

Kerio **WinRoute** Firewall 6™

Step-by-Step Configuration

Kerio Technologies

©2001-2004

Kerio Technologies. All Rights Reserved.

Printing Date: April 25, 2004

This guide provides detailed description on configuration of the local network which uses the *Kerio WinRoute Firewall*, version 6.0.0. All additional modifications and updates reserved.

For current product version, check <http://www.kerio.com/kwf>.

Contents

- 1 Introduction 5**
- 2 Headquarters configuration 7**
 - 2.1 Network Interface Configurations 7
 - 2.2 WinRoute Installation 8
 - 2.3 Basic Traffic Policy Configuration 9
 - 2.4 DHCP Server Configuration 13
 - 2.5 DNS Forwarder Configuration 16
 - 2.6 Creating User Accounts and Groups 17
 - 2.7 Address Groups and Time Ranges 19
 - 2.8 Web Rules Definition 25
 - 2.9 FTP Policy Configuration 30
 - 2.10 Antivirus Scanning Configuration 32
 - 2.11 Enabling Access to Services from the Internet 34
 - 2.12 Secured access of remote clients to LAN 34
 - 2.13 LAN Hosts Configuration 35
- 3 Interconnection of the headquarters and branch offices 37**
 - 3.1 Headquarters configuration 38
 - 3.2 Branch office configuration 39
 - 3.3 VPN test 43
- 4 Index 45**

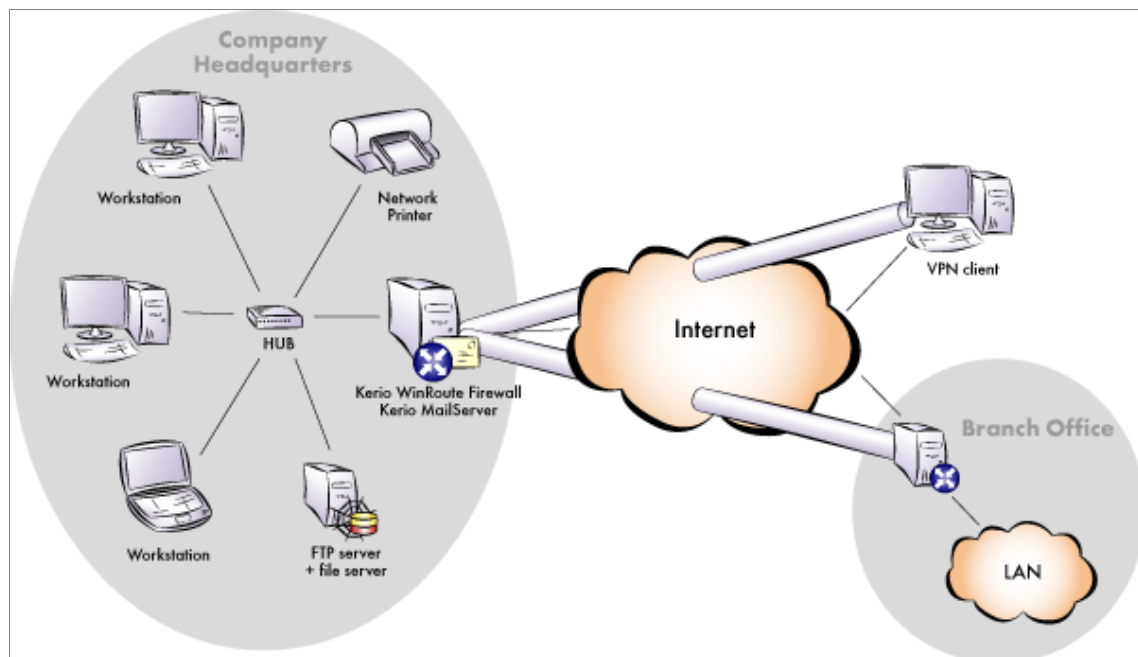
Chapter 1

Introduction

This guide describes in detail the steps needed to deploy *WinRoute* in an example network. This network includes most elements present in a real-life *WinRoute* network — Internet access from the local network, protection against attacks from the Internet, access to selected services on the LAN from the Internet, user access control, automatic configuration of clients on the LAN, etc.

This document also describes interconnection of the headquarters network with branch office network(s) by an encrypted channel (VPN tunnel) as well as secured access of clients to the local network via the Internet using *WinRoute* tools.

WinRoute configuration will be better understood through an example of a model network according to the following scheme.



Chapter 2

Headquarters configuration

This chapter provides detailed description on configuration of the local network and setup of *WinRoute* in company headquarters. The same guidance can also be followed for configuration of the network in branch offices (only the IP address range must differ).

2.1 Network Interface Configurations

Internet Interfaces

TCP/IP parameters of the Internet Interface must be set according to information provided by your ISP. In case of a dial-up connection (i.e. analog modem or ISDN), you must create the appropriate dial-up connection using the 'make new connection' wizard located in the network control panel.

Verify connectivity (i.e. by using the `ping` command or by opening a Web site using your browser).

Selection of IP addresses for LAN

The following options can be used to select IP addresses for your LAN:

- use public IP addresses. The ISP will assign a required IP range and set routing parameters.
- use private IP addresses and IP translation (NAT). We recommend using this option as it provides easier administration and technical maintenance.

Private addresses are represented by special IP ranges that are reserved for local networks which do not belong to the Internet (private networks). These addresses must not exist in the Internet (Internet routers are usually set in order to drop all packets that include these addresses).

The following IP ranges are reserved for private networks:

- 10.x.x.x, network mask 255.0.0.0
- 172.16.x.x, network mask 255.240.0.0
- 192.168.x.x, network mask 255.255.0.0

Chapter 2 Headquarters configuration

Warning: Do not use other IP addresses in private networks, otherwise some Web pages (those networks that have the same IP addresses) might be unavailable!

The 192.168.1.0 address (private IP address) with the 255.255.255.0 network mask is used for the local network in the following example.

LAN Interface

The following parameters will be set at the LAN Interface:

- *IP address* — the 192.168.1.1 IP address will be used
- *network mask* — 255.255.255.0
- *default gateway* — no default gateway is allowed at this interface!
- *DNS server* — the address of the DNS server at the firewall must be identical with the IP address of the interface connected to the local network so that DNS requests between headquarters and filial networks will be transferred correctly (see chapters 3.1 and 3.2) and also on-demand dialing from the firewall will work properly.

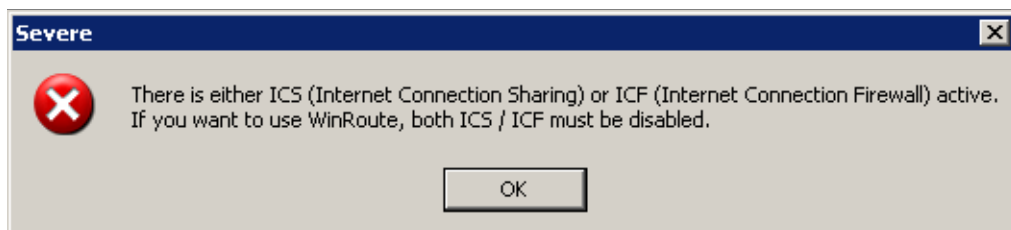
Use the *Preferred DNS server* entry to specify the IP address 192.168.1.1.

2.2 WinRoute Installation

Run the *WinRoute* installation program and select the

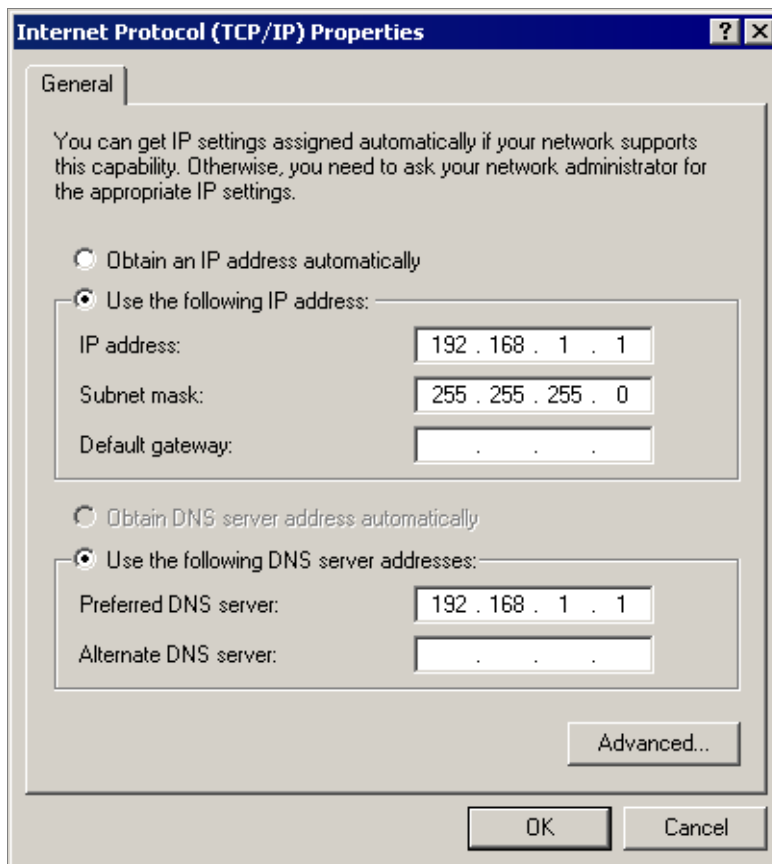
Typical installation.

Disable the *Internet Connection Sharing* (Windows Me, 2000, XP) or *Internet Connection Firewall* (Windows XP) services if detected by the installation program, otherwise *WinRoute* might not function correctly.



Define a username and password that will be used for the administrative account.

2.3 Basic Traffic Policy Configuration



Restart your machine when the installation is completed.

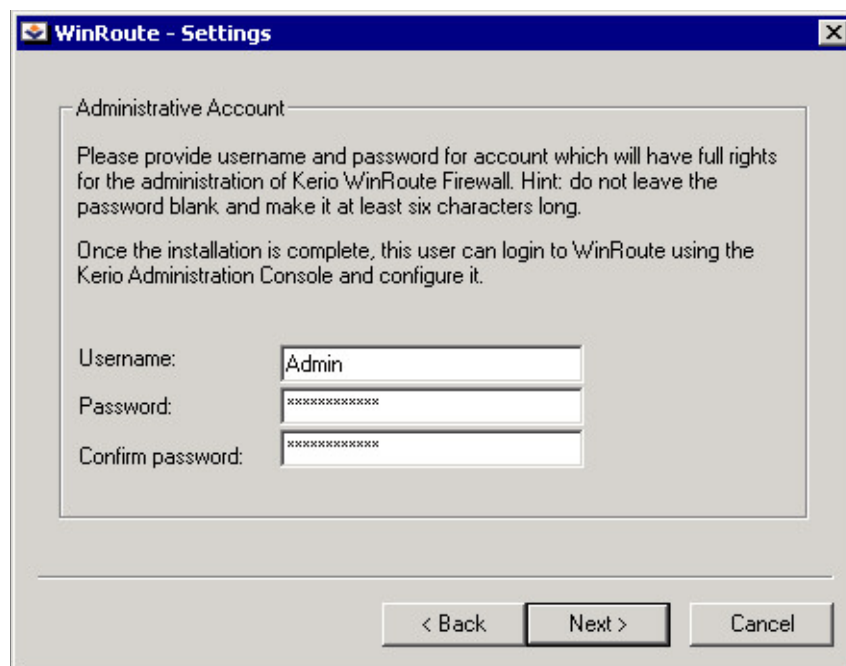
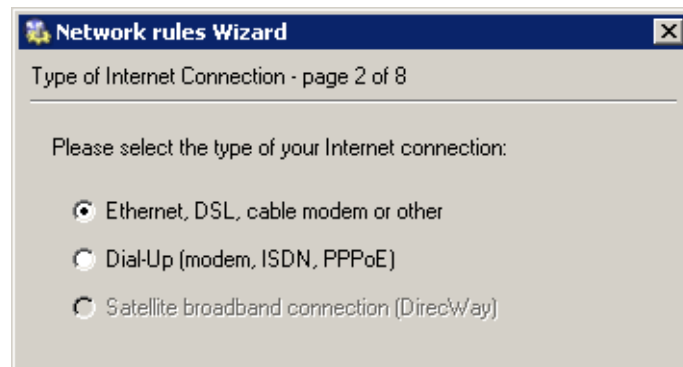
2.3 Basic Traffic Policy Configuration

After reboot, run the *Kerio Administration Console* (*Start / Programs / Kerio*). Connect to the localhost (the local computer) with the user name and password defined during installation. The *Network Rules Wizard* will be started automatically after the first login. Set the following parameters using the Wizard:

- Internet connection type (*Step 2*) — type of interface via which the firewall is connected to the Internet
- Internet interface (*Step 3*) — select an Internet interface or appropriate dial-up. Supply the username and password for the appropriate account if the selected type is a dial-up connection.

