipients assume that the packet is coming from a trustworthy IP address.

SSL

SSL is a protocol used to secure and encrypt network communication. SSL was originally designed in order to guarantee secure transfer of Web pages over HTTP protocol. Nowadays, it is used by almost all standard Internet protocols (SMTP, POP3, IMAP, LDAP, etc.).

At the beginning of communication, an encryption key is requested and transferred using asymmetrical encryption. This key is then used to encrypt (symmetrically) the data.

Subnet mask

Subnet mask divides an IP address in two parts: network mask and an address of a host in the network. Mask have the same form as IP addresses (i.e. `255.255.255.0`), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. Number one in a subnet mask represents a bit of the network address and zero stands for a host's address bit. All hosts within a particular subnet must have identical subnet mask and network part of IP address.

TCP

Transmission Control Protocol is a transmission protocol which ensures reliable and sequential data delivery. It establishes so called virtual connections and provides tools for error correction and data stream control. It is used by most of applications protocols which require reliable transmission of all data, such as *HTTP*, *FTP*, *SMTP*, *IMAP*, etc.
TCP protocol uses the following special control information — so called *flags*:

- *SYN* (Synchronize) — connection initiation (first packet in each connection)
- *ACK* (Acknowledgement) — acknowledgement of received data
- *RST* (Reset) — request on termination of a current connection and on initiation of a new one
- *URG* (Urgent) — urgent packet
- *PSH* (Push) — request on immediate transmission of the data to upper TCP/IP layers
- *FIN* (Finalize) — connection finalization

TCP/IP

Name used for all traffic protocols used in the Internet (i.e. for IP, ICMP, TCP, UDP, etc.). *TCP/IP* does not stand for any particular protocol!

TLS

Transport Layer Security. New version of SSL protocol. This version is approved by the IETF and it is accepted by all the top IT companies (i.e. *Microsoft Corporation*).

UDP

User Datagram Protocol is a transmission protocol which transfers data through individual messages (so called datagrams). It does not establish new connections nor it provides reliable and sequential data delivery, nor it enables error correction or data stream control. It is used for transfer of small-sized data (i.e. DNS queries) or for transmissions where speed is preferred from reliability (i.e. realtime audio and video files transmission).

VPN

Virtual Private Network, VPN represents secure interconnection of private networks (i.e. of individual offices of an organization) via the Internet. Traffic between both networks (so called tunnel) is encrypted. This protects networks from tapping. VPN incorporates special tunneling protocols, such as *PPTP* (*Point-to-Point Tunneling Protocol*) and *Microsoft's IPSec*.
Kerio Control contains a proprietary VPN implementation called *Kerio VPN*.

WINS

The *WINS (Windows Internet Name Service)* service is used for resolution of hostnames to IP addresses within *Microsoft Windows* networks.

Index