Kerio WinRoute Firewall 6

Step-by-Step Configuration

Kerio Technologies s. r. o.

This guide provides detailed description on configuration of the local network which uses the *Kerio WinRoute Firewall*, version *6.7*. All additional modifications and updates reserved.

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

Contents

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, user authentication in the *Active Directory* domain, user browsing behavior control, 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/firewall/manual.

Network configuration example

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

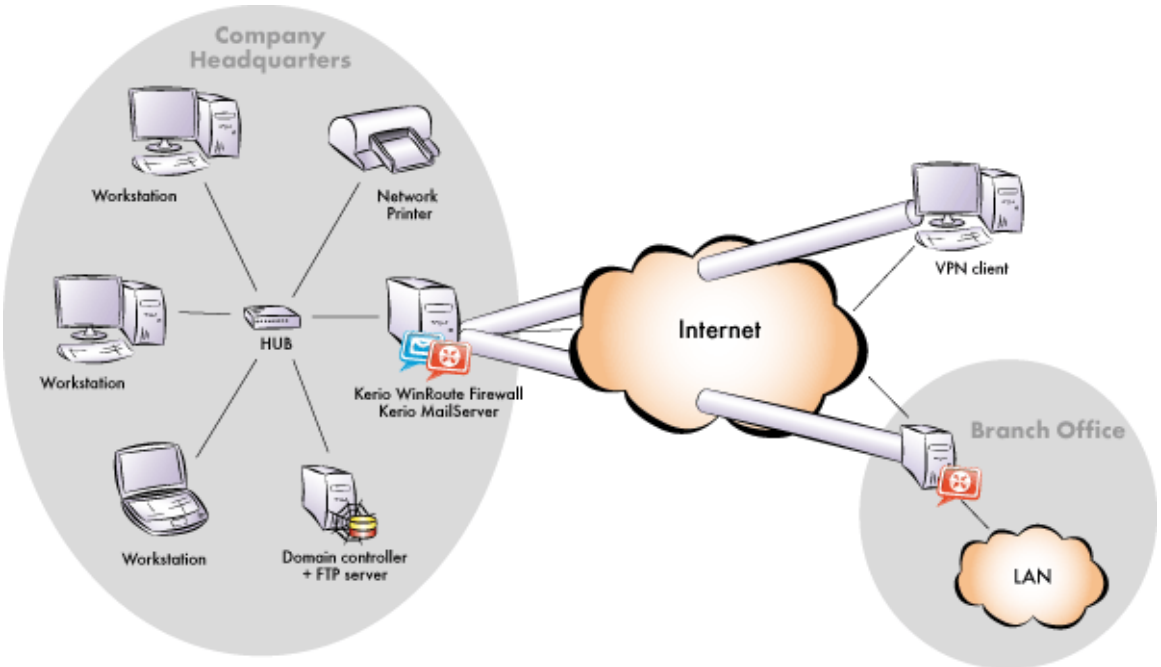

Figure 1.1 Network configuration example

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.

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).