In case of dial-up connection, *WinRoute* requires a corresponding username and password. Specification of this login data is not required if the information is already saved in the operating system. If not (or if you are unsure that this data is really

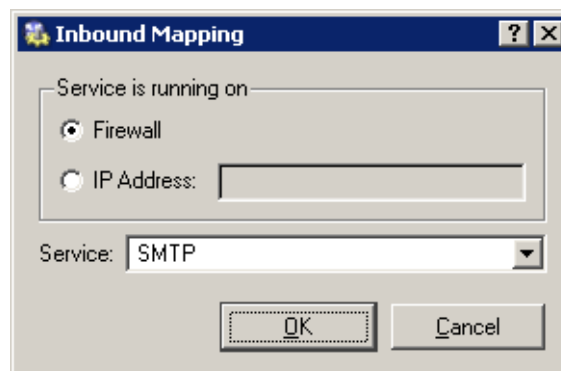
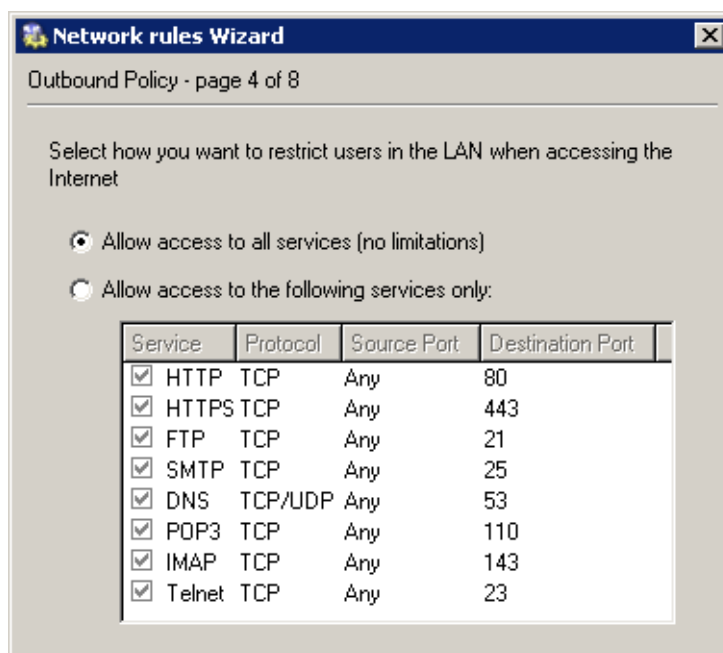
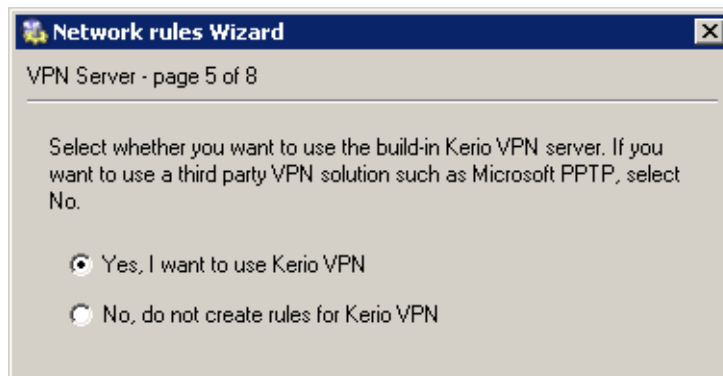
Chapter 2 Headquarters configuration



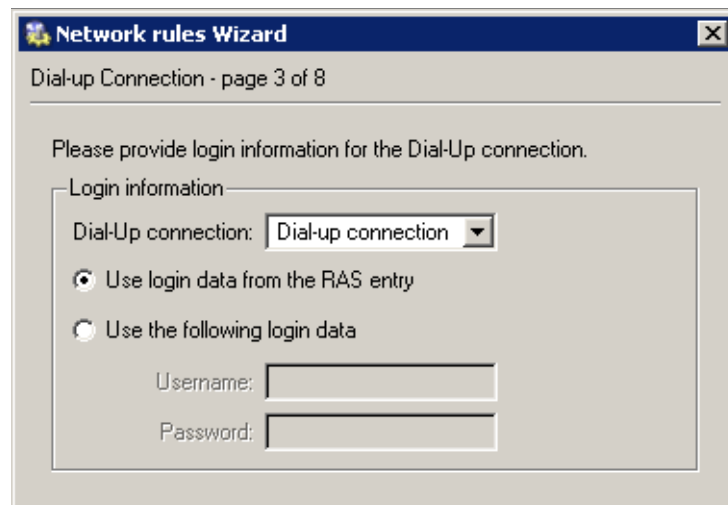
saved), select *Use the following login data* and specify a *Username* and *Password* for a corresponding dial-up connection.

- Rules used for outgoing traffic (*Step 4*) — these rules enable access to Internet services.
- *VPN Server* policy (*Step 5*) — check *Yes, I want to use Kerio VPN* to create rules that will enable interconnection of the headquarters with branch offices as well as connections of remote clients (refer to chapter 3).
- Rules for incoming traffic (*Step 6*) — for example, a mapping to an SMTP (email) server

2.3 Basic Traffic Policy Configuration

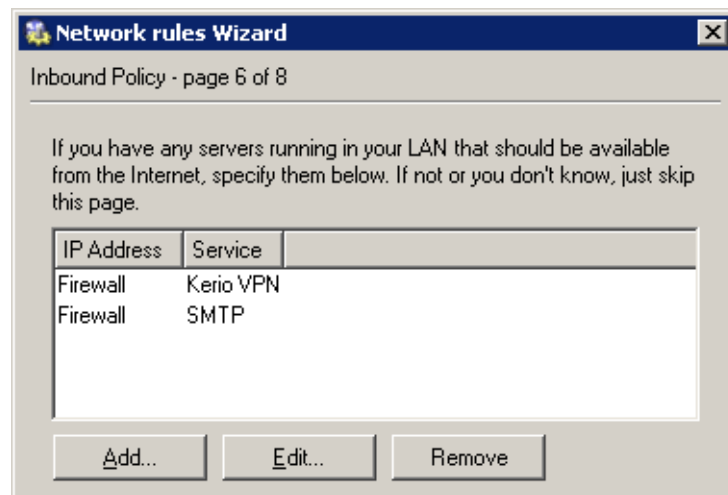


Chapter 2 Headquarters configuration



Note: In this step you can also define mapping for other hosted services such as an FTP server. This will be better understood through the second method — custom rule definition. For details refer to chapter 2.11.

- Sharing of the Internet connection (*Step 7*) — network address translation (NAT) must be enabled if private IP addresses will be used within the LAN



2.4 DHCP Server Configuration

Example Notes

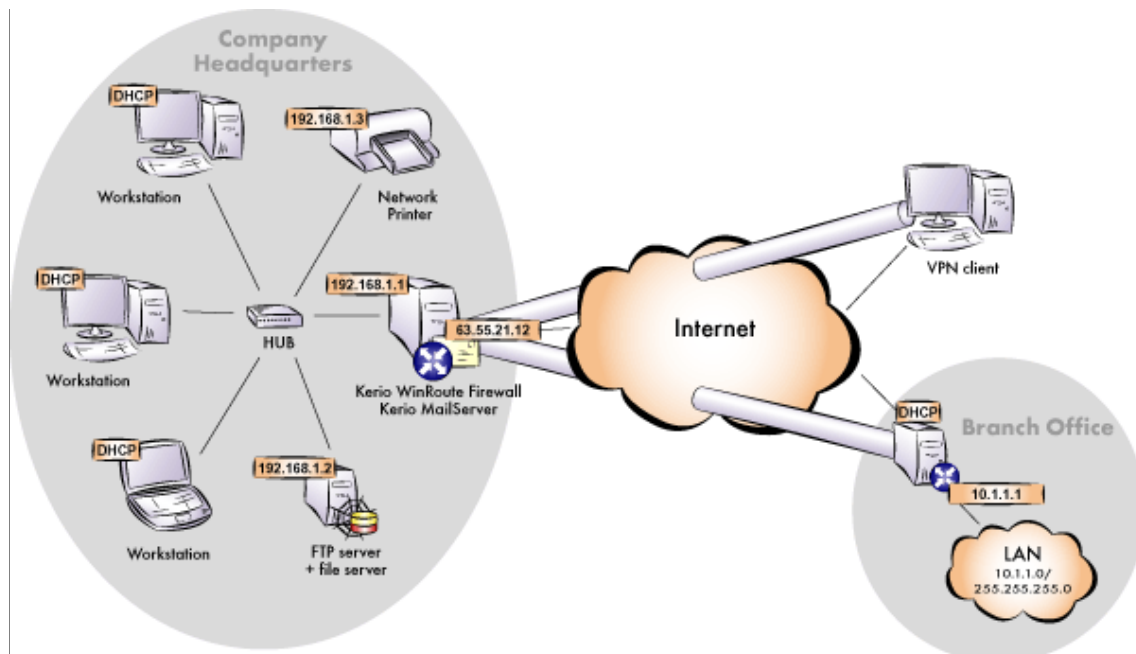
The following methods can be used to assign IP addresses to local hosts:

- The 192.168.1.2 static IP address will be assigned to the file server / FTP server (its IP address must not be changed, otherwise mapping from the Internet will not work).
- A Static IP address will be assigned to the network printer by the DHCP server (DHCP lease). Printing machines cannot have dynamic IP addresses, otherwise they would be unavailable from clients if the IP changes.

Note: IP addresses can be assigned to printing machines either manually or by a DHCP server. If a DHCP server is used, the printing machine is configured automatically and its address is listed in the DHCP lease list. If configured manually, the printing machine will be independent of the DHCP server's availability.

- Dynamic IP addresses will be assigned to local workstations (easier configuration).

The company.com DNS domain will be used in the local network.



Note: IP addresses 10.1.1.x with the mask 255.255.255.0 and the fil-ial.com DNS domain will be used in the network of the branch office.

Chapter 2 Headquarters configuration

DHCP Server Configuration

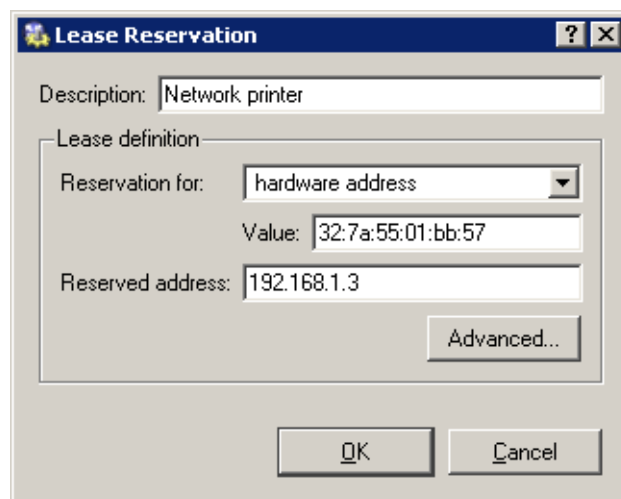
Go to the *Configuration / DHCP server* section in *Kerio Administration Console*. Open the *Scopes* tab to create an IP scope for hosts to which addresses will be assigned dynamically (the *Add / Scope* option). The following parameters must be specified to define address scopes:

- *First address* — select 192.168.1.10 (addresses from 192.168.1.1 to 192.168.1.9 will be reserved for servers and printing machines)
- *Last address* — 192.168.1.254 (address with the highest number that can be used for the particular network)
- *Network mask* — 255.255.255.0
- *Default gateway* — IP address of the firewall interface that is connected to the local network (192.168.1.1).

