

Kerio WinRoute Firewall 6

Step-by-Step Configuration

© Kerio Technologies. All Rights Reserved.

This guide provides detailed description on configuration of the local network which uses the *Kerio WinRoute Firewall*, version 6.6.0. All additional modifications and updates reserved.

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

Contents

- 1 Introduction 4**
- 2 Headquarters configuration 6**
 - 2.1 Selection of IP addresses for LAN 6
 - 2.2 Configuration of network interfaces of the Internet gateway 7
 - 2.3 WinRoute Installation 9
 - 2.4 Basic Traffic Policy Configuration 10
 - 2.5 DHCP Server Configuration 12
 - 2.6 DNS Forwarder configuration 14
 - 2.7 Web interface and SSL-VPN configuration 16
 - 2.8 Mapping of user accounts and groups from the Active Directory 17
 - 2.9 Address Groups and Time Ranges 20
 - 2.10 Web Rules Definition 22
 - 2.11 FTP Policy Configuration 29
 - 2.12 Antivirus Scanning Configuration 32
 - 2.13 Enabling access to local services from the Internet 32
 - 2.14 Secured access of remote clients to LAN 33
 - 2.15 LAN Hosts Configuration 34
- 3 Configuration of the LAN in a filial office 35**
 - 3.1 Configuration of network interfaces of the Internet gateway 35
 - 3.2 DNS Forwarder Configuration 36
 - 3.3 DHCP Server Configuration 37
- 4 Interconnection of the headquarters and branch offices 39**
 - 4.1 Headquarters configuration 40
 - 4.2 Configuration of a filial office 43
 - 4.3 VPN test 46
- A Legal Notices 47**

Chapter 1

Introduction

This guide describes 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.

Another issue is to provide interconnection of networks between the headquarters and a branch office by a secure (encrypted) channel (so called VPN tunnel) and secure access of clients to the local network via the Internet using *WinRoute*.

This manual provides guidelines for quick setup. Detailed information addressing individual *WinRoute* features and configuration instructions are provided in the *Kerio WinRoute Firewall — Administrator's Guide* available at <http://www.kerio.com/kwf-manual/>.

Network configuration example

WinRoute configuration will be better understood through an example of a model network shown at figure 1.1.

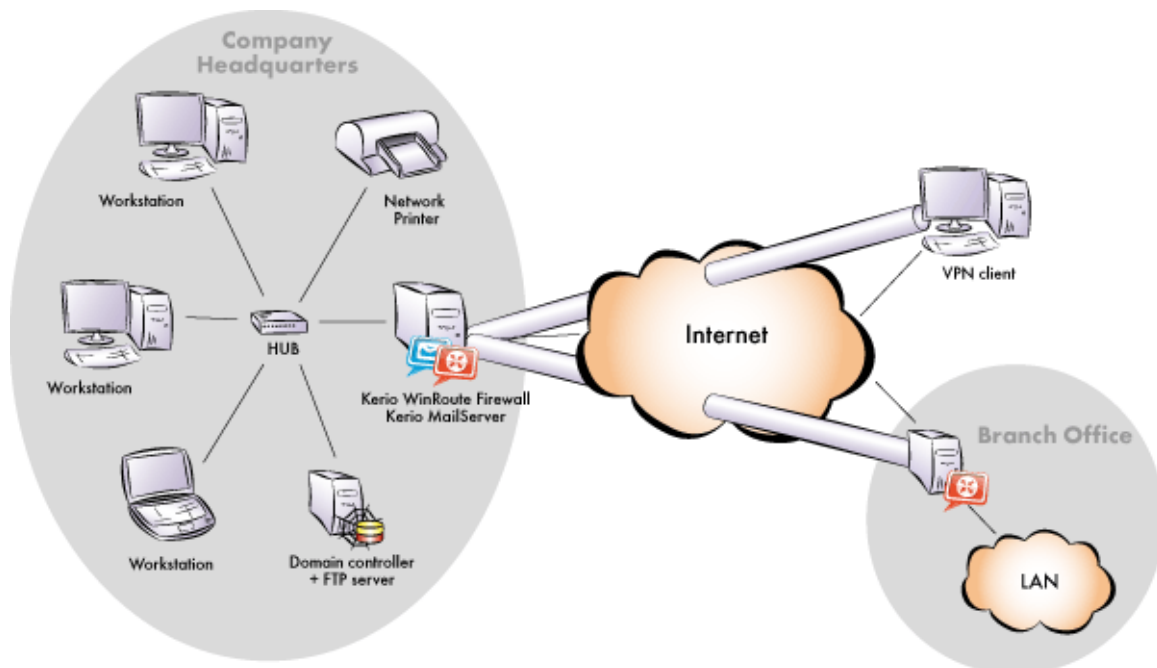


Figure 1.1 Network configuration example

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 subnet must be different).

For purposes of this example, it is supposed that an *Active Directory* domain *company.com* is created in the headquarters' LAN and all hosts in the network are included in this domain.

2.1 Selection of IP addresses for LAN

In our example, we will focus on private networks connected to the Internet through a single public IP address. Under such circumstances, the local network will be “hidden” behind this IP address entirely.

Local networks which do not belong to the Internet (so called private networks) use reserved special ranges of IP addresses. 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:

1. 10.x.x.x, network mask 255.0.0.0
2. 172.16.x.x, network mask 255.240.0.0
3. 192.168.x.x, network mask 255.255.0.0

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!

For the headquarters' LAN, the private addresses 192.168.1.x with subnet mask 255.255.255.0 (IP subnet 192.168.1.0) will be used whereas IP addresses 10.1.1.x with subnet mask 255.255.255.0 (IP subnet 10.1.1.0) will be used for the filial's LAN.

Setting IP addresses in an example network

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 domain 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.

2.2 Configuration of network interfaces of the Internet gateway

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).

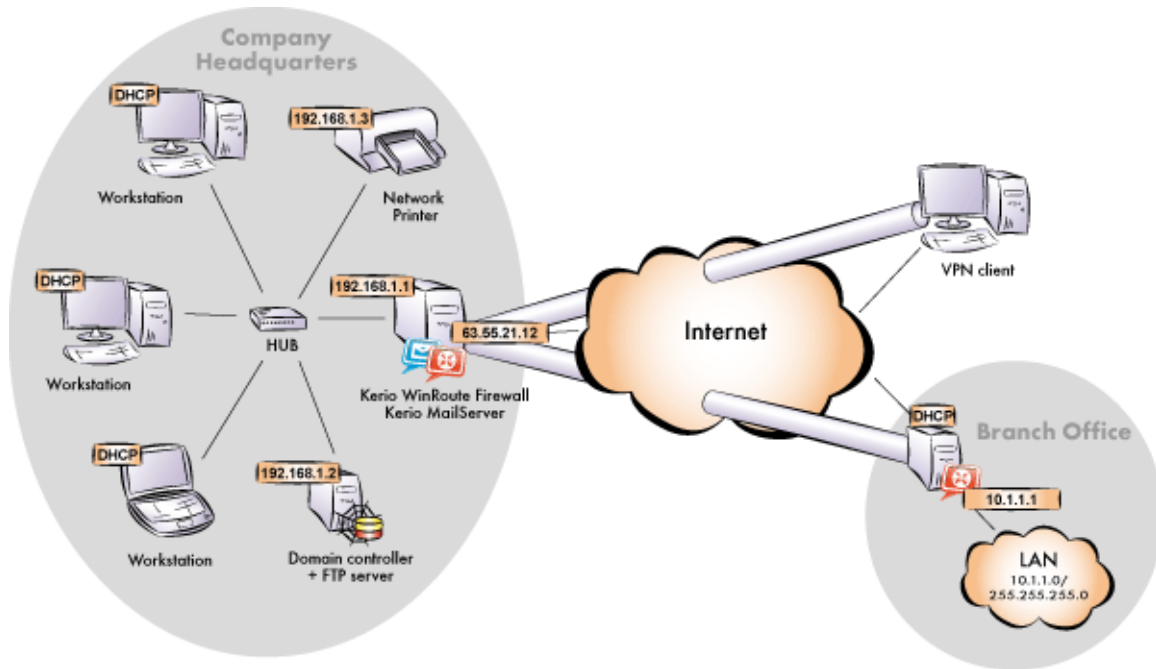


Figure 2.1 Example of configuration of a network with assigned IP addresses

Notes:

1. The DNS domain in the LAN must be identical with the *Active Directory* domain (i.e. *company.com*).
2. IP addresses 10.1.1.x with the mask 255.255.255.0 and the *filial.company.com* DNS domain will be used in the network of the branch office.

2.2 Configuration of network interfaces of the Internet gateway

Internet gateway is a host (or a server) at the boundary of LAN and the Internet. It is the machine where *WinRoute* will be installed (refer to chapter [2.3](#)).

Internet Interfaces

TCP/IP parameters of the Internet interface must be set according to information provided by your ISP. The following parameters are required for proper functionality of the Internet interface: IP address, subnet mask, default gateway and at least one DNS server's address.

The web interface of the company headquarter's firewall should have a fixed IP address to make it possible for the filial's server and VPN clients to connect to it (see requirements in chapter 1). Suppose that the ISP has assigned IP address 63.55.21.12. It is also recommended to assign a DNS name (e.g. kwf.company.com) to this IP address; otherwise all VPN clients will be required to define the server by the IP address.

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

LAN Interface

The following parameters will be set at the LAN Interface:

- *IP address* — we will use the 192.168.1.1 IP address (refer to chapter 2.1)
- *network mask* — 255.255.255.0
- *default gateway* — no default gateway is allowed at this interface!
- *DNS server* — for proper functionality of authentication in the *Active Directory*, the particular domain server must be set as the primary DNS server. Use the *Preferred DNS server* entry to specify the IP address of the domain server (192.168.1.2).

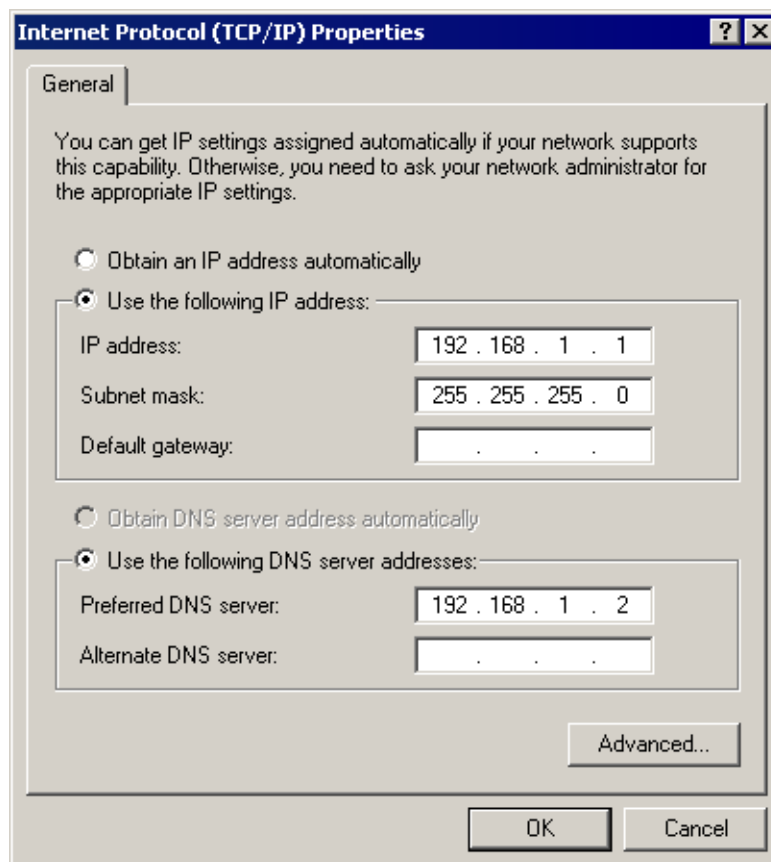


Figure 2.2 TCP/IP configuration at the firewall's interface connected to the local network

2.3 WinRoute Installation

On the host which is used as the Internet gateway (see chapter 2.1), start *WinRoute's* installation. Select *Full* installation.

If the installation module detects the *Windows Firewall / Internet Connection Sharing* service,¹ it asks whether the service should be disabled. It is strongly recommended to disable the service, otherwise low-level collisions might occur and *WinRoute* will not work correctly. It is also recommended to disable also other system services which might cause collisions — *Universal Plug and Play Device Host* and *SSDP Discovery Service*.



Figure 2.3 Installation — Detection of colliding system services

In the final stage of the installation, the *WinRoute's* initial configuration wizard is started where you set administration username and password.

Under usual circumstances, a reboot of the computer is not required after the installation is completed (a restart may be required if the installation program rewrites shared files which are currently in use). This will install the *WinRoute* low-level driver into the system kernel. *WinRoute Engine* will be automatically launched when the installation is complete. The engine runs as a system service.

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

2.4 Basic Traffic Policy Configuration

Run the *Kerio Administration Console* and 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 types (*Page 2*) — select Internet connection with a single leased line.

