

gateprotect Manual

Installation, Administration & Examples
of Next Generation UTM Appliances & Virtual Appliances

As of August 2012

| | | |
|----------|---|-----------|
| 1 | Introduction | 9 |
| 1.1 | Who is this manual aimed at? | 9 |
| 1.2 | General notes on this manual | 9 |
| 1.3 | Used symbols und hints..... | 9 |
| 1.4 | Data protection and data security..... | 10 |
| 2 | Installation | 11 |
| 2.1 | Installation of the Firewall Server | 11 |
| 2.1.1 | Installation of the appliance | 11 |
| 2.1.2 | Installation of the Firewall with VMware..... | 11 |
| 2.1.3 | Serial interface..... | 13 |
| 2.2 | Installation of the Firewall Administration Client..... | 13 |
| 2.3 | First configuration of the Firewall Server using the Administration Client..... | 13 |
| 2.3.1 | Starting the Configuration Assistant..... | 13 |
| 2.3.2 | First configuration in quick mode | 14 |
| 2.3.3 | Internet configuration assistant..... | 14 |
| 2.3.4 | Failover (Backup-connection)..... | 17 |
| 2.3.5 | Continuing the Configuration Assistant | 17 |
| 2.3.6 | First configuration in Normal Mode..... | 17 |
| 2.4 | Configuration changes..... | 18 |
| 2.5 | Licensing | 18 |
| 3 | Using the Administration Client..... | 19 |
| 3.1 | Program interface and controls..... | 19 |
| 3.2 | The Administration Client menu | 20 |
| 3.2.1 | Menu: File | 20 |
| 3.2.2 | Menu: Options | 21 |
| 3.2.3 | Menu: Security | 22 |
| 3.2.4 | Menu: VPN Settings..... | 22 |
| 3.2.5 | Menu: Network | 23 |
| 3.2.6 | Menu: Window | 23 |
| 3.2.7 | Menu: Info | 23 |
| 3.3 | The Configuration Desktop | 24 |
| 3.3.1 | Zooming the configuration interface | 25 |
| 3.3.2 | Layer | 25 |
| 3.3.3 | The toolbar..... | 26 |
| 3.3.4 | Active services | 28 |
| 3.3.5 | Further information | 28 |
| 3.3.6 | Search | 28 |
| 3.3.7 | Status bar..... | 28 |
| 3.4 | Reports..... | 29 |
| 3.5 | Denied accesses | 29 |
| 3.6 | Statistics | 30 |
| 3.6.1 | Filter possibilities..... | 30 |
| 3.6.2 | Top-Lists - Internet pages..... | 31 |
| 3.6.3 | Top-Lists - blocked URL..... | 31 |
| 3.6.4 | Top-Lists - services | 31 |
| 3.6.5 | Top-Lists – IDS/IPS..... | 31 |
| 3.6.6 | Users - Toplists..... | 31 |
| 3.6.7 | Users - Traffic | 31 |

| | | |
|-------------|--|-----------|
| 3.6.8 | Defence - Overview | 31 |
| 3.6.9 | Defence - defence | 32 |
| 3.6.10 | Traffic - All data..... | 32 |
| 3.6.11 | Traffic - Internet..... | 32 |
| 3.6.12 | Traffic - E-Mails..... | 32 |
| 3.7 | Firewall | 33 |
| 3.7.1 | Firewall - Security..... | 33 |
| 3.7.2 | Firewall - Date | 34 |
| 3.8 | Interfaces | 34 |
| 3.8.1 | Network interfaces | 35 |
| 3.8.2 | VLAN..... | 35 |
| 3.8.3 | Bridge..... | 36 |
| 3.8.4 | VPN-SSL-Interface | 36 |
| 3.9 | Internet settings | 37 |
| 3.9.1 | General internet settings..... | 37 |
| 3.9.2 | Time period for internet connections..... | 37 |
| 3.9.3 | Global DNS settings in the internet settings..... | 38 |
| 3.9.4 | Dynamic DNS Accounts..... | 38 |
| 3.10 | DHCP Server | 40 |
| 3.10.1 | DHCP Server | 40 |
| 3.10.2 | DHCP Relay | 40 |
| 3.11 | Automatic backup | 41 |
| 3.12 | Routing settings | 42 |
| 3.12.1 | Static routes | 42 |
| 3.12.2 | Routing-Protocols | 43 |
| 4 | Proxies | 57 |
| 4.1 | Introduction..... | 57 |
| 4.2 | HTTP Proxy..... | 57 |
| 4.2.1 | Transparent mode | 57 |
| 4.2.2 | Intransparent mode without authentication | 57 |
| 4.2.3 | Intransparent mode with authentication..... | 57 |
| 4.2.4 | Configuration of the cache | 58 |
| 4.3 | HTTPS Proxy | 58 |
| 4.4 | FTP Proxy..... | 59 |
| 4.5 | SMTP Proxy | 59 |
| 4.6 | POP3 Proxy..... | 59 |
| 4.7 | VoIP Proxy..... | 60 |
| 4.7.1 | General settings..... | 60 |
| 4.7.2 | SIP Proxy..... | 60 |
| 5 | User Authentication | 61 |
| 5.1 | Technical background and preparation..... | 61 |
| 5.1.1 | Aim of User Authentication..... | 61 |
| 5.1.2 | Technical background & preparations | 61 |
| 5.2 | Login | 63 |
| 5.2.1 | Login using a web browser | 63 |
| 5.2.2 | Login using the User Authentication Client (short: UA-Client)..... | 63 |
| 5.2.3 | Login using Single Sign On..... | 63 |

| | | |
|-----------|--|-----------|
| 5.3 | Users | 66 |
| 5.4 | Examples | 66 |
| 5.4.1 | Windows domain | 66 |
| 5.4.2 | Terminal server | 67 |
| 6 | Web-Filter (URL,Content and Application)..... | 68 |
| 6.1 | URL Filter | 68 |
| 6.1.1 | Switching the URL Filter on and off | 68 |
| 6.2 | Content Filter | 69 |
| 6.2.1 | Switching the Content Filter on and off..... | 69 |
| 6.2.2 | Configuration using the URL / Content Filter dialogue | 70 |
| 6.2.3 | Adding URLs using the Administration Client or Statistic Client..... | 72 |
| 6.3 | Application Filter | 73 |
| 6.3.1 | Create profiles | 73 |
| 6.3.2 | How to set up the Application Filter for connections | 74 |
| 6.3.3 | Common settings of the Application Filters | 74 |
| 6.3.4 | Statistics | 75 |
| 7 | LAN Accounting..... | 76 |
| 7.1 | Lan Accounting Introduction..... | 76 |
| 7.2 | Lan Accounting Configuration | 76 |
| 7.2.1 | Creating a time profile..... | 76 |
| 7.2.2 | Create a volume profile..... | 77 |
| 7.3 | Activate Lan Accounting..... | 78 |
| 8 | Traffic Shaping & Quality of Service | 79 |
| 8.1 | Introduction..... | 79 |
| 8.1.1 | Target..... | 79 |
| 8.1.2 | Technical background..... | 79 |
| 8.2 | Settings Traffic Shaping | 80 |
| 8.3 | Settings Quality of Service | 81 |
| 9 | Certificates..... | 82 |
| 9.1 | Introduction..... | 82 |
| 9.2 | Certificates..... | 83 |
| 9.3 | Templates | 86 |
| 9.4 | OCSP / CRL..... | 87 |
| 9.5 | Reports for certificates..... | 88 |
| 10 | Virtual Private Networks (VPN)..... | 89 |
| 10.1 | Introduction..... | 89 |
| 10.2 | PPTP connections..... | 90 |
| 10.2.1 | Setting up PPTP Client-to-Server connection manually | 90 |

| | |
|---|------------|
| 10.3 IPsec connections | 91 |
| 10.3.1 Setting up an IPsec connection manually..... | 91 |
| 10.3.2 L2TP / XAUTH..... | 93 |
| 10.4 VPN over SSL..... | 97 |
| 10.5 VPN over SSL without default gateway | 99 |
| 10.6 The gateprotect VPN Client | 100 |
| 10.6.1 Automatic creation of a VPN connection using a configuration file..... | 100 |
| 10.6.2 Manual creation or edit a VPN connection..... | 100 |
| 11 High Availability..... | 102 |
| 11.1 Functionality..... | 102 |
| 11.2 Downtime while failover | 102 |
| 11.3 Configuration | 103 |
| 11.3.1 IP addresses of the network interfaces | 103 |
| 11.3.2 Connecting the firewalls via dedicated links | 103 |
| 11.3.3 Activating the High Availability..... | 103 |
| 11.4 Edit the settings of High Availability | 105 |
| 11.5 Deactivating High Availability | 105 |
| 11.6 Role change..... | 105 |
| 11.7 Commissioning a firewall after the failure | 105 |
| 11.8 Restoring backup or performing a software Update | 105 |
| 11.9 Report messages..... | 106 |
| 12 Intrusion Detection and Prevention System (IDS/IPS) | 107 |
| 12.1 Configuring IDS/IPS Profiles..... | 107 |
| 12.2 Configuring IDS/IPS Internal/External Network | 108 |
| 12.3 Configuring IDS/IPS Restrictions | 108 |
| 12.4 Activating the Intrusion Detection and Prevention System..... | 109 |
| 12.5 The IDS and IPS rules can be extended with custom rules..... | 109 |
| 12.6 Updating IDS/IPS Patterns | 110 |
| 13 Reporting..... | 111 |
| 13.1 General | 111 |
| 13.2 Partitions..... | 111 |
| 13.3 Syslog-export | 112 |
| 13.4 SNMP | 113 |
| 14 Monitoring..... | 114 |
| 14.1 Introduction..... | 114 |
| 14.2 Components displayed in monitoring..... | 115 |
| 15 Anti-Spam / Mailfilter | 116 |
| 15.1 Mailfilter | 116 |
| 15.2 Anti-Spam | 116 |
| 15.3 Spam-tagging | 117 |

| | |
|---|------------|
| 16 Virus Protection | 118 |
| 16.1 Introduction..... | 118 |
| 16.2 Licensing | 118 |
| 16.3 Settings | 118 |
| 16.3.1 Antivirus settings: General | 118 |
| 16.3.2 Scanner | 119 |
| 16.3.3 White list..... | 119 |
| 16.3.4 Updates..... | 120 |
| | |
| 17 Updates | 121 |
| 17.1 Introduction..... | 121 |
| 17.2 Updates..... | 122 |
| 17.3 Download updates automatically | 123 |
| 17.4 Manually download updates..... | 123 |
| 17.5 Install updates | 123 |
| 17.6 Install updates from local storage device | 123 |
| 17.7 Update interaction..... | 124 |
| | |
| 18 Examples..... | 125 |
| 18.1 Introduction..... | 125 |
| 18.2 Setting up the internet connection with fixed IP address | 126 |
| 18.2.1 Setting up a dedicated line with fixed IP addresses using a router | 126 |
| 18.2.2 Setting up a DSL connection with fixed IP address | 127 |
| 18.2.3 18.2.3 Setting up a cable connection with DHCP IP addresses | 127 |
| 18.3 Demilitarized zone (DMZ)..... | 127 |
| 18.3.1 Simple port forwarding | 127 |
| 18.3.2 Port forwarding with port rerouting | 128 |
| 18.3.3 DMZ by source IP | 129 |
| 18.4 Examples for user authentication..... | 131 |
| 18.4.1 Windows domain | 131 |
| 18.4.2 Terminal server | 131 |
| | |
| 19 Statistics | 132 |
| 19.1 Using the Statistic Client / Statistics..... | 132 |
| 19.1.1 Toolbar..... | 132 |
| 19.1.2 Filter possibilities..... | 132 |
| 19.1.3 Statistics | 132 |

© 2012 gateprotect Aktiengesellschaft Germany. All rights reserved.

gateprotect Aktiengesellschaft Germany
Valentinskamp 24 - 20354 Hamburg /Germany
<http://www.gateprotect.com>

No part of this document may be duplicated or passed to third parties for any purpose without the express written approval of gateprotect AG Germany. This applies regardless of the manner or method, electronic or mechanical, in which this takes place.

The figures and data in this documentation can be changed without prior notification. We accept no guarantee for the accuracy of the content of this manual.

The names and data used in the examples are not real, unless stated otherwise.

All listed products, brands and names are the property of the relevant manufacturer.

FOREWORD

Thanks for choosing a product from gateprotect.

We always strive to improve our products for our customers. If you detect faults or have suggestions for improvement, please get in touch with us.

If you have further questions on gateprotect or our products, please contact your responsible reseller / specialist dealer or contact us directly at:

gateprotect Aktiengesellschaft Germany

Valentinskamp 24
20354 Hamburg
Germany

You can reach us at:

- Telephone : 01805 428 377 (12 Cent/min)
- Fax : 01805 428 332 (12 Cent/min)

You will find up-to-date security updates and other information at:

<http://www.gateprotect.com>

There you will find mygateprotect, which offers you helpful answers, important background information and an array of hints for daily use.

1 INTRODUCTION

With gateprotect Firewall you have chosen a security system that meets the latest security requirements and is very easy to operate using a graphic user interface with drag & drop.

1.1 Who is this manual aimed at?

This manual is aimed at system administrators who install and configure the gateprotect Firewall system. Specialist knowledge is required in the following areas to understand the functions, settings and processes:

- general knowledge in network technology and network protocols
- administration and configuration of Windows operating systems
- user and rights administration in Windows systems

1.2 General notes on this manual

This manual is organized into the following topic areas:

- Introductory chapter with general notes on the product and using the product documentation.
- System requirements, installation of the Firewall server and the Firewall Administration Client.
- Using the Firewall Administration Client and configuring the Firewall Server
- Technical description of the Firewall components and their set-up (Proxy, User Authentication, URL & Content Filter, Traffic Shaping, VPN, High Availability, Intrusion Detection, Reporting, Antispam and Antivirus).
- Description of the Statistic Client as own reporting software
- Typical case examples

1.3 Used symbols und hints



NOTE

THIS SYMBOL HIGHLIGHTS IMPORTANT AND HELPFUL INFORMATION.



ATTENTION

THIS SYMBOL SHOWS THAT PARTICULAR ATTENTION MUST BE PAID AT THIS POINT.



Example

This symbol indicates an explanatory example. Please note that values or entries given (unless stated otherwise) are only used as examples and may differ from the actual values.

Additional symbols are used in the text to mark certain characteristics or to indicate operating elements.

- Dialogue titles, options or buttons are highlighted in *red*.
- Scripts, keyboard or command entries are indicated by a `different font type` in the text.

1.4 Data protection and data security

Under certain circumstances personal data may be processed and used for gateprotect Firewall. In Germany the provisions of the Federal Data Protection Act (BDSG), amongst others, apply to the processing and use of such personal data. Please observe the relevant national laws for other countries.

Data protection protects individuals so that their personal rights are not affected by exposure of their personal data. Furthermore, data protection shields the data from misuse in all processing phases.

2 INSTALLATION

The Firewall consists of two parts. The actual Firewall Server and the Client to operate the Firewall. In this chapter, we describe the necessary steps to install these components and the associated set-up of the different system components.

2.1 Installation of the Firewall Server

Updating to the next major version or restoring the factory defaults are the only reasons to reinstall the Firewall. A CD Installation is only necessary if you bought a Virtual Appliance.

2.1.1 Installation of the appliance

A gateprotect Appliance is installed with a USB-firewall-installer-device. To create this USB-device, please download the designated version of firewall installer from www.gateprotect.com.

A USB-device with a capacity of more than 1GB is needed. Most of the USB-devices in trade should work. A list of tested USB-devices can be found at www.gateprotect.com.

Please connect the USB-device to your Windows-PC and run the USB-installer.



ATTENTION

ALL DATA ON THE DEVICE WILL BE LOST. AN INSTALLATION-WIZARD WILL GUIDE YOU THROUGH THE CONFIGURATION.

Specifics

You can create an auto-installation-USB-device as well.

If you select a backup file of a firewall in the USB-installation-wizard, this backup will be integrated in the USB-installation-device.



ATTENTION

THIS USB-DEVICE WILL INSTALL A FIREWALL IF BOOTED FROM THE DEVICE. PLEASE DO NOT LET THE DEVICE PLUGGED IN ANY OTHER PC WHILE BOOTING!!!

The firewall installation will start, as soon as the appliance boots from the device. (In some cases it must be activated in the BIOS.)

While using a Standard USB-installation-device, you will be guided similar to the CD installation on the console.

See 2.1.2.

Using a auto-install-USB-device, the installation will be done automatically. The appliance will do a peep, when the installation is finished. Please unplug the USB-Device and reboot the appliance.

2.1.2 Installation of the Firewall with VMware

With VMware (Workstation, ESX-Server) it is possible to mount the ISO image which is used for burning the CD. You can proceed as normal with the installation.

The hardware requirements for the virtual machine:

HDD: 20 GB

RAM: 512 MB

This requirements must be scaled to the intended purpose and number of users.

Step 1

Please insert the installation-CD in the CD-drive of the VMware-PC and start the virtual machine.



NOTE

IF THE CD IS NOT IDENTIFIED CORRECTLY, THE BIOS SETTINGS MUST BE CHANGED BEFORE INSTALLING.

Step 2

A UNIX operating system is then started by the CD. Wait until the start screen is opened by the installation program and follow the instructions on the screen.



NOTE

THE FIREWALL SERVER INSTALLATION PROGRAM DOES NOT SUPPORT MOUSE OPERATION. USE THE ARROW KEYS TO NAVIGATE WITHIN THE MENUS AND THE TAB BUTTON TO NAVIGATE BETWEEN THE MENUS. SELECTED OR ACTIVE OPTIONS ARE EITHER HIGHLIGHTED IN RED OR RED TEXT IS USED.

Step 3

Once the license conditions are accepted, automatic hardware recognition begins.

Step 4

Selection of the installation type

A. New installation

B. Installing a backup

If you want to bring in a backup of a previous Firewall configuration instead of a new installation, proceed as follows:



NOTE

THE BACKUP MUST BE ON A DISK OR A USB MEMORY STICK, WHICH CAN BE AUTOMATICALLY DETECTED BY THE SERVER. YOU CAN ALSO SKIP THE BACKUP AT THIS POINT AND PERFORM IT AFTER INSTALLATION VIA THE ADMINISTRATION CLIENT. YOU WILL FIND FURTHER INFORMATION ON THIS IN CHAP. 3.2.1 MENU: FILE – CREATE BACKUP.

Step 5

Hard drive selection

In the hard drive selection window you can determine whether the installation should be performed on one hard drive or a RAID installation on two hard drives.



NOTE

IF YOU ARE USING A VIRTUAL MACHINE, PLEASE USE JUST ONE VIRTUAL HARD DRIVE.

Step 6

Setting up the network devices

You must assign each network card its own IP address and an associated subnet mask. For each network card enter the IP address in the first field and the corresponding subnet mask in the second field, e.g. `192.168.1.1 / 255.255.255.0` for a class C network. DHCP cannot be selected in the installation.



NOTE

IF YOU DO NOT INPUT ANY IP ADDRESS, THE CARD WILL BE AUTOMATICALLY DEACTIVATED. THE FIELDS ARE FILLED IN WITH DEFAULT VALUES IF YOU PRESS "F12".

Step 7

Password entry

Enter a suitable password in the *Password* und *Confirm* fields.



ATTENTION

THE PASSWORD MUST BE AT LEAST 6 CHARACTERS AND CAN INCLUDE LETTERS, NUMBERS AND SYMBOLS. THIS PASSWORD IS ENCODED AND CANNOT BE USED FOR DIRECT LOG-IN TO THE FIREWALL SERVER WITHOUT HELP FROM SUPPORT AT GATEPROTECT. YOU CAN ACCESS THE FIREWALL SERVER VIA THE ADMINISTRATION CLIENT AND DIRECT LOG-IN IS NOT NECESSARY IN GENERAL. THIS ENSURES THAT NO UNAUTHORIZED PERSONNEL CAN LOG-IN INTO THE FIREWALL SERVER DIRECTLY.

The actual installation begins in the next stage.

Step 8

Installation progress

If the installation has been successful, the notification Successful! must appear next to each installation step. After successful installation remove the CD from the drive and hit the Return key to finish and to restart the Firewall Server.

Please wait until the computer has completely rebooted.

The Firewall Server is now ready for use.

2.1.3 Serial interface

The serial interface makes it possible to install the Firewall without an extra monitor and keyboard. You need a RS232 or RJ45 cable, to connect the serial port of the appliance with the serial port of the PC. You have to start a Terminal-Program (e.g. Putty or Hyperterm) with the following parameters:

| | |
|---------------|------|
| Speed: | 9600 |
| Data bits: | 8 |
| Parity: | none |
| Stop bits: | 1 |
| Flow control: | none |

Connect the serial interfaces, plug the USB-Device into the appliance and reboot the firewall. After a few seconds, the installation-dialog will show up in the dialog of the terminal program. You can now use the keyboard to make the settings.

2.2 Installation of the Firewall Administration Client

The Administration Client is on the CD (Autostart Menu) or on the Internet at www.gateprotect.com.

The installation begins automatically after starting the file.

2.3 First configuration of the Firewall Server using the Administration Client

After installation of the Firewall Server and the Administration Client, first perform an initial basic configuration. The Administration Client allows you to operate the Firewall Server either in quick mode or in normal mode.

2.3.1 Starting the Configuration Assistant

Step 1

Start the Administration Client by double clicking on the symbol on the desktop or by clicking on *Start > Programs > gateprotect Administration Client > gateprotect Administration Client*.

Step 2

The start window of the Configuration Assistant is displayed.

Connect the Administration Client to the Firewall Server. To do this, tick the *Search for Firewall* box and click on *Next>>*.