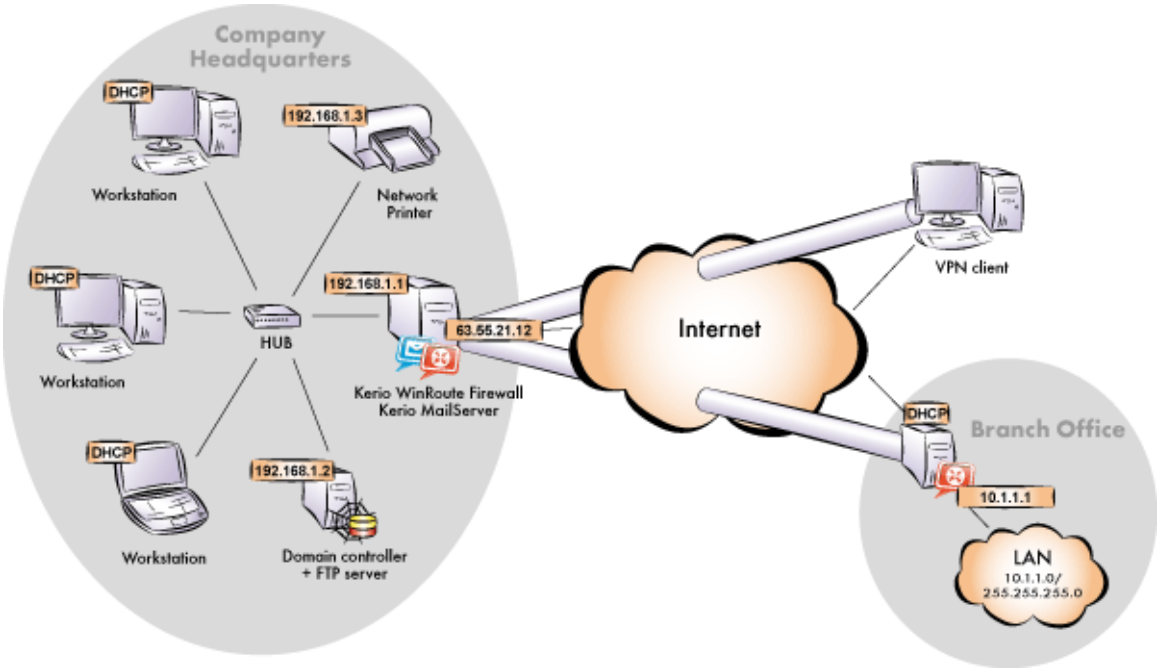

Figure 2.1 Example of configuration of a network with assigned IP addresses

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 aasigned IP adddress `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 (IP adresa `192.168.1.2`).

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 program detects the *Internet Connection Sharing* service, it is recommended to strictly disable this service, otherwise collisions might occur and *WinRoute* may work incorrectly. It is also recommended to disable also other system services which might cause collisions — *Universal Plug and Play Device Host* and *SSDP Discovery Service*.

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 Firewall Engine* and the *WinRoute Engine Monitor* will be automatically launched when the installation is complete.

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 persistent connection with a single Internet line.
- Internet interface (*page 3*) — select an interface connected to the Internet.
- Rules used for outgoing traffic (*page 4*) — these rules enable access to Internet services.
- Rules for VPN (*page 5*) — leave both options enabled: *Create rules for Kerio VPN* (this creates key traffic rules for interconnection of headquarters and filial networks and for connection of remote clients — see chapter 4) and *Create rules for Kerio Clientless SSL-VPN* (remote access to shared folders and files in the network via browser).

  Note: It is meaningless to create rules for *Kerio VPN* at the filial's firewall and for incoming traffic (the server uses a dynamic IP address and clients cannot connect to it). For this reason it is now necessary to disable creating of rules for *Clientless SSL-VPN*.
- Rules for incoming traffic (*Step 6*) — add mapping of SMTP service on the firewall.

  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.

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:

- *Address rsnge* — select `192.168.1.10 to 192.168.1.254` (addresses `from 192.168.1.1 to 192.168.1.9` will be reserved for servers and printing machines),
- *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 (`192.168.1.1` — 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.

Now add a reservation for the network printer. 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.

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. In the list of leased addresses, mark this IP address and click on *Reserve...*. This opens a dialog for IP address reservation with the corresponding MAC address already predefined. Change reserved IP address to the desired one (`192.168.1.3`), edit the description and click on *OK*. 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 enable (allow) 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 (`192.168.1.1`) as the default gateway and DNS server in parameters for this range on the DHCP server.

2.6 DNS configuration

In *Configuration → DNS*, keep the default settings (the *DNS forwarder* service and simple DNS translation woth the `hosts` file and a table of leased addresses are allowed) and set the advanced options:

- Enter the local DNS domain name — `company.com`.
- 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. This setting is required for correct communication of local computers with the domain server.

DNS name	Forward to DNS servers
_*	192.168.1.2

Table 2.1 Rule for 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 chapters 4.1 and 4.2.

2.7 Web interface and SSL-VPN certificates

WinRoute's web interface shows relevant information in case that any attempt to access forbidden web sites is detected (see chapter 2.10). Users can also use the web interface to set various parameters of their accounts or to access statistics. The *Clientless SSL-VPN* interface is used for secured remote connections to shared files in local networks by a web browser.

For proper functionality of web services, an SSL certificate is required that proves the server's identity. To create certificates for web interfaces, go to *Configuration → Advanced Options*, to the *Web Interface / SSL-VPN* tab. In advanced settings of individual interfaces, select *Change SSL certificate* and *Create certificate*.