Note: Default gateway specifies the route via which packets from the local network will be routed to the Internet. Routing via *WinRoute* will enable traffic filtering, user authentication, etc.

- *DNS server* — IP address of the firewall interface that is connected to the local network (see chapter 2.5)

Create a lease for the network printing machine using the *Add / Reservation...* option. The address you reserve need not necessarily belong to the scope described above, however, it must belong to the specified network (in this example the 192.168.1.3 address is reserved). You need to know the hardware (MAC) address of the printing machine to make the reservation.



2.4 DHCP Server Configuration

The screenshot shows the 'Address Scope' dialog box with the following configuration:

- Description: Local network
- Scope definition:
 - First address: 192.168.1.10
 - Last address: 192.168.1.254
 - Network mask: 255.255.255.0
 - Lease time: 4 day(s) 0 : 0
- Options:
 - Default gateway: 192.168.1.1 (checked)
 - Domain name server: 192.168.1.1 (checked)
 - WINS name server: (unchecked)
 - Domain name: company.com (checked)

TIP: Do not make the reservation manually unless you know the hardware address of your printing machine. Run the DHCP server and connect the machine to the network. An IP address from the formerly defined scope (see above) will be assigned to the printing machine. Mark this address in the *Leases* tab and use the *Reserve...* button to open a dialog where the appropriate hardware address will be already defined. Insert the appropriate IP address (and its description if desirable) and click on the *OK* button. Restart your printing machine. The appropriate IP address will be assigned to the printing machine by the DHCP server after the restart.

Notes:

1. Do not use the DHCP server unless all desired scopes and reservations are made or unless you need to determine a client's MAC address (see above).
2. You can also use another DHCP server to detect settings of your network equipment automatically. Set the firewall computer's internal IP address as the default gateway and DNS server in parameters for this range on the DHCP server.

2.5 DNS Forwarder Configuration

Go to *Configuration / DNS Forwarder* to configure DNS servers to which DNS queries will be forwarded. Check the *Forward DNS queries to the specified DNS servers* alternative and specify one or multiple DNS servers in the Internet. DNS servers of your Internet connection provider are the most convenient ones for this purpose (best availability). To get their IP addresses, contact the provider.

Warning: Automatic selection of DNS servers cannot be used since the DNS server at the interface connected to the local network uses the same IP address as the DNS server at the firewall (see chapter 2.1)— DNS servers must always be specified in the *DNS Forwarder*, otherwise the *DNS Forwarder* will not function well.

DNS Forwarder

Enable DNS forwarding

DNS forwarding

Forward DNS queries to the server automatically selected from DNS servers known to the operating system

Forward DNS queries to the specified DNS server(s)

DNS Server(s): Use semicolons (;) to separate individual entries

Enable cache for faster response to repeated queries

Use custom forwarding

Simple DNS resolution

Before forwarding a query, try to find name in:

'hosts' file

DHCP lease table

When resolving name from 'hosts' file or lease table combine it with DNS domain below:

Advanced parameters of the *DNS Forwarder*:

- It is recommended to enable the *Enable cache...* option (this will fasten responses to repeated DNS queries).
- Enable the *Use custom forwarding* option to set parameters necessary for correct forwarding of DNS queries between the headquarters network and networks of branch

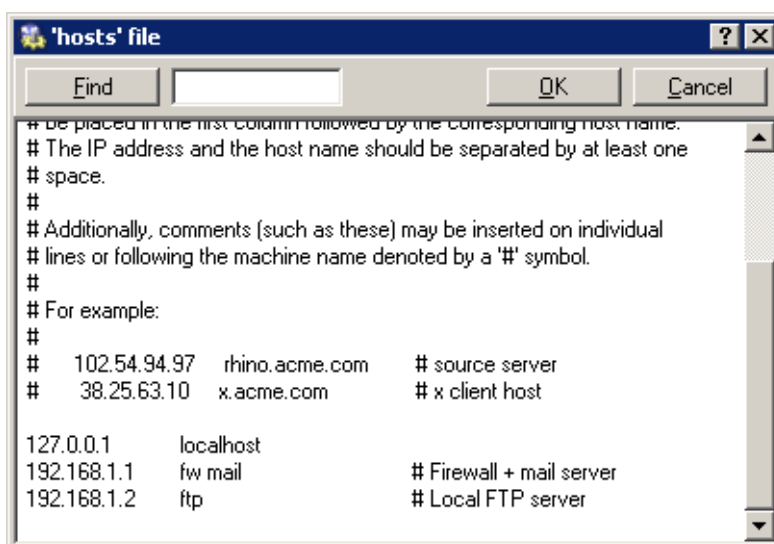
2.6 Creating User Accounts and Groups

offices. For detailed description on these settings, refer to chapter 3.1 (or to chapter 3.2).

- Both the *'hosts' file* and the *DHCP lease table* options must be enabled (the *DNS Forwarder* uses the hosts file and/or the DHCP lease table to search for names and IP addresses of local hosts).

Use the *When resolving name...* entry to specify the *company.com* local DNS domain. *DNS Forwarder* will then be able to respond correctly to queries regarding hostnames in local network (e.g. fw) as well as their full DNS names(e.g. fw.company.com).

Use the *Edit file...* button to edit the hosts system file. In this dialog, specify all IP addresses and hostnames of hosts to which IP addresses have been assigned manually (including the firewall).



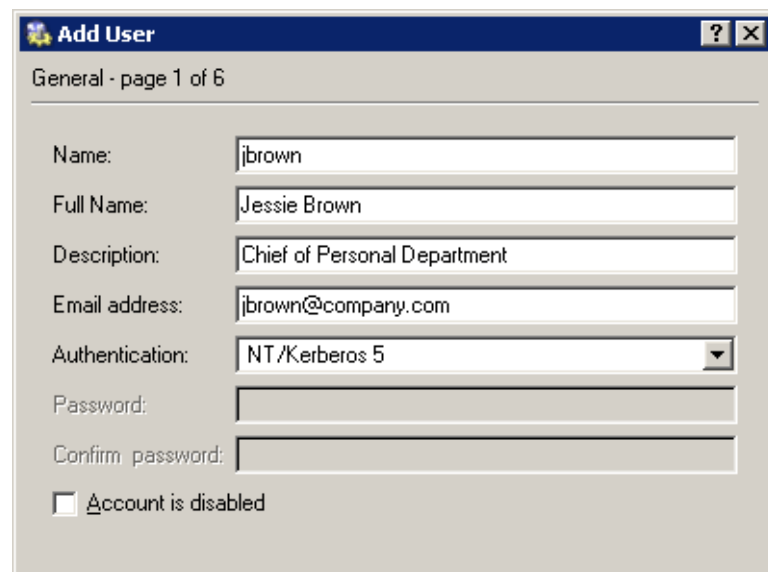
2.6 Creating User Accounts and Groups

Go to the *Users and Groups / Users* section to create user accounts for all users within the local network.

If a Windows NT or Windows 2000 domain is used in the local domain, user accounts can be imported and/or configured in this domain. All users will have an identical username and password to access all network resources.

Name of the Windows NT/Windows 2000 domain must be defined in the appropriate entry in *Advanced Options / User Authentication*.

Chapter 2 Headquarters configuration



Add User [?] [X]

General - page 1 of 6

Name:

Full Name:

Description:

Email address:

Authentication:

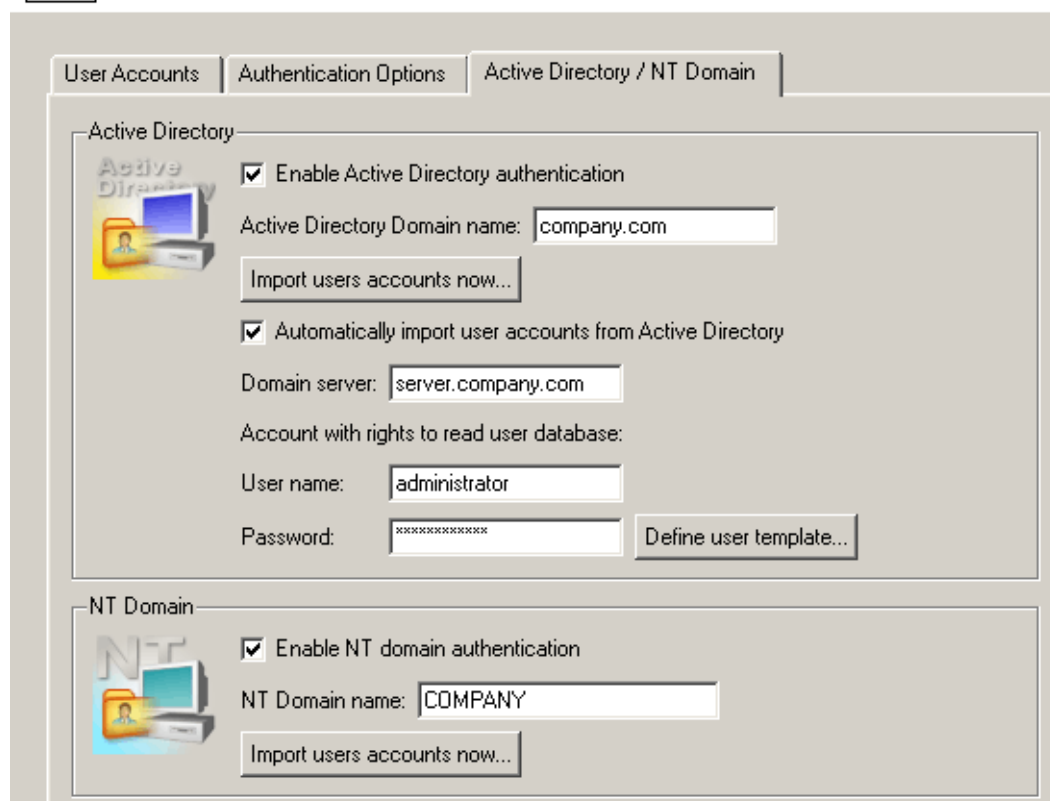
Password:

Confirm password:

Account is disabled



Users



User Accounts | Authentication Options | **Active Directory / NT Domain**

Active Directory

Enable Active Directory authentication

Active Directory Domain name:

Automatically import user accounts from Active Directory

Domain server:

Account with rights to read user database:

User name:

Password:

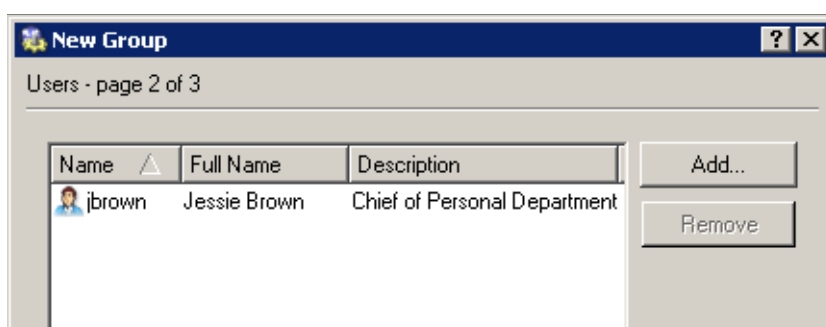
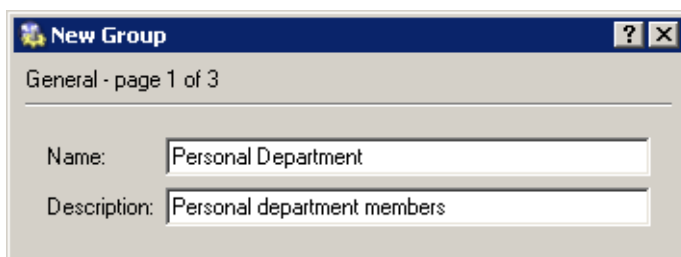
NT Domain

Enable NT domain authentication

NT Domain name:

2.7 Address Groups and Time Ranges

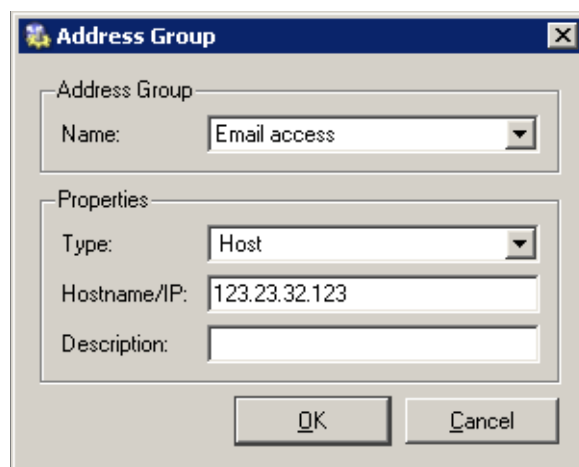
Go to *Users and Groups / Groups* to create user groups that will be used to control user access to the Internet. Sort users into appropriate groups.