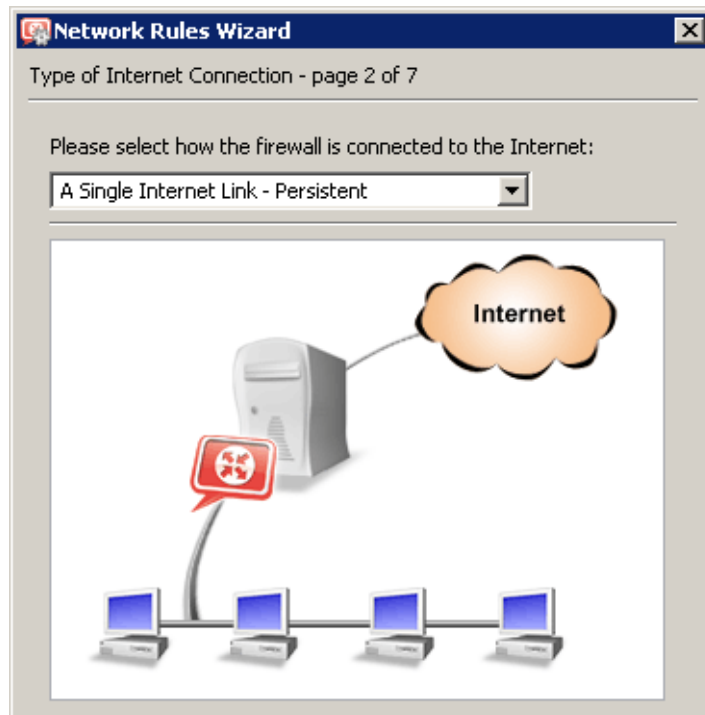


Figure 2.4 Network Policy Wizard — selection of Internet connection type

- Internet interface (*Step 3*) — select an Internet interface or appropriate dial-up.

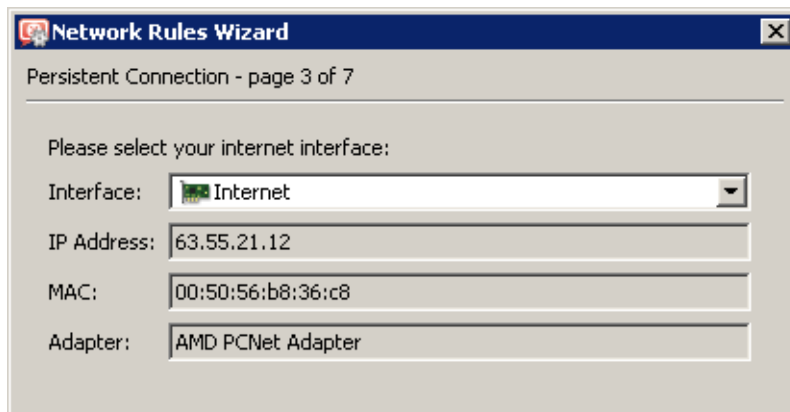


Figure 2.5 Network Policy Wizard — selection of Internet interface

- Rules used for outgoing traffic (*Step 4*) — these rules enable access to Internet services.

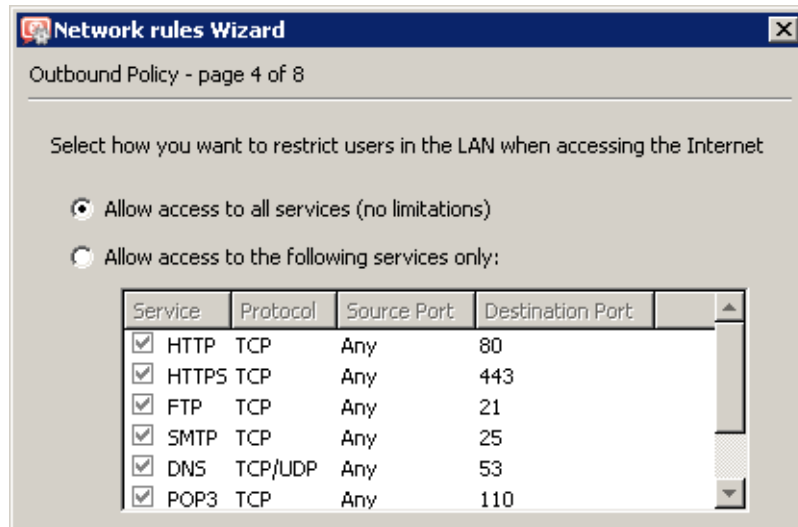


Figure 2.6 Network Policy Wizard — rules for outgoing traffic

- *VPN Server* policy (*Step 5*) — check *Yes, I want to use Kerio VPN* to create traffic rules that will enable interconnection of the headquarters with branch offices as well as connections of remote clients (refer to chapter 4).

To allow remote access to shared folders and files in the network by a web browser, enable the *Create rules for Kerio Clientless SSL-VPN* option.

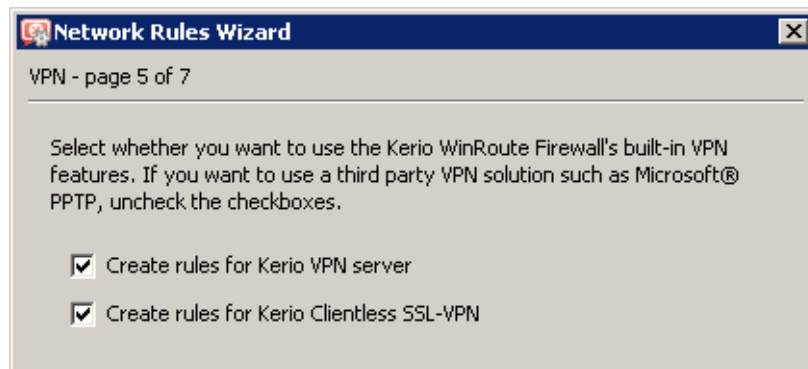


Figure 2.7 Network Policy Wizard — rules for Kerio VPN

- Rules for incoming traffic (*Step 6*) — for example, mapping to SMTP (email) server.

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, see chapter 2.13.

Note: It is meaningless to create rules for *Kerio VPN* at the filial's server and for incoming traffic (the server uses a dynamic IP address and clients cannot connect to it).

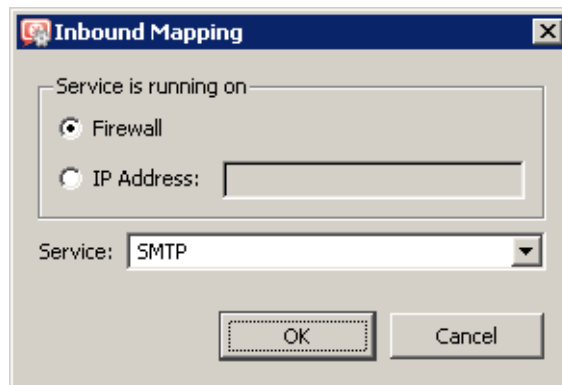


Figure 2.8 Network Policy Wizard — mapping of SMTP server

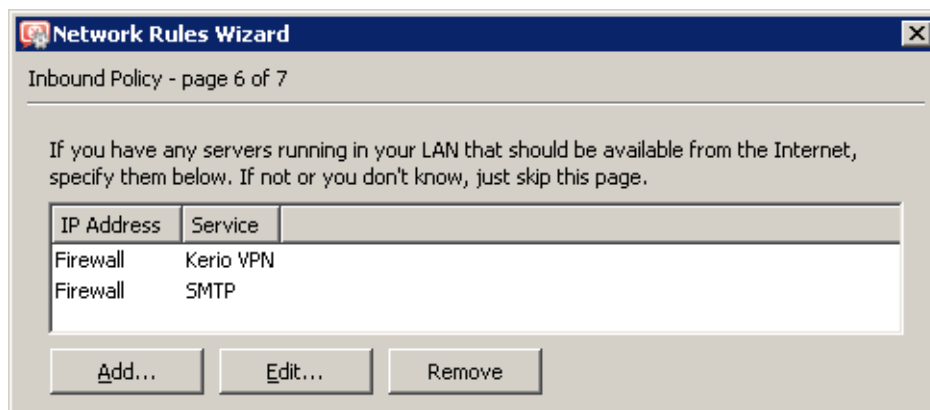


Figure 2.9 Network Policy Wizard — rules for incoming traffic

2.5 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).
- *DNS server* — IP address of the firewall interface that is connected to the local network (the same as the default gateway). The *WinRoute's DNS forwarder* will be used as the primary DNS server. The forwarder will procure correct forwarding of requests between the company's offices and to the Internet.

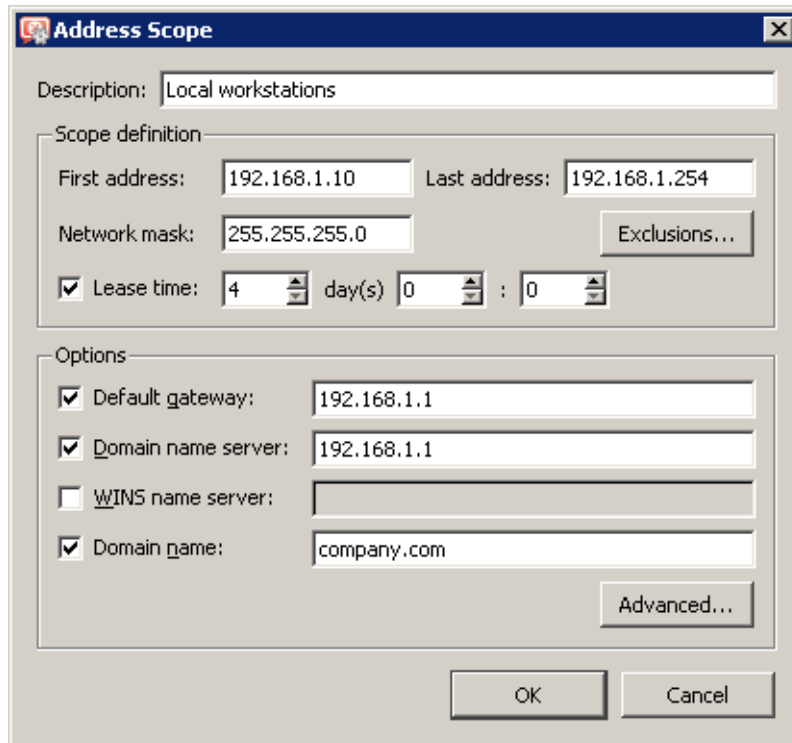


Figure 2.10 DHCP server — definition of IP range for workstations

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.

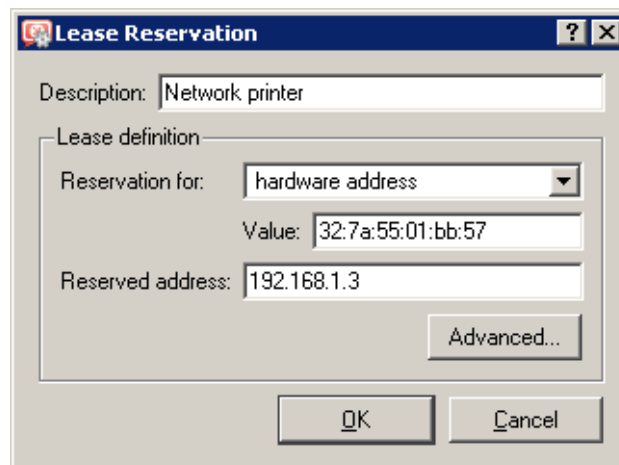


Figure 2.11 DHCP server — reserving an IP address for a printer

Hint

Do not make the reservation manually unless you know the MAC 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 MAC 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.

2.6 DNS Forwarder configuration

In *Configuration* → *DNS forwarder*, allow forwarding of DNS requests and set parameters for the *DNS forwarder*.

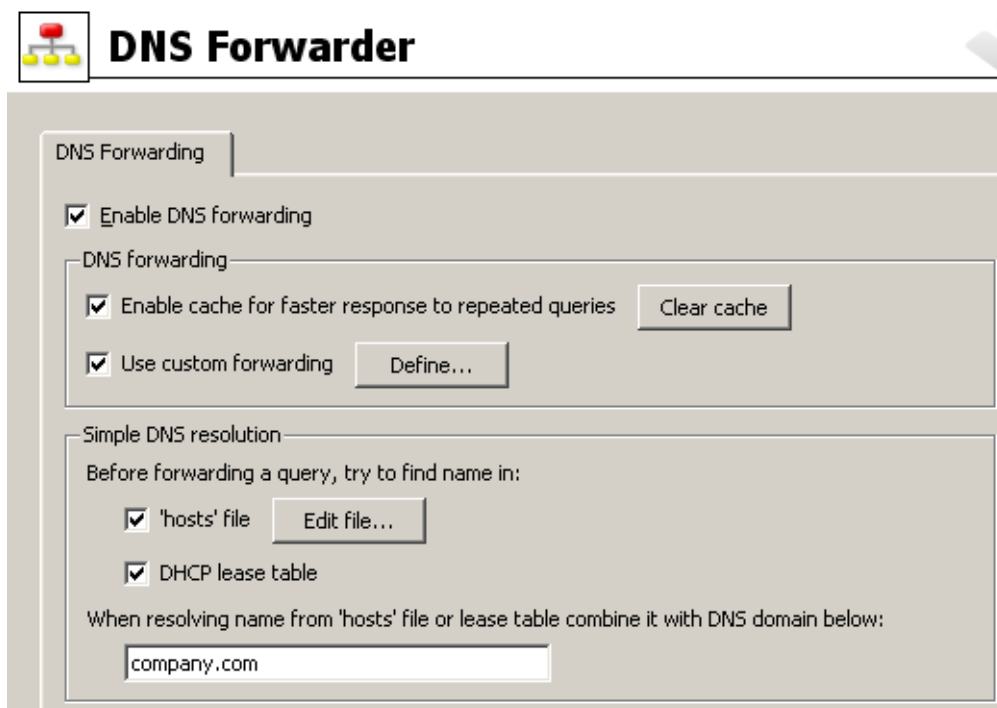


Figure 2.12 DNS Forwarder configuration

- It is recommended to enable the *Enable cache...* option (this will fasten responses to repeated DNS queries).
- Enable the *Use custom forwarding* option Add the rule for forwarding of requests to the *Active Directory*, i.e. of all requests for names starting with _ (underscore), to the domain server in the LAN — see figure 2.13. This setting is required for correct communication of local computers with the domain server.