The Configuration Assistant first searches for the Firewall Server in the network of the computer on which the Administration Client was installed, automatically for the first (xxx.xxx.xxx.1) and last IP address (xxx.xxx.xxx.254). If the Configuration Assistant finds the Firewall Server on one of the two addresses, you can skip the following point 3 and carry straight on with the first configuration in quick (*Chap. 2.3.2 First configuration in quick mode*) or normal mode (*Chap. 2.3.6 First configuration in normal mode*).

If the Configuration Assistant does not find the Firewall Server on either of the two addresses, you must enter the address of the Firewall Server manually as described in point 3.

Step 3

The registration dialogue box is opened for you to create the manual connection.

Click on *Add*.

- a.) The IP address dialogue box for the Firewall Server is opened.
- b.) Enter the name and address of the Firewall Server in the appropriate fields. Leave the Port unchanged (Port 3436) and click on *Accept*.
- c.) The *registration* dialogue box is displayed again.

Enter the appropriate values for access to the Firewall Server in the *user name* and *password* fields. Then click on *Register*.



NOTE

FOR A NEW CONFIGURATION OF THE FIREWALL SERVER, THE USER NAME AND PASSWORD IS ALWAYS *ADMIN*. YOU SHOULD CHANGE THIS AS SOON AS POSSIBLE. IF YOU HAVE INSTALLED THE FIREWALL SERVER AS A BACKUP, USE THE USER NAME AND ASSOCIATED PASSWORD SET UP FOR THIS BACKUP.

Connection to the Firewall Server is now established and the Configuration Assistant continues with selection of the configuration mode.

2.3.2 First configuration in quick mode

You can make further adjustments to the settings after the first configuration using the Administration Client.

Step 1

Choose the quick option.

Step 2

The dialogue box to select the desired functions is displayed.

Select the desired options (as described in the dialogue box) by ticking the relevant boxes.

The configuration continues with the Internet Configuration Assistant at point 2.3.3.

2.3.3 Internet configuration assistant

The dialogue box to select the connection type is opened. The gateprotect Firewall Server supports dial-in to the Internet via ISDN, DSL modem or Router. Depending on which Internet connection you use, please follow the appropriate configuration steps in the next chapters.

2.3.3.1 Setting up an ISDN connection

Step 1

Select the option *ISDN Dial-Up Connection* in the dialogue box for selecting the connection type.

Step 2

A list of the available hardware is displayed in the following dialogue box. Choose one of the ISDN cards from the list.

Step 3

Now enter a dial-in number for your Internet access. The *prefix* field must only be activated if you are setting up Internet access via a telephone system. Enter the number in the *prefix* field that you require for an exchange line. Enter the data for the code and number in the appropriate fields.

Step 4

Enter the access data for your ISDN Internet connection given by your Internet service provider.

Step 5

Enter the dial-in settings for your ISDN connection. If you are not sure which settings you should use, please read the information on your ISDN connection or telephone system.

Step 6

Enter the extended settings for the Internet connection. If you are using an internal DNS server, enter the IP address of the server here or use the standard settings.

Step 7

With defined backup control for failover (Internet)

If this control is to act as a master control and, at the same time, is defined as a backup control that can be switched to if necessary, you need to specify 1-2 external servers. You should specify two IP addresses here, which should be hosted by different providers if possible. As pings are regularly sent to the external servers to check the availability of the Internet connection, you should check in advance whether these allow ping. The Firewall Server then checks whether these servers are still available and whether there is a connection.

**NOTE**

FOR ISDN CONNECTIONS WITH A DEFINED TIMEOUT, NO TEST SERVER SHOULD BE ENTERED HERE. OTHERWISE THE TIMEOUT SETTINGS WOULD BE INVALID.

Select the corresponding options or enter the data in the appropriate fields and click on *Next>>*.

Step 8

Enter a clear and meaningful name for the ISDN connection, e.g. "Internet connection by ISDN". Enter the name in the appropriate field and click on "Finished". Your Internet connection is now set up. If you only use this Internet connection via ISDN you can now skip the next steps and continue with the Configuration Assistant.

2.3.3.2 Setting up a PPPoE connection

You must perform the following steps if you are connecting the network cards directly to a DSL modem. If you are using a DSL router for your Internet connection, skip this step and continue with the next section *Chap. 2.3.3.3 - Router connection*.

Step 1

Select the option *PPPoE Connection* in the dialogue box.

Step 2

A list of the installed network cards is displayed in the following dialogue box. Select the network card that is connected to the DSL modem.

Step 3

Enter the access data for your DSL Internet connection given by your Internet service provider.

Step 4

Enter the dial-in settings for your DSL connection. If you are not sure which settings you should use, please read the information on your DSL modem or DSL Internet connection.

Select the corresponding options or enter the data in the appropriate fields.

Step 5

Enter the extended settings for the Internet connection. If you are using an internal DNS server, enter the IP address of the server here or use the standard settings.

With defined backup control for failover (Internet)

If this control is to act as a master control and, at the same time, is defined as a backup control that can be switched to if necessary, you need to specify 1-2 external servers. You should specify two IP addresses here, which should be hosted by different providers if possible. As pings are regularly sent to the external servers to check the availability of the Internet connection, you should check in advance whether these allow ping. The Firewall Server then checks whether these servers are still available and whether there is a connection.

Select the corresponding options or enter the data in the appropriate fields.

Step 6

Enter a clear and meaningful name for the DSL connection, e.g. "Internet connection by DSL modem". Your Internet connection is now set up.

If you only use this Internet connection via DSL you can now skip the next steps and continue with the Configuration Assistant.

2.3.3.3 Setting up a Router connection

You must only perform the following steps if you are connecting the external Firewall connection via a router, e.g. a DSL router to the Internet. If you are using a DSL modem for your Internet connection, please read the previous section on Setting up a DSL connection.

Step 1

Select the option *Router Connection* in the dialog box for selecting the connection type.

Step 2

A list of the installed network cards is displayed in the following dialogue box.

Select the network card that is connected to the Router.

Step 3

Enter the extended settings for the Internet connection. If you are using an internal DNS server, enter the IP address of the server here or use the standard settings.

With defined backup control for failover (Internet)

If this control is to act as a master control and, at the same time, is defined as a backup control that can be switched to if necessary, you need to specify 1-2 external servers. You should specify two IP addresses here, which should be hosted by different providers if possible. As pings are regularly sent to the external servers to check the availability of the Internet connection, you should check in advance whether these allow ping. The Firewall Server then checks whether these servers are still available and whether there is a connection.

Step 4

Enter a clear and meaningful name for this Router connection, e.g. "Internet connection via company router". Enter the name in the appropriate field and click on *Finished*. Your Internet connection is now set up.

2.3.4 Failover (Backup-connection)

If you have already configured an internet connection and you want to configure another connection, it is possible to configure it as a backup-connection. The backup-connection is chosen if your main connection is cancelled. As soon as the main connection works again, the firewall will switch back to it.



NOTE

IN THIS CASE, AN IP ADDRESS (EXTERNAL SERVER) MUST BE ENTERED IN THE MAIN CONNECTION. WITH THIS ADDRESS THE FIREWALL CHECKS IF THERE IS STILL A CONNECTION. (NOTES TO CONFIGURE EXTERNAL SERVERS ARE GIVEN IN THE SECTIONS OF THE DIFFERENT CONNECTION TYPES -ISDN, DSL, ROUTER).

2.3.5 Continuing the Configuration Assistant

Step 1

Enter a password for the Administration Client in the following dialogue box of the Configuration Assistant. The password must be at least 6 characters and can include letters, numbers and symbols. Enter the password in the *New password* field. Confirm this password by entering it in the *Password confirmation* field.

Step 2

Enter the settings for the date and time of the Firewall Server. Choose the current time zone or specify if the server time will be regularly adjusted by a time server from the Internet.

Step 3

All necessary information has now been entered and the Configuration Assistant can be closed.

Step 4

If you already have a valid license number for the gateprotect Firewall Server, the gateprotect Content Filter or gateprotect Antivirus, you can now activate this license(s) directly if this has not already been done. However, you can also perform activation at a later time. You will find further information on the license manager and licensing the gateprotect Firewall Server in *Chapter 2.5 "Licensing"*.

The configuration is now complete. The configuration data are now transferred to the Firewall and the gateprotect Administration Client switches to the configuration interface.

2.3.6 First configuration in Normal Mode

If you have already performed first configuration in quick mode, you can skip this chapter.

Step 1

Choose the *normal* option.

Step 2

Enter a password for the Administration Client in the following dialogue box of the Configuration Assistant. The password must be at least 6 characters and can include letters, numbers and symbols.

Step 3

Enter the settings for the date and time of the Firewall Server. Choose the current time zone or specify if the server time will be regularly adjusted by a time server from the Internet.



NOTE

IT IS NOT POSSIBLE TO ACTIVATE THE NTP SERVICE AT THIS POINT, AS NO INTERNET CONNECTION HAS BEEN SET UP IN NORMAL MODE. ACTIVATE THIS OPTION IN THE ADMINISTRATION CLIENT AT A LATER TIME, ONCE YOU HAVE SET UP AN INTERNET CONNECTION.

Step 4

All necessary information has now been entered and Configuration Assistant can be closed.

Step 5

If you already have a valid license number for the gateprotect Firewall Server, the gateprotect Content Filter or gateprotect Antivirus, you can now activate this license(s) directly if this has not already been done. However, you can also perform activation at a later time. You will find further information on the license manager and licensing the gateprotect Firewall Server in *Chapter 2.5 "Licensing"*.

The configuration is now complete. The configuration data are now transferred to the Firewall and the gateprotect Administration Client switches to the configuration interface.

2.4 Configuration changes

If you want to adjust the Firewall Server to your individual requirements, you will find further information on the relevant topics and setting possibilities in the following chapters.

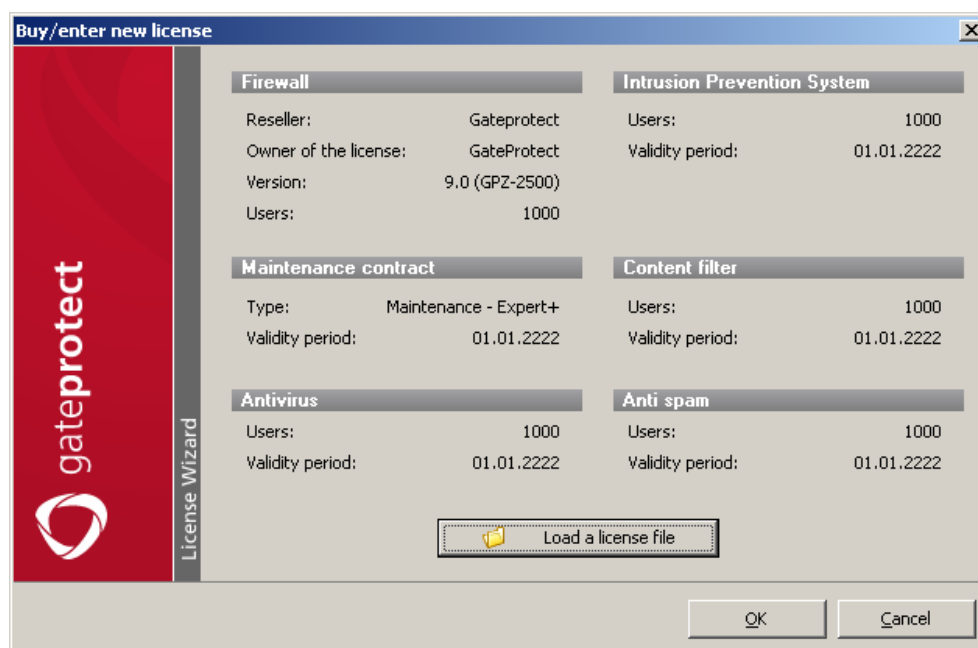
2.5 Licensing



ATTENTION

YOUR FIREWALL RUNS FOR 45 DAYS AS A TEST VERSION AFTER INSTALLATION OF THE SERVER. YOU WILL SEE THIS WHEN YOU REGISTER TO START THE ADMINISTRATION CLIENT. ONCE THIS TIME HAS LAPSED, THE FIREWALL REMAINS ACTIVE WITH YOUR CONFIGURATION, BUT YOU CANNOT PERFORM ANY CHANGES AND THE HTTP PROTOCOL IS BLOCKED.

The licensing is managed by the License-Wizard, which can be found in the menu *Info*.



The licensing works with a .gplf formatted data file.

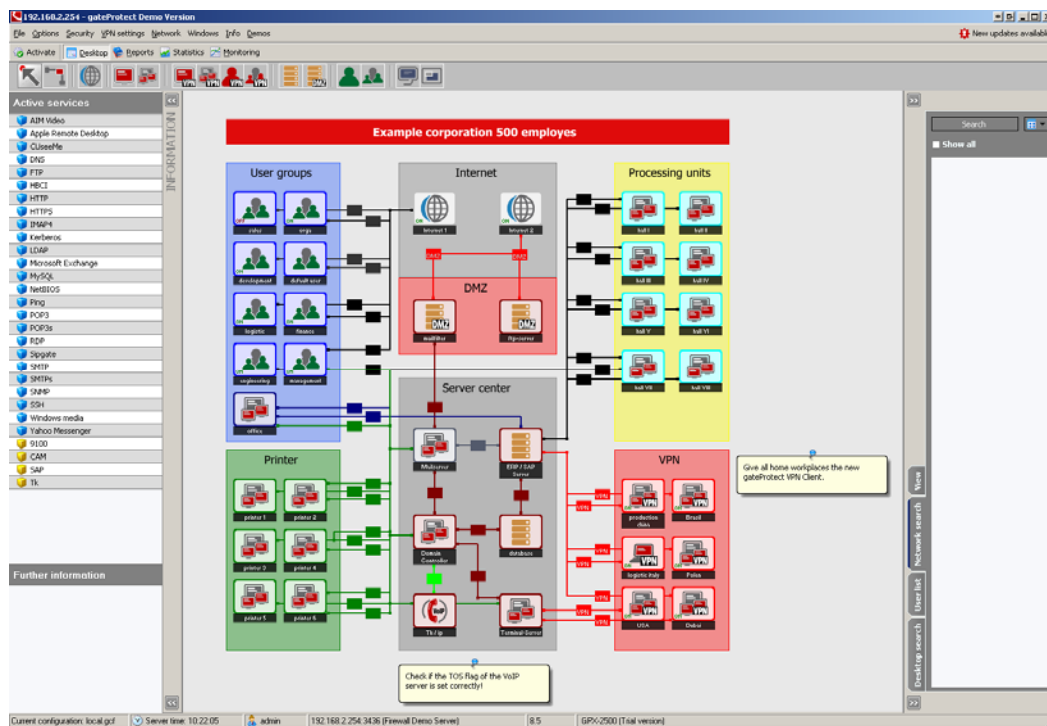
You can upload this file to the firewall, all data about the license and licensee are automatically added in the firewall.

3 USING THE ADMINISTRATION CLIENT

You can manage all settings of the gateprotect Firewall Server using the Administration Client. This chapter explains how to use this program, what possibilities the Administration Client offers and how you can perform basic configuration settings.

3.1 Program interface and controls

When the program starts for the first time you will find yourself in the configuration desktop. This is the central administration interface, with which you can make all necessary setting adjustments to the Firewall.



3.2 The Administration Client menu

3.2.1 Menu: File

In the File menu you will find the usual Windows options for opening, saving, printing and ending the program. Additionally, there are also functions for creating and loading backups of the Firewall Server.

| Option | Function |
|-----------------------------------|--|
| New | Creates a new Firewall configuration. |
| Open... | Opens an existing Firewall configuration either directly from a connected Firewall or from a saved configuration file. |
| Save | Saves the current Firewall configuration directly to a connected Firewall. |
| Save as... | Saves the current Firewall configuration directly to a connected Firewall or in a configuration file on the computer or in the network. |
| Print... | Prints the current configuration, the statistics or the monitoring to a connected printer. |
| Create Backup | Creates a backup of the current Firewall configuration in any storage medium. Use this function, for example to reload a configuration after a new installation, or to transfer a configuration to a second (secondary) Firewall for a high availability solution. |
| Import Backup | Loads a Firewall configuration from a backup file and then activates this. |
| Automatic Backup | Configuration of the automatic Backup function <i>Chap. 3.11 Automatic Backups</i> |
| Rerun to the configuration wizard | Starts the Configuration Assistant in quick or normal mode, to configure a basic configuration <i>Chap. 2.3 First configuration of the Firewall Server using the Administration Client</i> |
| Activate | Transfers a configuration to the Firewall Server, without closing the Administration Client first. |
| Language | Changes the language of the Administration Client |
| Exit... | Closes the gateprotect Administration Client after displaying several options for closing the program in a dialogue box and you have confirmed that you want to exit. |

3.2.2 Menu: Options

You can configure the settings of the Server and the Administration Client using the Options menu.

| Option | Function |
|---------------------|---|
| Firewall | Adjusts the general server settings to your needs, e.g. network or host name, network cards, security settings for the administration or date and time settings . |
| Command Center | Adjustment and creation of Command Center certificates |
| Interfaces | Configuration of the network interfaces, V-LANs, Bridges and VPN-SSL Interfaces |
| Routing | Management of routing protocols and routes. |
| User management | Manges the users and their specific rights on the Firewall. |
| Internet | Manages the Internet connections and changes global DNS settings or settings for dynamic DNS. |
| Proxy | Activates and configures the settings for the HTTP and VoIP Proxy of the Firewall Server <i>Chap. 4 Proxies.</i> |
| Traffic-Shaping | Configures the settings for Traffic Shaping and Quality of Service <i>Chap. 7 Traffic Shaping & Quality of Service.</i> |
| High availability | Defines settings for several Firewall Servers, which run as a high availability solution <i>Chap. 11 High Availability.</i> |
| DHCP | Configuration of DHCP Server and Relay. |
| Reporting | Manages the reporting settings, e.g. the recipient options for the e-mail notification and the settings for the partitions <i>Chap. 13 Reporting</i> |
| User authentication | Configures the options for the User authentication and registration to the HTTP Proxy <i>Chap. 5 User Authentication.</i> |
| Updates | Update management of the Firewall. |

3.2.3 Menu: Security

You can use this menu to manage the different safety settings of the Firewall Server.

| Option | Function |
|------------------------|---|
| URL-/Contentfilter... | Activates and configures the settings for the URL and Content Filter <i>Chap. 6 URL- and Content-Filter.</i> |
| Anti-Spam / Mailfilter | Creates black and white lists for the spam filter and adjust the level of sensibility <i>Chap. 15 Anti-Spam/Mailfilter</i> |
| Anti-Virus | Activates and manages the settings for the Antivirus scanner <i>Chap. 16 Virus protection</i> |
| IDS / IPS | Manages the settings for the Intrusion Detection and Prevention System <i>Chap. 12 Intrusion Detection and Prevention</i> |
| Certificate | Opens the certificate administration for Certificate Authorities, Requests and Host Certificates. |
| DMZ-list | Shows the DMZ objects |
| Denied accesses ... | Shows a list of the rejected accesses and enables you to release or reject these connections. |

3.2.4 Menu: VPN Settings

You can manage the settings for the VPN connections to the Firewall Server using this menu.

| Option | Function |
|------------|---|
| PPTP | Activates the PPTP settings of the Firewall Server <i>Chap. 10.2 PPTP-connections.</i> |
| IPSec | Activates the IPSec settings and manages IPSec connections <i>Chap. 10.3 IPSec-connections.</i> |
| VPN-SSL | Activates VPN-SSL connections and manages the VPN-SSL characteristics and Client <i>Chap. 10.4 VPN over SSL.</i> |
| VPN Wizard | Creates a new VPN connection and sets up all necessary configuration settings for the VPN connection. |

3.2.5 Menu: Network

This menu contains tools, which support you in configuration, for network tests or in problem solving and error searches.

| Option | Function |
|-----------------------|---|
| Ping | Issues a PING command to a computer / server in the network or in the Internet. Select as an option whether the PING command is to be issued from the local computer or from the Firewall Server. |
| Traceroute | Issues a TRACEROUTE command to a computer / server in the network or in the Internet. |
| Query name server | Queries information on an address with the name server. |
| Web blocking analysis | Performs a check of a URL or a website using the URL and Content Filter <i>Chap. 6 URL- and Content-Filter</i> . |

3.2.6 Menu: Window

Switches between the different views in the Administration Client.

| Option | Function |
|------------|--|
| Desktop | Switches to the Configuration Desktop to manage network and Firewall settings. |
| Reports | Switches to the report view with up-to-date system and security notifications. |
| Statistics | Statistics Shows general and security-relevant statistics on users, network objects and the Firewall Server. |
| Monitoring | Delivers up-to-date information on hardware and system processes of the Firewall Server. |

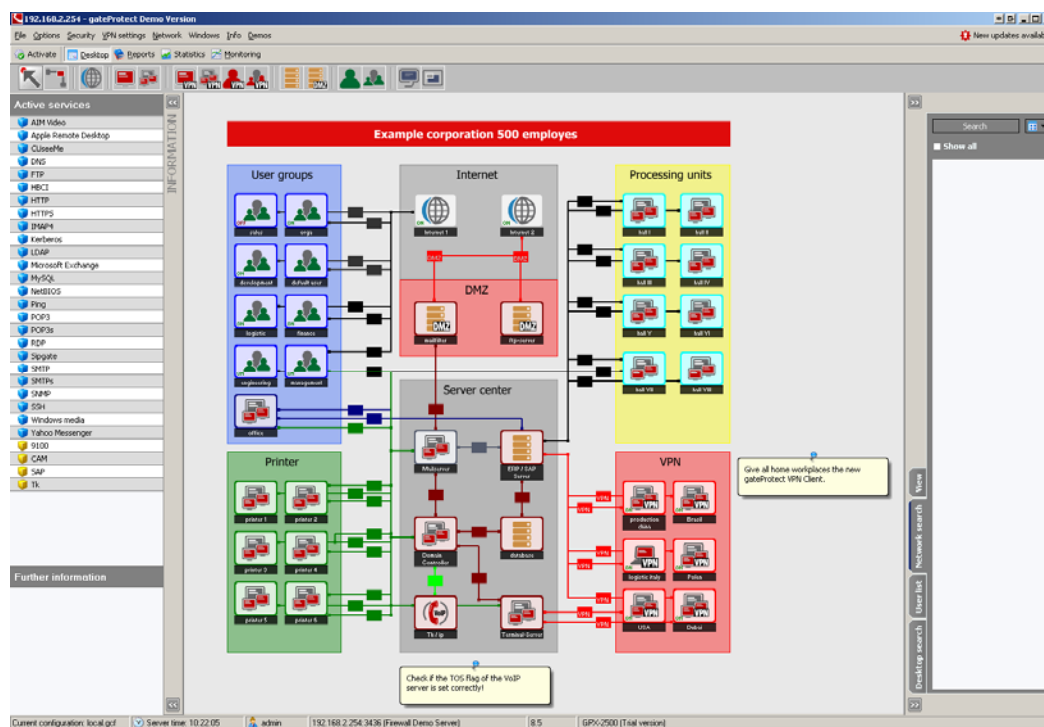
3.2.7 Menu: Info

Offers the user the standard Windows help and support functions.

| Option | Function |
|---------------------|---|
| User manual | Opens this manual |
| Licence gateprotect | Opens the licensing dialogue box to licence the Firewall and UTM products |
| Show license terms | Displays the current licence conditions as a PDF document. |
| About | Provides version information on the Administration Client. |

3.3 The Configuration Desktop

The user interface shows the main work area of the gateprotect Firewall. Using the configuration desktop; you always have a complete overview of your entire network.