2.7 Address Groups and Time Ranges

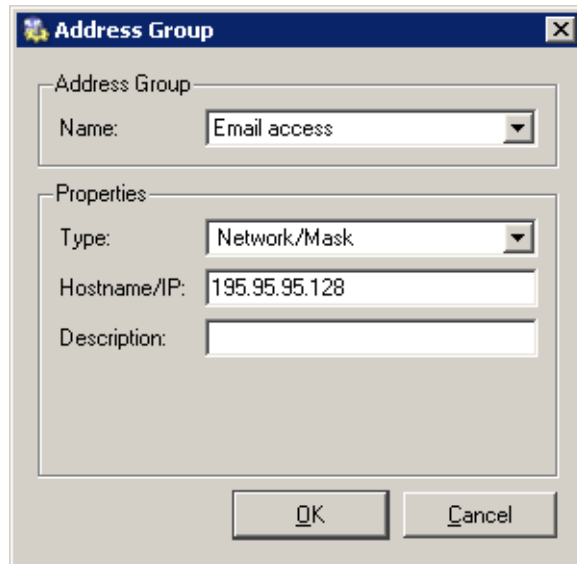
Open the *Definitions / Address Groups* section to create IP groups that will be used to limit access to email accounts (refer to chapter 2.11). This group will consist of the 123.23.32.123 and 50.60.70.80 IP addresses and of the entire 195.95.95.128 network with the 255.255.255.248 network mask.

Adding an IP address:



Chapter 2 Headquarters configuration

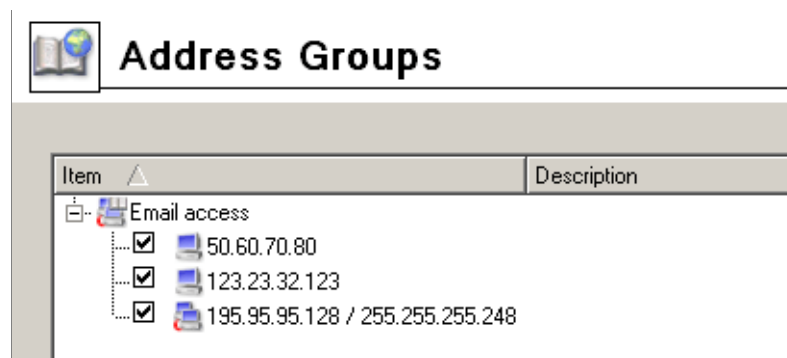
Adding a network:



The screenshot shows a dialog box titled "Address Group". It has a "Name" field with a dropdown menu set to "Email access". Below this is a "Properties" section with three fields: "Type" (dropdown menu set to "Network/Mask"), "Hostname/IP" (text field containing "195.95.95.128"), and "Description" (empty text field). At the bottom of the dialog are "OK" and "Cancel" buttons.

Note: Name must be identical for all items so that all items will be added to the same group.

Resultant address group:

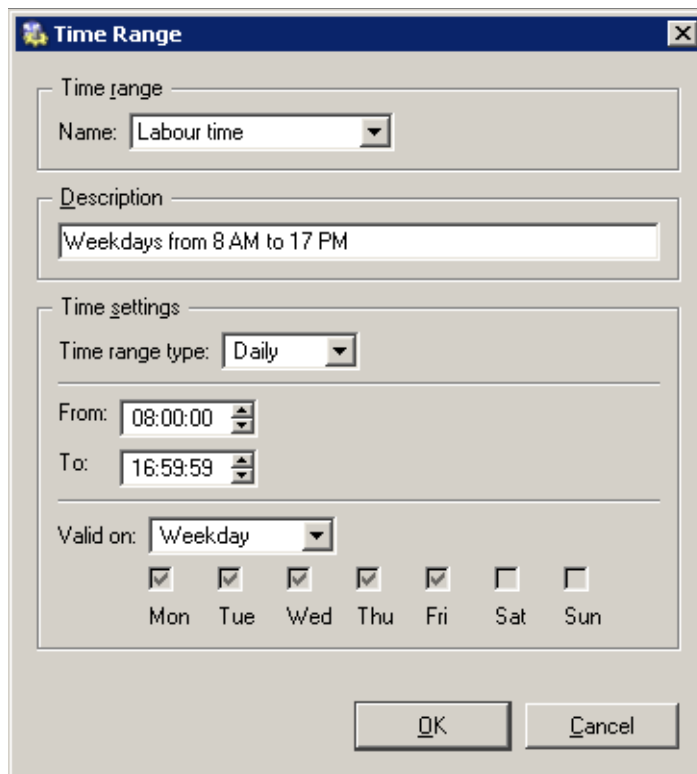


Go to *Definitions / Time Ranges* to create a group that will be limited to accessing Internet services during the labor hours (from Monday to Friday from 8 A.M. to 4:30 P.M., Saturdays and Sundays from 8 A.M. to 12 A.M.).

Labor time definition working days (from Monday to Friday):

Labor time definition for weekends (Saturday and Sunday):

2.7 Address Groups and Time Ranges



Time Range

Time range

Name: Labour time

Description

Weekdays from 8 AM to 17 PM

Time settings

Time range type: Daily

From: 08:00:00

To: 16:59:59

Valid on: Weekday

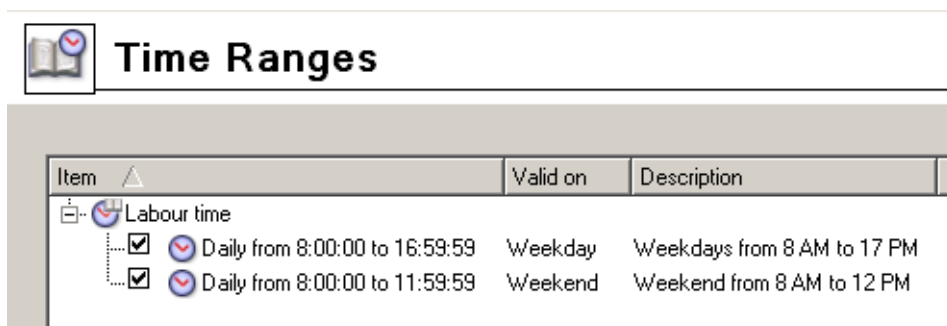
Mon Tue Wed Thu Fri Sat Sun

OK Cancel

Notes:

1. You can use predefined day groups (*Weekday* or *Weekend*) to define the *Valid on* entry — it is not necessary to tick each day individually.
2. The *Name* entries must be identical so that only one time range will be created.

This is the result *Labor time* time range:



Item	Valid on	Description
Labour time		
<input checked="" type="checkbox"/> Daily from 8:00:00 to 16:59:59	Weekday	Weekdays from 8 AM to 17 PM
<input checked="" type="checkbox"/> Daily from 8:00:00 to 11:59:59	Weekend	Weekend from 8 AM to 12 PM

Chapter 2 Headquarters configuration

The screenshot shows a 'Time Range' dialog box with the following configuration:

- Name:** Labour time
- Description:** Weekend from 8 AM to 12 PM
- Time range type:** Daily
- From:** 08:00:00
- To:** 11:59:59
- Valid on:** Weekend
- Days:** Mon, Tue, Wed, Thu, Fri, Sat, Sun

User accounts

Go to the *Users and Groups / Users* section to create user accounts for all users within the local network.

If a Windows NT or Windows 2000/2003 (Active Directory) domain is used in the local domain, user accounts can be imported and/or authenticated in this domain. All users will have an identical username and password to access all network resources.

Assign access rights for the VPN server to each user who will connect remotely to the local network (as a VPN client — see chapter 2.12).

If you intend to use authentication through Windows NT or Active Directory, enable this authentication and specify a corresponding domain in the *Active Directory / NT domain* tab.

TIPS:

1. It is also possible to import user accounts from an NT domain or from Active Directory (i.e. to download users from the domain and generate user accounts in

2.7 Address Groups and Time Ranges

The screenshot shows the 'Users' configuration window in WinRoute. The 'Active Directory / NT Domain' tab is active. Under the 'Active Directory' section, the following options are visible:

- Enable Active Directory authentication
- Active Directory Domain name:
-
- Automatically import user accounts from Active Directory
- Domain server:
- Account with rights to read user database:
 - User name:
 - Password:
 -

Under the 'NT Domain' section, the following options are visible:

- Enable NT domain authentication
- NT Domain name:
-

WinRoute). This operation may save valuable time and reduces the volume of effort required for the administration.

2. For the Active Directory, automatic import of user accounts is available. This function requires the name or IP address of a corresponding domain server as well as user authentication through username and password (any user login data belonging to the particular domain can be used). It is also possible to define a template which will be used for setting specific *WinRoute* related parameters (such as groups, rights, quotas, etc.) to the imported users. Individual user accounts will be generated automatically upon the first successful login of a corresponding user.

User groups

Go to the *Users and Groups / Groups* section to create groups of users which will be later used for maintenance of user access to the Internet. Select users for each group.

Chapter 2 Headquarters configuration

Add User ? X

Rights - page 3 of 6

User Rights

- No access to administration
- Read only access to administration
- Full access to administration

Additional Rights

- User can override WWW content rules
- User can unlock URL rules
- User can dial RAS connection
- User can connect using VPN
- User is allowed to use P2P networks

Add User ? X

General - page 1 of 6

Name:

Full Name:

Description:

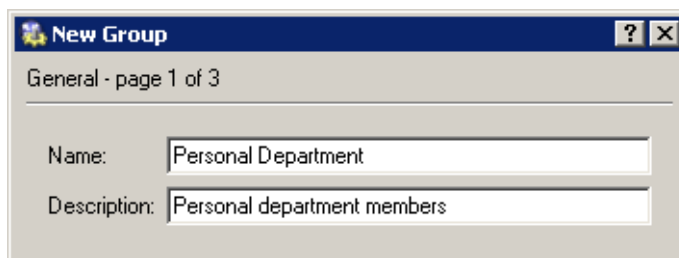
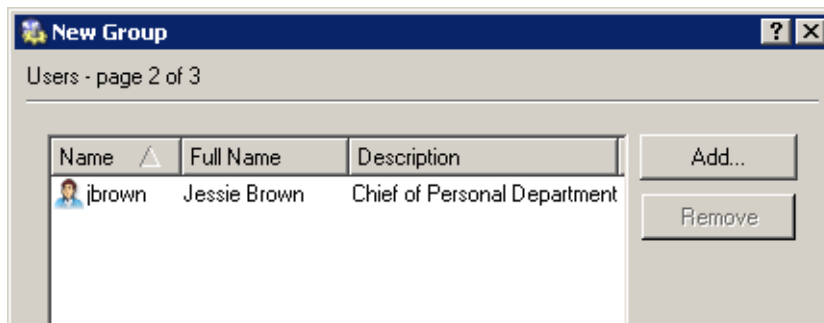
Email address:

Authentication:

Password:

Confirm password:

Account is disabled



2.8 Web Rules Definition

Requirements

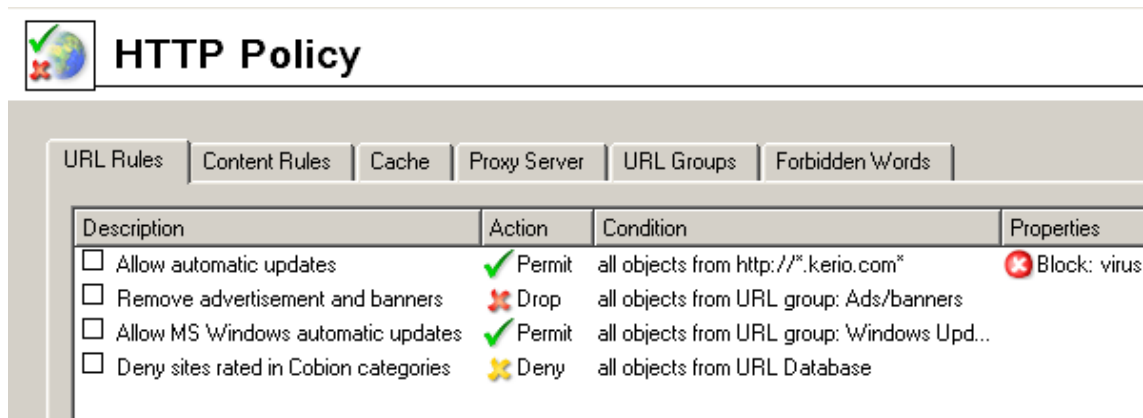
Access to Web pages will be limited by the following restrictions:

- filtering of advertisements included in Web pages
- access to pages with erotic/sexual content is denied
- access to Web pages that offer jobs is denied (only users working in Personal Departments are allowed to access these pages)
- user authentication will be required before access to the Internet is allowed (this way you can monitor which pages are opened by each user)

Predefined HTTP Rules

The following basic HTTP rules are already predefined and available in the *URL Rules* tab in *Configuration / Content Filtering / HTTP Policy*:

Allow automatic updates This rule allows automatic updates of *WinRoute* and the *McAfee* antivirus from the Kerio Technologies website. This rule can be helpful if rules denying automatic updates are defined.



Remove advertisement and banners Filtering of advertisements and banners. According to this rule all objects matching with the predefined *Ads/banners* URL group are dropped. Tick this rule to activate it.

Note: It might happen that a page that does not represent any advertisement is dropped. If so, remove an appropriate item (the one that causes the problem) from the *Ads/banners* group or add an exceptional rule for particular pages (we recommend using the second method).

Allow MS Windows automatic updates The rule allows automatic updates of Windows operating systems from Microsoft's servers. This rule can be helpful if rules denying automatic updates are defined.

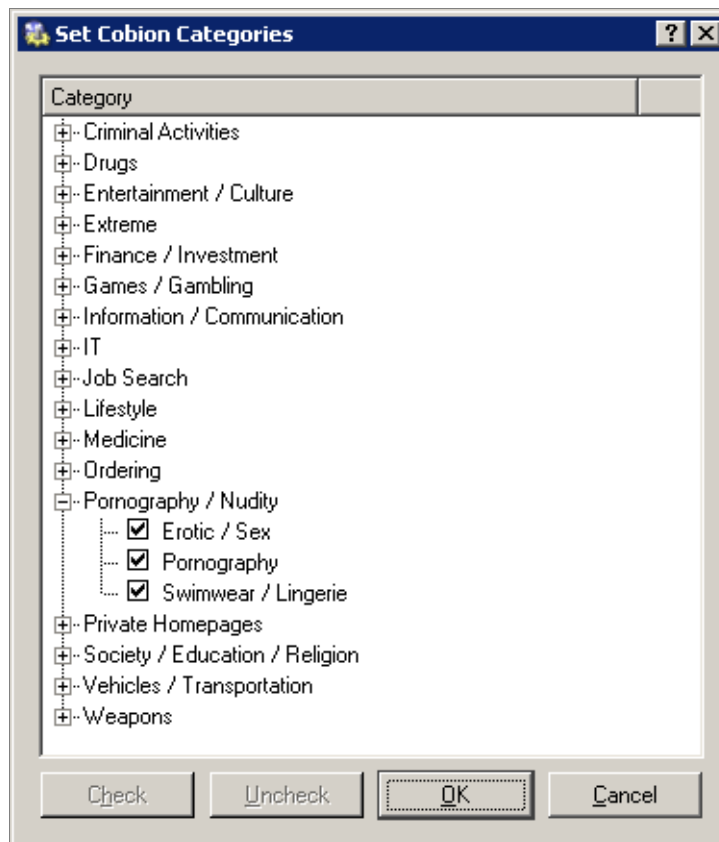
Deny sites rated in Cobion categories This rule denies access to Web sites that match selected *Cobion Orange Filter* module categories.

Use the *Select Rating...* button to select categories that will be blocked first. Select appropriate categories in the *Pornography* section to deny access to pages with erotic/sexual content.

Notes:

1. The basic *WinRoute* license does not provide the *Cobion* system (a special license version must be purchased). However, this system is available in the *WinRoute* trial version.
2. The *Cobion* system included in *WinRoute* must communicate with specific Internet database servers. This means that the traffic policy must enable access to the *COFS* service (6000/tcp) from the firewall. Traffic rules created by the Wizard allow all traffic from the firewall to the Internet — it is not necessary to define a new rule.

2.8 Web Rules Definition



3. You can define multiple URL rules that will use the *Cobion Orange Filter* rating technology. Multiple categories may be used for each rule.
4. We recommend you to enable the “unlock” option in rules that use the *Cobion Orange Filter* rating technology as a page may be classified incorrectly and useful information might be blocked under certain conditions. All unlock queries are logged into the *Filter* log — here you can monitor whether unlock queries were appropriate or not.

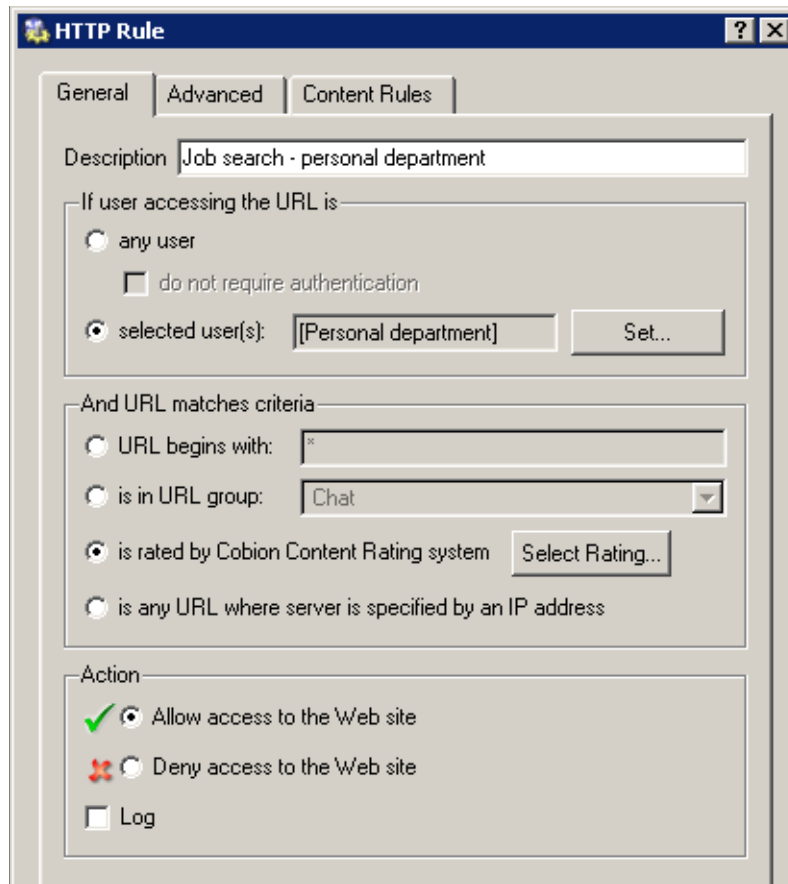
Note: You can insert the information that will be displayed in the *Advanced* tab (URL Rules) or forward users to another page when an attempt for connection to a denied page is detected.

Creating Custom URL Rules

Rules that will be used for certain users or user groups may be added after the rule that requires authentication for all users.

Chapter 2 Headquarters configuration

You can add a rule that will enable users belonging to the *Personal Department* group to access pages where jobs are offered.



A rule that will deny all users to access pages with job offers must be added after the previous rule.

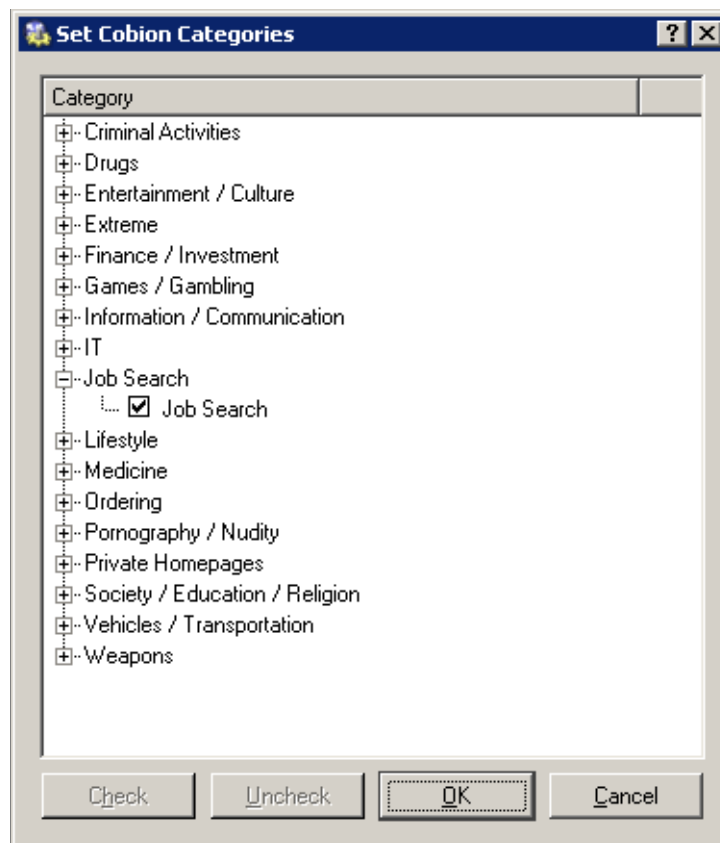
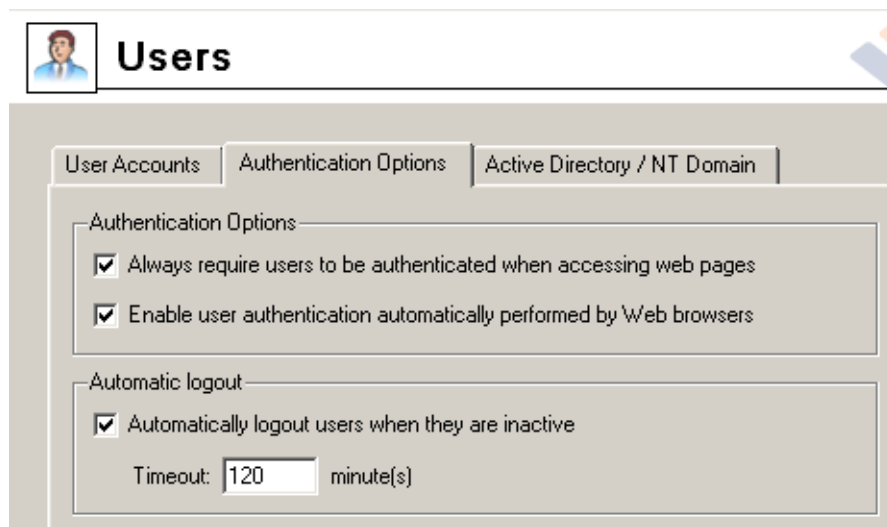
Notes:

1. It is recommended to enable the *do not require authentication* option in the rule which denies access for all users, otherwise unauthenticated users attempting to open a denied page will be forwarded to the login page before receiving the denial page.
2. In both rules mentioned above only the *JobSearch* category is selected.