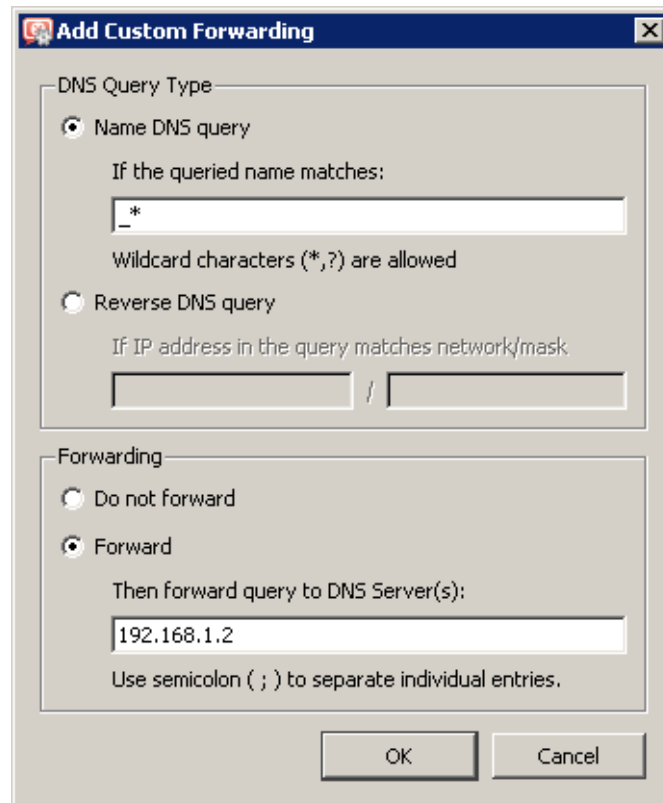


Figure 2.13 Forwarding of DNS requests to Active Directory

It is also necessary to add rules for correct forwarding of DNS queries between the headquarters' network and networks of branch offices. For detailed description on these settings, refer to chapter 4.1 (or to chapter 4.2).

- Enable options *'hosts' file* and *DHCP lease table*. Cooperation with DHCP server allows that *DNS forwarder* can response to requests for names of computers with IP addresses assigned dynamically. Then it is possible to add custom records manually as needed in the *hosts* file.

2.7 Web interface and SSL-VPN configuration

In *Configuration* → *Advanced Options* → *Web Interface / SSL-VPN*, enable the *Clientless SSL-VPN* interface and the *WinRoute's* web interface. The *Clientless SSL-VPN* interface is used for secured remote connections to shared files in local networks by a web browser. The *WinRoute's* web interface is used for viewing of information on attempts for access to denied websites (see chapter 2.10) and it can be also used for setting of some user account parameters or for access to statistics.

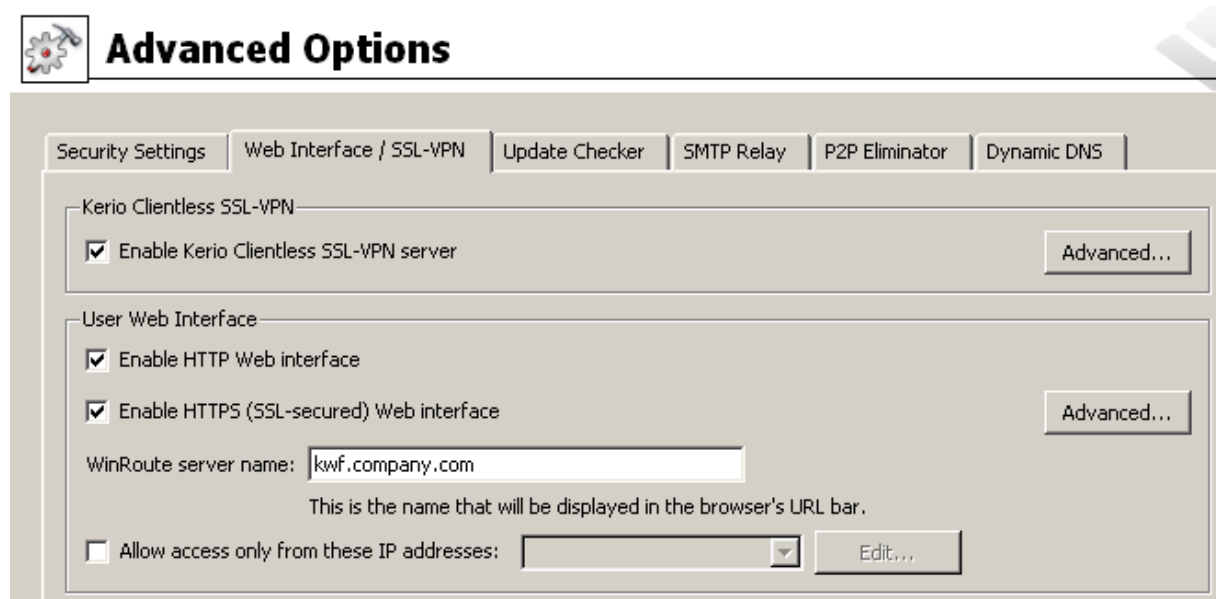


Figure 2.14 Setting of paramateres for the Clientless SSL-VPN and the web interface

In *Kerio SSL-VPN*, enable the *Clientless SSL-VPN* interface's server. Use the *Advanced* → *Change SSL certificate* → *Create SSL certificate* option to create a new certificate (a self-signed certificate) with servername `kwf.company.com`.

In *User web interface*, enable the web interface and use the same method as describe to create a certificate.

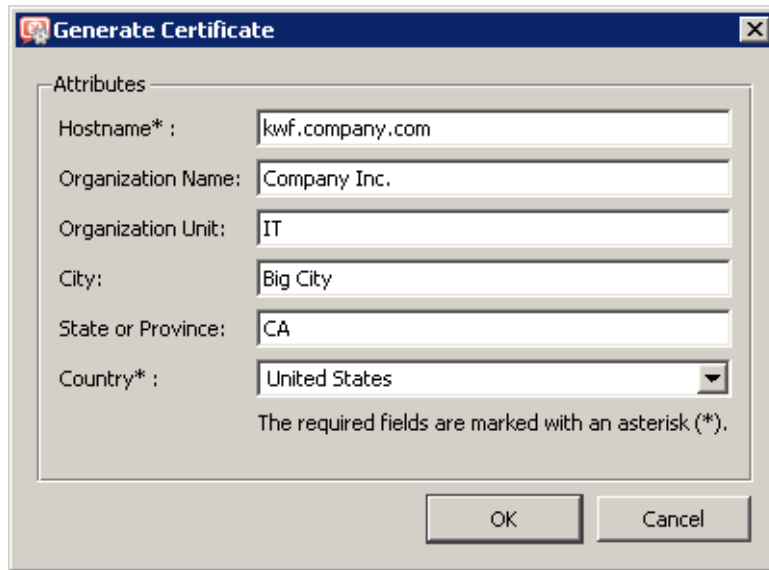


Figure 2.15 Creating SSL certificate for the Clientless SSL-VPN and the web rozhraní

Hint

Self-signed certificates created here can be later replaced by certificates issued by a public certification authority.

2.8 Mapping of user accounts and groups from the Active Directory

To enable disposal of *Active Directory* user accounts, set mapping of a corresponding domain and define a template that will apply specific *WinRoute* parameters (user rights, data transfer quotas, etc.) to all users.

Domain mapping

There is an *Active Directory* domain created in the local network. Therefore, it is not necessary to define local user accounts in *WinRoute*. Simply map a corresponding domain.

To set *Active Directory* domain mapping, go to the *Active Directory* tab under *User and Groups* → *Users*.

Active Directory mapping

Enter the DNS name of the — *company.com* domain to the *Active Directory domain name* entry.

The *Description* item is for better reference only.

Domain Access

WinRoute needs to know username and password for access to the *Active Directory* database. Access with read rights is satisfactory for this purpose. This means that it is possible to use any user account belonging to the particular domain.

Note: It is not necessary to set the *Advanced* parameters.

The screenshot shows the 'Users' configuration window with three tabs: 'User Accounts', 'Authentication Options', and 'Active Directory®'. The 'Active Directory®' tab is selected. It contains three main sections:

- Active Directory® Mapping:** A checkbox labeled 'Map user accounts from the Active Directory® domain to Kerio WinRoute Firewall' is checked. Below it, the 'Active Directory® domain name' is 'company.com' and the 'Description' is 'Company headquarters' domain'.
- Domain Access:** A section titled 'Domain Access' with a sub-label 'Account with rights to read user database:'. The 'Username' is 'Administrator' and the 'Password' is '*****'. There is an 'Advanced...' button below.
- Windows NT® Authentication:** A checkbox labeled 'Enable Windows NT® domain authentication for this domain' is checked. Below it, the 'Windows NT® domain name' is 'COMPANY'.

Figure 2.16 Settings of Active Directory domain mapping

NT authentication

To enable automatic user authentication from web browsers and to keep compatibility with older *Windows* versions, it is recommended to enable authentication against *Windows NT* domain.

Use the *NT domain name* entry to insert a corresponding *Windows NT* domain name, i.e. COMPANY.

Creating templates for user accounts

On the *User Accounts* tab, select the mapped *Active Directory* domain, i.e. `company.com`.

Click on the *Template* button to define a template for user accounts. It is also intended to enable remote users to access the local network by *Kerio VPN Client* or *Clientless SSL-VPN* (see chapter 1). Set user rights on the *Rights* tab.

2.8 Mapping of user accounts and groups from the Active Directory

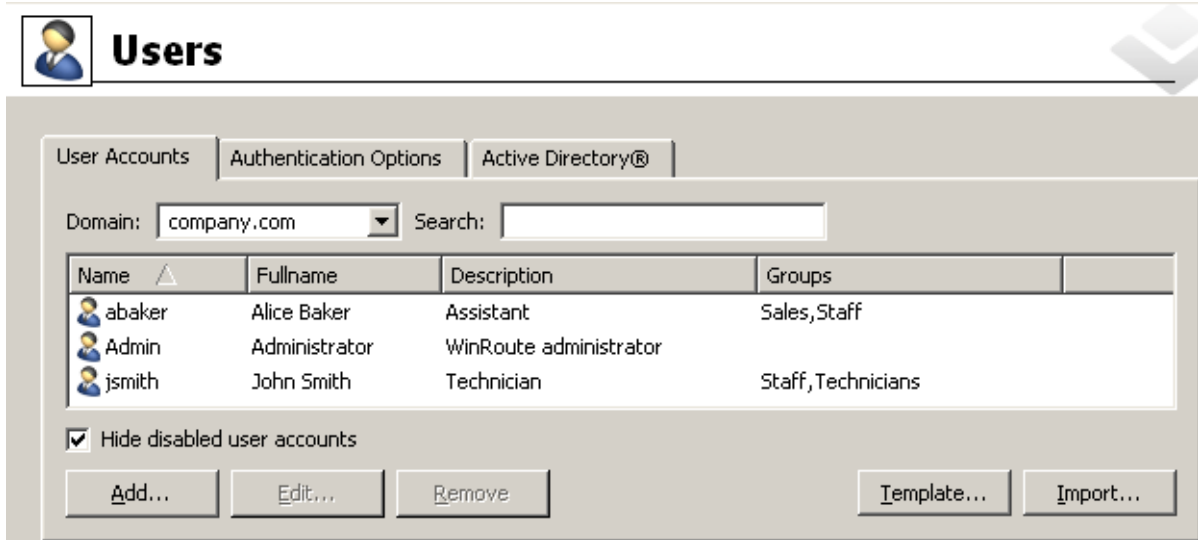


Figure 2.17 Overview of user accounts in the mapped domain

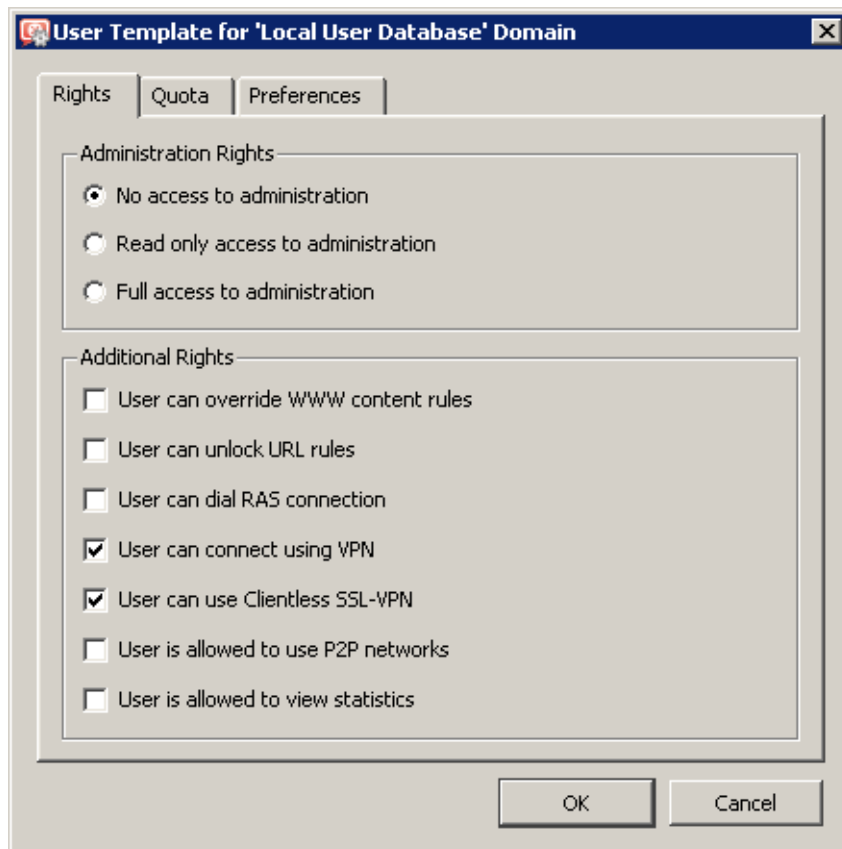


Figure 2.18 Template for user accounts — setting rights for Kerio VPN and Clientless SSL-VPN

2.9 Address Groups and Time Ranges

Open the *Definitions* → *Address Groups* section to create IP group *Email Access* that will be used to limit access to email accounts (refer to chapter 2.13). 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.