Name of the server for which the certificate is issued should match the name of the server (including domain) detected from the operating system (see the *Name of the WinRoute host* section in the `kwf.kerio.cz` example). For access to *WinRoute* interfaces from the Internet, a record for this name must exist also in public DNS.

Hint

It is recommended to replace the created SSL certificates by full SSL certificate issued by a public certification authority (one certificate can be used both for the web interface and the *Clientless SSL-VPN* interface — there is no need to pay for two certificates).

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

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*.

To set mapping, DNS name of the domain is required — `company.com` in our example, along with login data of any user belonging to this domain. For automatic authentication with *NTLM* (web browsers, *Kerio Outlook Connector*, etc.), name of the corresponding *Windows NT* domain is also required (i.e. `COMPANY`).

Creating templates for user accounts

On the *User Accounts* tab, select the mapped *Active Directory* domain, i.e. `company.com`. If mapping is set correctly, all user accounts included in the domain will be displayed here.

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*. Set user rights on the *Rights* tab.

Hint

In case you do not want to use any of the domain accounts, you can block them in *WinRoute* and hide blocked accounts. The accounts will be blocked only in *WinRoute*, they will stay active in the domain. Accounts blocked on the domain server will not be even imported to *WinRoute*.

2.9 Address Groups and Time Ranges

Open the *Configuration → 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: Definition of the first group requires name of the new group, later additions allow selection of an existing group.

Likely, go to *Configuration → Definition → Time Ranges* to create a time interval 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.).

Note: You can use predefined day groups (*Weekday* or *Weekend*) to define the *Valid on* entry it is not necessary to tick each day individually.

2.10 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).

Ads filtering and blocking access to specific website categories

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

- It is recommended to keep rules *Allow automatic updates for Kerio software* and *Allow automatic updates and MS Windows activation* enabled, so that *WinRoute* automatic updates and the server's operating system activations work correctly.

- Rules *Allow popular search engines* and *Remove advertisement and banners* can be used according to your needs.

- Rule *Deny sites rated in Kerio Web Filter categories*can be used to block all users access to pages with erotic contents.

  Use the *Select Rating...* button to select *Kerio Web Filter* categories that will be blocked. Then 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.

Restrictions of web pages with job offers

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

1. Add a rule allowing users from the *Human Resources Department* group to access pages categorized by *Kerio Web Filter* as *Job Offers*.
2. Behind this rule, add a rule blocking access to the same category for any other users.
   It is recommended not to require user authentication in this rule. This prevents from redirecting unauthenticated users' browser to the authentication page before showing the information that the page is blocked.

User authentication for accessing Websites

The last optional restriction is user authentication while accessing Web pages. To enable this feature, use the corresponding option under *Users and Groups → Users*, the *Authentication Options* tab.

User authentication is performed within redirection to the *WinRoute* web interface's authentication page. It is necessary that the web interface is enabled and all its parameters set correctly (refer to chapter 2.7). Upon entering a valid username and password, the browser will be redirected to the solicited page.

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*.

With respect to free disk space, modify the cache size. The `1 GB` (`1024 MB`) value is set by the default, the maximum value is almost `2 GB` (`2047 MB`).

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

FTP restrictions specified by predefined 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.
- Modify the *Forbid *.avi files* rule by going to the *Advanced* tab and setting the time when the rule is valid in the *Working hours* range (see chapter 2.9).
- To make it possible for all files transferred by FTP to be checked by the antivirus thoroughly, it is also recommended to enable the *Forbid resume due to antivirus scanning* rule.

FTP server in local network

?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:

- On the *General* tab set the following condition: "if any user acesses FTP server `192.168.1.10`, then allow."
- On the *Advanced* tab, set the operation type to *Upload* and use the wildcard for 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 also 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. The ideal solution is to combine the integrated and an external antivirus (so called dual antivirus check).

In *Configuration → Content Filtering → Antivirus*, on the *Antivirus* tab, set antiviruses and, if applicable, also advanced settings for the selected external antivirus. For complete list of supported antiviruses and their detailed configuration guides, refer to http://www.kerio.com/firewall/third-party#av.