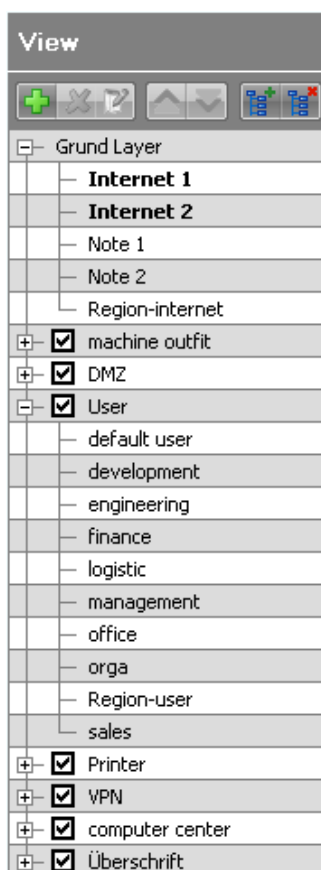


- All objects connected to the network (computers, servers, computer groups, VPN users, etc.) are displayed with their associated connections.
- New objects can be added at any time with "Drag & Drop".
- You can create rules for the connections simply by clicking on the intersections of the connection lines.
- Individual objects can be compiled in groups using "drag and drop" and configured jointly.
- If you drag one object onto another one, you will be asked whether you want to create a group of both the individual objects
- Several objects and points can be selected simultaneously by clicking on an empty place on the desktop and defining the desired range with the mouse. Individual objects and points can be added to / removed from the selection using Ctrl + left mouse button.
- Ctrl + A selects all objects and points on the desktop.
- If needed, connection lines can be wrapped several times for a better overview. Double clicking on the line creates a new wrapping point at this position. The rule point and the wrapping points can be moved freely on the desktop.
- The end points of a line "snap" to the respective object however can be freely moved on its sides.
- Double clicking on a wrapping point (except the end points) deletes it.

3.3.1 Zooming the configuration interface

The desktop has a zoom function. This is supported by a thumbnail (bottom right in the View frame). The desktop can be reduced to an area between 30% and 100%. If the complete desktop is not visible, the visible range is shown as a blue rectangle in the thumbnail. The thumbnail can be used for navigation (when parts of the desktop are not visible).

3.3.2 Layer



The desktop has a standard and several user-defined layers. The standard layer, called the base layer, can be renamed but not deleted. It is always the first one in the list.







The user-defined layers can be hidden. Doing this hides the objects on the respective layer and all associated lines for them. The order of the user-defined layers can be changed in any way. The user-defined layers can be deleted. Their objects migrate to the base layer.










Objects can be moved freely on all layers. The exceptions are the Internet objects. They are always on the base layer. Objects on a "lower" layer are displayed last on the desktop and cross faded objects from an "upper" layer.

3.3.3 The toolbar

In order to create an object on the configuration desktop, click on the desired object in the toolbar, keep the mouse button pressed and drag the object onto the configuration desktop. Depending on the type of object, a window is automatically opened where you can input the data for the object.

In order to *delete* an object from the configuration desktop, click on the object with the right mouse button and select the "Delete" menu item from the context menu

| Symbol | Function |
|---|---|
|  | <p>Selection tool</p> <p>You can perform all actions on the Configuration Desktop with the selection tool. You can add symbols, move objects or select certain functions.</p> |
|  | <p>Connection tool</p> <p>You can connect symbols with one another on the configuration desktop using the connection tool. First click on the symbol of the connection tool and then on the first symbol and then on the second. The two symbols are connected to one another and the rules editor opens automatically to determine connection rules.</p> |
|  | <p>Internet</p> <p>If you double click on this object you can configure your Internet connections.</p> |
|  | <p>Equipment</p> <p>Drag a piece of equipment (computer, server, network printer, laptop or IP telephone) to the Configuration Desktop and enter further object characteristics for the computer in the open dialogue box.</p> <p>Naturally, you can amend each piece of equipment by choosing the type of the object using one of the buttons in the characteristics of the object dialogue box.</p>  |
|  | <p>Group</p> <p>The aim of a computer group is clarity and simple configuration. Several computers in one department can be configured together. Each computer receives all rights that its group has.</p> <p>Drag a group to the Configuration Desktop, enter further characteristics for the group in the open dialogue box and create new objects within this group.</p> <p>Drag individual objects already on the Configuration Desktop to a group symbol with the mouse to assign this individual object to this group.</p> <p>A computer group contains individual computers, which are manually added or directly accepted into this group from the Configuration Desktop.</p> |

| Symbol | Function |
|---|---|
|  | <p>Group</p> <p>For a network group, select a network card of the Firewall Server and all connected computers then belong to this group.</p> <p>The mode IP-Range allows configuring a start and ending address. If DHCP is configured for this interface, it is also possible to choose this range.</p> |
|  | <p>VPN computer and VPN server</p> <p>Drag a VPN computer to the desktop, specify general settings for the VPN computer in the open dialogue box and create a new VPN connection. You will find further information on VPN objects and their set-up in <i>Chap. 10 Virtual Private Networks (VPN)</i></p> |
|  | <p>VPN group</p> <p>Drag a VPN group to the desktop, specify general settings for the VPN group in the open dialogue box and add existing VPN users to this VPN group.</p> <p>You will find further information on VPN groups and their set-up in <i>Chap. 10 Virtual Private Networks (VPN)</i></p> |
|  | <p>VPN-User</p> <p>VPN-User can register via L2TP or XAUTH.</p> |
|  | <p>DMZ-Object</p> <p>After adding a DMZ-Object on the configuration desktop, the DMZ-Wizard starts automatically and guides you in all necessary configuration steps.</p> |
|  | <p>Users</p> <p>Drag a user to the desktop and enter further user characteristics in the open dialogue box.</p> <p>You will find further information on users and their set-up in <i>Chap. 5 User Authentication.</i></p> |
|  | <p>User groups</p> <p>Drag a user group to the desktop, enter further settings for the group in the open dialogue box and add existing users to this user group.</p> <p>You will find further information on users and their set-up in <i>Chap. 5 User Authentication.</i></p> |
|  | <p>Notes objects can simply be dragged onto the desktop. The Notes object can be used for any notes on the desktop and is saved with the configuration like any other object.</p> |
|  | <p>The Regions object is an aid for highlighting groups and areas in color. Simply drag the object onto the desktop, select the color and degree of transparency and give it a name. Now you can move the object any way you like and adapt its size.</p> |

3.3.4 Active services

In the *Active Services* window on the left-hand side of the Configuration Desktop you will find a list of all predefined or self-defined services previously entered into the network. If you click on a service from the list with the mouse, all object and connection lines that include this service are highlighted in color. All other objects and connection lines remain grey.

3.3.5 Further information

If you click on a service in the list, an object or a user on the Configuration Desktop, you will see supplementary information on the relevant service, object or user in the *Further Information* window.

3.3.6 Search

In the *Search* window on the right-hand side of the Configuration Desktop you can search for individual computers, users, groups or connections.

Network search

You can use the network search to find switched on computers, which have not yet been included as independent objects or as part of a computer group. To search for computers that are already on the Configuration Desktop as an object or part of a computer group, select the *Display All* box.



NOTE

PLEASE NOTE THAT A COMPUTER CAN ONLY BE FOUND IF IT IS IN THE NETWORK AND ACCESSIBLE.

If you drag a found computer with the mouse to an existing group on the Configuration Desktop, this computer will automatically be assigned the rights of this group.

User list

The user list contains all entered users (this concerns already defined users, not the computers). If you select a user with the mouse, you will see on the desktop which group this user is assigned to.

Desktop search

You can use the desktop search to look through all already configured elements on the whole Configuration Desktop. The results of the search as displayed in an expandable list sorted by group or type of object.

3.3.7 Status bar

The status bar at the bottom of the Administration Client shows further information on the Administration Client:

- Current configuration
- Server time
- Registered users
- IP address of the firewall server
- Version number and version description of the Administration Client
- Type of license

3.4 Reports

The Administration Client displays system and intrusion detection reports produced by the Firewall Server.

1. You can access the report view by clicking on the *report* symbol in the toolbar or by selecting *Reports* from the main menu window.
2. The *Current Reports* window shows a list of the last 30 system reports from the Firewall Server. The *Update Reports* button loads the current data from the Firewall Server to the report display.

| Report ID | Date | Type | Message |
|-----------|---------------------|----------|--|
| 1 | 22.12.2009 01:00:00 | Internet | IPSec ending on signal IS |
| 2 | 22.12.2009 01:00:00 | Server | IPSec driver unloaded successfully |
| 3 | 22.12.2009 01:00:00 | Server | IPSec starting with 9 devices... |
| 4 | 22.12.2009 01:00:00 | Server | IPSec driver loaded successfully |
| 5 | 22.12.2009 01:00:00 | Server | Checking IPsec after NAT on POSTROUTING |
| 6 | 22.12.2009 01:00:00 | Server | Checking IPsec before NAT on POSTROUTING |
| 7 | 22.12.2009 01:00:00 | Internet | IPsec v. 2.0.0 user |
| 8 | 22.12.2009 01:00:00 | Internet | kernel time sync status (000) |
| 9 | 22.12.2009 01:00:00 | Server | Short initialization completed successfully (ipsec=217172, interface=ppp1) |
| 10 | 22.12.2009 01:00:00 | Server | Terminated ipsec on interface ppp1 |
| 11 | 22.12.2009 01:00:00 | Server | Started ipsec on interface ppp1 |
| 12 | 22.12.2009 01:00:00 | Server | IPsec DynEMG update was successful |
| 13 | 22.12.2009 01:00:00 | Server | IPsec driver unloaded successfully |
| 14 | 22.12.2009 01:00:00 | Server | IPsec starting with 9 devices... |
| 15 | 22.12.2009 01:00:00 | Server | IPsec driver loaded successfully |
| 16 | 22.12.2009 01:00:00 | Server | Checking IPsec after NAT on POSTROUTING |
| 17 | 22.12.2009 01:00:00 | Server | Checking IPsec before NAT on POSTROUTING |
| 18 | 22.12.2009 01:00:00 | Server | Short initialization completed successfully (ipsec=20120, interface=ppp1) |
| 19 | 22.12.2009 01:00:00 | Server | Terminated ipsec on interface ppp1 |
| 20 | 22.12.2009 01:00:00 | Server | Started ipsec on interface ppp1 |
| 21 | 22.12.2009 01:00:00 | Server | Short initialization completed successfully (ipsec=20199, interface=ppp1) |
| 22 | 22.12.2009 01:00:00 | Server | kernel time sync status change (000) |
| 23 | 22.12.2009 01:03:00 | Internet | time reset: 45.145229 s |
| 24 | 22.12.2009 08:10:00 | User | Accepted password for root from 192.168.11.60 port 50298 via telnet |
| 25 | 22.12.2009 08:50:00 | User | DUP: User "root" logged in via SSH from 192.168.11.60/50298 |
| 26 | 22.12.2009 09:10:00 | Server | DUP:PACK on 10.106.111.68 to 10.106.94.51:4352 (system default) via eth2 |
| 27 | 22.12.2009 11:18:00 | Server | To enabled backup "Backup of 192.168.11.16 ip" to 10.106.9.20 via scp |
| 28 | 22.12.2009 15:53:00 | Server | accepted connection from 192.168.11.60 |

3. The *Overall Report* window contains a list of all system reports from the Firewall Server, which can be filtered by different criteria:
 - by period with date and time for start and end
 - by type and status of the report
 - by user-defined text
 - number of reports
4. The *IDS / IPS Report* window shows the current log data of the Intrusion Detection and Prevention System.

3.5 Denied accesses

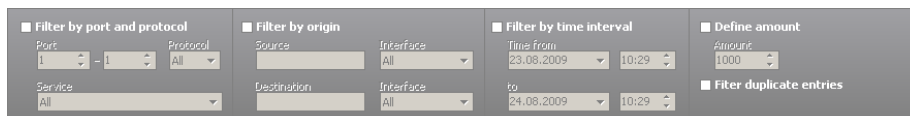
Open the dialogue box from the main menu *Security*, then select *Denied Accesses*.

| Protocol | Port | Source | User | In-Iface | Destination | User | Out-Iface | Date/Time |
|----------|------|----------------|---------------|----------|---------------|------|-----------|---------------------|
| tcp | 21 | 192.168.5.100 | | eth0 | 192.168.9.100 | | eth1 | 24.08.2009 07:12:56 |
| tcp | 80 | 192.168.1.101 | | eth0 | 192.168.9.101 | | eth1 | 24.08.2009 01:19:28 |
| tcp | 139 | 45.237.121.188 | | internet | 192.168.8.254 | | eth2 | 24.08.2009 02:20:49 |
| tcp | 6667 | 62.40.120.5 | | internet | 192.168.8.254 | | eth2 | 23.08.2009 15:23:06 |
| tcp | 21 | 192.168.4.6 | Mr. Schneider | eth2 | 21.4.10.5 | | internet | 23.08.2009 20:10:05 |
| tcp | 34 | 192.168.4.6 | Mr. Schneider | eth2 | 21.4.10.5 | | internet | 24.08.2009 03:45:35 |
| tcp | 4284 | 41.21.3.2 | | internet | 21.4.10.5 | | firewall | 23.08.2009 17:01:31 |

Legend:
 → internal -> external
 → external -> internal
 ↻ intern -> intern
 ✓ Allowed
 ✗ Forbidden

7 denied accesses found.

1. First update the list by clicking on the *Update* button.
The list shows all connections blocked by the Firewall Server. The red or green arrow in the *Service* column shows whether the origin of the connection is in the internal network (green arrow) or in the external network (red arrow) for each rejected connection.
2. If the list becomes difficult to review because of a high number of rejected connections, you can create a filter that only displays certain rejected connections. Click on the *Display Filter* button to do this.



Several filter options are now displayed above the list. You can filter the blocked connections by port and protocol, by origin and target, or by period and limit the number of connections displayed. Double entries are collated and the number of ignored connections is displayed.

3.6 Statistics

To display statistics you can either use the integrated statistics area in the Administration Client or the external, separately installed Statistics Client. Both programmes have the same range of functions. However, you can only connect one entity of the Administration Client with one Firewall Server, while as many entities as you like from the Statistics Client can be connected to a Firewall Server at the same time.

3.6.1 Filter possibilities

You can filter the displayed results in the upper part of the statistics window depending on the prepared statistics data:

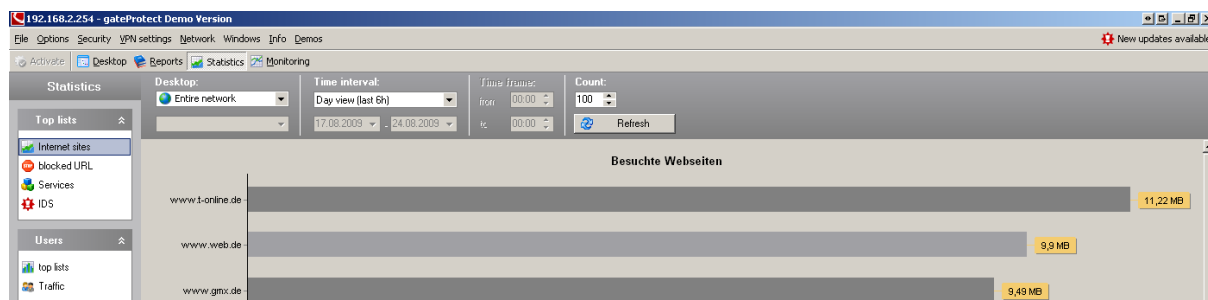
- Desktop: entire network, user or computer
- Period: 6, 12 or 24 hours, 7 or 14 days, 1, 3 or 12 months.
- Self-defined period with entry of date and time for beginning and end
- Time window: any time of day with entry of beginning and end
- Rejected accesses: incoming or outgoing

The *Update* button loads the current data from the Firewall Server.

3.6.2 Top-Lists - Internet pages

This diagram shows the visited web pages, sorted by the amount of downloaded data. If you want to block a URL, right-click on the bar and select an appropriate blacklist category for the URL from the context menu.

Double clicking on the bar transfers the statistics for the relevant domain to the User Top-Lists view (see 3.6.6. - *User Top-Lists*).



3.6.3 Top-Lists - blocked URL

This diagram shows blocked URLs sorted by number of access attempts. If you want to release a blocked URL, right-click on the corresponding bar and select the appropriate whitelist category for this URL from the context menu.

Double clicking on the bar transfers the statistics for the relevant domain to the User Top-Lists view (see 3.6.6. - *User Top-Lists*).

3.6.4 Top-Lists - services

This diagram shows the use of services or protocols, sorted by amount of data. Double clicking on the bar transfers the statistics for the relevant domain to the User Top-Lists view (see 3.6.6. - *Employee Top-Lists*).

3.6.5 Top-Lists - IDS/IPS

This diagram shows the events registered by the Intrusion Detection and Prevention System, sorted by frequency. If you want further information on a certain event, click on the corresponding bar. You can access a data source on the Internet from the context menu, which provides additional information on the relevant event.

3.6.6 Users - Toplists

This diagram shows which users have visited which websites, sorted by amount of data.

3.6.7 Users - Traffic

This diagram shows the amount of data transferred to or from the Internet by the users.

3.6.8 Defence - Overview

This table shows a collation of the statistics on blocked accesses, viruses found, Intrusion Detection events and spam over several periods.

3.6.9 Defence - defence

This diagram shows, depending on the selected period, the number of repelled potential attacks. Incoming accesses are shown in red, outgoing are in green.

3.6.10 Traffic - All data

This diagram gives information on the amount of data (traffic), which has run through the Firewall Server in a definable period in all protocols.

3.6.11 Traffic - Internet

This diagram gives information on the amount of data (traffic), which has run through the Firewall Server in a definable period only in the Internet protocols.

3.6.12 Traffic - E-Mails

Shows all the e-mail traffic that has run through the Firewall in a definable period.

3.7 Firewall

You can adjust settings and make changes to or for the server using this menu. The settings menu is accessed via the *Server settings* option.

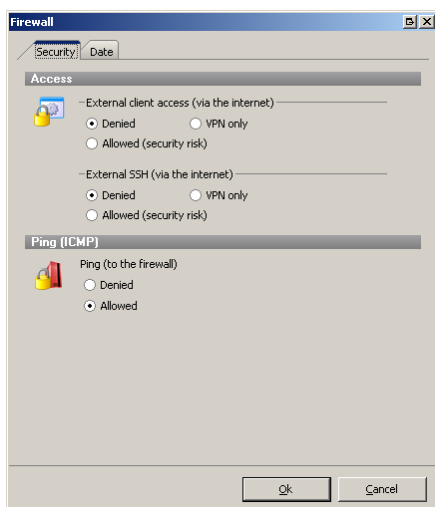
3.7.1 Firewall - Security

Using the *Security* tab in the *Server Settings* dialogue box you can change settings for access to the Firewall Server from the external network or the Internet and specify how the Firewall Server should react to ICMP queries (e.g. for a PING command).



NOTE

THESE SETTINGS ONLY REFER TO EXTERNAL ACCESS TO THE FIREWALL SERVER FOR THE DEFINED USERS. ACCESS FROM THE INTERNAL NETWORK IS ALWAYS POSSIBLE.



In the Access area specify whether and how access may be made to the Firewall from the external network.

Select one of the options from *Denied*, *VPN only* or *Allowed*.

| Option | Function |
|----------|--|
| Denied | Only computers from the internal network may access the Firewall Server from the Administration Client, external access is denied. |
| VPN only | Same settings as <i>Denied</i> , but access is also possible to the Firewall Server from the external network by VPN. |
| Allowed | Access to the server is allowed from the internal and external network. |



ATTENTION !

THE ALLOWED OPTION MEANS A SECURITY RISK, AS IT ENABLES ATTACKERS TO HAVE ACCESS TO THE FIREWALL UNDER CERTAIN CIRCUMSTANCES AND THEREFORE MUST NOT BE USED PERMANENTLY.

For security reasons the Firewall Server can be set up in this way so that it does not respond to ICMP commands (PING) to the Firewall.

Select one of the options from *Denied*, or *Allowed* in the PING (ICMP) area.