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

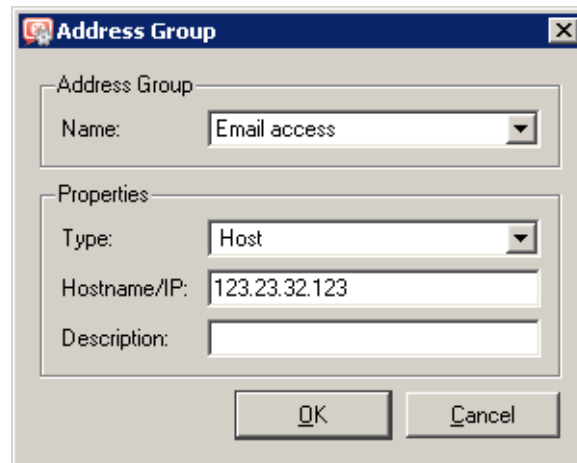


Figure 2.19 IP address group — addition of a host

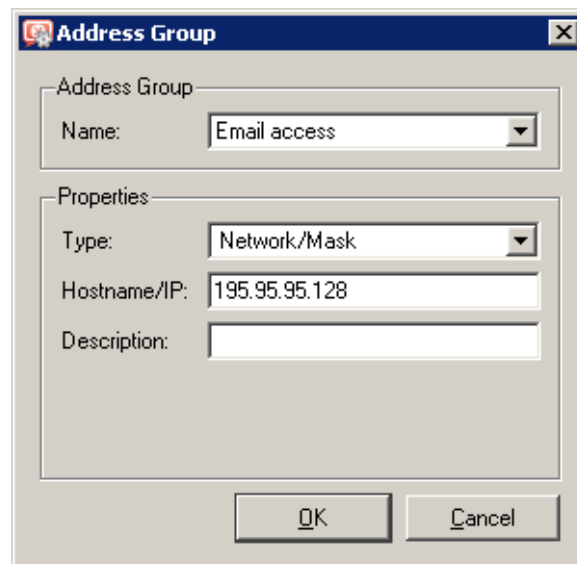


Figure 2.20 IP address group — addition of a subnet

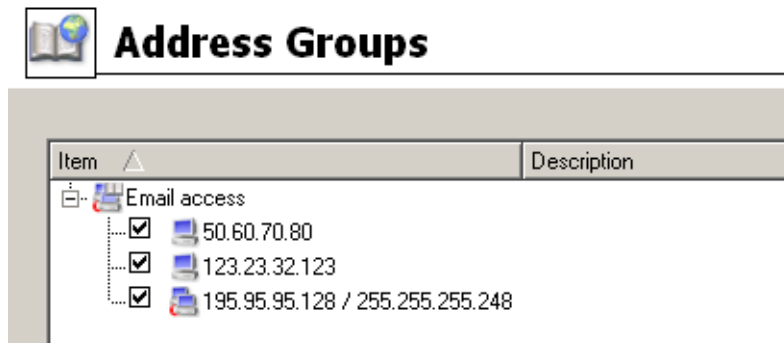


Figure 2.21 Resultant address group

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.).

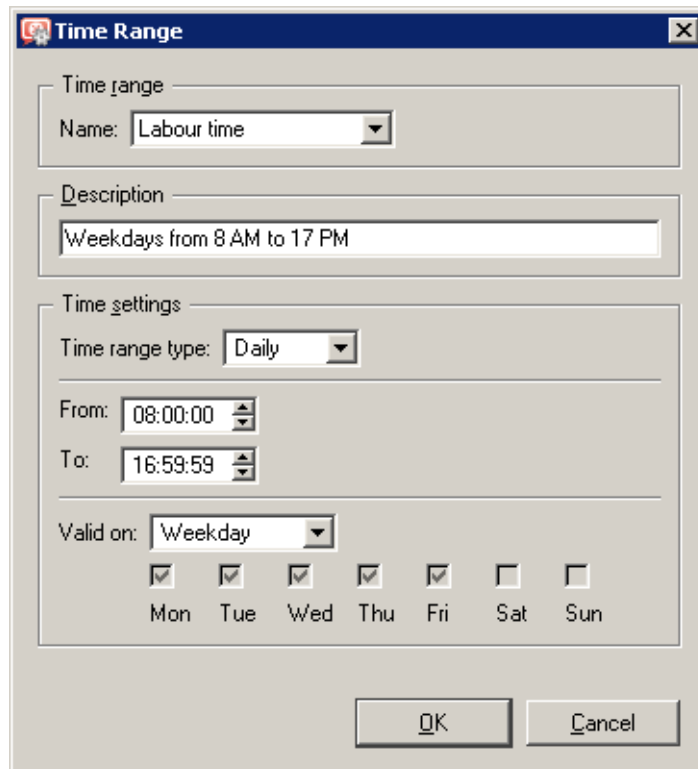


Figure 2.22 Labor time definition for working days (from Monday to Friday)

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.

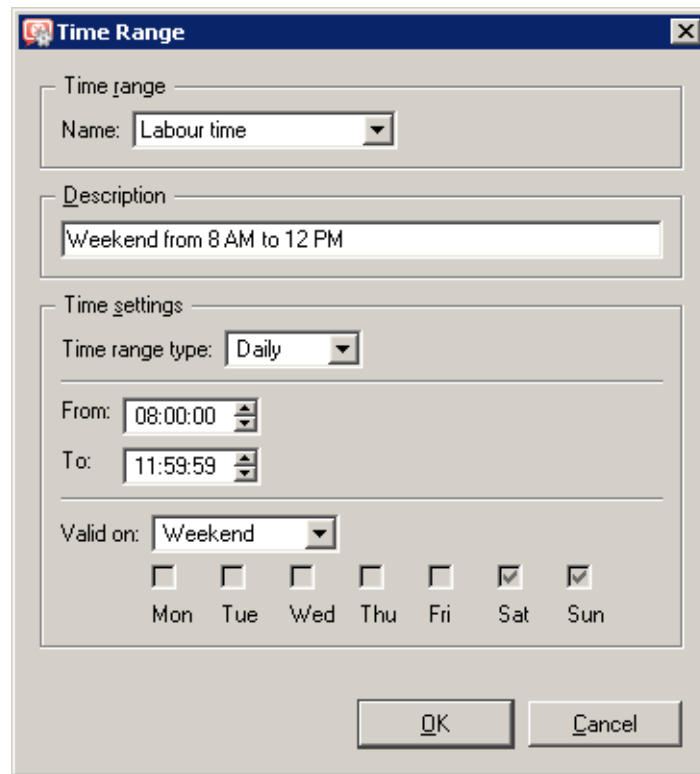


Figure 2.23 Labor time definition for weekends (Saturday and Sunday)

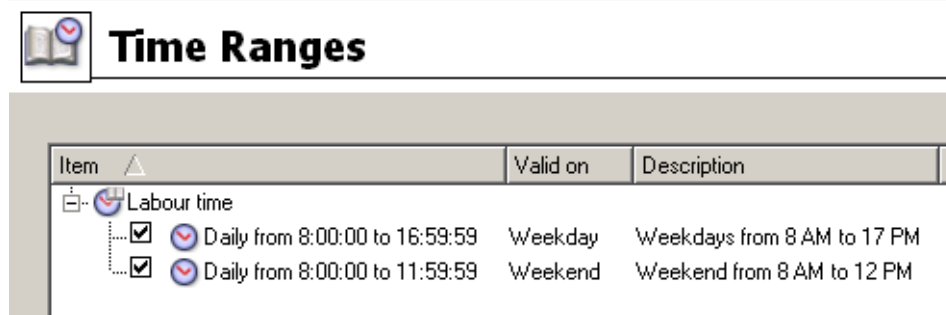


Figure 2.24 This is the result Labor time range

2.10 Web Rules Definition

Requirements

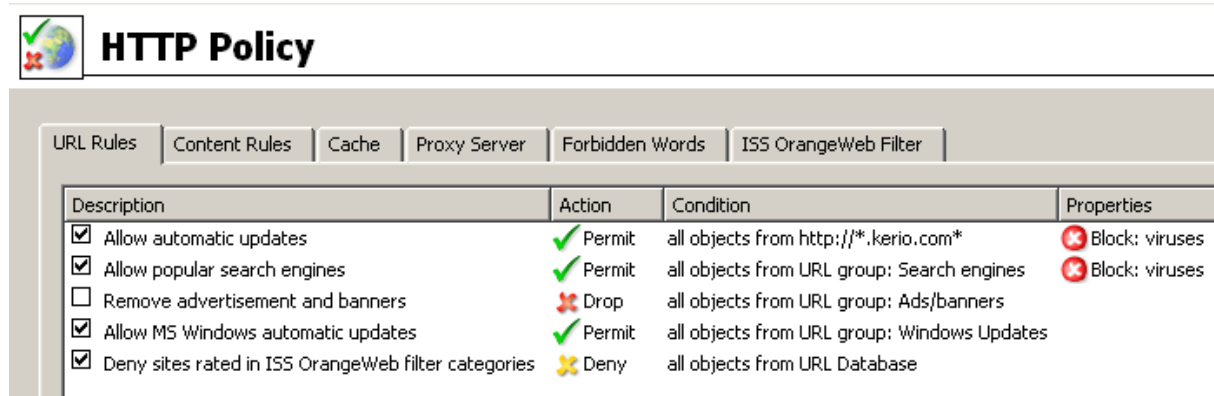
Access to Web pages will be limited by the following restrictions:

- 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*:



The screenshot shows the 'HTTP Policy' configuration window with the 'URL Rules' tab selected. It displays a table of predefined rules with columns for Description, Action, Condition, and Properties.

Description	Action	Condition	Properties
<input checked="" type="checkbox"/> Allow automatic updates	✓ Permit	all objects from http://*.kerio.com*	✗ Block: viruses
<input checked="" type="checkbox"/> Allow popular search engines	✓ Permit	all objects from URL group: Search engines	✗ Block: viruses
<input type="checkbox"/> Remove advertisement and banners	✗ Drop	all objects from URL group: Ads/banners	
<input checked="" type="checkbox"/> Allow MS Windows automatic updates	✓ Permit	all objects from URL group: Windows Updates	
<input checked="" type="checkbox"/> Deny sites rated in ISS OrangeWeb filter categories	✗ Deny	all objects from URL Database	

Figure 2.25 Predefined rules for web filtering

- It is recommended to leave the *Allow automatic updates* and *Allow MS Windows automatic updates* rules enabled which makes automatic updates of *WinRoute* and the operating system work.
- Use of the *Allow popular search engines* and *Remove advertisement and banners* rules depends on your decision.
- The *Deny sites rated in ISS OrangeWeb Filter categories* rule can be used to keep all users from accessing pages with erotic content.

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

On the *Advanced* tab, enter the text which will be displayed if a user to access a page with forbidden content or set redirection to another webpage.

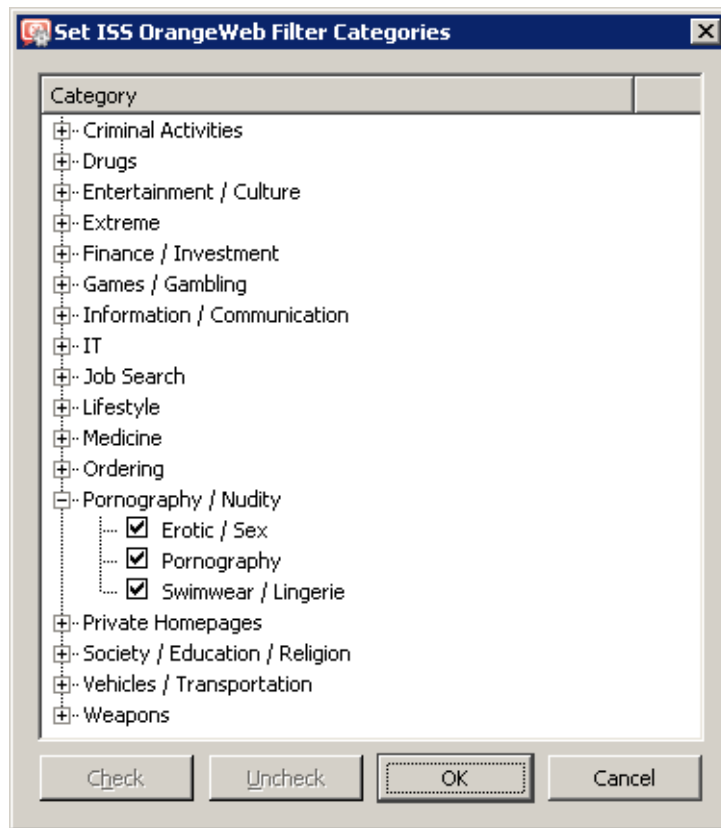


Figure 2.26 Setting ISS OrangeWeb Filter categories

Definition of custom rules

To restrict access to websites with job offers, use the following rules:

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.