User authentication for accessing Websites

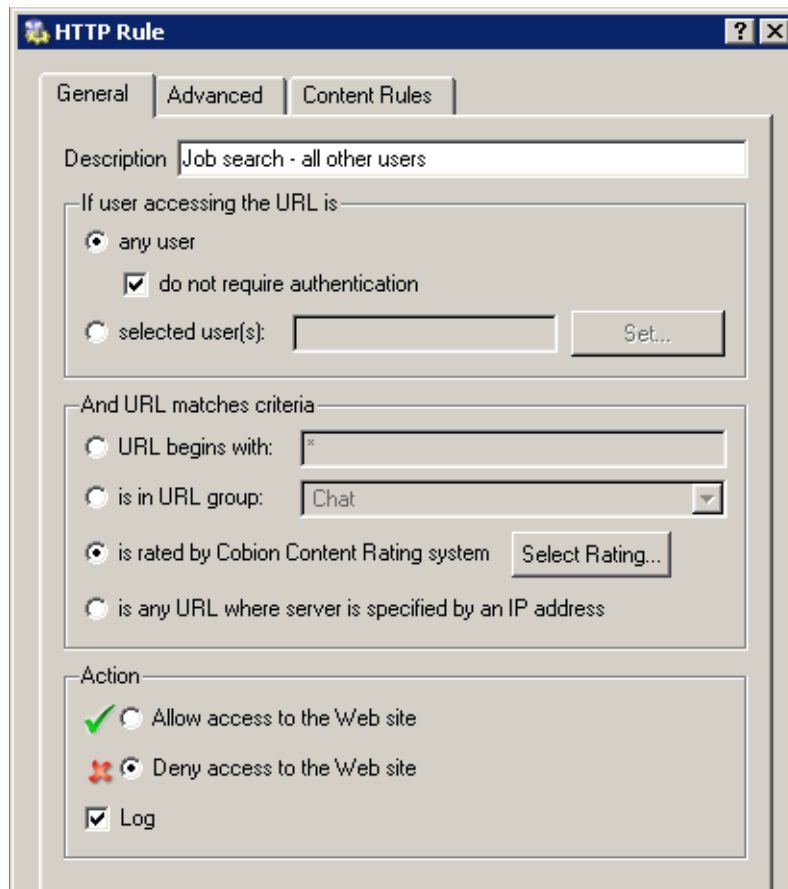
The last optional restriction is user authentication while accessing Web pages. To enable this authentication, use the *Always require users to be authenticated when accessing web pages* option in the *Authentication Options* tab under *Users and groups / Users*.

2.8 Web Rules Definition



HTTP Cache Configuration

Cache accelerates access to repeatedly opened Web pages, thus reducing Internet traffic. Cache can be enabled from the *Enable cache on transparent proxy* and the *Enable cache*



on proxy server options in *Configuration / Content Filtering / HTTP Policy*. Set the cache to the desirable size with respect to the free memory on the disc using the *Cache size* entry. The 1 GB (1024 MB) value is set by the default, the maximum value is 2 GB (2048 MB).

2.9 FTP Policy Configuration

Requirements

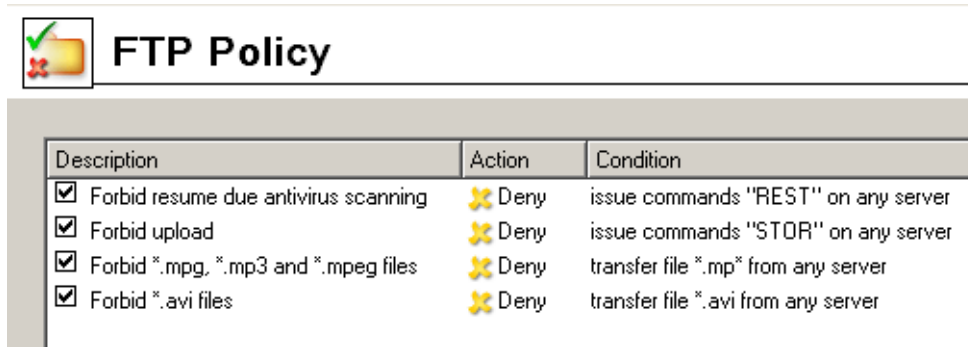
FTP usage will be limited by the following restrictions:

- transmission of music files in the MP3 format will be denied
- transmission of video files (*.avi) will be denied during labor time
- uploads (storing files at FTP servers) will be denied — protection of important company information

2.9 FTP Policy Configuration

Predefined FTP Rules

Go to *Configuration / Content Filtering / FTP Policy* to set FTP limitations. The following rules are predefined rules and can be used for all intended restrictions.



Description	Action	Condition
<input checked="" type="checkbox"/> Forbid resume due antivirus scanning	Deny	issue commands "REST" on any server
<input checked="" type="checkbox"/> Forbid upload	Deny	issue commands "STOR" on any server
<input checked="" type="checkbox"/> Forbid *.mpg, *.mp3 and *.mpeg files	Deny	transfer file *.mp* from any server
<input checked="" type="checkbox"/> Forbid *.avi files	Deny	transfer file *.avi from any server

Forbid resume due antivirus scanning This rule denies resuming interrupted data transfer (e.g. caused by a network error). If files transmitted by FTP are scanned, it is recommended to enable this rule (files transmitted “in pieces” cannot be reliably scanned).

Forbid upload Deny storing data at FTP servers — this rule is already defined and it is satisfactory to switch it on if you intend to use it.

Forbid *.mpg, *.mp3 and *.mpeg files This option denies transmission of sound files of the listed formats. This rule is already available and it can be enabled easily.

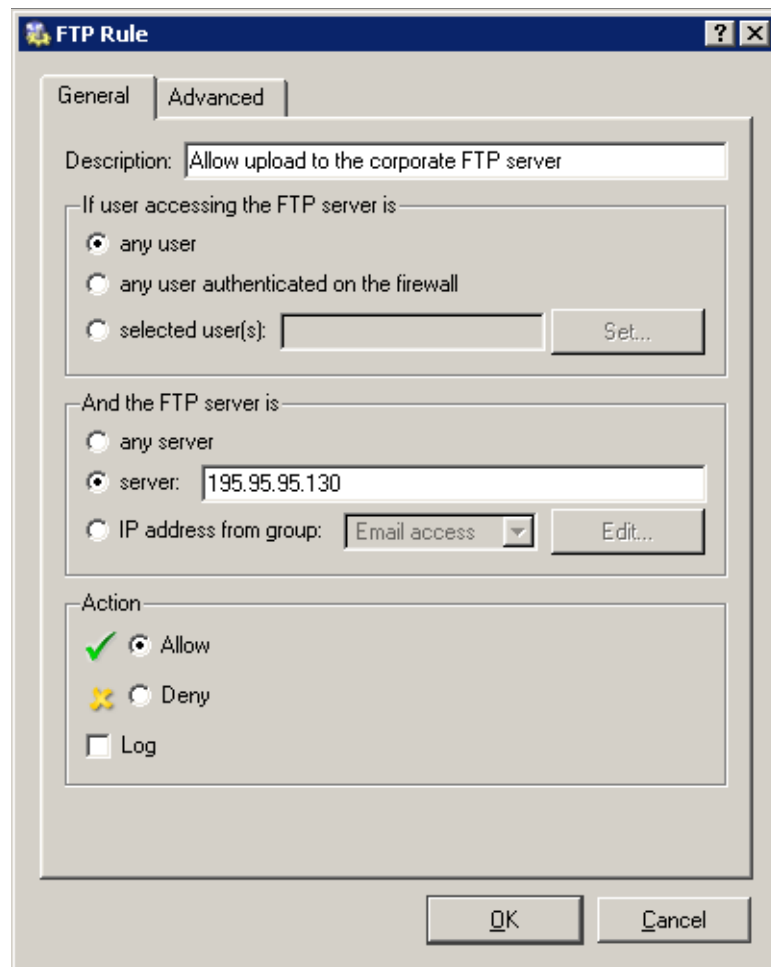
Forbid *.avi files This rule will deny transmission of video files. Enable this rule, use the *Edit* button to open the appropriate dialog and define the *Labor time* time range in the *Advanced* tab.

Warning: The FTP policy refers to all FTP traffic that is processed by the FTP protocol inspector.

In the following example, we intend to enable the local FTP server from the Internet. The *Forbid upload* rule denies even upload to this server which is not always desirable. For this reason we must add a rule that would enable upload to this server before the *Forbid upload* rule.

Notes:

1. The IP address of the host where the appropriate FTP service is running must be used to define the FTP server’s IP address. It is not possible to use only the firewall’s



external IP address from which the FTP server is mapped (IP translation is performed before content filtering rules are applied)!

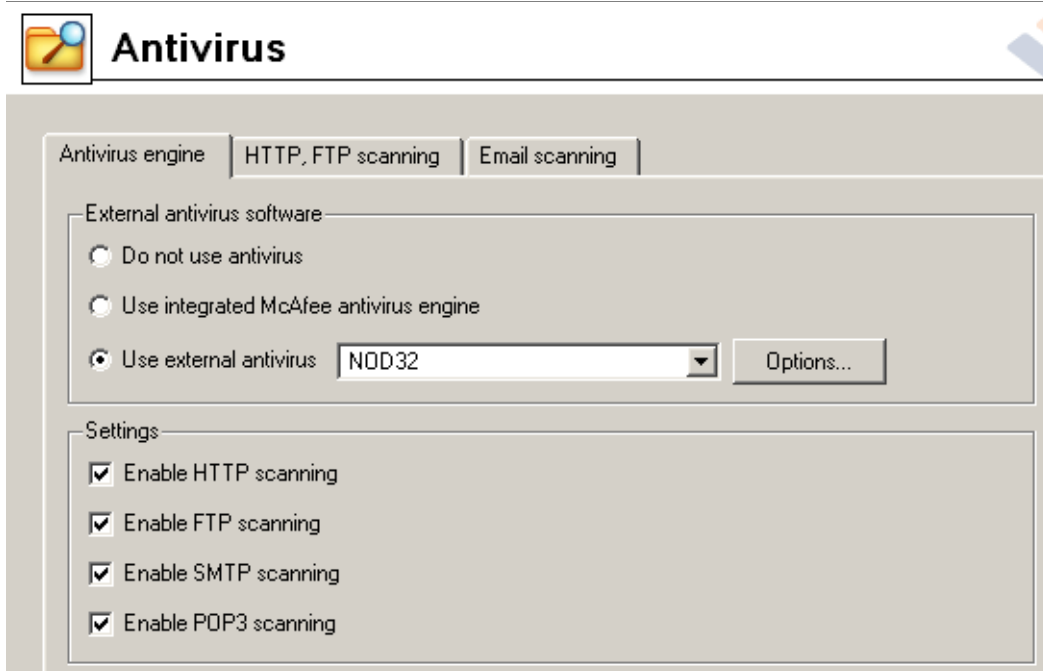
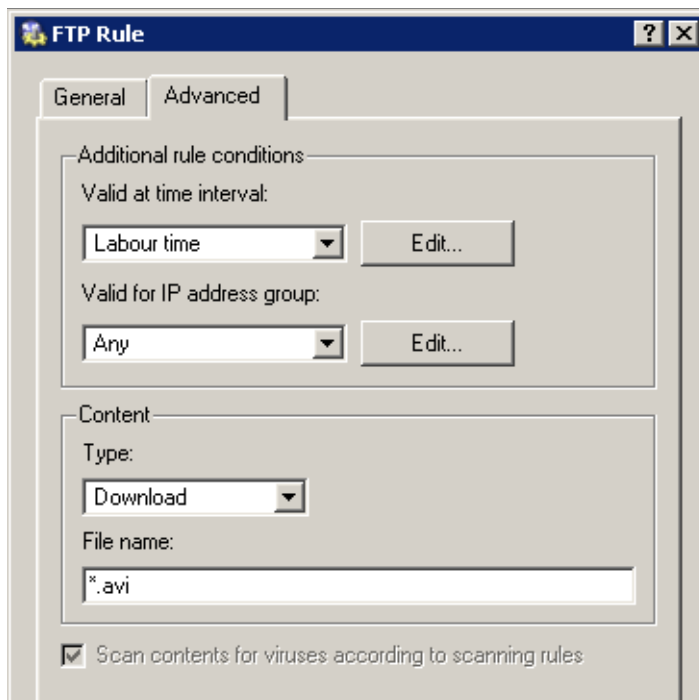
2. The same method can be applied to enable upload to a particular FTP server in the Internet whereas upload to other FTP servers will be forbidden.