NOTE

BLOCKING ICMP COMMANDS CAN INCREASE THE SECURITY OF THE FIREWALL SERVER, BUT AT THE SAME TIME IT IMPEDES ANY ERROR SEARCH IN THE NETWORK. IF AN ERROR DOES OCCUR IN THE NETWORK, YOU SHOULD THEREFORE SET THIS OPTION TO ALLOW BEFORE PERFORMING AN ERROR SEARCH.

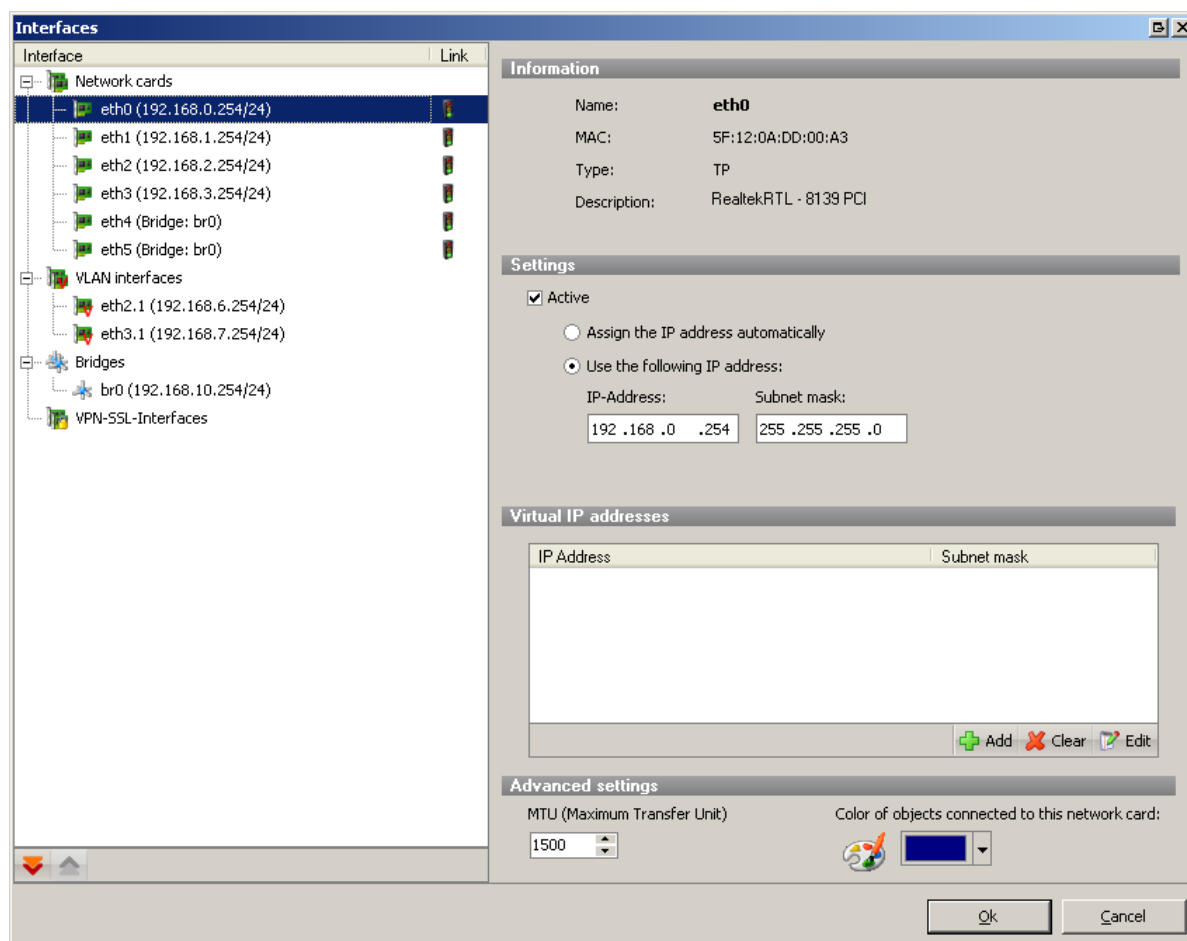
3.7.2 Firewall - Date

The gateprotect Firewall Server works with time-dependent rules. For this reason correct date and time settings are required. You can configure the settings for using a time server on the *Date* tab.

1. Select one of the given time zones from the *Time Zones* dropdown list.
2. Check the current system time of the Firewall Server in the *Date and Time* fields.
3. If you want to user an NTP server, tick the *Active* box in the NTP server section.
4. You can either use the given time server or enter your own NTP server in the list.
 - a.) Click on the *Add* button to add a new time server.
 - b.) Enter the name of the time server into the entry field.
5. If you want the system time of the Firewall Server to be available in the internal network, tick the *Time available to internal network* box. The Firewall Server then works at the same time as the internal time server.

3.8 Interfaces

The dialog *Interfaces* can be found at *Options > Interfaces*.



On the left side there is a tree which shows the network cards, VLANs, VPN-SSL-interfaces and bridges. After selecting a branch on the left site the details were shown on the right side.

3.8.1 Network interfaces

Here you can change different settings.

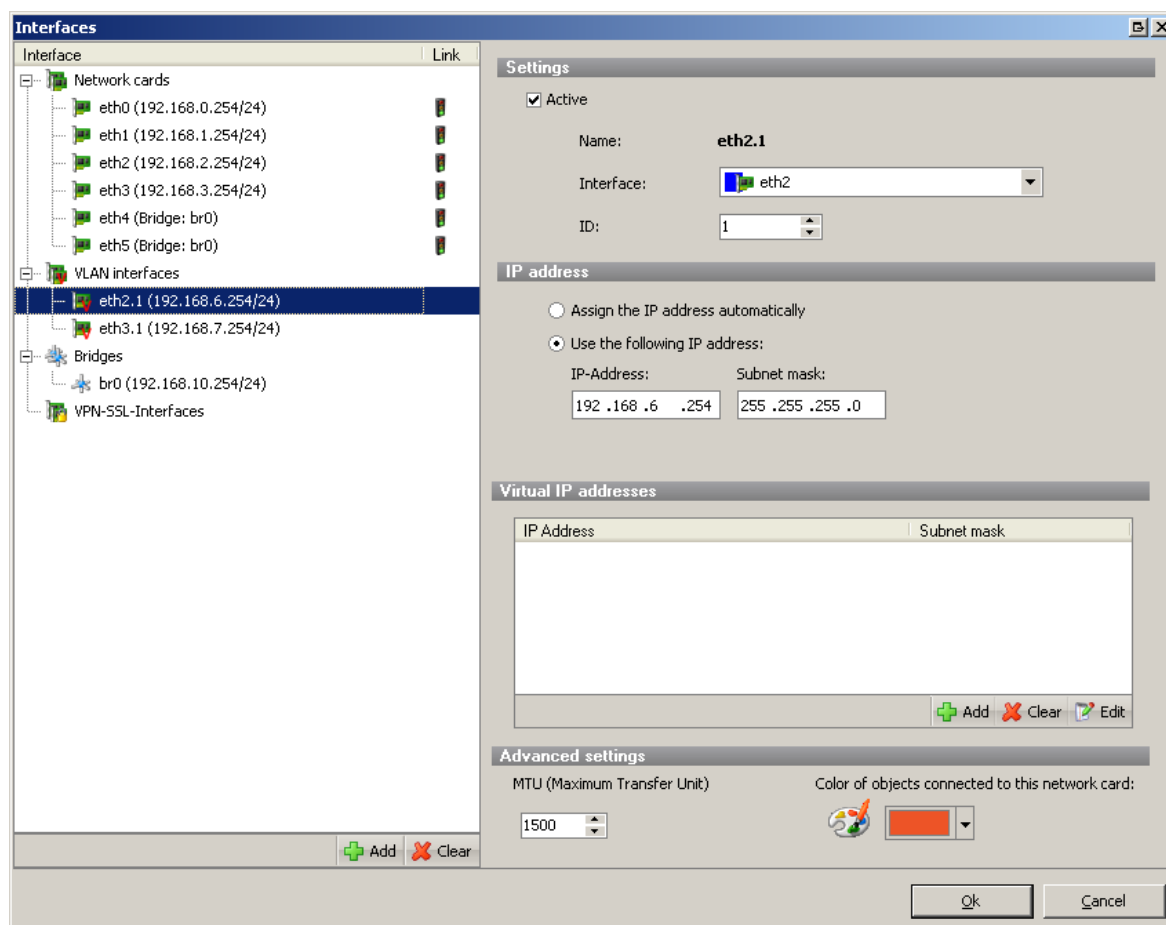
- The activity state of the network interface can be changed
- The way the interface receives the IP address
- Adding virtual IP addresses
- Defining the MTU
- Setting the color for the configuration desktop

3.8.2 VLAN

VLAN (Virtual Local Area Network) is supported as defined in IEEE 802.1Q. VLAN on a physical interface is treated like a virtual ethernet-interface with the same characteristics like the physical one it is attached to. To use VLANs in the gateprotect firewall you can select the VLAN interface on every menu where you can select network card interfaces or bridge interfaces. The name of a VLAN interface is created of the name of the physical network interface name and the VLAN-ID i.e. "eth3.1415". „eth3“ is the name of the physical interface and „1415“ is the VLAN-ID.

VLAN can be created in two ways.

If you select *VLAN* in the tree on the left side an *Add* button appears. By clicking this button a new VLAN will be created. On the right site you could define the settings of this VLAN.



Another way is to drag and drop a Network card or bridge interface on the words *VLAN interfaces*. In this case a new VLAN will be created by using this interface.

You can't create a VLAN in the following cases:

- VLAN interfaces can't be created on VLAN interfaces.
- You can't create a VLAN on a network interface which is already a port of a bridge interface.
- You can't create a VLAN on a bridge interface which already uses a VLAN interface as a port.
- VLAN interfaces can't be created on VPN-SSL interfaces.
- You can't create a VLAN on an interface which is used to synchronize high availability.

Configuring the VLAN interfaces is more or less like configuring a network card interface. Additionally you have to set an unique ID. This ID has to be between 1 and 4094.

**NOTE**

YOU CAN USE THE SAME VLAN-ID ON MULTIPLE PHYSICAL INTERFACES BUT THEY WON'T BE CONNECTED AUTOMATICALLY BY THIS!

To connect VLANs to each other you can use even routing or bridging.

Using a bridge to connect the VLANs integrate the VLAN interfaces in a bridge as ordinary Ethernet interfaces.

To route one VLAN to another you have to create desktop-icons of the VLANs and connect them to each other.

3.8.3 Bridge

Next to physical network cards even VLAN and VPN-SSL interface can be ports of a bridge.

There are multiple ways to create a bridge:

Mark multiple interfaces. On the right side appears a button *Create Bridge*. If you marked interfaces which are not possible to bind to a bridge there will be a warning message.

You can drag and drop interfaces on the word *Bridges* on the left side to create a new bridge.

You can select bridge in the tree on the left side and press the *Add* button. See VLAN (3.8.2)

You can't create a bridge in the following cases:

- Bridges can't be a port of another bridge.
- You can't create a bridge on an interface which is used to synchronize high availability
- Bridges can't use interfaces which are already used by another bridge.
- Bridges can't be created on VLAN interfaces which are created on another bridge.
- Bridges can't use physical network card interfaces whose VLAN interfaces are used on the config-desktop of the Administration Client.
- You can't use a network card and their VLAN in the same bridge.
- You can't create a bridge in an interface the admin-client is connected over.

3.8.4 VPN-SSL-Interface

To use the VPN-SSL interface you first have to create a VPN-SSL-bridge tunnel on *VPN settings > VPN-SSL*.

In the interfaces dialog you can only bind this existing VPN-SSL interface to a bridge. Drag and drop the interface on a bridge or create a new bridge interface and use the VPN-SSL (this is shown there if it you have one) as one port of your bridge.

3.9 Internet settings

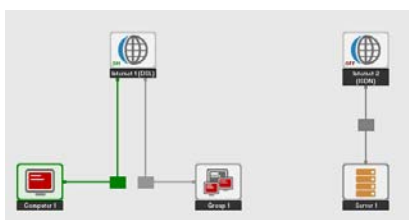
Here you can configure your connections to the internet. You can add several connections and limit them by time. You can set up an ISDN dial-up connection, an ASDL connection or a router connection. You have to choose router connection for all connections that use a gateway. How to set up the different types of connections is explained below. You can reach the Internet dialogue via *Options > Internet*.

3.9.1 General internet settings

The *General* tab is used to add a new connection to the list of current internet connections, delete no longer required internet connections or edit the settings of a connection.

Load Balancing (Concurrent Connections)

Load balancing across several internet objects is advanced routing based on the different internet connections.



It is possible to create several internet objects on the desktop using "drag and drop". Any rules can be created for these internet objects. The service for the corresponding rule is only routed via this internet connection.

It is even possible to connect one object with several internet objects. In this case, the corresponding services are distributed on both internet connections.



NOTE

IF A PROXY SHOULD BE USED, ALL INTERNET CONNECTIONS WERE AUTOMATICALLY CONNECTED TO THE SELECTED OBJECT.

Step 1

To add a new internet connection, click on the *Add* button.

Step 2

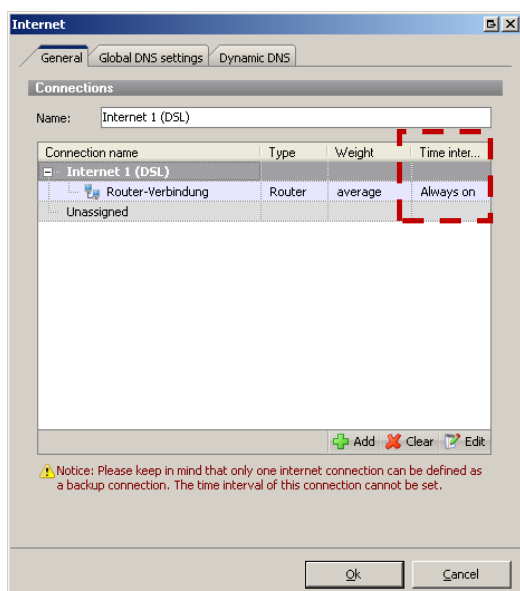
The internet connection assistant opens up. Follow its instructions until the set up of the new connection is completed. See *chapter 2.3.2 First configuration in quick Mode*

Step 3

If you have created a new internet connection, you can assign this to the internet objects using "drag and drop".

3.9.2 Time period for internet connections

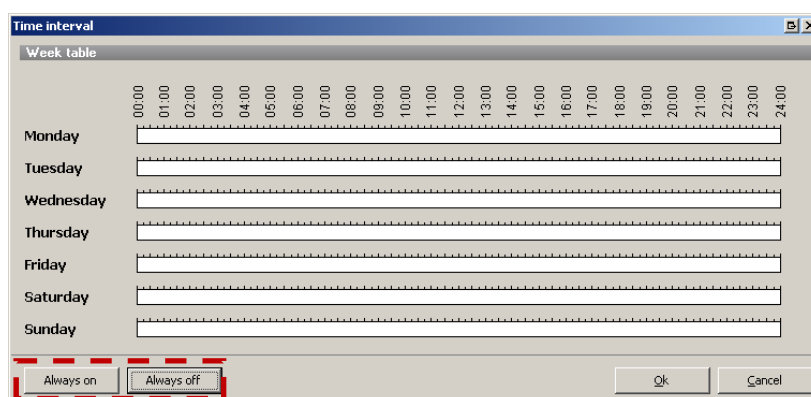
To use different internet connections at different times, you can limit them by time.



To define time periods for you internet connections, click on the *Period* column of the corresponding connection in the *Internet settings* dialogue.

By holding down the left mouse button and dragging over the fields at the same time, you can mark these grey (active) or white (inactive).

Furthermore, you can set individual fields as active or inactive with the mouse or the complete connection using the buttons *Always on* or *Always off*.



NOTE

THE "INTERNET CLOUD" SHOWS WITH "ON" OR "OFF" WHETHER OR NOT YOUR INTERNET CONNECTION IS CURRENTLY ESTABLISHED, OR WHETHER YOUR ROUTER CONNECTION BETWEEN THE FIREWALL AND ROUTER PHYSICALLY EXISTS AND IS ACTIVE. BY CLICKING ON THE INTERNET CLOUD YOU CAN SEE ON THE CONFIGURATION DESKTOP IN THE LOWER LEFT WHICH IP ADDRESS YOUR INTERNET CONNECTION HAS.

3.9.3 Global DNS settings in the internet settings

If you establish a direct internet connection, the global DNS is determined by the router / gateway or by the provider as a rule. If you use another DNS server, e.g. if you run your own DNS server, you can enter its address in the global DNS settings of the firewall server.

Step 1

Activate the *Automatically search for a DNS server* box to use the DNS server specified by the router or provider.

Step 2

If you want to use a custom DNS server, deactivate the *Automatically search for a DNS server* box and enter the IP address of at least one DNS server in the appropriate field.

3.9.4 Dynamic DNS Accounts

To be able to connect from the external network, e.g. by VPN to the firewall server, the servers IP address has to be recognized in the internet. Using dynamic DNS, the firewall server gets a fixed host name, e.g. yourcompany.dyndns.org in the internet, even if it has no fixed IP address for dial-in procedure by ISDN or DSL for example.



NOTE

YOU REQUIRE A CONFIGURED DYNDNS ACCOUNT. FURTHER INFORMATION ON DYNAMIC DNS AND REGISTRATION FOR THE DYNAMIC DNS PROCESS CAN BE FOUND AT E.G. [HTTP://WWW.DYNDNS.ORG](http://www.dyndns.org).

Operation sequence for multiple DynDNS accounts::

Step 1

Create one or more DynDNS accounts on a supported DynDNS provider (e.g. www.dyndns.org).

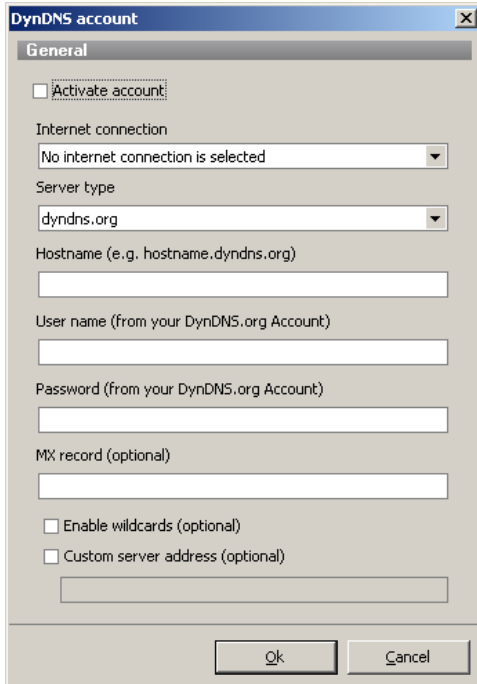
Step 2

Set up one or more internet connections on the firewall.

Step 3

Set up your DynDNS accounts on the firewall.

To set up the dynamic DNS access, open the *Internet* dialogue in the main menu *Options*.


Step 4

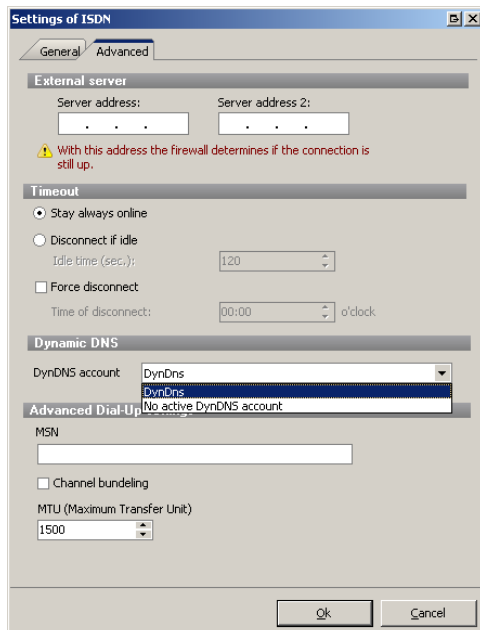
Tick the *Activate account* box to use this account.

Step 5

Enter the data provided after your DynDNS registration in the *Server type*, *Hostname*, *User name* and *Password* fields.

Step 6

If you want to use subdomains of your DynDNS account, tick the *Enable wildcards* box and choose the desired internet connection.



You can also assign the DynDNS accounts in the settings dialogues of the internet connections.

3.10 DHCP Server

The gateprotect firewall offers the ability of assigning IP addresses as well as other configuration parameters (like gateway, DNS server, NTP server ...) using a DHCP server.

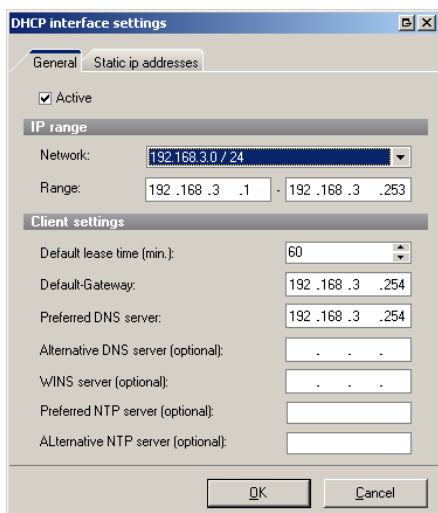
On the other hand, it is also possible to forward an existing DHCP server in other networks so it can also configure the other network (DHCP Relay).

You can choose between two operating modes:

- Server
- Relay

3.10.1 DHCP Server

You can select on which interfaces the server should run.



- One address range per interface can be defined.
- Fixed address allocations using the MAC address can be specified per interface.
- Static IP-Addresses
The pool of dynamically assigned IP-Addresses must not contain the static IP-Addresses. The pool should be adapted to provide enough addresses for static IP-address allocation.