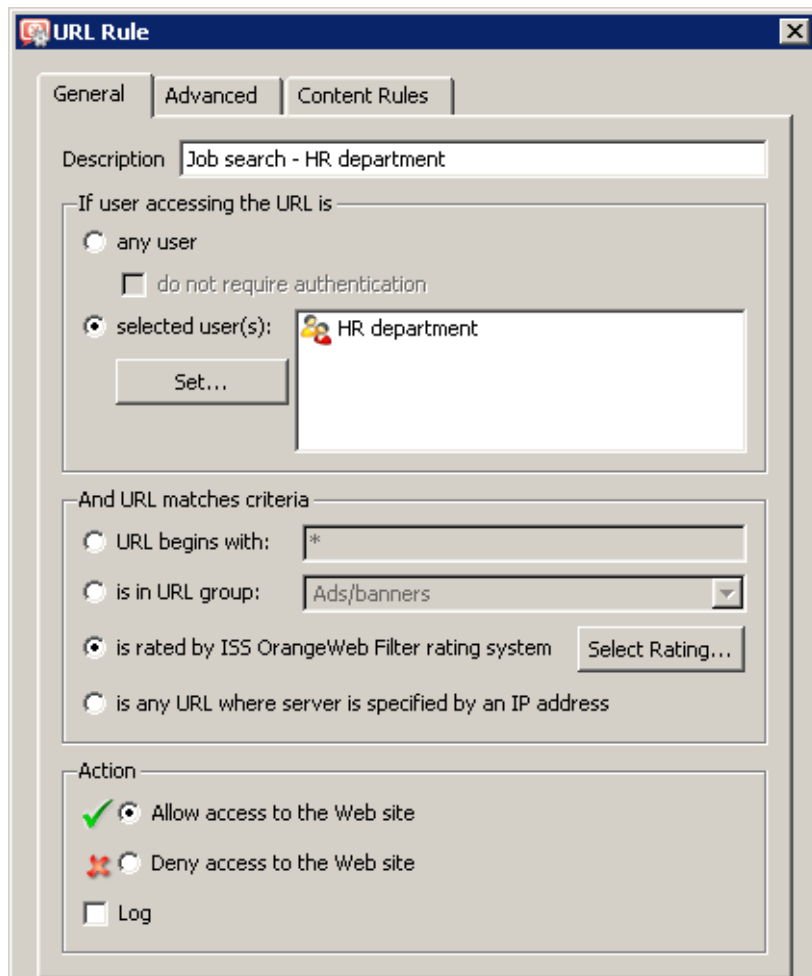


Figure 2.27 URL rule — allowing a user group to access a web category

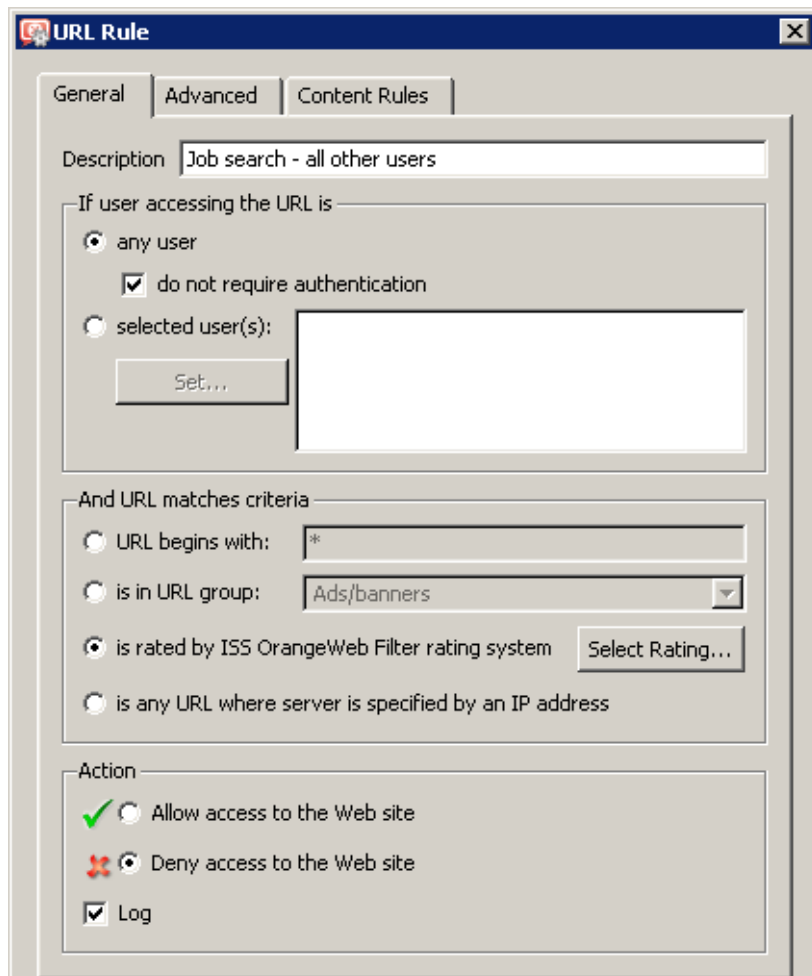


Figure 2.28 URL rule — disallowing any other users to access a web category

Notes:

1. It is recommended to enable the *do not require authentication* option in the rule which denies access for all users, This will skip redirection to the authentication page before displaying denial information.
2. In both rules mentioned above only the *Job search* category is selected.

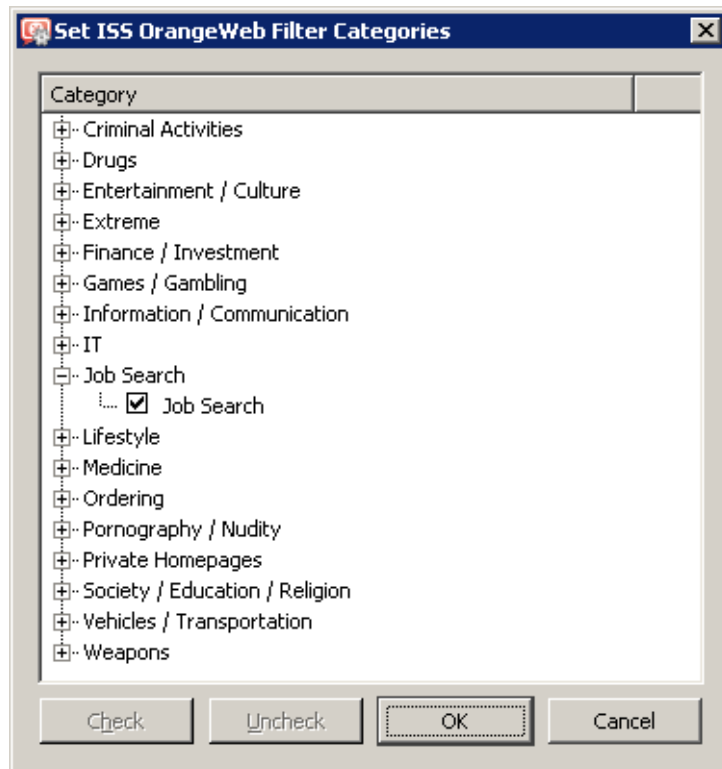


Figure 2.29 URL rule — selection of web categories

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*.

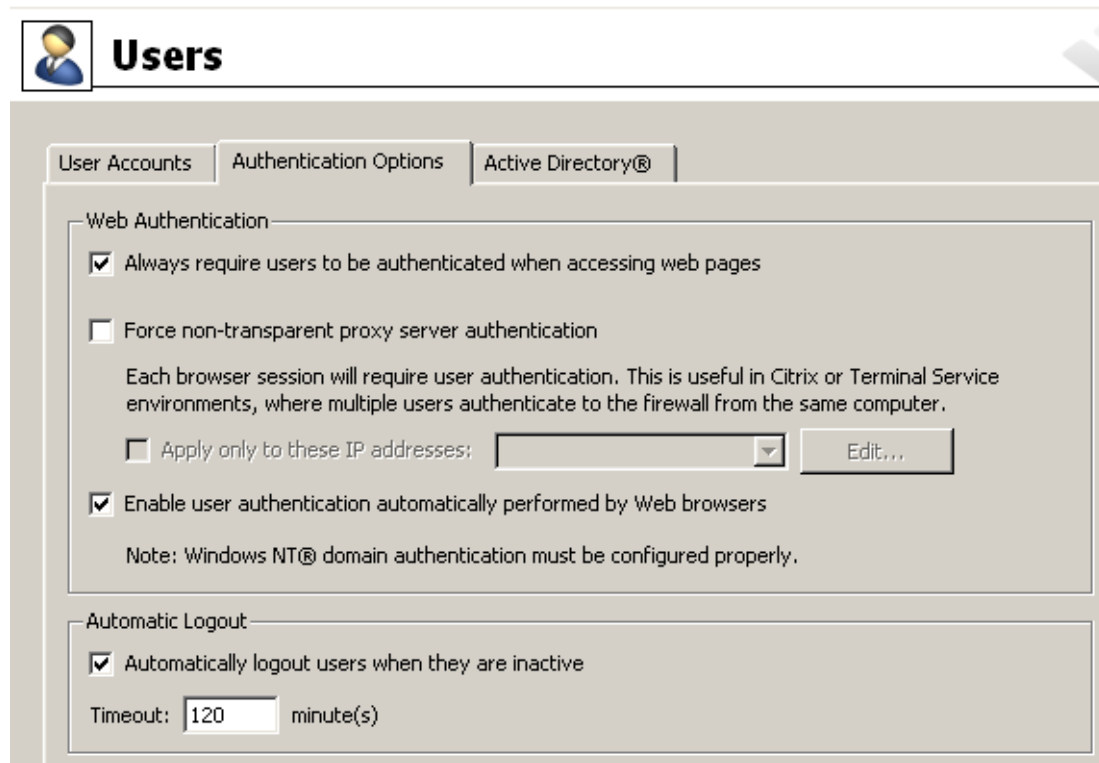


Figure 2.30 User authentication for accessing Websites

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 almost 2 GB (2047 MB).

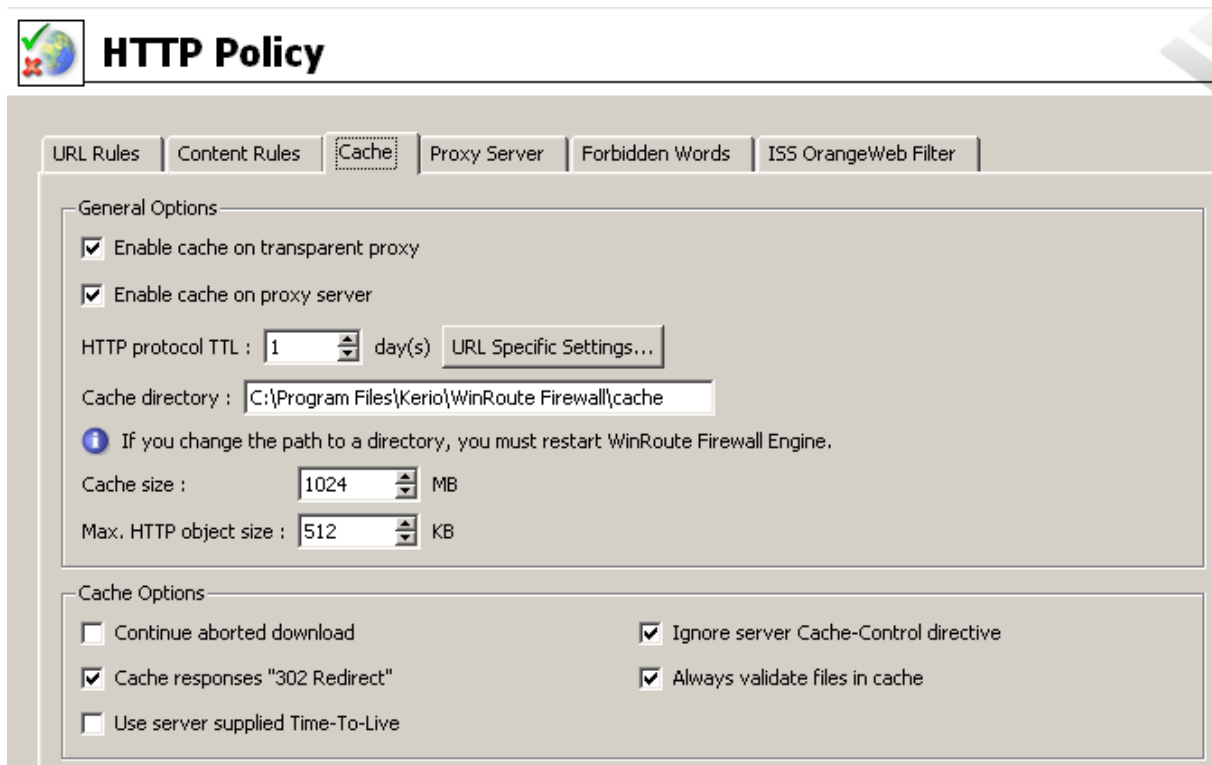


Figure 2.31 HTTP cache configuration

2.11 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 within working hours
- uploads (storing files at FTP servers) will be denied — protection of important company information

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:

- Rules *Forbid *.mpg, *.mp3 and *.mpeg files* and *Forbid upload* are ready to use.
- To use the *Forbid *.avi files* rule, go to the *Advanced* tab and set the time interval the rule will apply to.