WinRoute allows to select protocols which antivirus check will be applied to. The *HTTP, FTP scanning*, *Email scanning* and *SSL-VPN 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
Access to FTP server	*Any*	*Firewall*	*FTP*	*Allow*	*Mapping 192.168.1.2*

Table 2.2 Making the local FTP servers available from the Internet

- Access to other mail server services (save SMTP) — allowed only from certain IP addresses in the *Working hours* time range.

Name	Source	Destination	Service	Action	Translation	Valid in
Access to email	Group *Access to email*	*Firewall*	*IMAP* *IMAPS* *POP3* *POP3S*	*Allow*		*Working hours*

Table 2.3 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 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.

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

Kerio VPN Client

Kerio VPN Client must be installed at each remote host to enable their connection to the VPN server in *WinRoute*. This application is available for *Windows*, *Mac OS X* and *Linux*. Installation files can be downloaded from http://www.kerio.com/firewall/download.

Clients will connect to the server at the headquarters (i.e. to `63.55.21.12`) and they will be authenticated through their domain usernames and passwords (see chapter 2.8).

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

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.

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

2.16 Viewing statistics of Internet usage and user browsing behavior

WinRoute also includes a web interface called *Kerio StaR* (*statistics and reporting*) which allows to view user browsing behavior as well as statistics in tables and charts.

The monitored activity items include:

- visited websites,
- email messages and instant messaging,
- large file transfers,
- multimedia (online audio and video streaming),
- remote access (terminal access and VPN connection).

Tables and charts are available for the following statistical issues:

- volume of transferred data,
- used protocols (services),
- top visited web domains,
- top requested web categories.

Statistics can be either showed for the overall traffic or for individual users.

Access and authentication to the statistics

Internet usage statistics may include fragile information. For this reason, a special right is used for access to this information, assigned only to the *Admin* by default. Therefore, it is first necessary to grant rights for statistics viewing to specific users and/or groups under *Users and Groups*.

Statistics are available via the *WinRoute* web interface. You can enter the web interface at the URL following this pattern:

`https://<firewall>:4081/`

which is in our example:

`https://kwf.company.com:4081/`

Users with rights to view statistics see the *Kerio StaR* page with overall statistics upon their logon to the web interface. *Kerio StaR*. Other users see the web interface welcome page first.

By default, the web interface is available from the LAN. To make it available from the Internet, it is necessary to define a corresponding traffic rule (see chapter 2.13).

Detailed information addressing the *WinRoute* web interface and *Kerio StaR* is provided in the *Kerio WinRoute Firewall — User's Guide* available at http://www.kerio.com/firewall/manual.

Chapter 3

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 in DNS and DHCP configuration. Supposing that there is no domain server or any other DNS server in the filial's network. The *WinRoute's DNS* module 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!

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

3.2 DNS configuration

In *Configuration → DNS*, keep the default settings (the *DNS forwarder* service and simple DNS translation woth the `hosts` file and a table of leased addresses are allowed) and set the advanced options:

- Enter the local DNS domain name — `filial.company.com`.
- Enable the *Use custom forwarding* option The settings are addressed in details in chapter 4.2.
- 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:
  `10.1.1.1 server`

3.3 DHCP Server Configuration

Go to the *Configuration → DHCP server* section 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:

- *Address range* — select `10.1.1.10 - 10.1.1.254` (addresses `from 10.1.1.1 to 10.1.1.9` will be reserved for servers and printing machines),
- *Network mask* — `255.255.255.0`
- *Default gateway* — IP address of the firewall interface that is connected to the local network (`10.1.1.1`).
- *DNS server* — IP address of the firewall interface that is connected to the local network (`10.1.1.1` — 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.

Chapter 4

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.