2.10 Antivirus Scanning Configuration

Any supported external antivirus application that you intend to use must be installed first. The *McAfee* antivirus application is integrated into *WinRoute* and you will need a special license to run it.

Select an appropriate antivirus application in the *Antivirus* tab under *Configuration / Content Filtering / Antivirus* and choose protocols that will be scanned. All executables and *Microsoft Office* files are scanned by default.

2.10 Antivirus Scanning Configuration










The *HTTP, FTP scanning* and *Email scanning* tabs enable detailed configuration of scanning of individual protocols. Usually, the default settings are convenient.

Chapter 2 Headquarters configuration

2.11 Enabling Access to Services from the Internet

Go to *Configuration / Traffic Policy* to add rules for services that will be available from the Internet.

- access to other mail server services —allowed from certain IP addresses only

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Access to the email	 Email access	 Firewall	 IMAP  IMAPS  POP3  POP3S		

Notes:

1. This rule enables access to *IMAP* and *POP3* services in both encrypted and unencrypted versions — client can select which service they will use.
 2. Based on this example, the *SMTP* service was mapped by the traffic rules Wizard (refer to chapter 2.3) — the appropriate rule already exists.
 3. Access to the *SMTP* service must not be limited to certain IP addresses only as anyone is allowed to send an email to the local domain.
- mapping of the local FTP server

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> FTP server mapping	 Internet	 Firewall	 FTP		MAP 192.168.1.2

Note: Rules are processed from top to bottom. Once a rule is matched, there will be no further processing of filter rules. Therefore, all permission rules must be located prior to denial rules.

2.12 Secured access of remote clients to LAN

Enable the VPN server for secured access of remote clients (“VPN clients”) to LAN in the *Interfaces* tab under *Configuration / Interfaces* (for details, see chapter 3.1). No additional settings are required. Communication of VPN clients is already allowed by the traffic policy created by the wizard — refer to chapter 2.3.

Notes:

- *Kerio VPN Client* must be installed at each remote client to enable their connection to the VPN server in *WinRoute*. Clients will connect to the server at the headquarters

2.13 LAN Hosts Configuration

(i.e. to 63.55.21.12) and they will be authenticated through their usernames and passwords for their *WinRoute* accounts (see chapter 2.6).

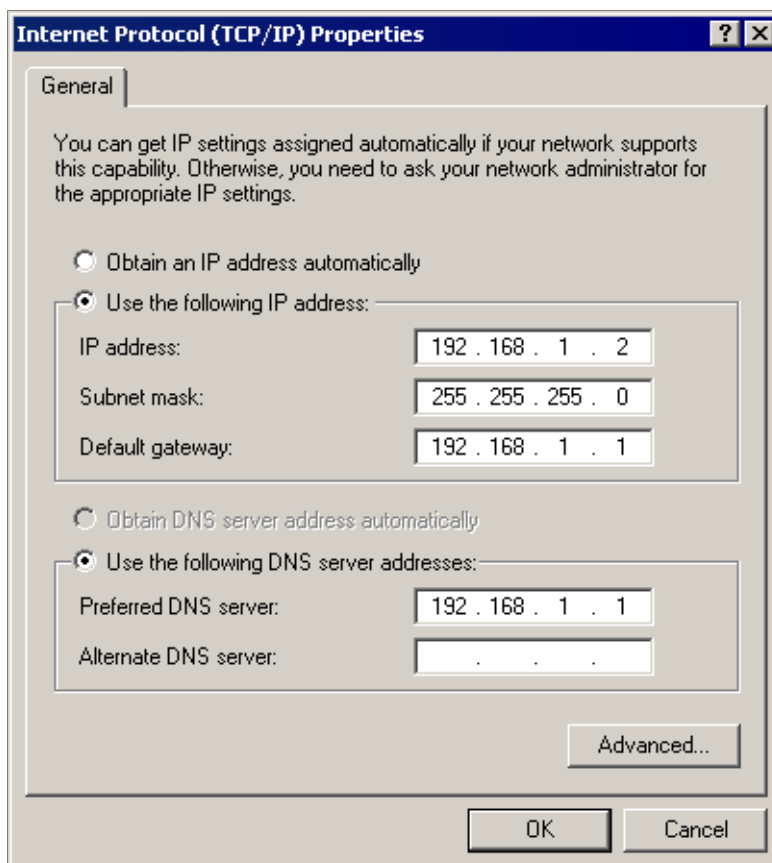
For detailed information, refer to the *Kerio VPN Client — User Guide* document.

- VPN clients will connect only to the headquarters server. No settings for VPN clients are required at the branch office server(s).

2.13 LAN Hosts Configuration

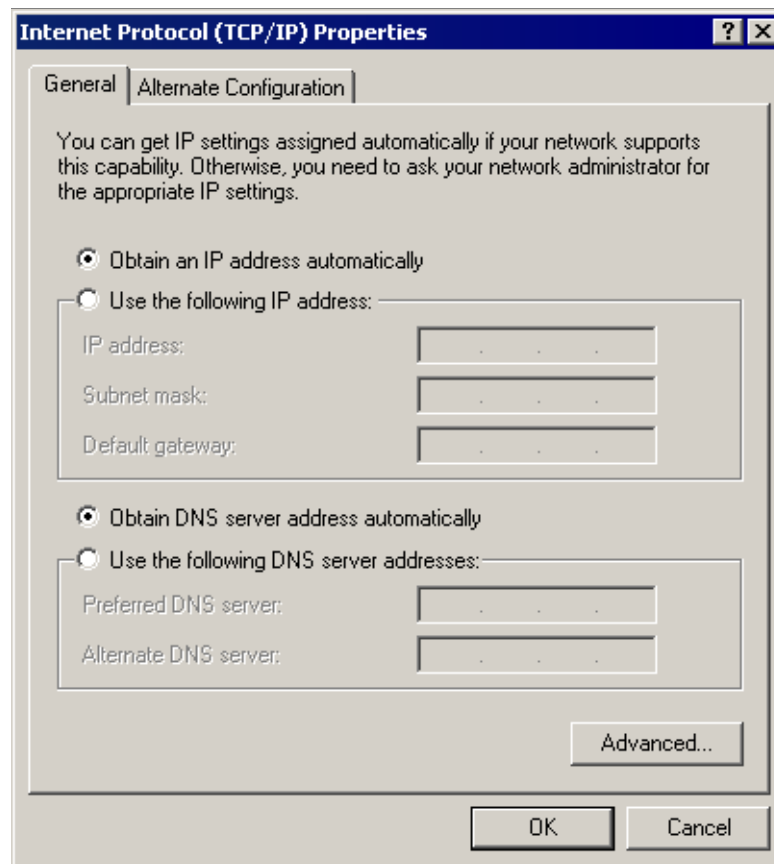
TCP/IP parameters for the hosts that are used as the file server and as the FTP server must be configured manually (its IP address must not be changed):

- *IP address* — we will use the 192.168.1.2 address (refer to chapter 2.4)
- *Default gateway, DNS server* — use IP address of the appropriate firewall interface (192.168.1.1)



Set automatic configuration (using DHCP) at all workstations (it is set by default under most operating systems).

Chapter 2 Headquarters configuration



Chapter 3

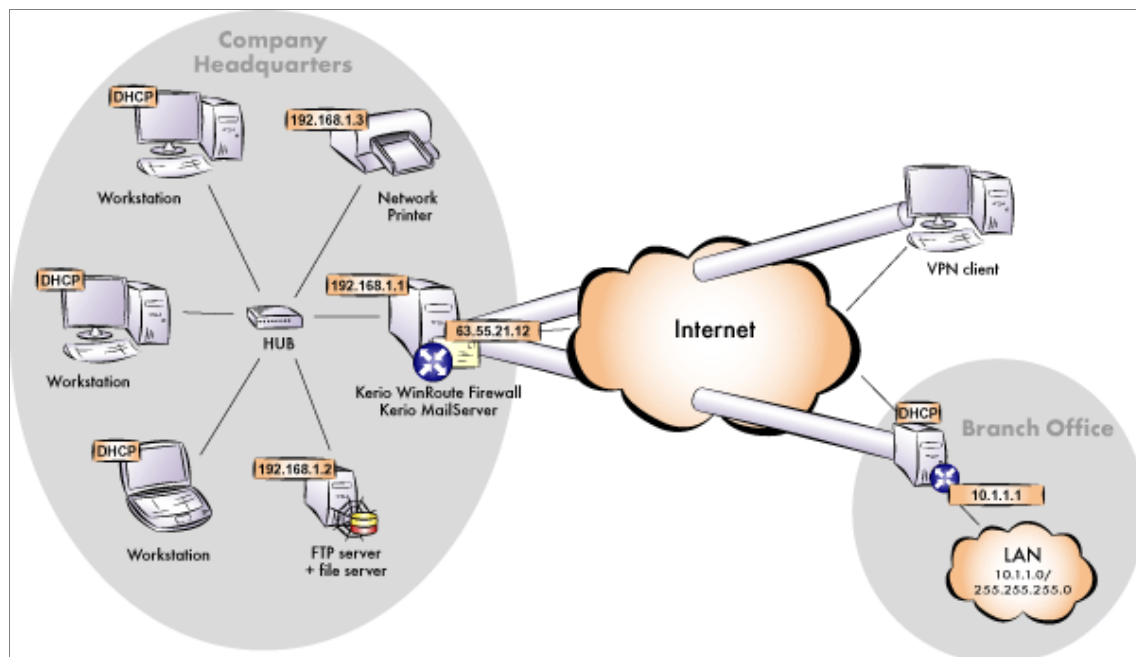
Interconnection of the headquarters and branch offices

This chapter provides information on interconnection of headquarters and branch office servers by an encrypted channel (“VPN tunnel”). The following example describes only the basic configuration of a VPN tunnel between two networks. No tips related to access restrictions or other specific settings are included here. For example of a more complex VPN configuration, refer to the *Kerio WinRoute Firewall — User Guide* document.

The example is divided into two sections: the first one provides guidelines for configuration of the headquarters and the second one describes settings of a branch office. It is supposed that both networks have been already configured as described in chapter 2 and that connection to the Internet is available.

Information related to the example

For better reference, review the figure providing a graphical description of interconnected networks, including their IP addresses.



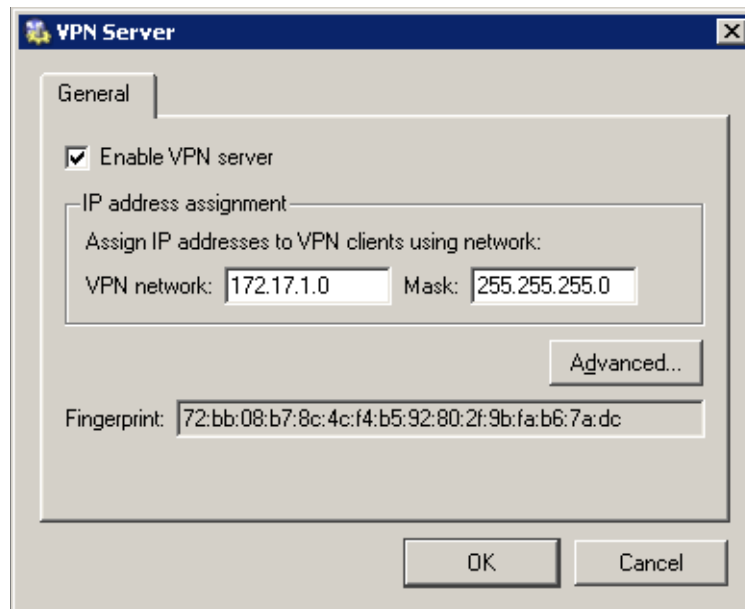
Chapter 3 Interconnection of the headquarters and branch offices

The headquarters uses IP addresses 192.168.1.x with the network mask 255.255.255.0 and with DNS domain company.com. The branch office uses IP addresses 10.1.1.x with network mask 255.255.255.0 and with the subdomain filial.company.com.