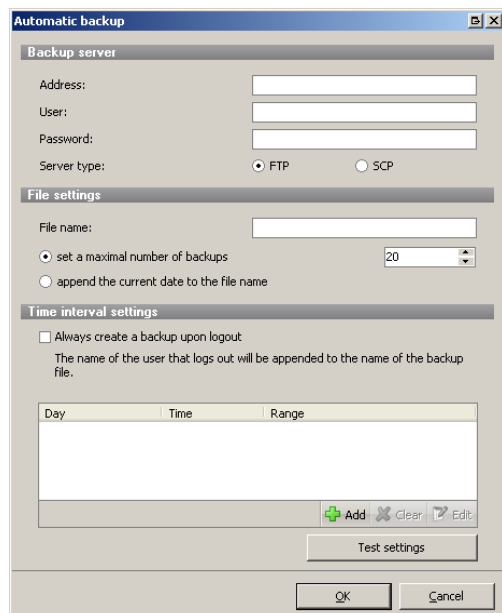
3.10.2 DHCP Relay

You can select the address of the server to which DHCP requests are forwarded.

The interfaces from which DHCP requests should be forwarded also have to be selected (multiple selections are possible).

3.11 Automatic backup

It is possible to configure the creation of automatic backups. In the menu *File > Automatic backup* you will find the following window.



Here you can configure the settings of the backup receiving server. You can choose if you want to use FTP or SCP for the file transfer.

 **ATTENTION UNENCRYPTED!!!**

In the *File settings*, you can enter a name for the Backup File.

If you set a *maximal number of backups*, a number will be attached to the file name. After reaching the selected number of backups (default 20), the number will repeat and overwrite the latest backup.

Selecting to append the *current date* to the file name creates a file including file name and date. The date never repeats, that's why old backups won't be overwritten.

It is only possible to select one of the points.

In the *time interval* settings, it is possible to add a hook to create a backup when exiting the Administration Client. This backup is named with the name of the Administrator. It is also possible to make timed backups.

The Button *Test settings* tries to send a test file (named "file name_test") to the entered backup server. If the settings are correct, there will be a popup, with a positive response and you can delete the test file from the backup server.

3.12 Routing settings

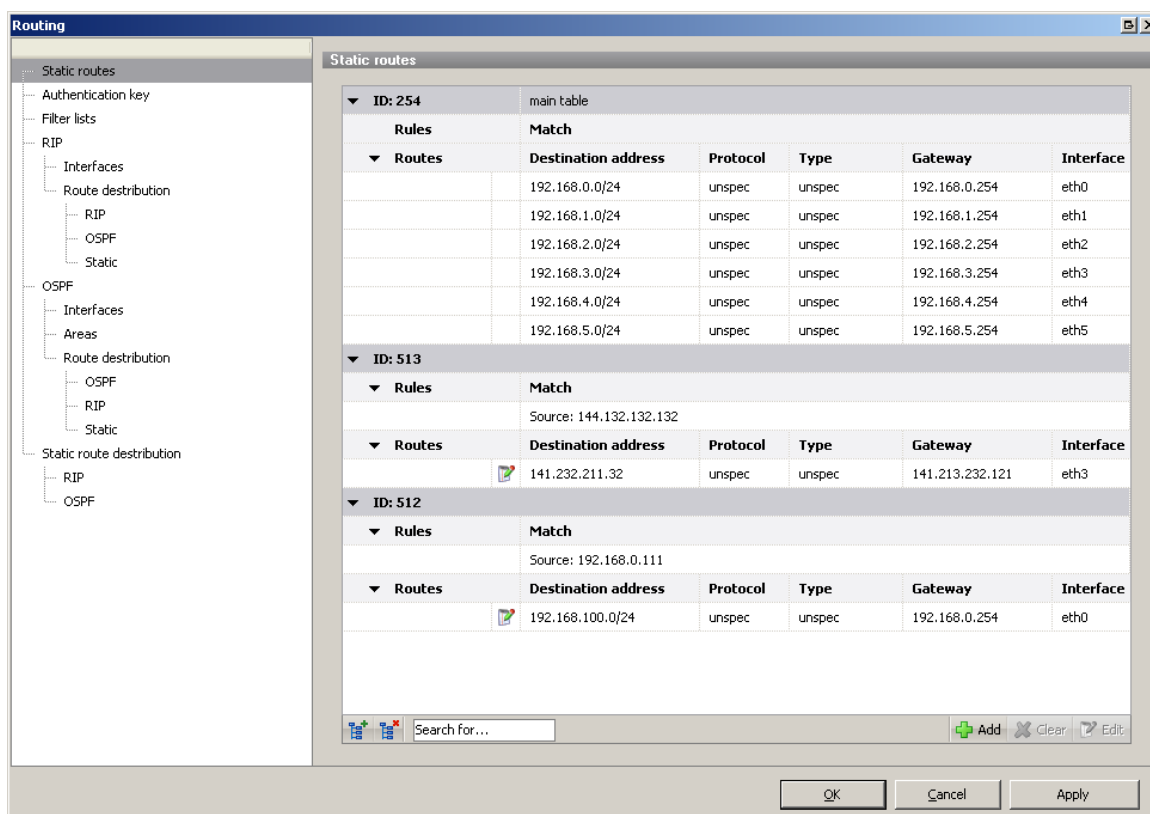
The routing settings are splitted into two groups. The management of statistic routes and the management of routing protocols like OSPF and RIP.

Static routes affect all firewalls and are interesting for Administrators of smaller networks.

The management of routing protocols are more suitable for managing larger networks with huge WAN structures.

3.12.1 Static routes

Standard-Routing



The screenshot shows the 'Routing' window with a tree view on the left and a 'Static routes' table on the right. The tree view includes categories like 'Static routes', 'RIP', 'OSPF', and 'Static route distribution'. The 'Static routes' table displays three tables: ID 254 (main table), ID 513, and ID 512. Each table has a 'Rules' section with a 'Match' condition and a 'Routes' section with columns for 'Destination address', 'Protocol', 'Type', 'Gateway', and 'Interface'.

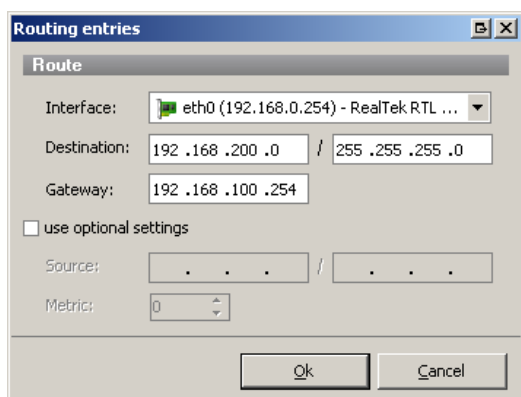
| Static routes | | | | | | |
|-------------------------|---------------------|----------|--------|-----------------|-----------|--|
| ID: 254 | | | | | | |
| main table | | | | | | |
| Rules | | | | | | |
| Match | | | | | | |
| Routes | | | | | | |
| | Destination address | Protocol | Type | Gateway | Interface | |
| | 192.168.0.0/24 | unspec | unspec | 192.168.0.254 | eth0 | |
| | 192.168.1.0/24 | unspec | unspec | 192.168.1.254 | eth1 | |
| | 192.168.2.0/24 | unspec | unspec | 192.168.2.254 | eth2 | |
| | 192.168.3.0/24 | unspec | unspec | 192.168.3.254 | eth3 | |
| | 192.168.4.0/24 | unspec | unspec | 192.168.4.254 | eth4 | |
| | 192.168.5.0/24 | unspec | unspec | 192.168.5.254 | eth5 | |
| ID: 513 | | | | | | |
| Rules | | | | | | |
| Match | | | | | | |
| Source: 144.132.132.132 | | | | | | |
| Routes | | | | | | |
| | Destination address | Protocol | Type | Gateway | Interface | |
| | 141.232.211.32 | unspec | unspec | 141.213.232.121 | eth3 | |
| ID: 512 | | | | | | |
| Rules | | | | | | |
| Match | | | | | | |
| Source: 192.168.0.111 | | | | | | |
| Routes | | | | | | |
| | Destination address | Protocol | Type | Gateway | Interface | |
| | 192.168.100.0/24 | unspec | unspec | 192.168.0.254 | eth0 | |

All routing tables containing at least one route are shown. The table with ID 254 is the main routing table which contains the user defined route. Because of the importance of this route it is shown as first in the list. Table 255 is containing exclusively local routes for all known interfaces. Tables with the IDs 1 to 63 are for Loadbalancing and Internet connections. Routes added to the main table are also written in this tables. The tables 64 to 250 are reserved for routes with source addresses (Policy-Routing) and shown up when a route with source IP-address are added.

The column "destination address" contains the IP-address of the routing destination. "Protocol" shows who added the route. Routes with the Protocol "kernel" or "boot" are added by the system, user defined routes are named gpuser. The column "Type" contains the type of the route, in most cases this is "unicast". "Gateway" shows up the IP-address of the gateway, if packets are routed to one when the destination is not reachable by the link. "Interface" shows up the interface of the firewall by which the packets leave. If there is a gateway entered, it must be reachable by the interface connected to.

Every routing table can contain routing-rules, which are part of the policy-routing. Routing-rules can not be added explicitly, they are created automatically if:

- a new route with source IP has been added
- a new internet-connection has been added (Loadbalancing)



In the "Match" column the criterion for redirect IP-packets into other tables is written.

If a route is editable or addable, an icon in the second column will be shown.

(Optional) source: decides that just packets from a certain source address are routed. Metric: The metric shows the route "cost" and is interesting in combination with routing protocols.



NOTE

THESE SETTINGS ARE NORMALLY NOT REQUIRED AND SHOULD BE USED UNDER CERTAIN CIRCUMSTANCES.

3.12.2 Routing-Protocols

Introduction

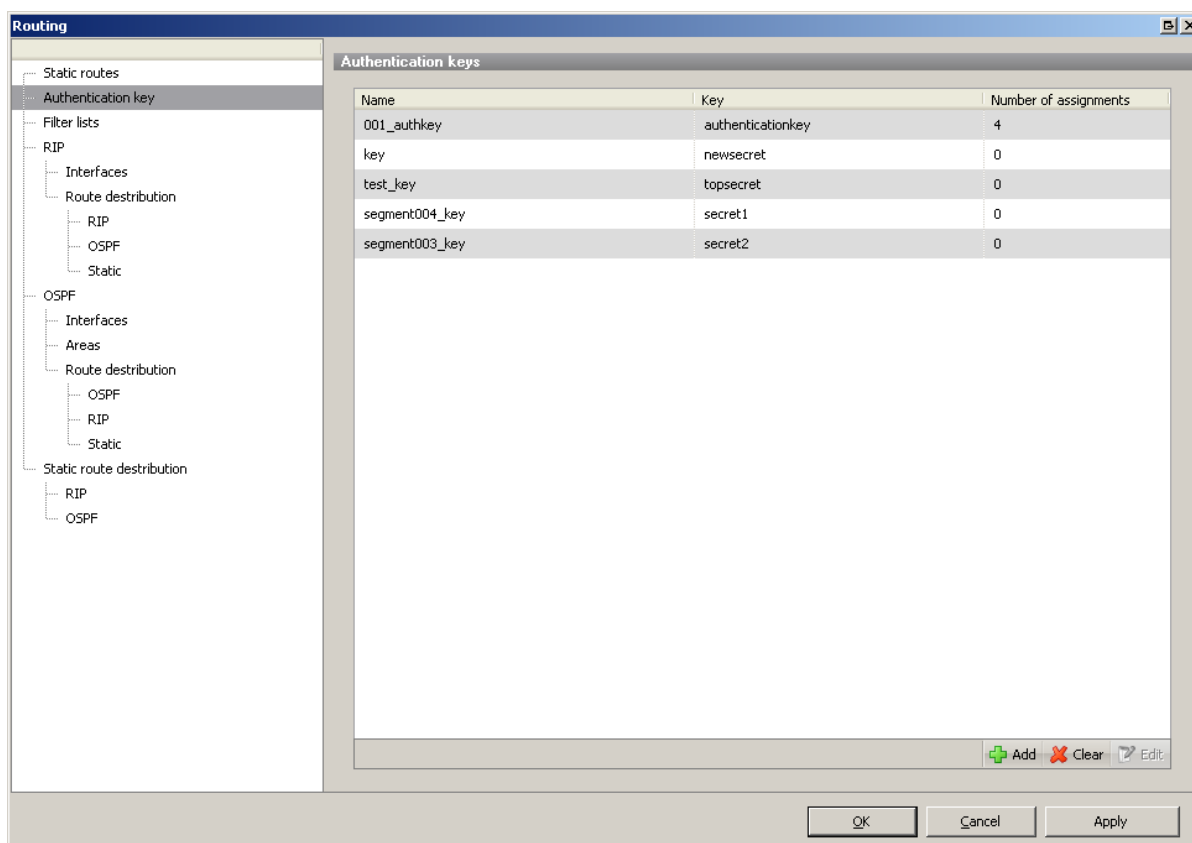
Routing for IP protocols decides the forwarding of IP packets, based on their destination address, on a host. The routed packets can be foreign packets of another host, or local generated packets from the same host.

The easiest way is an existing static route table on the host, which decides on the basis of the destination address, the outgoing interface for the packets. A static routing configuration is typical for smaller networks because in most cases there is just one host acting as router. (*Chap. 3.12.1 Static routes*).

In larger networks it is more different, complex and fault-prone to manage static routing configurations because every router or host has to be configured manually. For such networks with multiple routers different protocols for dynamic routing have been composed. Each of these protocols makes it possible to the routes to communicate with each other and publicize differences in the network topology. The network administrator does not have to configure every device, because the difference in the configuration is being told autonomously.

Dynamic routing makes it possible, to react in case of certain events with a change of the configuration. When the uplink to the Backbone of one router crashes, the router can inform the other routers to search a different route to the destination by the routing protocols.

"Routing-information" is a route which is assigned by routing protocols.

Authentication keys (are for RIP and OSPF)


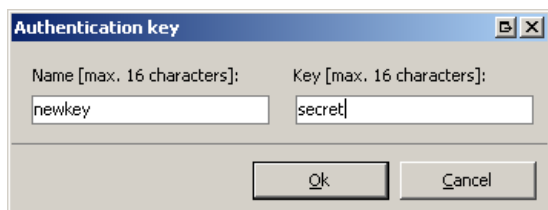
Here you can create keys for the Message-Digest-Authentication with OSPF and RIP. The keys can be edited with a name, for being found in the dialogues easily.

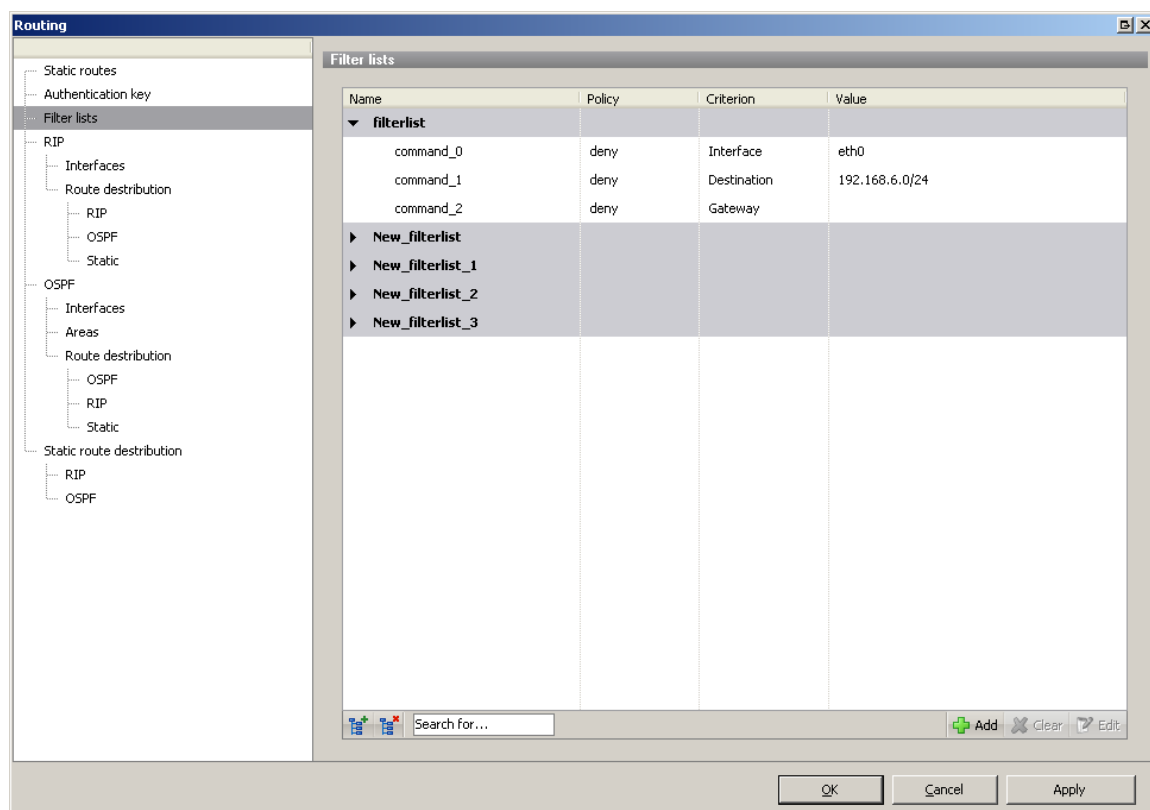


ATTENTION: THE NAME HAS A SPECIAL RELEVANCE FOR OSPF, BECAUSE THE NAME IS TRANSMITTED WHILE AUTHENTICATION AND MAY BE CORRESPONDING TO THE KEY-ID OF OTHER OSPF ROUTERS.

The keys are entered in clear text and have a maximum character length of 16 signs.

These keys are available for authentication with md5

Adding or editing of keys


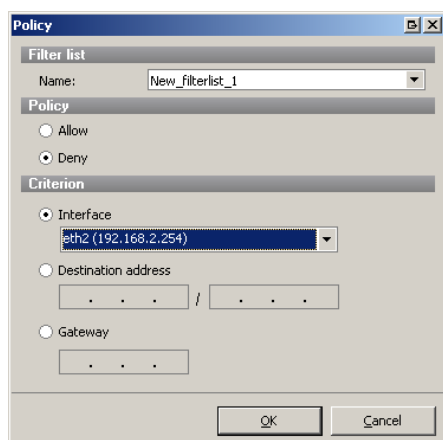
Filter lists (are for all sections of routing distribution)

Create new Filter lists

These filter lists allow the filtering of routing information, which were transferred via RIP or OSPF. Because of that, only specified information is forwarded or stored local.


NOTE

FILTERING OF ROUTING INFORMATION IS NORMALLY NOT REQUIRED AND SHOULD ONLY BE USED UNDER CERTAIN CIRCUMSTANCES

A filter list consists of one or more rules which were iterated in order. These rules allow or deny the forwarding of specified information using several criteria. Every filter list gets a name, with which it can be referenced later.

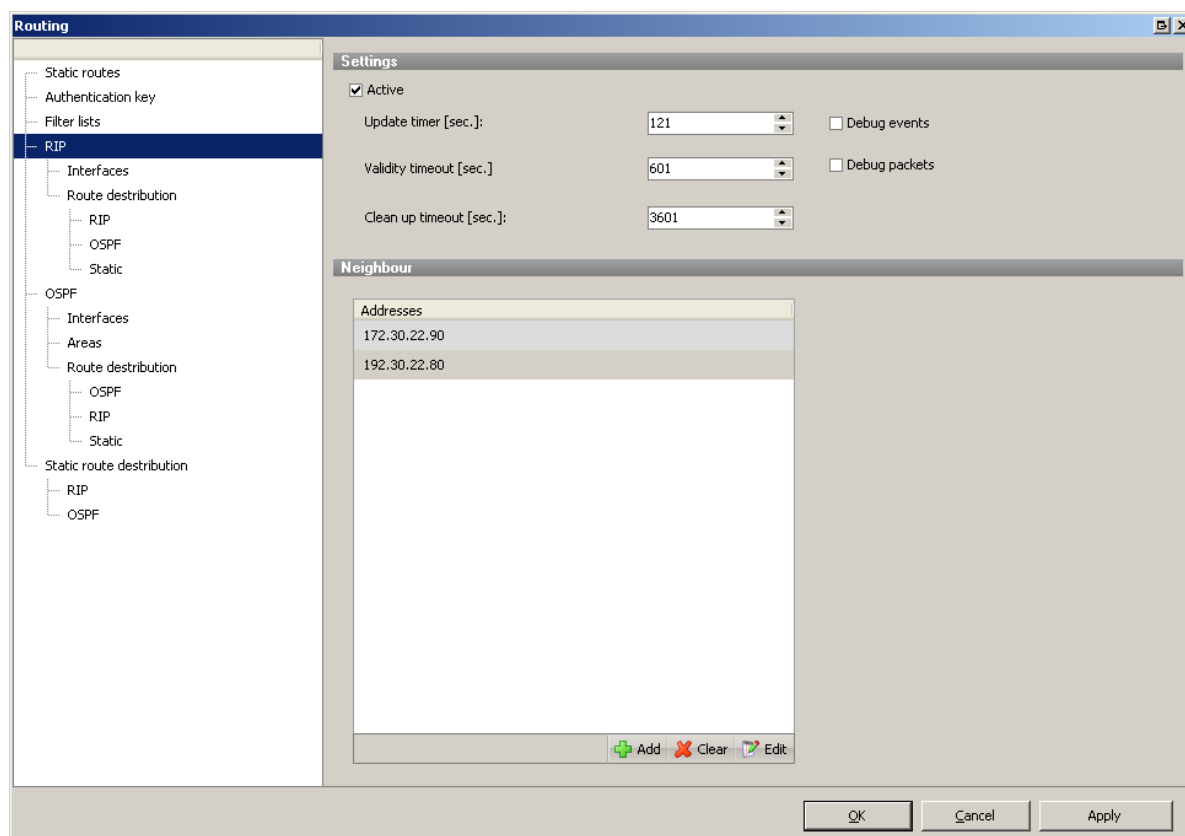

Create new Rules and add them to existing Filter lists

The name defines the filter list, to which the rule should be added. You can choose, if the rule should allow or deny the forwarding of the matching routing information.