FTP Policy

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

Figure 2.32 Predefined FTP Rules

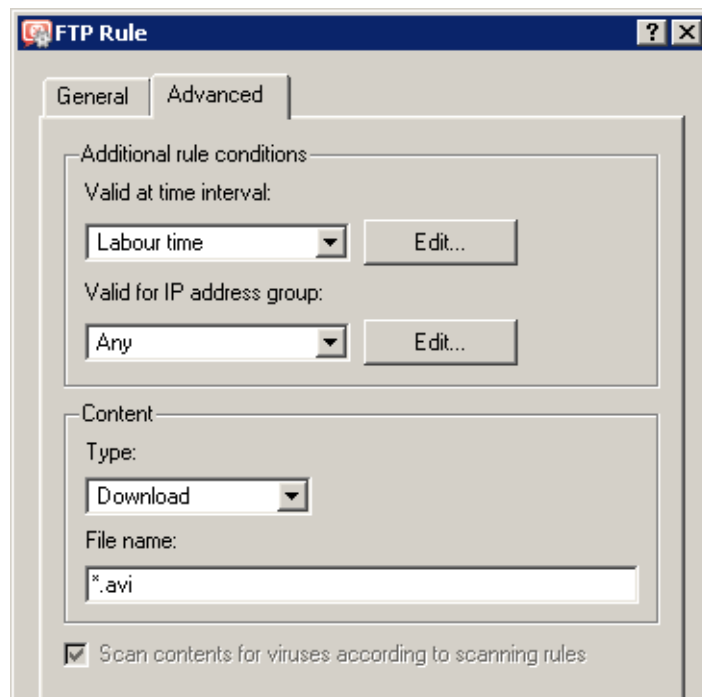


Figure 2.33 The Forbid *.avi files rule — setting time interval when the rule will be applied

- It is also recommended to enable rule *Forbid resume due to antivirus scanning*. This makes all files transferred via FTP thoroughly scanned by an antivirus program.

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.

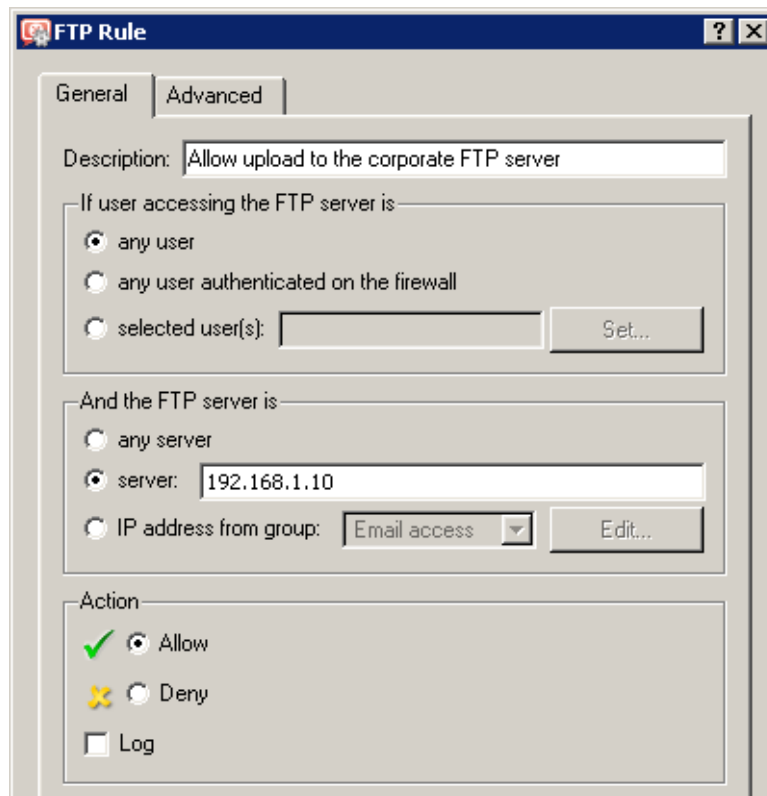


Figure 2.34 FTP rule — allowing uploads to the corporate FTP server

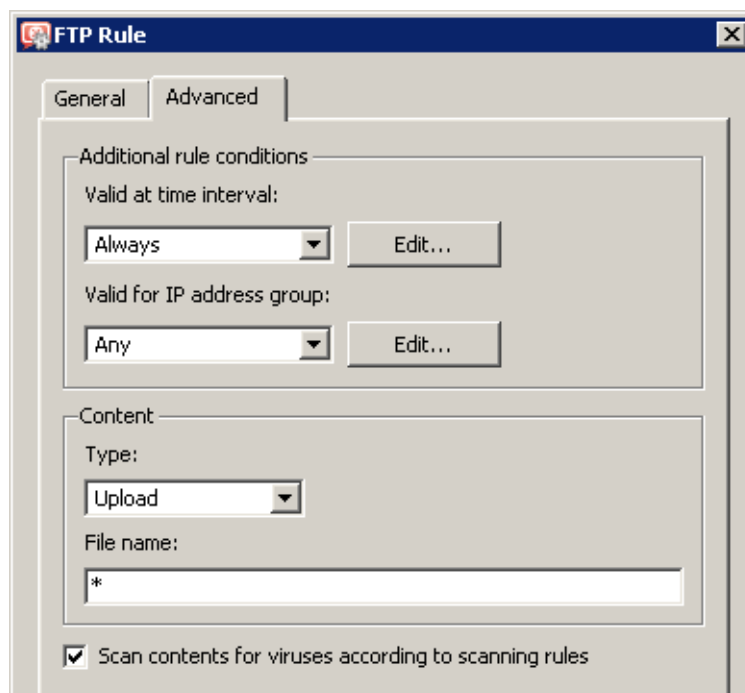


Figure 2.35 FTP rule — allowing upload of any file

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 an outbound IP address of the firewall that the FTP server is mapped from (unless the FTP server runs on the firewall)! IP addresses are translated before the 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.

2.12 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 set protocols that will be scanned.

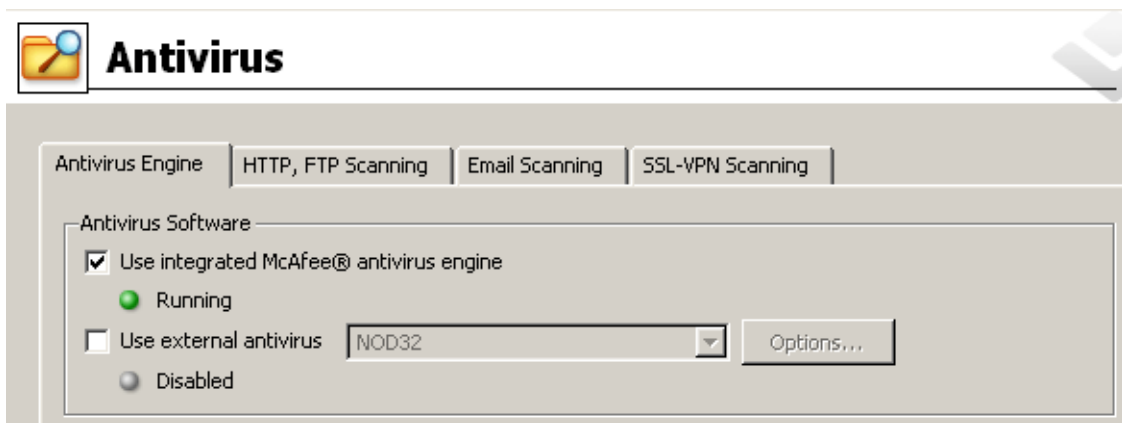


Figure 2.36 Antivirus Scanning Configuration

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

2.13 Enabling access to local services from the Internet

Go to *Configuration* → *Traffic Policy* to add rules for services that will be available from the Internet. Rules for service mapping should be always at the top of the traffic rules table.

- Mapping of local FTP server — unsecured access only is supposed which makes it possible to filter traffic and scan it for viruses.

Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> FTP server mapping	 Any	 Firewall	 FTP		MAP 129.168.1.2

Figure 2.37 Making the local FTP servers available from the Internet

- Access to other mail server services (save SMTP) — allowed from certain IP addresses only.








Name	Source	Destination	Service	Action	Translation
<input checked="" type="checkbox"/> Mail server access	 Email access	 Firewall	 IMAP  IMAPS  POP3  POP3S		

Figure 2.38 Enabling access to the firewall's mailserver services

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 2.4) — 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.

2.14 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 4.1). No additional settings are required. Communication of VPN clients is already allowed by the traffic policy created by the wizard — refer to chapter 2.4.

Notes:

1. *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 (i.e. to 63.55.21.12) and they will be authenticated through their usernames and passwords for their *WinRoute* accounts (see chapter 2.8).

For help details, see *Kerio VPN Client — User's Guide* (<http://www.kerio.com/kwf-manual>).

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

2.15 LAN Hosts Configuration

TCP/IP parameters for the hosts that are used as the domain 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 2.5),
- *Default gateway* — use IP address of the appropriate firewall interface (192.168.1.1),
- *DNS server* — since *Microsoft DNS* is running on the host, the system sets the local loopback address (*loopback* — 127.0.0.1) as the primary DNS server.

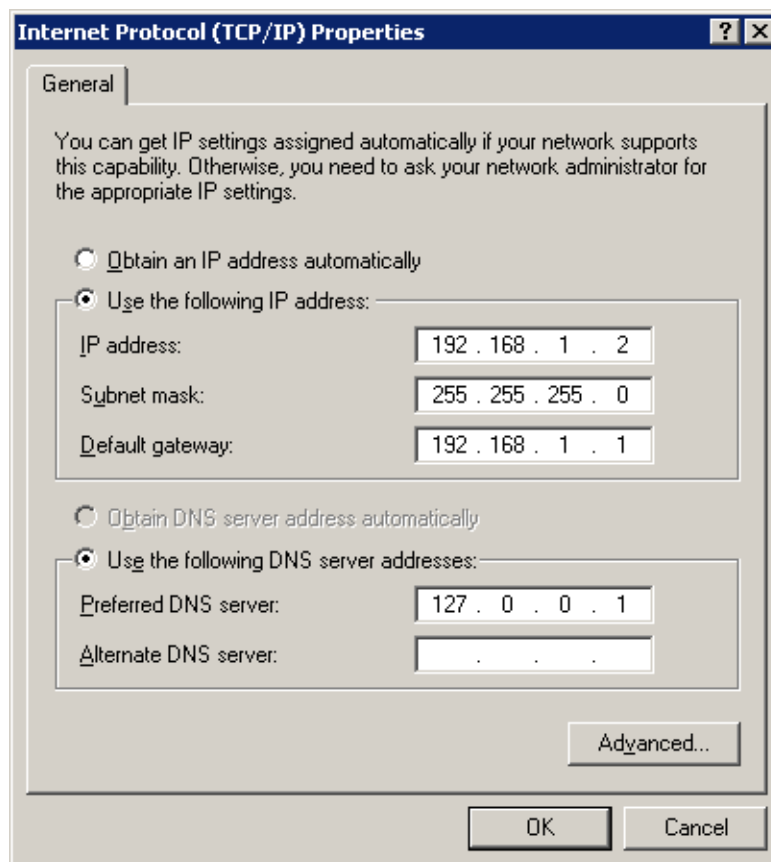


Figure 2.39 TCP/IP configuration on the file/FTP server

Set automatic configuration of both IP address and DNS server (using DHCP) at all workstations (it is set by default under most operating systems).

Configuration of the LAN in a filial office

For quick configuration of the filial's LAN, it is possible to follow similar method as for the headquarter's network (see chapter 2). The only difference is the DNS configuration. Supposing that there is no domain server or any other DNS server in the filial's network. The *WinRoute's DNS Forwarder* will be used as the primary DNS server.

3.1 Configuration of network interfaces of the Internet gateway

Set a fixed IP address (e.g. 10.1.1.1) at the firewall's interface connected to the local network. Set the same IP address as the primary DNS server (this ensures that also DNS queries from the local host will be forwarded to the *DNS Forwarder* — this is important especially in case that dial-up connection is used). Make sure that no default gateway is set on this interface!

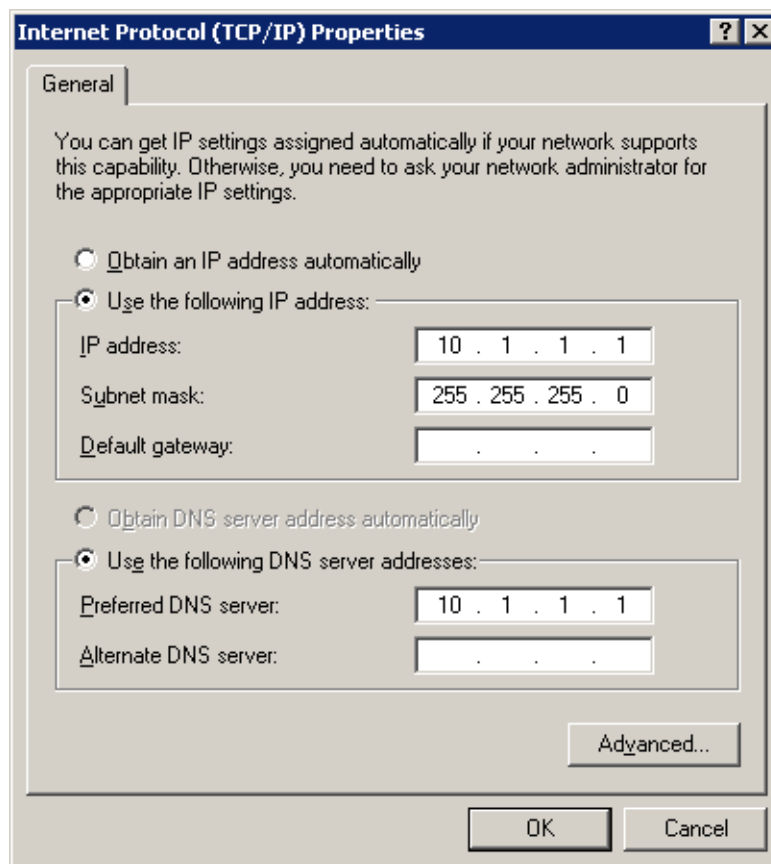


Figure 3.1 Filial — configuration of the firewall's local interface

Follow the ISP's instructions to set the interface connected to the Internet.