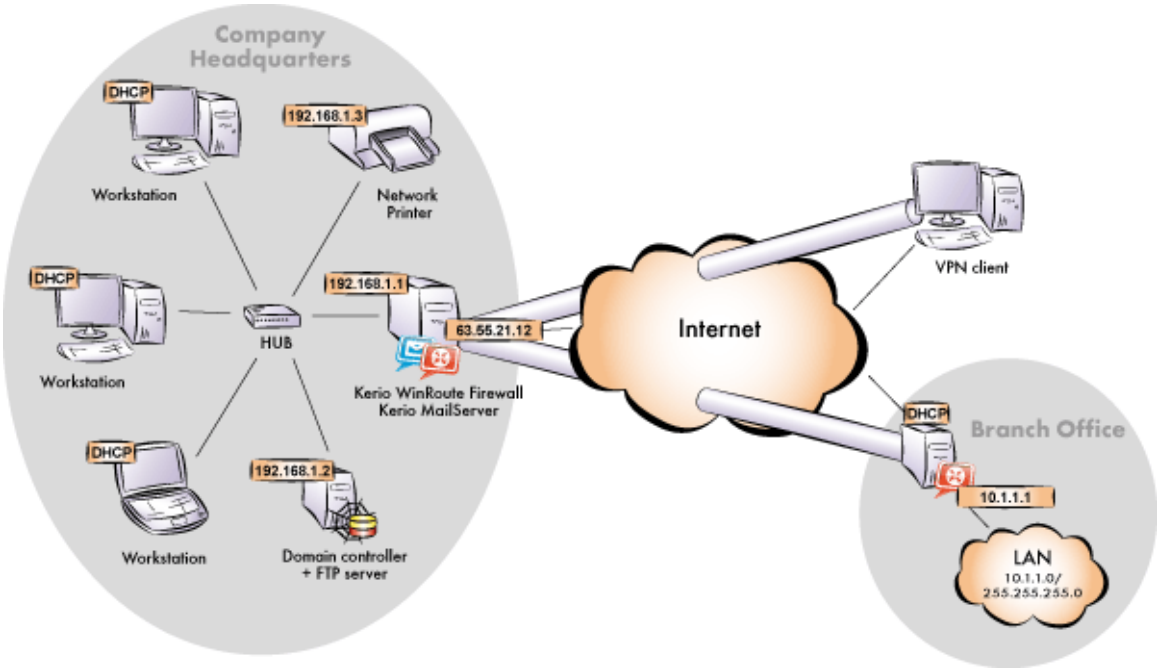

Figure 4.1 Example of configuration of a network with assigned IP addresses

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. In *WinRoute* under *Configuration / Interfaces* select a *VPN server*, open its settings dialog and enable it.
   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.
   Use the *Edit SSL certificate* button to create an SSL certificate with the name of the corresponding server (e.g. `kwf.company.com`). This certificate is used for identification of the VPN 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* endpoint of the VPN tunnel (the office's server uses a dynamic IP address — therefore there must be the active endpoint of the tunnel at the office). Specify the remote endpoint SSL certificate's fingerprint by the fingerprint of the certificate of the branch office VPN server.
3. Complete the *Local Traffic* rule (created by the *Network Rules Wizard* — see chapter 2.4) with the VPN tunnel.

Name	Source	Destination	Service	Action	Translation
Local Traffic	*Firewall* *All VPN clients* *Tunnel to the office* *Trusted / local*	*Firewall* *All VPN clients* *Tunnel to the office* *Trusted / local*	*Any*	*Allow*	

Table 4.1 Headquarters — the Local Traffic rule

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).

Domain / Network	DNS server(s)
`10.1.1.0 / 255.255.255.0`	`10.1.1.1`
`filial.company.com`	`10.1.1.1`

Table 4.2 Headquarters — DNS forwarding configuration

4.2 Configuration of a filial office

1. In *WinRoute* under *Configuration / Interfaces* select a *VPN server*, open its settings dialog and enable it.
   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.
   Use the *Edit SSL certificate* button to create an SSL certificate with the name of the corresponding server (e.g. `server.officebrazil.company.com`). This certificate is used for identification of the VPN server. The fingerprint of the created SSL certificate will be required for definition of the VPN tunnel on the headquarters server (see chapter 4.1). Select it, copy it to the clipboard and paste it to an email message, text file, etc.
   Note: It is recommended to later replace this generated certificate with a certificate authorized by a reliable public certification authority.
2. Create an *active* endpoint of the VPN tunnel which connects to the company's headquarters server (`kwf.company.com`). 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.

Name	Source	Destination	Service	Action	Translation
Local Traffic	*Firewall* *Tunnel to office* *Trusted / local*	*Firewall* *Tunnel to office* *Trusted / local*	*Any*	*Allow*	

Table 4.3 Office (Filial) — the Local Traffic rule

4. 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.

Domain / Network	DNS server(s)
`192.168.1.0 / 255.255.255.0`	`192.168.1.2`
`company.com`	`192.168.1.2`

Table 4.4 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 registered trademarks or trademarks of *Microsoft Corporation*.

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