Criteria:

- Interface: The Interface that the outbound routing information is sent to.
- Destination: The destination address of the routing information.
- Gateway: The gateway of the routing information.

3.12.2.1 RIP settings



Active activates or deactivates RIP support.

The *Update timer* sets the interval (in seconds), in which the routing information should be submitted to other RIP routers in the network. Default is 30 seconds. If you set a higher value, it takes longer to publicize the changed routing information. A lower value increases the network traffic.

The *Validity timeout* sets the interval, after which RIP routes were invalid. If no *Update* is received until the timeout is reached, the route gets deleted and other RIP routers were informed about this circumstance. The Validity timeout interval has to be longer than the update interval.

The *Clean up* timeout defines in which interval an invalid route which was received via RIP gets deleted.

Debug events turns on the debugging of RIP events like the receiving of new routing information.

Debug packets turns on the debugging of transmitted and received RIP packets. The debug information can be found in the report.

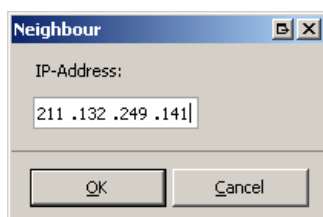


ATTENTION!

ONLY ACTIVATE THESE OPTIONS, IF YOU NEED THE INFORMATION FOR DEBUGGING. DEACTIVATE THEM IF YOU DON'T NEED THEM ANYMORE.

Via *Neighbor*, you can enter RIP router explicitly, which weren't accessible via IP multicast. Normally, this isn't necessary, because all RIP routers can find each other using IP multicast, but if you have one that doesn't support IP multicast, you can enter his address here.

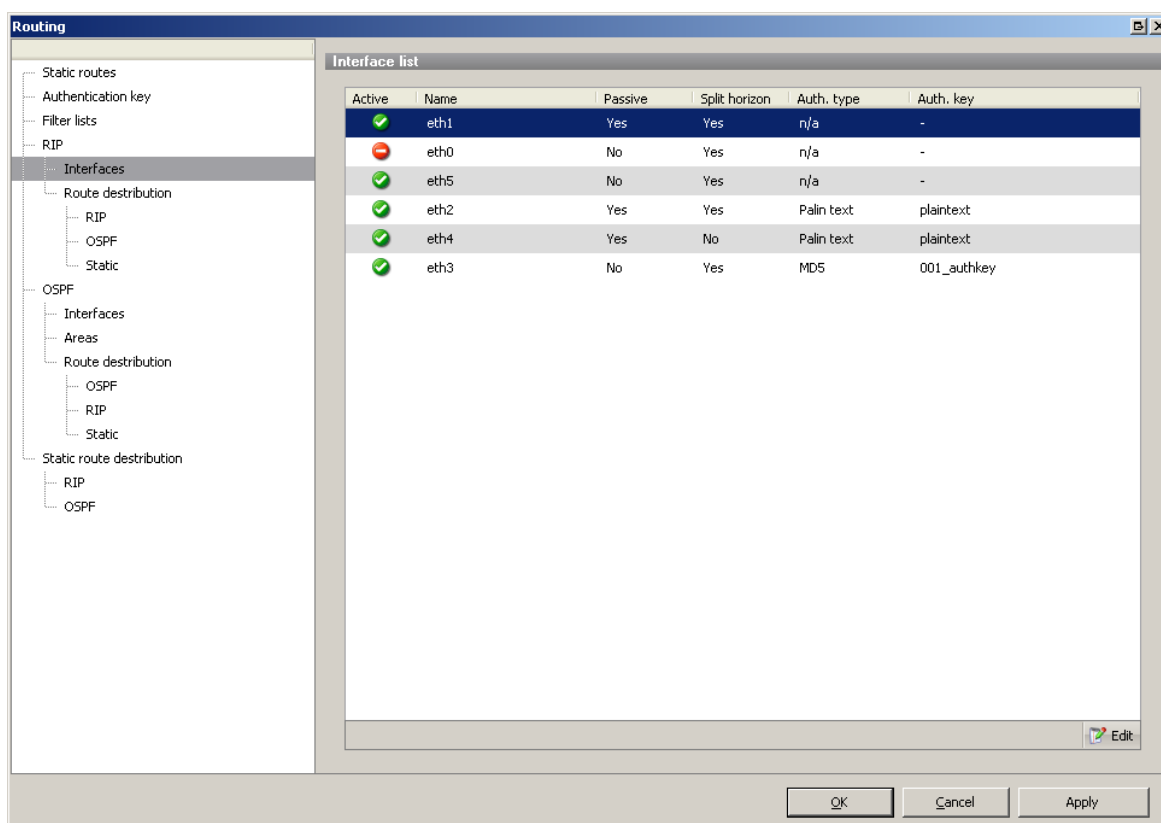
Creation of the neighbour list, simple IP list



Neighbour dialog box showing IP-Address: 211.132.249.141

RIP interface list

Overview of all available interfaces and their current settings.



| Active | Name | Passive | Split horizon | Auth. type | Auth. key |
|-------------------------------------|------|---------|---------------|------------|-------------|
| <input checked="" type="checkbox"/> | eth1 | Yes | Yes | n/a | - |
| <input type="checkbox"/> | eth0 | No | Yes | n/a | - |
| <input checked="" type="checkbox"/> | eth5 | No | Yes | n/a | - |
| <input checked="" type="checkbox"/> | eth2 | Yes | Yes | Plain text | plaintext |
| <input checked="" type="checkbox"/> | eth4 | Yes | No | Plain text | plaintext |
| <input checked="" type="checkbox"/> | eth3 | No | Yes | MD5 | 001_authkey |

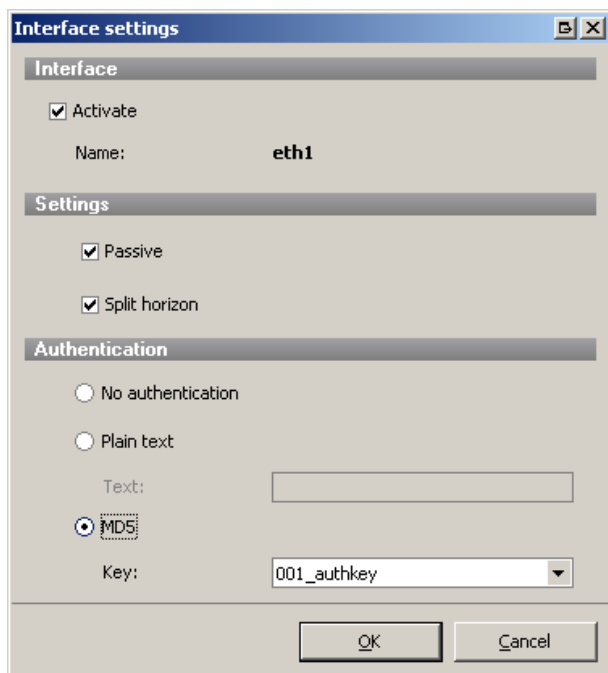
All interfaces on your system which are usable for RIP are listed here. It is not possible/necessary to add or delete interfaces. Here you can activate RIP on interfaces which are in networks with other RIP routers.

The column *Active* shows, whether the interface has RIP activated or not. If an interface is used for RIP, RIP updates were transmitted and received using this interface. If an interface is marked as *Passive*, it only receives RIP updates and doesn't send them.

Split horizon is needed to prevent routing loops in more complex networks.

The column *Auth. type* shows if RIP updates were transmitted/received using authentication and if so, which authentication method is used.

Auth. key shows the password if plaintext authentication is used. Using MD5 authentication, it shows the name of the entry in the Auth key list.

Available interfaces can only be edited


Activate activates the interface for RIP.

Passive turns on the passive mode (only receive) and *Split horizon* activates the "Split horizon with poisoned reverse" function to prevent routing loops.

In the *Authentication* area, you can select the type of authentication. If you choose *plaintext*, you have to enter a password, using *MD5*, a dropdown menu offers already defined MD5 keys (see Auth keys).

Forwarding of routing information (route distribution)

The settings of routing distribution are the same in RIP, OSPF and Static route distribution, so the dialogue is only explained once.

The sub items of *routing distribution* define the target of forwarding; the source is the context of the item *routing distribution*.

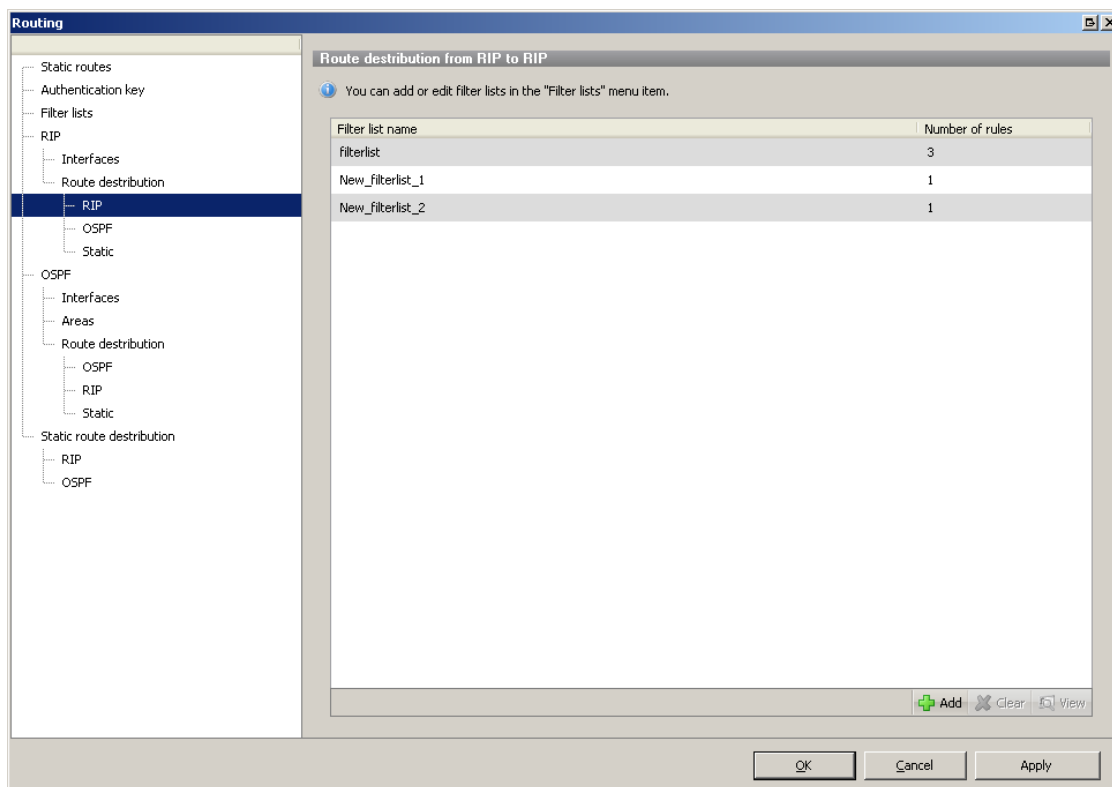
There are several possibilities of routing distribution:

- RIP to RIP
- RIP to OSPF
- RIP to local system (static)
- OSPF to OSPF
- OSPF to RIP
- OSPF to local system (static)
- Local system (static) to RIP and to OSPF


ATTENTION!

THE ROUTING DISTRIBUTION IS ONLY IMPORTANT IF YOU WANT TO FILTER THE FORWARDING OF ROUTING INFORMATION! TO DO THIS, THE FILTER LISTS ARE NEEDED. IF YOU DON'T SPECIFY FILTER LISTS, ALL ROUTING INFORMATION IS FORWARDED, WHICH IS THE REGULAR CASE.

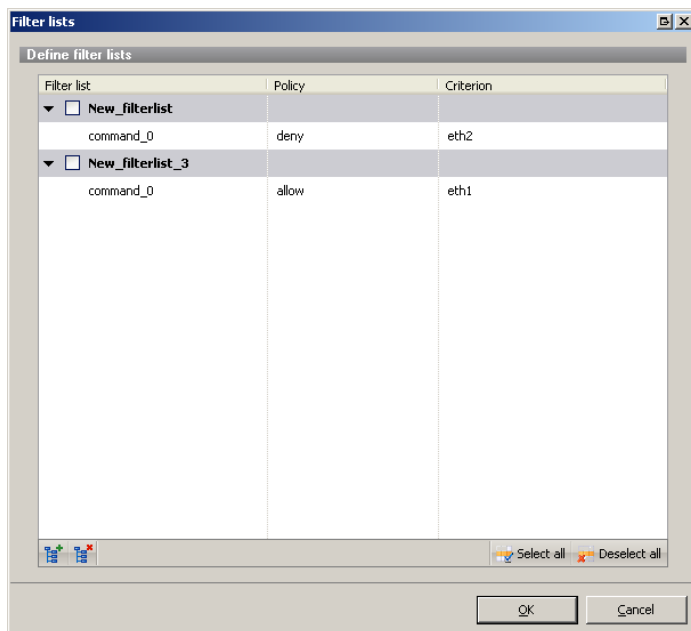
All routing distributions have the same interface: for this example, RIP is shown.



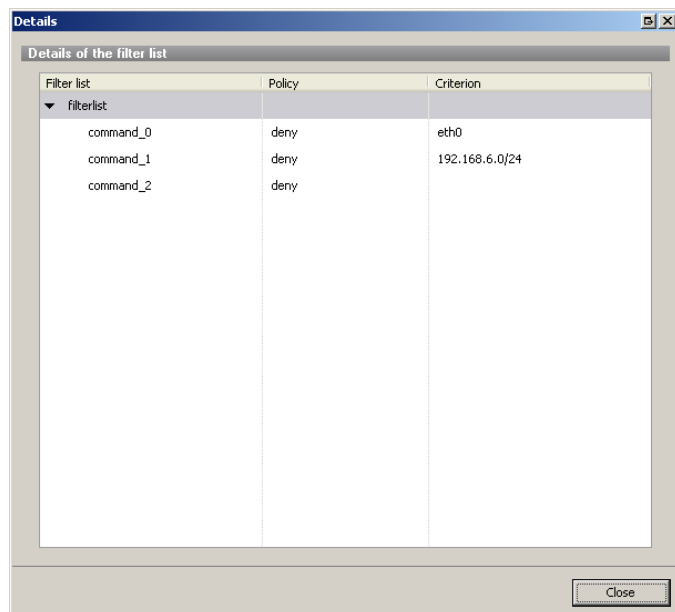
The previously created filter lists can be added or deleted in this interface. You can edit them in the *Filter lists* tab.

Add new lists

This dialogue shows all entries which weren't shown in the list.



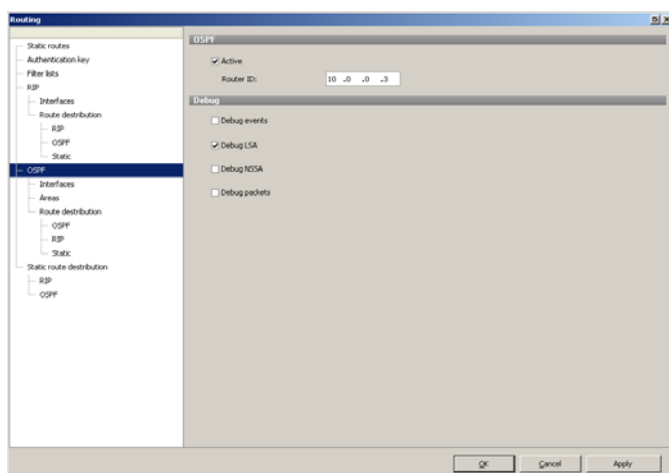
The interface equates the add dialogue but without checkboxes and choose buttons. Details were only shown for the selected list.



3.12.2.2 OSPF settings

Ticking *Active* activates OSPF support.

The *Router ID* has to be entered and should be unique. You don't have to enter an existing or valid IP address.



If *Debug events* is activated, OSPF events (like failing of a OSPF router) were shown in the debug report.

If *Debug LSA* is activated, details of LSA packets (Link State Announcement) were also shown in the debug report.

If *Debug NSSA* is activated, details of eventually existing NSSA areas were shown in the debug report.

If *Debug packets* is activated, details of all OSPF packets were shown in the debug report.

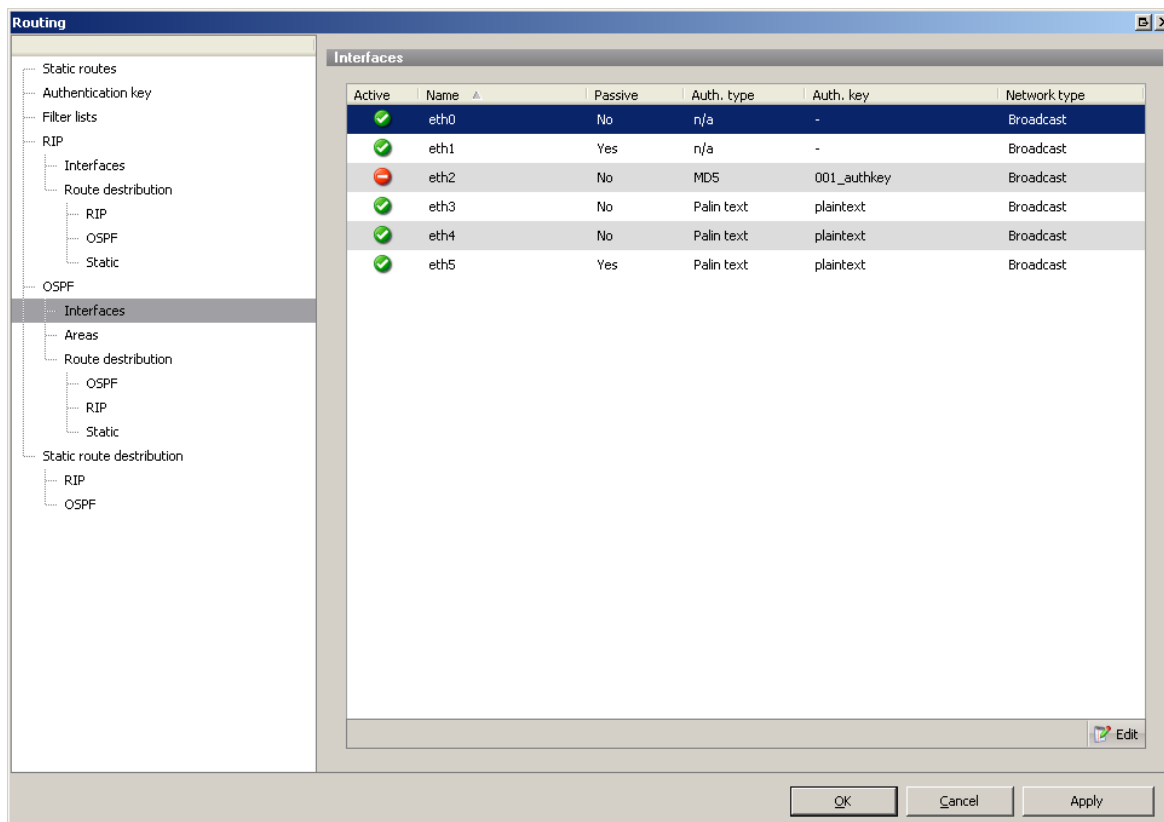


ATTENTION!

ACTIVATE THESE OPTIONS ONLY IF YOU NEED TO DEBUG AND DEACTIVATE THEM IF THE PROBLEM IS FIXED.

OSPF interfaces, similar to RIP interfaces

All interfaces on your system which are usable for OSPF are listed here. It is not possible/necessary to add or delete interfaces.



The screenshot shows the 'Routing' configuration window with the 'OSPF' section selected. The 'Interfaces' table lists the following data:

| Active | Name | Passive | Auth. type | Auth. key | Network type |
|--------|------|---------|------------|-------------|--------------|
| ✓ | eth0 | No | n/a | - | Broadcast |
| ✓ | eth1 | Yes | n/a | - | Broadcast |
| ✗ | eth2 | No | MD5 | 001_authkey | Broadcast |
| ✓ | eth3 | No | Plain text | plaintext | Broadcast |
| ✓ | eth4 | No | Plain text | plaintext | Broadcast |
| ✓ | eth5 | Yes | Plain text | plaintext | Broadcast |

Passive indicates whether an interface is in passive mode or not. If it is, it only receives OSPF packets and doesn't send them.

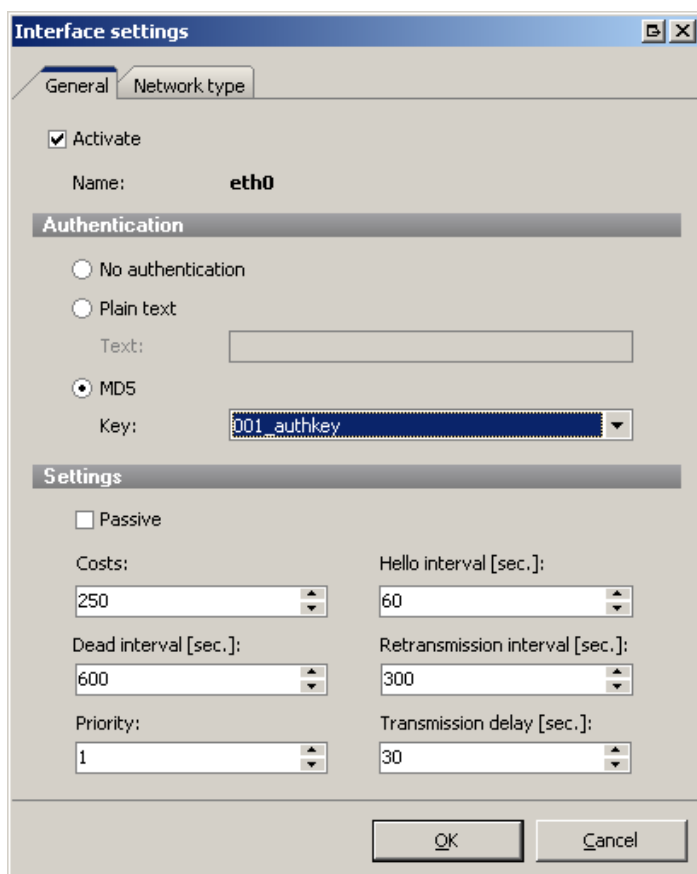
Auth. type shows the authentication mode.