3.2 DNS Forwarder Configuration

In the *DNS Forwarder* configuration, enable simple DNS resolution. Use the *When resolving name...* entry to specify the local DNS domain, i.e. `filial.company.com`.

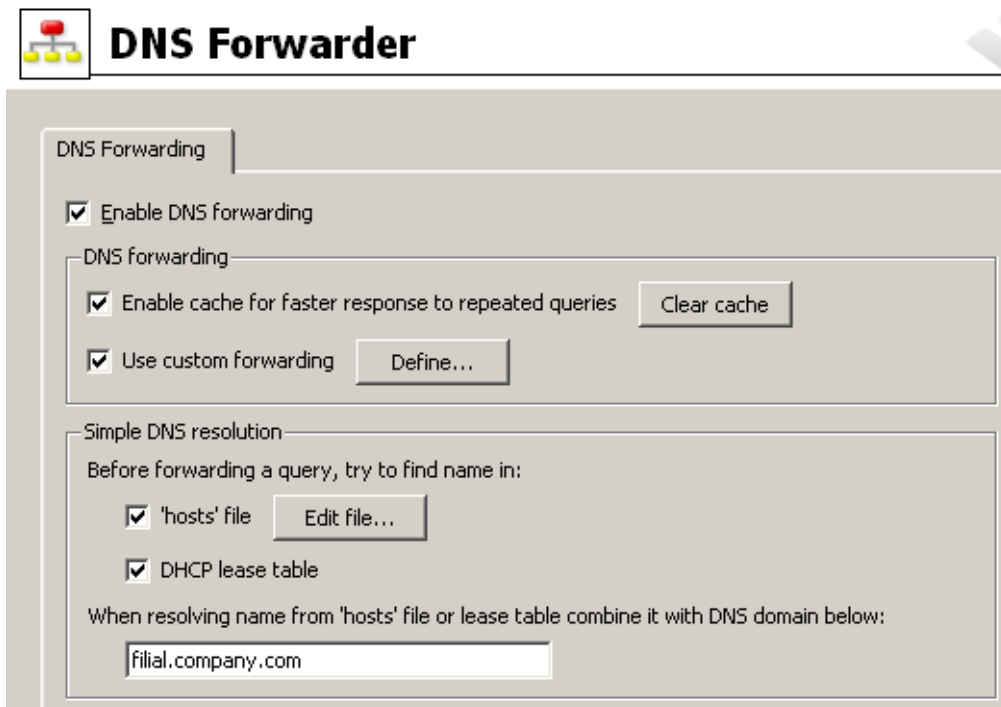


Figure 3.2 Filial office — DNS Forwarder configuration

It is recommended to add a record about the server (or about other hosts to which a fixed IP address will be assigned) to the *hosts* file .

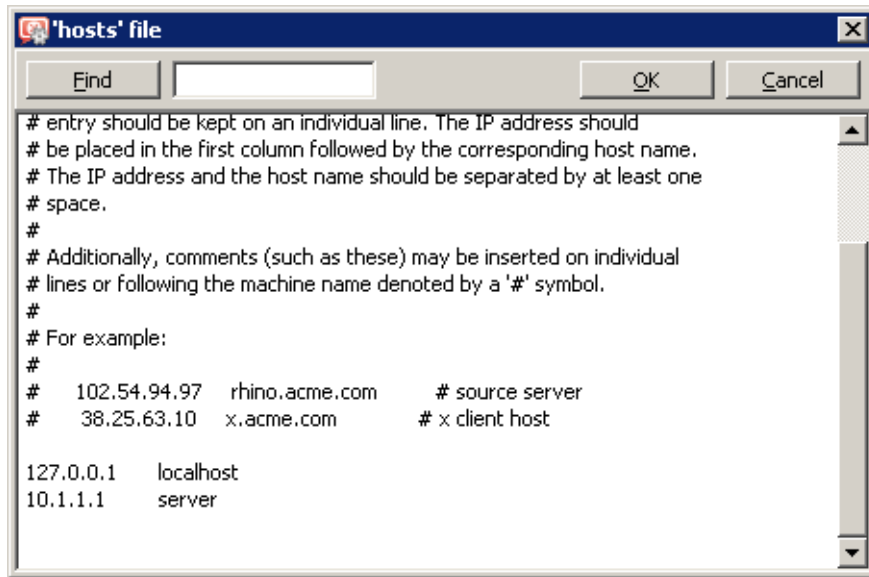


Figure 3.3 Filial — adding a record about the server to the 'hosts' file

3.3 DHCP Server Configuration

In the DHCP server configuration, define IP range for hosts in the filial's LAN. Use the IP address of the local office's firewall interface (10.1.1.1) as the address of the DNS server's default gateway.

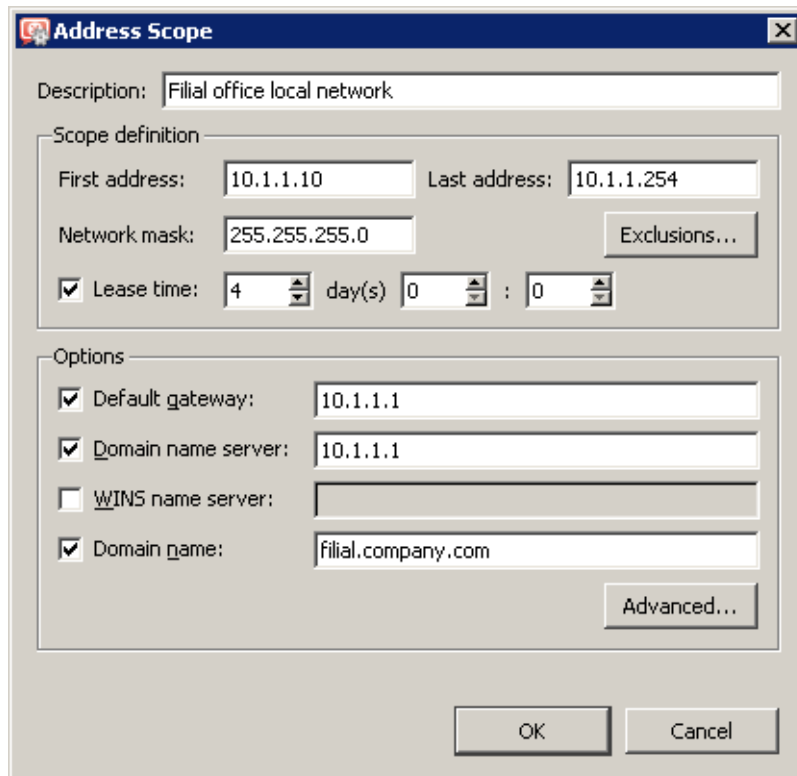


Figure 3.4 Filial — setting range for IP addresses leased by the DHCP server

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 configuration consists of two parts: settings in the headquarters and settings of the filial. 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.

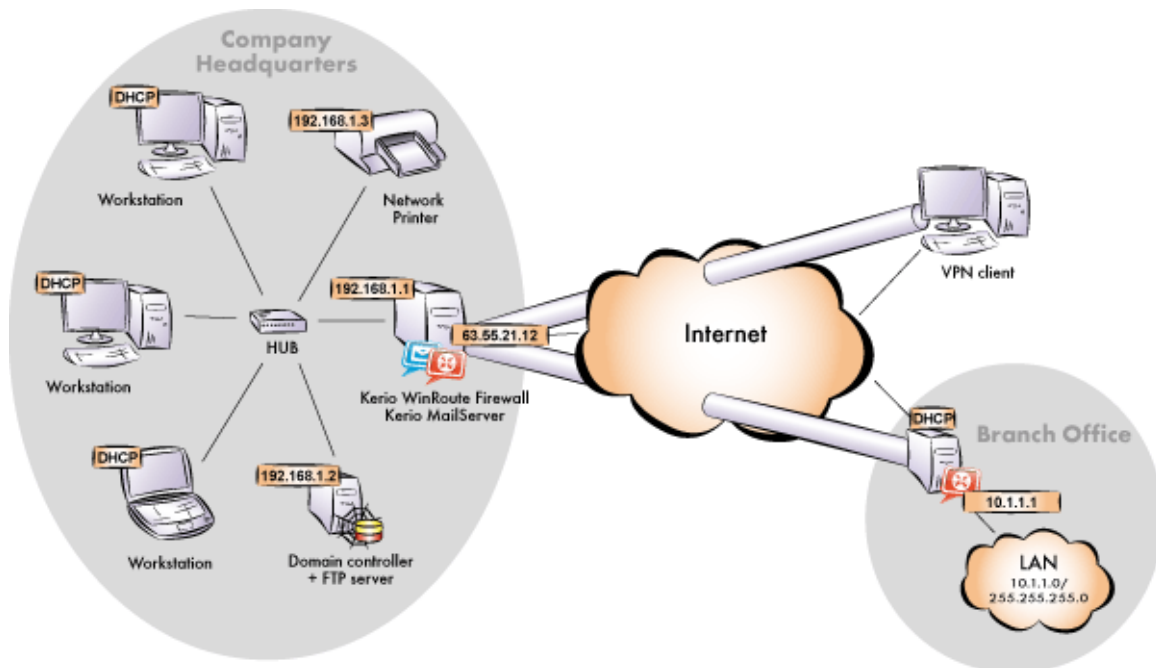


Figure 4.1 Example of configuration of a network with assigned IP addresses

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.

4.1 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 free subnet which has been selected for VPN is now specified automatically in the *VPN network* and *Mask* entries. There is no reason to change the network.

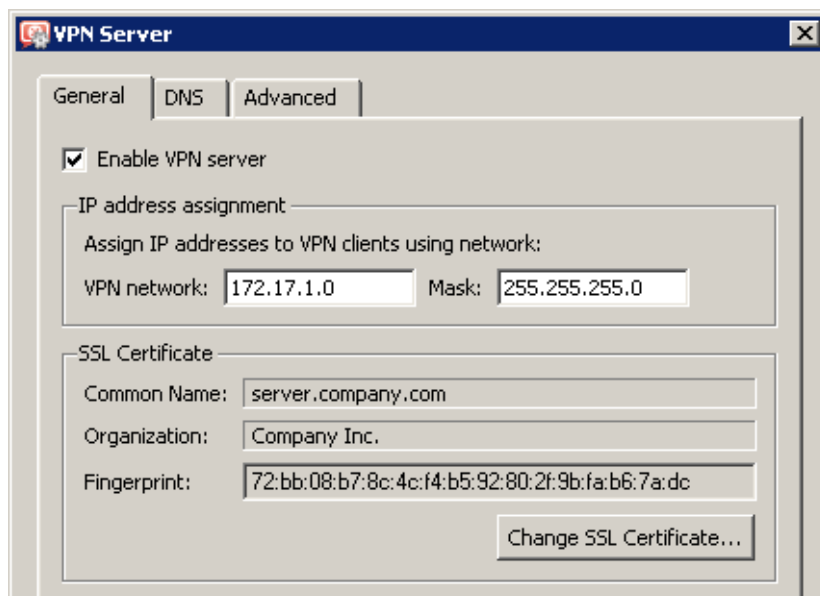


Figure 4.2 Headquarters — VPN server configuration

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 with a certificate authorized 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.