3.1 Headquarters configuration

1. Select the *VPN server* item in the *Interfaces* tab under *Configuration / Interfaces*. Double-click it (or use the *Edit* button) to open a dialog where parameters for the VPN server can be set. Check the *Enable VPN server* in the *General* tab.

Note: A selected free subnet is specified automatically in the *VPN network* and *Mask* entries. There is no reason to change the network.



Press *Advanced* and then click on *Change SSL Certificate*. Use the *Generate Certificate* button to generate a SSL certificate of the VPN server (ID of the server).

Note: It is recommended to later replace this generated certificate by a certificate issued by a reliable public certification authority.

2. 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.

3.2 Branch office configuration

- Complete the *Local Traffic* rule (created by the *Network Rules Wizard* — see chapter 2.3) with the VPN tunnel.

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Local Traffic	<ul style="list-style-type: none"> Firewall LAN Tunnel to branch office VPN clients 	<ul style="list-style-type: none"> Firewall LAN Tunnel to branch office VPN clients 	Any	✓
<input checked="" type="checkbox"/> Service Kerio VPN	Internet	Firewall	Kerio VPN	✓

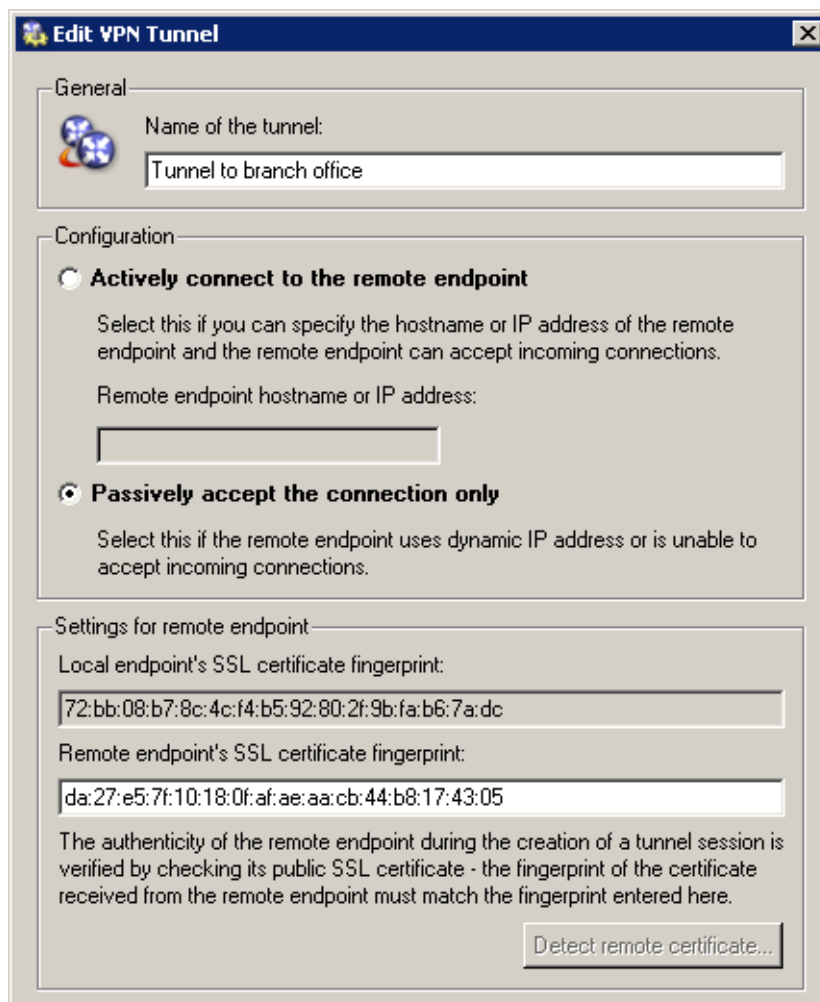
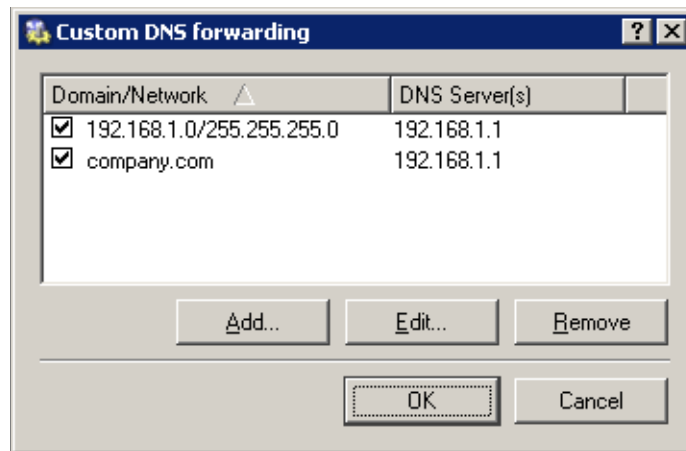
- In the configuration of the *DNS Forwarder* (refer to chapter 2.5), enable the *Use custom forwarding*. Define rules for the `filial.company.com` domain. Specify the server for DNS forwarding by the IP address of the remote firewall host's interface (i.e. interface connected to the local network at the other end of the tunnel).

3.2 Branch office configuration

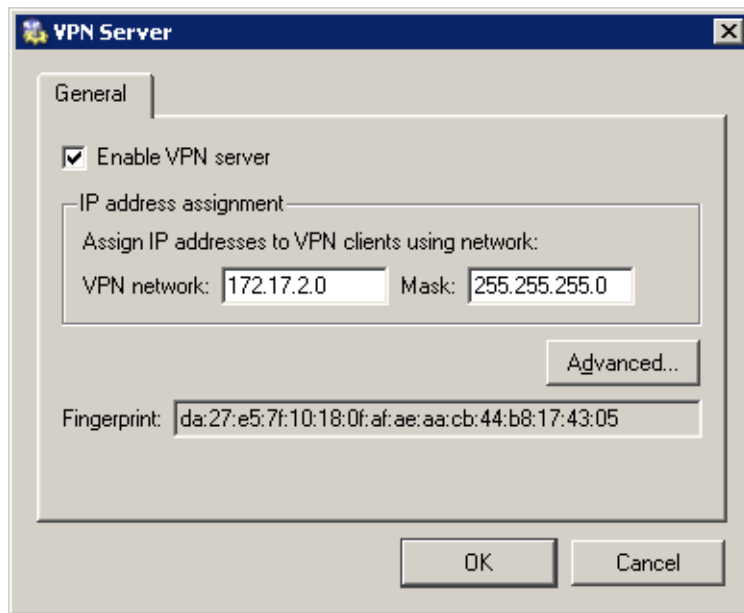
- Select the *VPN server* item in the *Interfaces* tab under *Configuration / Interfaces*. Double-click it (or use the *Edit* button) to open a dialog where parameters for the VPN server can be set. Check the *Enable VPN server* in the *General* tab.

Note: A selected free subnet is specified automatically in the *VPN network* and *Mask* entries. There is no reason to change the network.

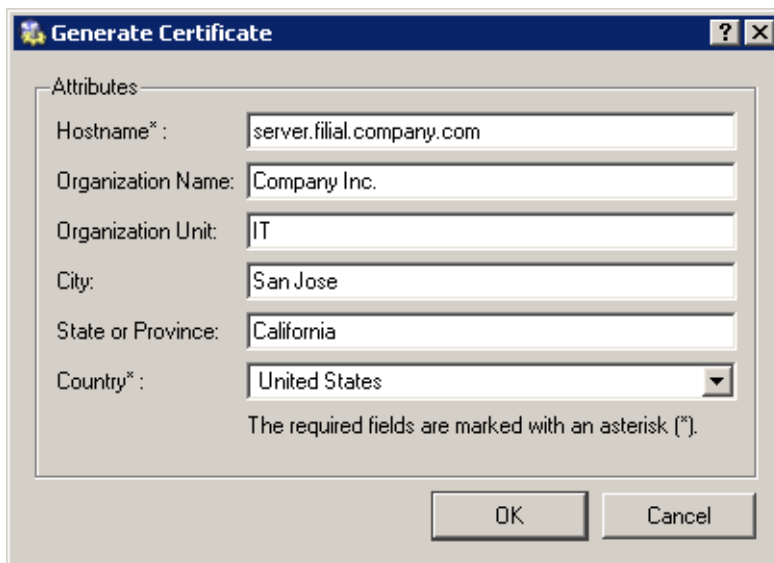
Chapter 3 Interconnection of the headquarters and branch offices



3.2 Branch office configuration



Press *Advanced* and then click on *Change SSL Certificate*. Use the *Generate Certificate* button to generate a SSL certificate of the VPN server (ID of the server).



Note the fingerprint of the generated certificate — it will be required during the definition of the VPN tunnel at the headquarters.

Chapter 3 Interconnection of the headquarters and branch offices

Note: It is recommended to later replace this generated certificate with a certificate authorized by a reliable public certification authority.

2. Create an active end of the VPN tunnel (the branch office server uses a dynamic IP address). The fingerprint of the VPN server certificate can be set simply by clicking on *Detect remote certificate*.

Add VPN Tunnel

General

Name of the tunnel:
Tunnel to company headquarters

Configuration

Actively connect to the remote endpoint
Select this if you can specify the hostname or IP address of the remote endpoint and the remote endpoint can accept incoming connections.
Remote endpoint hostname or IP address:
server.company.com

Passively accept the connection only
Select this if the remote endpoint uses dynamic IP address or is unable to accept 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:
72:bb:08:b7:8c:4c:f4:b5:92:80:2f:9b:fa:b6:7a:dc

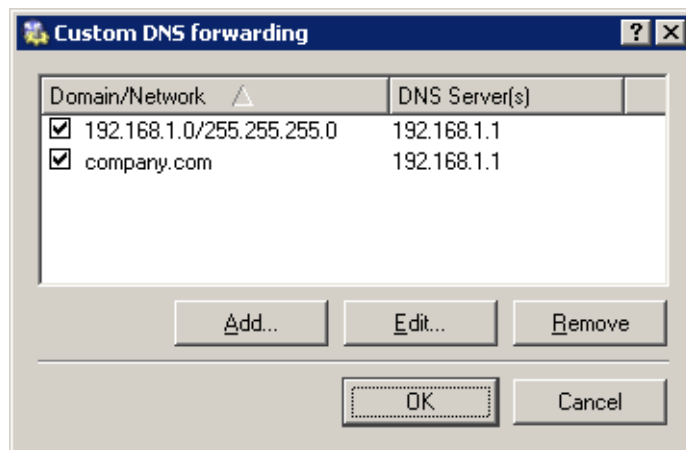
The authenticity of the remote endpoint during the creation of a tunnel session is verified by checking its public SSL certificate - the fingerprint of the certificate received from the remote endpoint must match the fingerprint entered here.

Detect remote certificate...

3. Complete the *Local Traffic* rule (created by the *Network Rules Wizard* — see chapter 2.3) with the VPN tunnel.
4. In the configuration of the *DNS Forwarder* (refer to chapter 2.5), enable the *Use custom forwarding*. Define rules for the *filial.company.com* domain. Specify the server for DNS forwarding by the IP address of the remote firewall host's interface (i.e. interface connected to the local network at the other end of the tunnel).

3.3 VPN test

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Local Traffic	Firewall LAN Tunnel to company headquarters VPN clients	Firewall LAN Tunnel to company headquarters VPN clients	Any	✓
<input checked="" type="checkbox"/> Service Kerio VPN	Internet	Firewall	Kerio VPN	✓



3.3 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` 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.

Note: VPN clients connecting to the headquarters server can access both the headquarters and the branch office (the access is not limited by any restrictions). Therefore, it is recommended to test connection to both networks also from the VPN client.

Chapter 3 Interconnection of the headquarters and branch offices

Chapter 4

Index