Auth. key shows the password if it is in *plaintext* mode. If *MD5* is used, it shows the name of the entry in the Auth key list.

Network type shows the type of the interface. In most cases, it should be *broadcast*.

It is only possible to edit the available interfaces.

Settings of OSPF interfaces
General tab



Activate activates OSPF on this interface.

In the *Authentication* area, you can choose the authentication type like with RIP.

The *Passive* checkbox turns on the passive mode so OSPF data will only be received and not transmitted.

You can define the *Costs* for this interface. The higher the routing costs are, the less this interface should be used. These settings are only important in more complex networks.

Dead interval defines the interval for the waiting and inactivity timers and has to be the same value on all OSPF routers in the network.

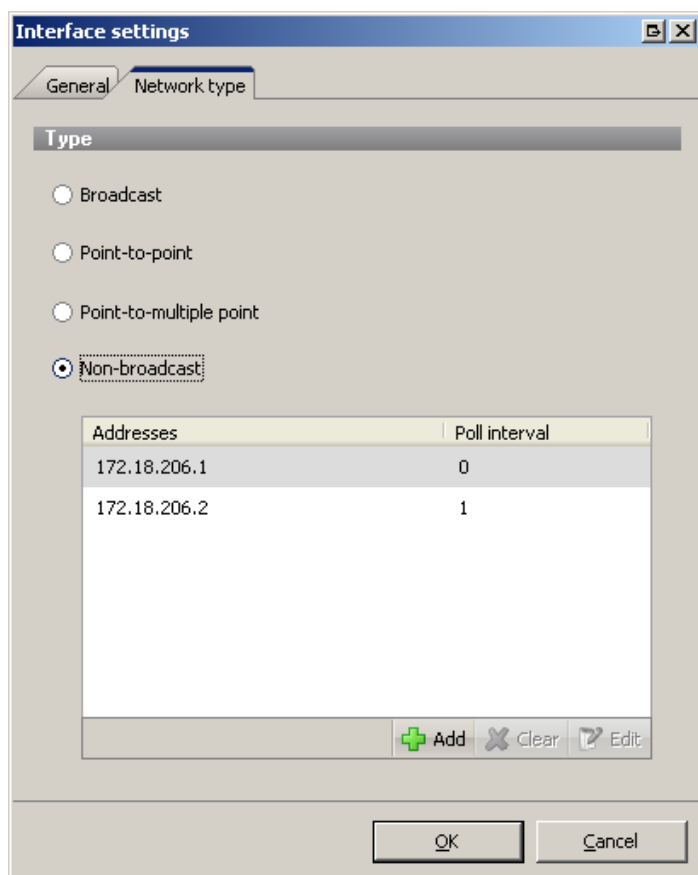
Priority defines the priority of the OSPF router. The router with the highest priority becomes the "Designated router".

Hello interval defines the interval in which hello packets were sent to other routers. This informs the other routers about the presence of this one.

Retransmission interval defines the interval in which the routing database and LSR (Link State Request) packets were retransmitted if a previous transmission failed.

Transmission delay defines the delay used to send LSA packets so multiple information can be sent in a LSA packet.

Network type tab



Interface settings

General | **Network type**

Type

Broadcast
 Point-to-point
 Point-to-multiple point
 Non-broadcast

| Addresses | Poll interval |
|--------------|---------------|
| 172.18.206.1 | 0 |
| 172.18.206.2 | 1 |

Defines the network type of the interface.

In most cases, it is always *Broadcast*.

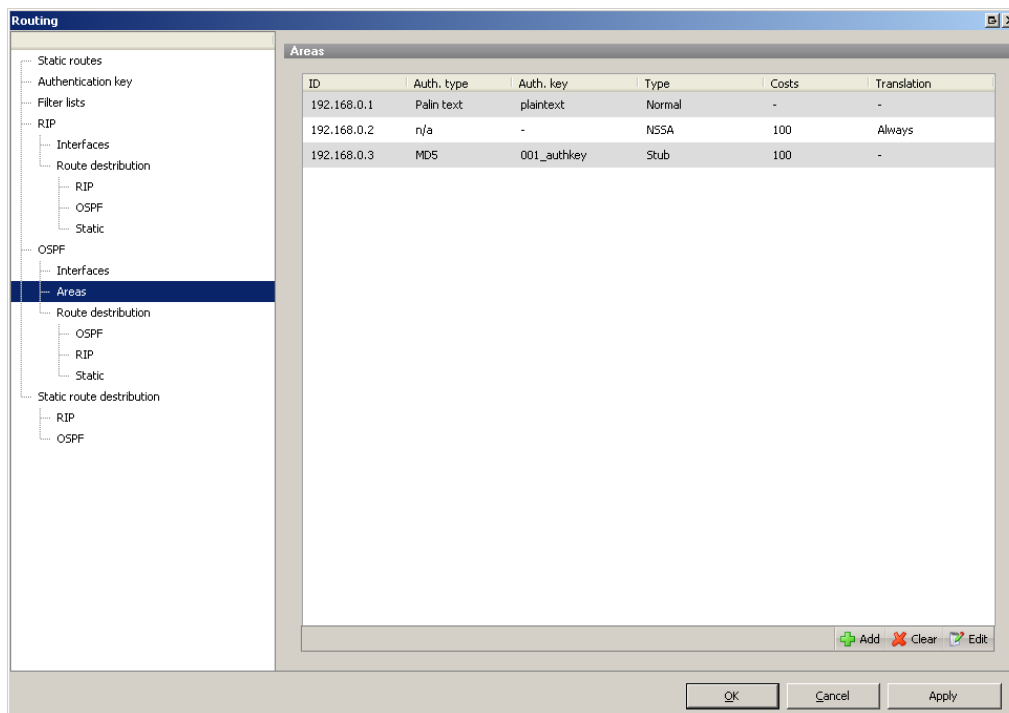
Point-to-point and *Point-to-multiple point* are only used in very special network configurations.

Non-broadcast can make sense if no broadcast/multicast packets were forwarded in the connected network.

In this case, all known OSPF router have to be entered in the Neighbor list, because they can't be found automatically.

OSPF areas

OSPF areas are logical units to group or separate networks.



Every OSPF area has its own unique ID which is presented as IP address. This IP address doesn't have to be existent or valid. A special case is the area with the ID 0.0.0.0, this is the backbone area. Every area has to be directly connected to the backbone area. If this is not possible, a direct connection to the backbone area can also be established using a virtual link.

Areas can use authentication as OSPF interfaces.



ATTENTION

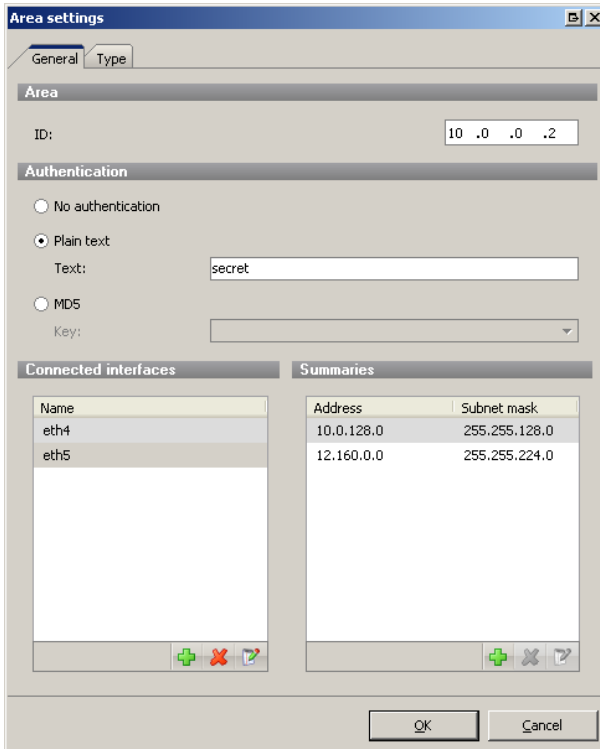
THE AUTHENTICATION SETTINGS OF THE INTERFACES ARE MORE IMPORTANT THAN THE SETTINGS OF THE AREAS.

There are three types of areas:

- Normal
- NSSA
- Stub

Add or edit areas

General tab



Area settings

General | Type

Area

ID: 10 .0 .0 .2

Authentication

No authentication

Plain text

Text: secret

MD5

Key:

Connected interfaces

| Name |
|------|
| eth4 |
| eth5 |

Summaries

| Address | Subnet mask |
|------------|---------------|
| 10.0.128.0 | 255.255.128.0 |
| 12.160.0.0 | 255.255.224.0 |

OK Cancel

ID is the ID of the area which can be entered as IP address.

Authentication is equal to the settings of OSPF interfaces.

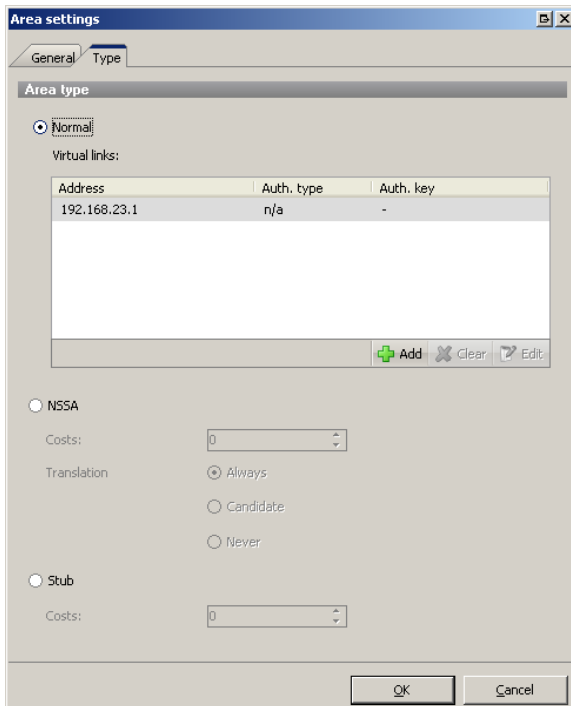
In *Connected interfaces*, you can enter the interfaces which should belong to this area.

You can summarize networks in *Summaries* (Supernetting).

The single networks weren't announced to the outside anymore but their summary.

Type tab

Here you can select the area's type.



Area settings

General | Type

Area type

Normal

Virtual links:

| Address | Auth. type | Auth. key |
|--------------|------------|-----------|
| 192.168.23.1 | n/a | - |

NSSA

Costs: 0

Translation

Always

Candidate

Never

Stub

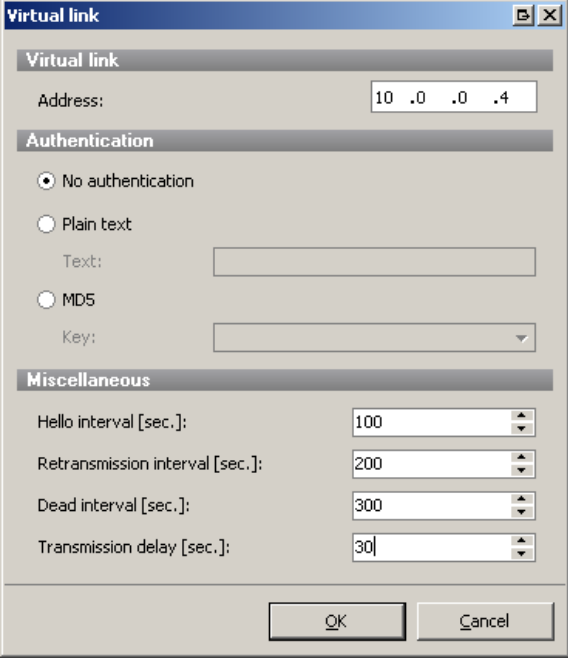
Costs: 0

OK Cancel

Because *Virtual links* are only allowed in normal areas, they can only be entered here.

NSSA and *Stub areas* can define default *Costs* which were assigned to the default LSA. With *NSSA*, you can also define the Translation type which defines the translation from Type-7 to Type-5 LSA. *Always*: it will always be translated. *Candidate*: the OSPF router participates in the automatic election for the translator. *Never*: it won't be translated.

Virtual link



The screenshot shows a dialog box titled "Virtual link" with the following sections and fields:

- Virtual link**
 - Address: 10 .0 .0 .4
- Authentication**
 - No authentication
 - Plain text
 - Text: [empty text box]
 - MD5
 - Key: [dropdown menu]
- Miscellaneous**
 - Hello interval [sec.]: 100
 - Retransmission interval [sec.]: 200
 - Dead interval [sec.]: 300
 - Transmission delay [sec.]: 30

Buttons: OK, Cancel

Address is the IP address of the router to which the virtual link should be established (this router also has a direct connection to the backbone area). A virtual link acts like an OSPF interface to offer the possibility of a direct connection to the backbone area.

4 PROXIES

4.1 Introduction

A proxy is a program, which communicates between a client (an application, e.g. a web browser) and a server (e.g. a web server). In the simplest case, a proxy simply forwards the data. However, a proxy usually fulfils several functions at the same time, for example caching (intermediate storage) or access control.

The gateprotect firewall offers different proxies for different services:

- HTTP Proxy (protects from threats when surfing the internet)
- HTTPS Proxy (allows to scan for viruses in encrypted webpages, too)
- FTP Proxy (protects from threats when transferring data via FTP)
- SMTP Proxy (protects from threats when sending and receiving e-mails)
- POP3 Proxy (protects from threats when receiving e-mails)
- VoIP Proxy (protects from threats when using speech communication over IP networks)



NOTE

IN CONTRAST TO EARLIER VERSIONS OF THE FIREWALL, THE ACTIVATION OF A PROXY FOR A CONNECTION DOES NOT IMPLICATE NAT ANYMORE, IF THE PROXY RUNS IN TRANSPARENT MODE. IF YOU WANT TO USE NAT, IT HAS TO BE ACTIVATED SEPARATELY.

4.2 HTTP Proxy

The gateprotect firewall server uses the well-tested and extremely stable Squid proxy. It acts as an interface for the optional Content Filter and the Antivirus solution. The proxy can work either in transparent or intransparent mode and offers an adjustable caching function. The HTTP proxy is required to use the web page statistics.



ATTENTION !

THE HTTP PROXY MUST ONLY BE USED AS AN OUTBOUND FILTER AND MUST NEVER BE USED IN A DMZ.

You can access the HTTP proxy settings through the Administration Client via *Options > Proxy > HTTP Proxy* tab.

To use the HTTP proxy, you have to select one of the following modes.

4.2.1 Transparent mode

In transparent mode, the firewall server automatically runs all queries that are made using port 80 (HTTP) through the proxy. The users don't have to make any additional settings in the web browser.

4.2.2 Intransparent mode without authentication

In intransparent mode without authentication, the HTTP proxy of the firewall server has to be explicitly addressed to port 10080. All users have to enter this special port in their browsers internet settings.



ATTENTION !

PLEASE NOTE THAT ONLY HTTP DATA PACKETS ARE ROUTED THROUGH THE PROXY. IF A PROGRAM OR AN ATTACKER ATTEMPTS TO RUN OTHER PROTOCOLS THROUGH THIS PORT, THESE PACKETS ARE BLOCKED AND REJECTED.

4.2.3 Intransparent mode with authentication

This mode requires additional user authentication. Here you can choose between the gateprotect local user authentication and authentication by an external radius server.

4.2.4 Configuration of the cache

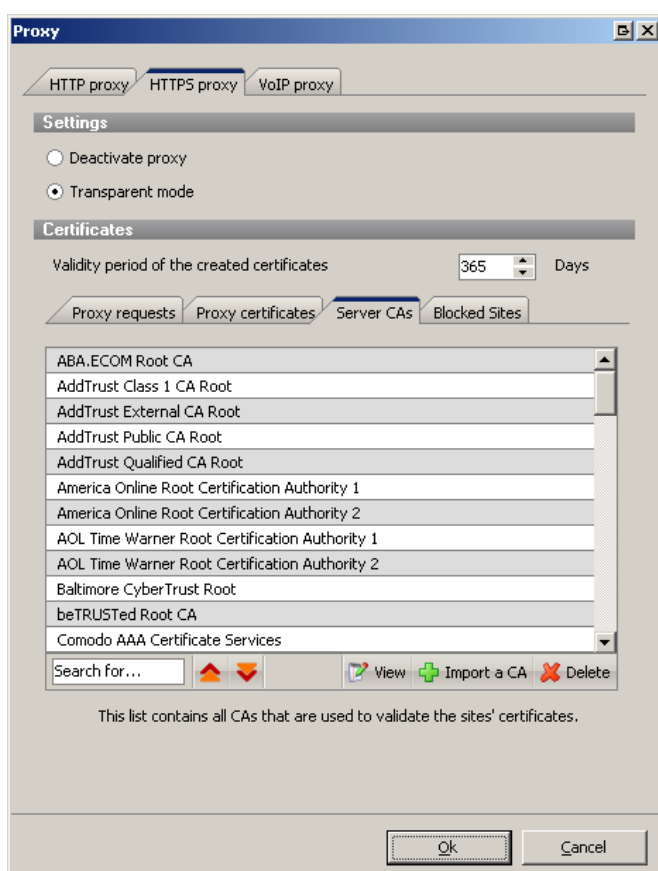
You can configure the cache entirely according to your needs.

You can adjust the size of the cache (in MB) and the minimum and the maximum sizes of objects.

4.3 HTTPS Proxy

If the HTTPS proxy is activated in a connection line, the HTTPS (encrypted) connection is managed by the transparent proxy on the firewall. This means that the user does not have to make any proxy settings in his web browser.

The HTTPS proxy operates as "man in the middle"; this means it makes its own connections to the web browser and to the web server. Operating in this way, it can check contents, use web blocking, content filtering and scanning for viruses. The settings for this were inherited from the HTTP proxy.



Only pages which have been signed by a listed CA can be visited through the HTTPS proxy. However, it is possible to import its own CA. The most common CA certificates for checking the web server certificates are installed; others can be added (and also deleted) by the firewall administrator. The HTTPS proxy operates with "forged" web server certificates issued from an own CA on the firewall which is provided to the web browser.

This CA should be imported into the web browser as trusted. For this purpose, it can be exported or replaced by a self-created CA.

Requests from web browser to new web servers will initially be rejected. All new requests were presented in a list from which the administrator only has to select the desired ones.

This request has to be unlocked by creating of a "forged" web server certificate.

The validity period of these certificates can be freely selected (365 days by default).

If the firewall administrator does not want his users to connect to this web server via HTTPS, he is able to add the domain of the web server to a blacklist.

Workflow of the HTTPS Proxy:

Step 1

The browser calls a https:// page. An empty page will be displayed, but a request is written to the Administration Client.

Step 2

The Administrator opens the Proxy dialogue in the Administration Client.

- a. He authorizes the page. A replacement certificate is created.
- b. He does not authorize the page. The page remains blocked.

Step 3

The browser calls the https:// page again.

- a. It receives the page with a "forged" certificate.
- b. It cannot see the page and a request is never made to the Administration Client again.



NOTE

IF A PAGE IS REQUESTED WHOSE CERTIFICATE HAS NOT BEEN SIGNED BY ONE OF THE SUPPLIED CAs, THE CA OF THE CERTIFICATE HAS TO BE IMPORTED INTO THE HTTPS PROXY DIALOGUE IN ADVANCE. IF THE CERTIFICATE OF THE HTTPS PAGE IS SELF-SIGNED, THIS CERTIFICATE MUST PREVIOUSLY BE IMPORTED INTO THE HTTPS PROXY DIALOGUE AS A CA.

4.4 FTP Proxy

The open source program frox acts as FTP Proxy in the gateprotect firewall server. This proxy acts as an interface for the antivirus solution and supports active FTP.



ATTENTION !

THE FTP PROXY MUST ONLY BE USED AS AN OUTBOUND FILTER AND MUST NEVER BE USED IN A DMZ.

4.5 SMTP Proxy

The SMTP Proxy pimp has been developed by the gateprotect AG. It acts as an interface for the antivirus solution and for the spam filter. It is the only proxy which is to configure in the DMZ with its own mail server.

4.6 POP3 Proxy

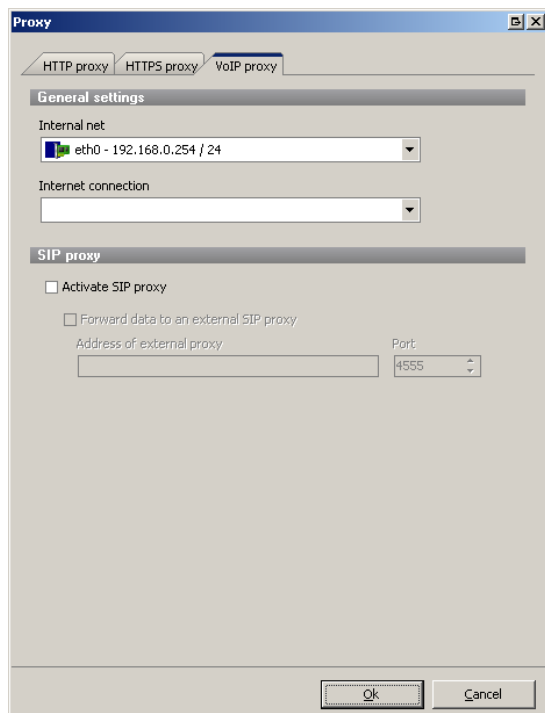
The POP3 Proxy pimp has also been developed by the gateprotect AG. It also acts as an interface for the antivirus solution and for the spam filter.