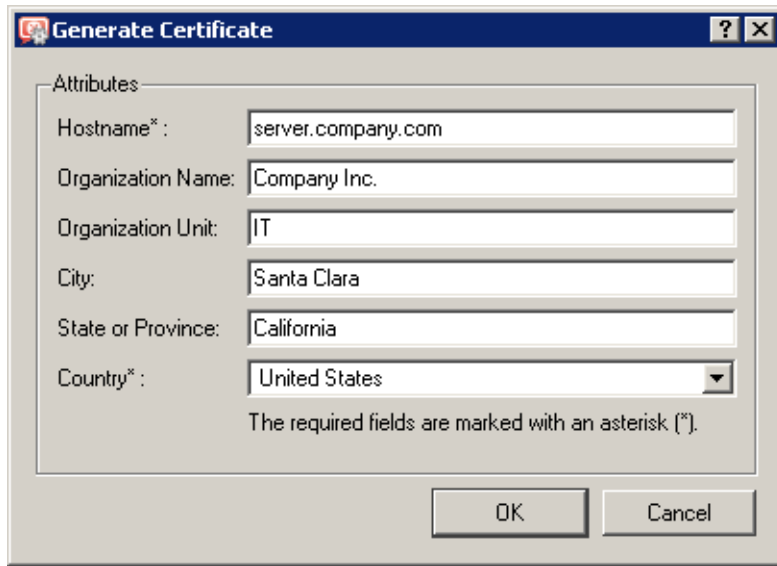


Figure 4.3 Headquarters — creating of the VPN server's SSL certificate

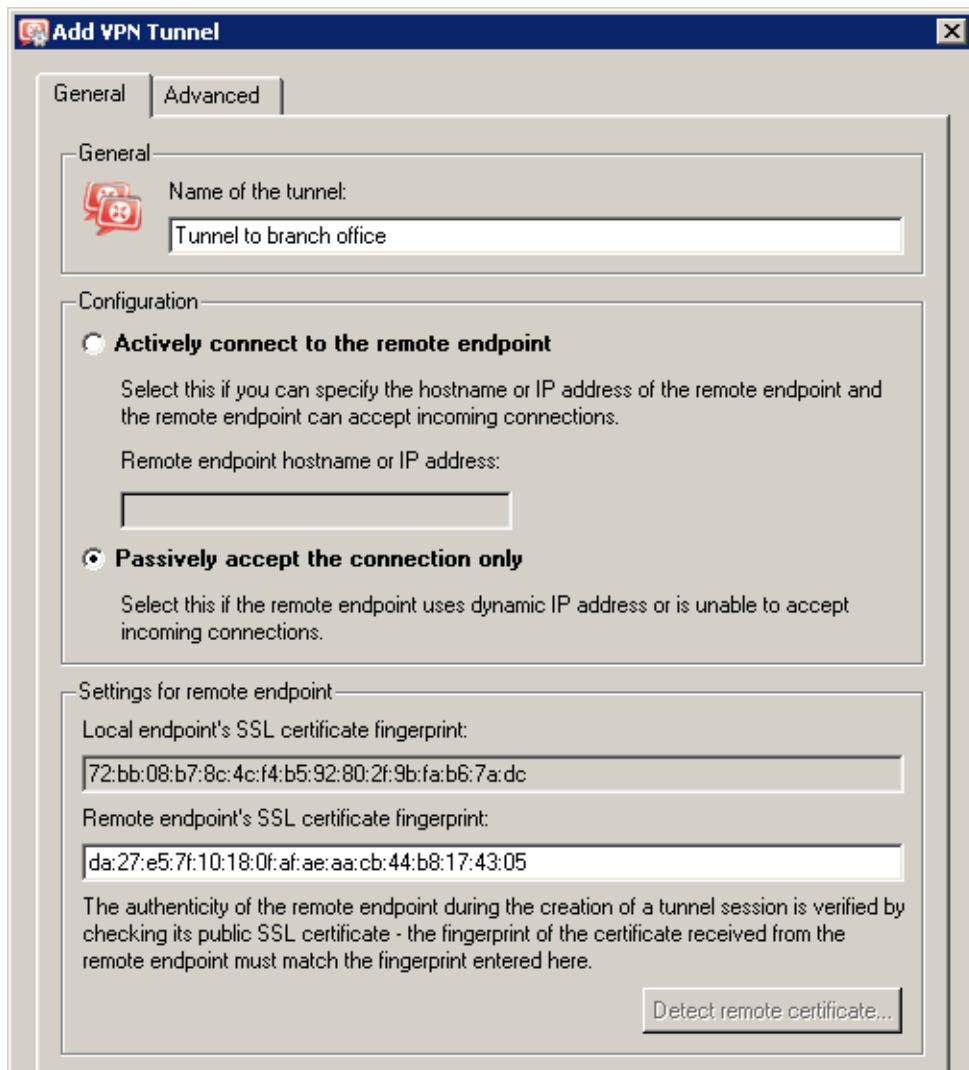


Figure 4.4 Headquarters — the passive endpoint of the filial office's VPN tunnel

- Complete the *Local Traffic* rule (created by the *Network Rules Wizard* — see chapter 2.4) with the VPN tunnel.

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Service Kerio VPN	Any	Firewall	Kerio VPN	✓
<input checked="" type="checkbox"/> Local traffic	Firewall All VPN clients Tunnel to branch office Trusted/Local	Firewall All VPN clients Tunnel to branch office Trusted/Local	Any	✓
<input checked="" type="checkbox"/> Firewall traffic	Firewall	Any	Any	✓

Figure 4.5 Headquarters — adding the VPN tunnel to the traffic rules

Note: The *Firewall traffic* and the *Kerio VPN service* rules are shown at figure 4.5 — both of them are necessary for establishment of the VPN tunnel.

4. In the configuration of the *DNS Forwarder* (refer to chapter 2.6), 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).

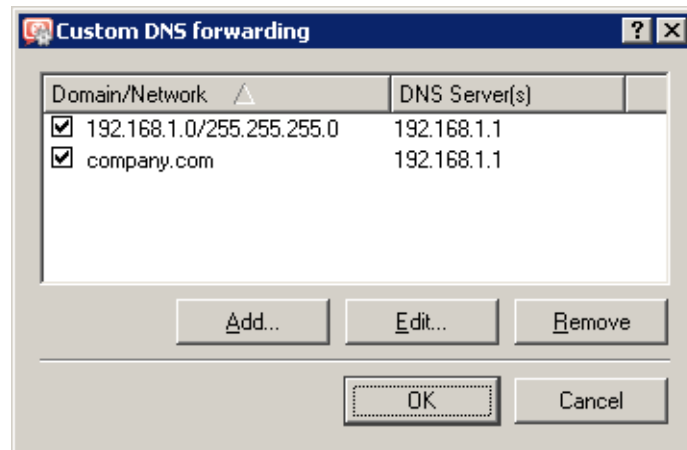


Figure 4.6 Headquarters — DNS forwarding configuration

4.2 Configuration of a filial office

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 free subnet which has been selected for VPN is now 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 the fingerprint of the generated certificate — it will be required during the definition of the VPN tunnel at the headquarters.

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

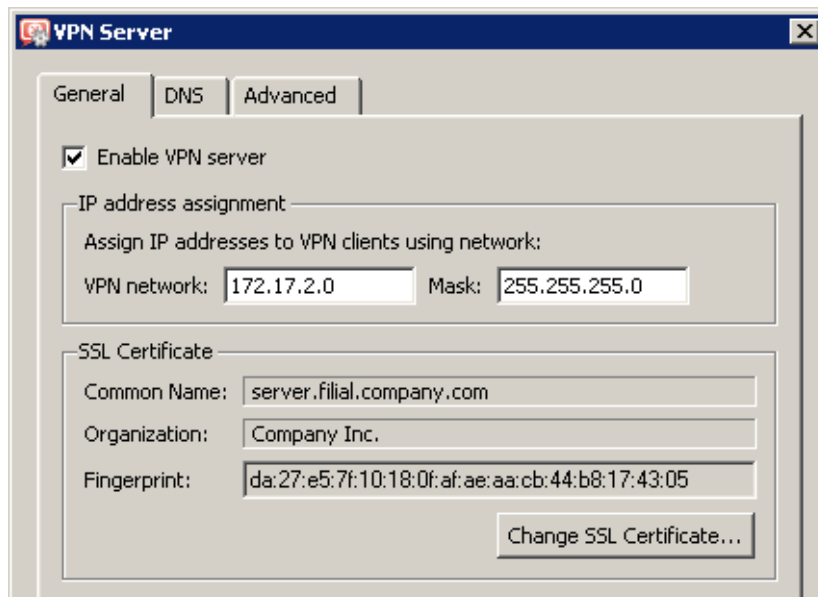


Figure 4.7 Filial office — VPN server configuration

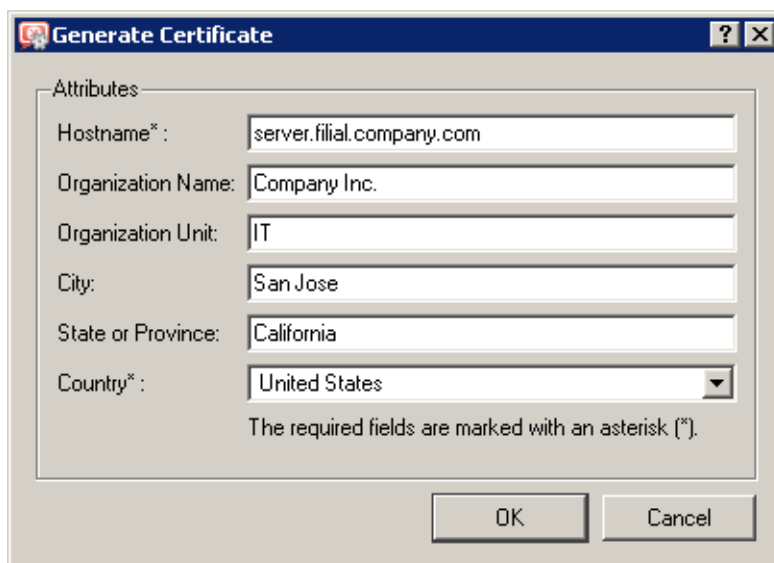


Figure 4.8 Filial — creating of the VPN server's SSL certificate

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*.
3. Complete the *Local Traffic* rule (created by the *Network Rules Wizard* — see chapter 2.4) with the VPN tunnel.

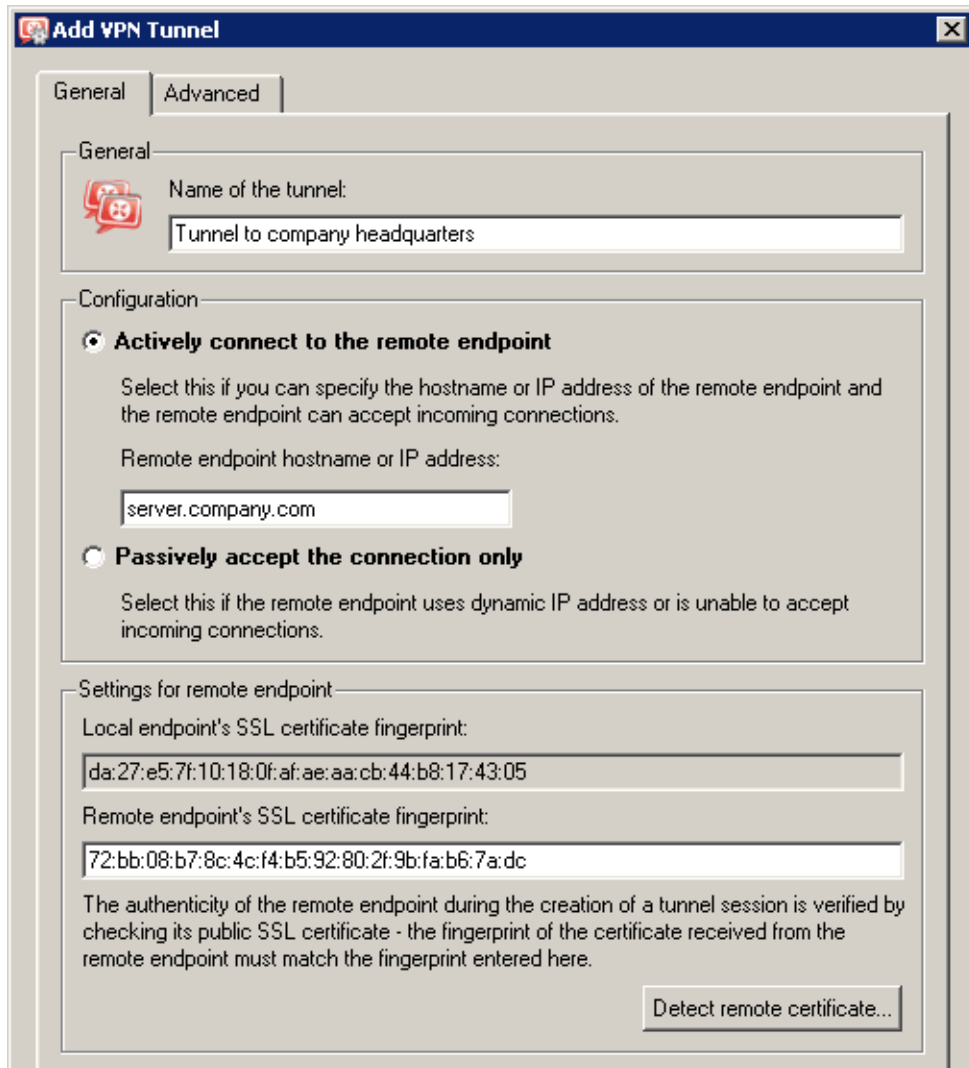


Figure 4.9 Filial — the active endpoint of the VPN tunnel to the headquarters

Name	Source	Destination	Service	Action
<input checked="" type="checkbox"/> Service Kerio VPN	Any	Firewall	Kerio VPN	✓
<input checked="" type="checkbox"/> Local traffic	Firewall Tunnel to company headquarters Trusted/Local	Firewall Tunnel to company head Trusted/Local	Any	✓
<input checked="" type="checkbox"/> Firewall traffic	Firewall	Any	Any	✓

Figure 4.10 Filial — adding the VPN tunnel to the traffic rules

Note: The *Firewall Traffic* rule is shown in figure 4.10 — this rule is necessary for establishing of VPN tunnel.

- In the configuration of the *DNS Forwarder* (refer to chapter 2.6), enable the *Use custom forwarding*. Define rules for the *company.com* domain. Set the IP address of the

headquarter's domain server (192.168.1.2) which is used as the primary server for the company.com domain as the DNS server used for forwarding.

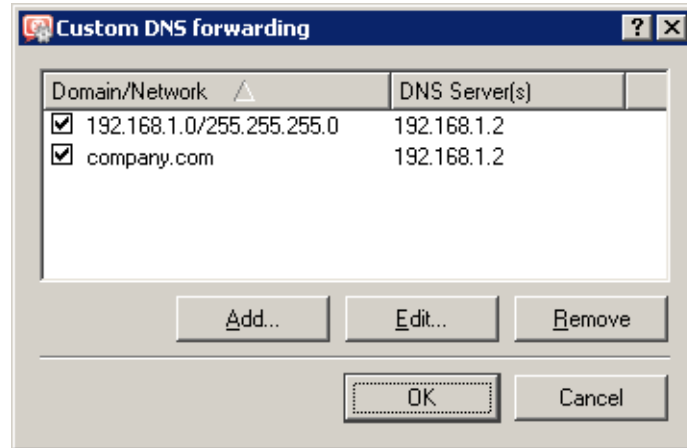


Figure 4.11 Filial — DNS forwarding configuration

4.3 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.

Appendix A

Legal Notices

Microsoft®, *Windows®*, *Windows NT®*, and *Active Directory®* are trademarks or registered trademarks of *Microsoft Corporation*.

Other names of real companies and products mentioned in this document may be registered trademarks or trademarks of their owners.