ATTENTION !

THE POP3 PROXY MUST ONLY BE USED AS AN OUTBOUND FILTER AND MUST NEVER BE USED IN A DMZ.

4.7 VoIP Proxy



With the VoIP Proxy, you can use the gateprotect firewall server as a proxy for the SIP protocol. You find the settings of the VoIP Proxy in the Administration Client via *Options > Proxy > VoIP proxy* tab.

4.7.1 General settings

This dialogue provides following options:

| Option | Description |
|---------------------|---|
| Internal network | Here you can select your local network, which is to be used for telephone calls, from the drop-down list of available networks. |
| Internet connection | Here you select the Internet connection, which the Firewall Server uses to forward the VoIP connections, from the drop-down list of available networks. |



NOTE

TO BE ABLE TO USE THE VoIP PROXY, YOU HAVE TO ENTER THE IP ADDRESS OF THE GATEPROTECT FIREWALL SERVER WITH PORT 5060 IN YOUR VoIP DEVICES. YOU WILL FIND FURTHER INFORMATION ON THIS IN THE DOCUMENTATION OF YOUR VoIP EQUIPMENT.

4.7.2 SIP Proxy

In this dialogue, you can activate the VoIP proxy and set following options:

| Option | Description |
|---------------------------------------|---|
| Activate SIP Proxy | If you tick this box, the firewall server acts as a VoIP Proxy for the SIP protocol and can be addressed on port 5060. |
| Forward data to an external SIP Proxy | If you tick this box VoIP data in the SIP protocol are forwarded to an external SIP proxy. Enter the IP address and the port of the external SIP proxy in the appropriate fields. |

5 USER AUTHENTICATION

5.1 Technical background and preparation

5.1.1 Aim of User Authentication

By using the user authentication, Firewall regulations can be set not just for computers in the network, but also for individual users independent of computer.

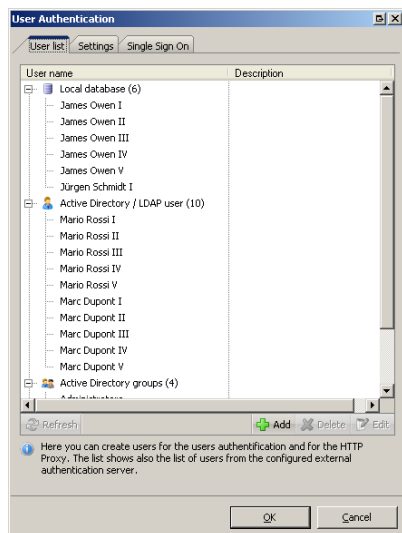
5.1.2 Technical background & preparations

The User Authentication offers the ability to set regulations for individual users and user groups. The firewall runs a web server that exclusively processes user logins that are validated by an authentication demon. The login data is compared to a local user database on the firewall. In case of a mismatch the authentication demon additionally checks for a Microsoft Active Directory or openLDAP server using the Kerberos protocol. If the authentication is successful, the IP address the request came from is assigned to the firewall regulations of the user. Users who are registered in the local database of the firewall can change their password using the web server. The password can contain up to 248 characters. Longer passwords are accepted, but will be reduced automatically.

Specific computers such as a terminal server or servers for administrative purposes can be excluded from the user authentication. Login requests from these computers will be blocked by the web server and authentication demon.

The HTTP-Proxy can be set to intransparent mode to force users on a terminal server to login. In this scenario the permission request is negotiated by the HTTP-Proxy and the authentication demon.

Local user logins



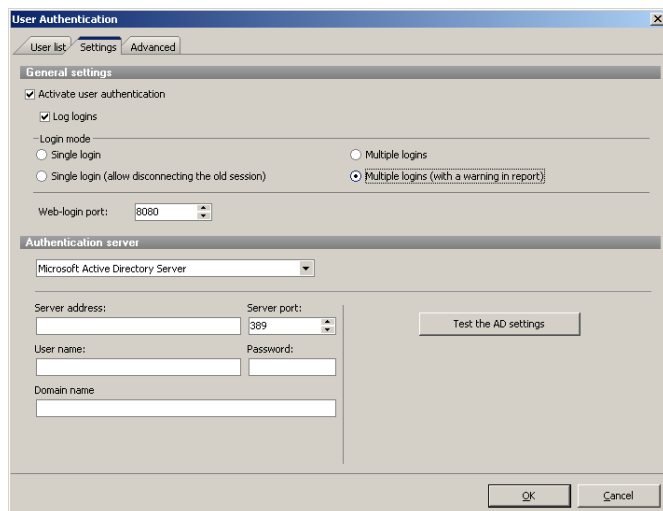
The gateprotect firewall offers local user administration for smaller companies without central administration.

In the first tab, *User list*, you can add, delete or edit users of the local database. You will need to enter a user name and a password.

By ticking the *Change password at next login* box a user has to change the password at the next login. The user will be guided to the password change page. The authentication demon only accepts logins after the password has been changed successfully.

Authentication server

In the lower section of the tab *Option > User authentication > Settings* you can adjust settings for the authentication server. The settings tab allows to configure a Microsoft Active Directory server or an openLDAP server.



For the Microsoft Active Directory server enter the server address, LDAP-Port, user name and password of the administrator (it is useful to create a dedicated user) and the domain name (e.g. company.local) here.

To configure an openLDAP server the address, port and additionally the User and Base-DN. The account requires reading permissions.

General settings

In the general settings the user authentication can be activated. The login mode and the log option is set here. For the login mode determine upon the methods:

| Setting | Description |
|--|---|
| Simple log-on | With simple log-on each user can only be logged on from one IP address at a time |
| Simple log-on with session separation | Session separation means that previous log-ons are only logged off when a user logs on from a different IP address. Without session separation in simple log-on each subsequent log-on would be declined. |
| Multiple log-on (with warning in the report) | Warnings are written in the report in this log-on mode. |
| Multiple log-on | With multiple log-on a user can be logged on at the same time from up to 254 different IP addresses. |
| Web-login port | At this point, the HTTPS-Port can also be set for web log-in. The standard port 443 is preset for HTTPS. |



NOTE

CREATE A LOCAL "SUPERUSER". SO YOU ARE ABLE TO GET ADMINISTRATIVE RIGHTS ON THE FIREWALL ON EVERY WINDOWS PC. TO UNLOCK THEM, YOU DON'T HAVE TO LOG OFF BUT YOU GET RIGHTS ON THE CLIENT (E.G. RDP).

Active Directory Groups:

If you use a Microsoft Active Directory server for authentication, the firewall will show you the AD-Groups. You can handle them equivalently to users. The Active Directory manages the user's rights, meaning the AD-Users have to be assigned to defined AD-Groups. Only the AD-Groups are configured on the firewall.

Advanced settings

In the advanced settings tab the Kerberos services can be activated and if needed the firewalls hostname and domain can be adjusted. If you use Kerberos the key can be imported here.

Finally you have the choice to display a *landing page* when someone unauthorized tries to access the internet.

5.2 Login

You can log in on different ways:

- Login using a web browser
- Login using the User Authentication Client
- Login using Single Sign On

5.2.1 Login using a web browser

Logging in using a browser is very easy.

At first, you have to type in the IP-address of the firewall-server in the address-field of you browser, for example:

https://192.168.12.1 (in this example, the predefined port 443 is used)

Afterwards, it is necessary to enter username and password. The login is completed after a click on *Connect*. This way to log in works with every web browser and is encrypted with SSL. The window which was used to log in has to stay open the whole session; otherwise your Session will be closed automatically. This is necessary for security so that a pc on which a user forgot to log off isn't available to everyone.

5.2.2 Login using the User Authentication Client (short: UA-Client)



After installing the bundled UA-Client, the firewall's IP-address, the username and the corresponding password has to be inserted.

If the password should be stored for future logins, the *Remember password* box has to be ticked.

5.2.3 Login using Single Sign On

Single Sign On (SSO) under the gateprotect Firewall means the one-time login of a domain user to the Active Directory domain for simultaneous creation of the firewall rules.

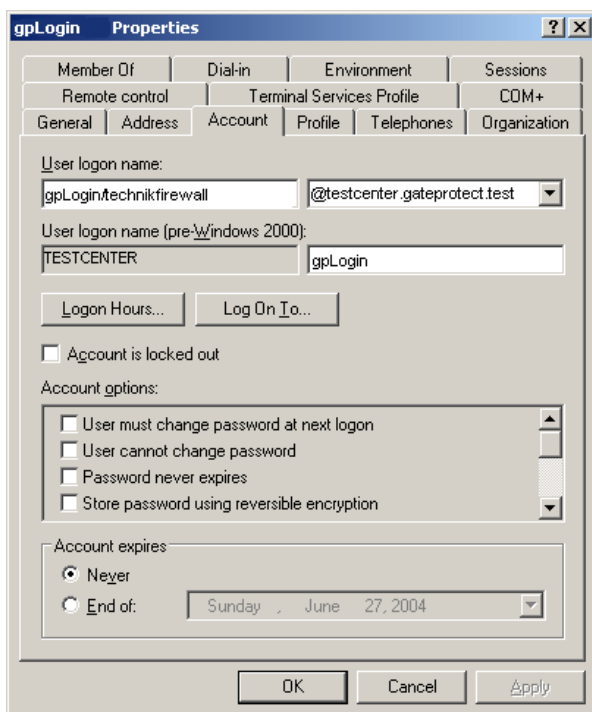
Some conditions must be satisfied in order to implement a Single Sign On in an Active Directory environment with the gateprotect Firewall.

These include the following steps:

- Creation of a special user on the domain server (gpLogin)
- Creation of a special key on the Active Directory Server
- Preparation of the firewall
- Installation of the authentication client
- Testing the configuration

Creating the special user "gpLogin"

It is absolutely necessary to create a special user in the Active Directory. A so-called "principal" will be assigned to this user later. This "principal" is then the actual key which is used for communication with the firewall. The user does not need any special permission as it is only used as a "hanger" for the Principal. It is sufficient to create the user as a normal domain user in the domain. The password should have 8 characters for security.



Create a user with custom first and last name.

The login name has to be *gpLogin*. It is important that the username is typed with capital L.

This user is created as a normal domain user.

It is important that the option *Use DES encryption types for this account* is activated.

Creating the key file

A key (principal) must be created on the Active Directory Server and imported into the gateprotect Client so that the client computer can login automatically to the firewall after the login of the user to the Windows domain. The firewall needs a so-called "key file" for this. The Windows program "ktpass.exe" is needed to create the Principal and this file. This program is contained in the Microsoft Resource Kit.

The syntax for creating the key file is:

```
ktpass -out key.fw -princ gpLogin/x-series@testcenter.gateprotect.test -pass hello1 -crypto DES-CBC-CRC -ptype KRB5_NT_PRINCIPAL -mapuser domain\gpLogin
```

Explanation of the PARAMETERS

- out -> The name of the key file is stated here (This will be imported to the firewall later)
- princ -> Username/HostnameoftheFirewall@CompleteDomainName
- pass -> Password of the user
- crypto -> Encoding algorithm (always DES-CBC-CRC here)
- ptype -> The Principal type (always KRB5_NT_PRINCIPAL here)
- mapuser -> The user this Principal is bound to.

In this example, the parameters look like the following:

- User: gpLogin
- Hostname of the Firewall: x-series
- Complete Domain Name: testcenter.gateprotect.test
- Password of the user: hello1

Preparation of the Firewall

The Kerberos authentication can now be activated under *Options > User authentication > Single Sign On* and the previously created key file can be imported.

(Please give attention to the outputs in the report if the import fails.)

Preparation of the Windows client

There is a directory UAClientSSO on the gateprotect installation media. This contains three files. The first one is the pure UAClientSSO.exe. Two parameters must be supplied when starting the program. The first one is the hostname of the firewall (under *Settings > User authentication > Single Sign On*) and the second is the IP address of the firewall.



Example

c:\Program Files\gateprotect\UAClientSSO.exe x-series 192.168.0.1
(It is probably the easiest to make a shortcut containing these parameters)

The second file is UAClientSSOSetup.exe.

This setup program installs the UAClientSSO.exe as c:\Program Files\gateprotect\UAClientSSO.exe.

Both parameters must also be supplied here.

The third file is UAClientSSO.msi.

This is the installation routine as an MSI file which can be distributed to the computers automatically via software distribution (group regulations).

Both parameters must also be supplied here. It is not possible to pass parameters to a MSI file.



NOTE

COPY UAClientSSO.EXE TO A NETWORK SHARE "NETLOGON" OF THE AD SERVER AND CONFIGURE A NETLOGON SCRIPT.



Example

.Start \\<SERVERNAME>\NETLOGON\UAClientSSO.exe <hostname of the firewall> <IP address of the firewall>

Troubleshooting

If you worked through the steps, it's time to test the settings.

Log in from a domain computer. If everything works fine, you should see an icon in the system's tray, which shows that you are logged in.

In case of an error, check all steps again.

Test the user authentication without SSO using the web client.

Start UAClientSSO.exe with the parameters from command line.

Restart the Windows client.

Check the firewall's report.

Check time-differences between the domain controller, the firewall and the clients (Kerberos is very time-critical; it's useful to use timeservers). If it doesn't work at all: Delete the user gpLogin and create him again. Afterwards, create the key file again and import it again.

5.3 Users

Users and AD-Groups, just like computers, can be assigned to the desktop as individuals or as user groups. You then define the rules for these objects, which are assigned to the users as soon as they log on.

If a user logs on from a computer, which itself has certain rules, the user is subject to the rules of that computer as well as his personal rules.

In the user groups on the desktop you can choose users from the local Firewall list or from the openLDAP or Active Directory Server authentication server.

There is also a special Default User Group.

No users can be added to this group. It comprises all users who can log on, but who are not on the desktop as individual users or members of other user groups. If such a default group is set up on the desktop and you have assigned rules to it, any user subsequently set up in the Active Directory Server is automatically assigned to this user group. After logging on this new user is then automatically assigned the default rules. This removes the need for additional administration for each user.

5.4 Examples

5.4.1 Windows domain

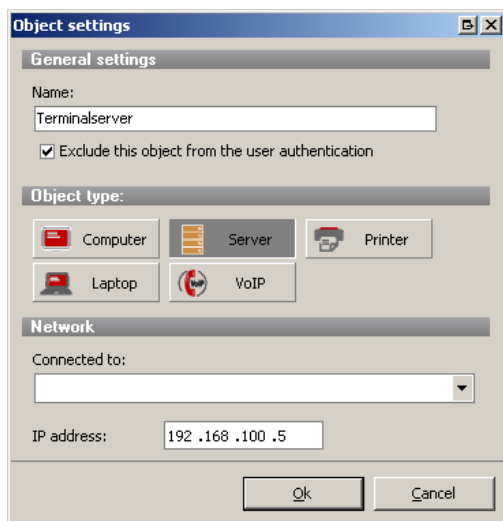
If you have a Windows domain, you can connect user authentication to the Windows Domain Controller.

Enter the data of your domain controller on the Settings tab of the Authentication Server dialogue box. In the user list you will see all users who are in this domain. Then you can drag user icons to the Configuration Desktop and assign rules to them.

The users must now call up the IP address of the Firewall with "https" in their browser and log on. If log-on is successful, the user's Firewall rules are applied to the supplied IP address.

If the browser window is closed the session cookie lapses and the rules expire.

5.4.2 Terminal server



If you use a terminal server, this should be removed from the user authentication, as otherwise when one user has logged on, all further users will receive the same rights as the first user.

To remove the terminal server from user authentication proceed as follows:

- Double click on the terminal server symbol on the configuration desktop.
- Tick the *Exclude this object from user authentication* box.

There is the intransparent HTTP Proxy for a terminal server. Adjust the HTTP Proxy to intransparent for this purpose under Settings > Proxy Settings.



NOTE

FOR THE HTTP PROXY THE BROWSER MUST HAVE FIREWALL IP ADDRESS IN ITS SUB NETWORK AND PORT 10080. TO AVOID DOWNLOAD LOOPS, THIS FIREWALL IP ADDRESS SHOULD BE ENTERED IN "EXCLUDE THIS IP ADDRESS FROM PROXY" IN THE BROWSER.

All users who now log on to the terminal server will first receive a notification when they open the browser asking for user name and password. As soon as they have authenticated using local user authentication, the Active Directory or the openLDAP/Krb5, they can use the terminal server to surf the Internet.

The logged on users can surf until the last browser entity is closed. When the browser is reopened, they also have to log on again.

Logged-on users receive their own URL and Content Filter settings and are logged in the statistics individually under their names.

6 WEB-FILTER (URL, CONTENT AND APPLICATION)

6.1 URL Filter

The URL Filter function of the gateprotect Firewall Server checks Internet addresses (URL, Uniform Resource Locator consisting of server names, path and file names) received in the HTTP data communication for allowed and/or not allowed terms according to their classification in the black and whitelists.



NOTE

THE HTTP DATA COMMUNICATION OF A CONNECTION CAN ONLY BE FILTERED BY URL LISTS AS WELL, IF USE OF THE HTTP PROXY IS ACTIVATED IN THE RULES EDITOR FOR THIS CONNECTION.

If the URL of a website contains terms that are on a blacklist, access to this site will be blocked. If certain terms are removed from the blocking list, they can be added to a whitelist.



Examples

<http://www.servername.com/sex/index.html>

The term "sex" is on a blacklist. The listed URL is therefore blocked.

<http://www.servername.com/sussex.html>

The website name of the historic county Sussex also contains the term "sex" and would therefore also be blocked. To prevent this, the term "sussex" must be entered into a whitelist.

During installation of the Administration Client predefined blacklists and different categories for the URL Filter are created by gateprotect. These predefined categories and lists can be supplemented at any time via the Administration Client and any existing terms may be removed.

6.1.1 Switching the URL Filter on and off

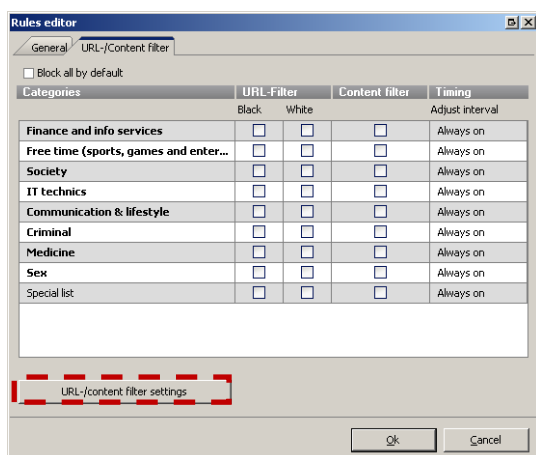
Activate or deactivate URL Filter categories using the Rules Editor:

Step 1

Double click on a connection on the *Configuration Desktop*.

Step 2

Click on the *URL / Content Filter* tab in the *Rules Editor* dialogue box.



Step 3

On this tab you can switch the individual URL Filter categories on and off.

In the *URL Filter* column for each category tick to add that category to the black or whitelist.

Step 4

To edit the individual categories and URL lists, click on the *URL / Content Filter Settings* button.

In the *URL / Content Filter* dialogue described below, you can adjust the categories and lists of the URL Filter individually.

6.2 Content Filter

If websites have no checkable terms in their URLs, a URL Filter alone, as described in the previous chapter, is insufficient. Therefore, as a further filter method the gateprotect Firewall Server enables to filter HTTP data communication using the content of the websites. For this purpose, a Content Filter is integrated into the Firewall Server, which is based on Commtouch's content filter technology.

Similar to search machines on the Internet, Commtouch searches available websites, analyses and categorizes them and collates the results in a database.



NOTE

THE HTTP DATA COMMUNICATION OF A CONNECTION CAN ONLY BE FILTERED BY CONTENT AS WELL, IF USE OF THE HTTP PROXY IS ACTIVATED IN THE RULES EDITOR FOR THIS CONNECTION. ALL CONTENT FILTER FUNCTIONS WILL AUTOMATICALLY BE DEACTIVATED ONCE THE 30-DAY TRIAL PERIOD HAS LAPSED. IF YOU WOULD LIKE TO CONTINUE USING THESE FUNCTIONS, YOU REQUIRE AN ADDITIONAL LICENSE FOR THE CONTENT FILTER. PLEASE CONTACT OUR SALES DEPARTMENT FOR FURTHER INFORMATION ON LICENSING THE COMMTOUCH CONTENT FILTER TECHNOLOGY IN THE GATEPROTECT FIREWALL SERVER.

6.2.1 Switching the Content Filter on and off

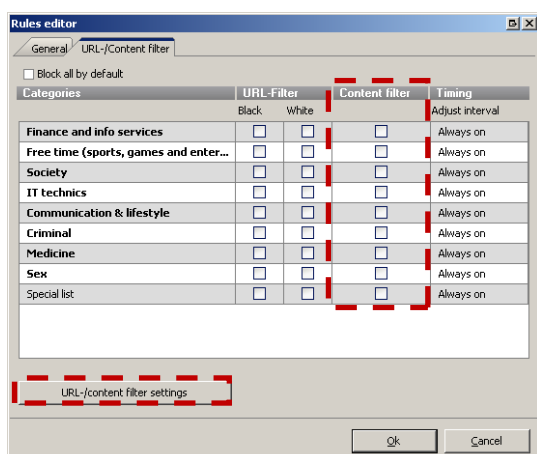
Activate or deactivate Content Filter categories using the Rules Editor:

Step 1

Double click on a connection on the *Configuration Desktop*.

Step 2

Click on the *URL / Content Filter* tab in the *Rules Editor*.



Step 3

You can adjust general settings for the Content Filter on this tab.

Use the *Content Filter* column to activate or deactivate the corresponding options for the individual categories.

Step 4

To edit the existing categories or URL lists, click on the *URL / Content Filter Settings* button

(cf. Chap. 6.2.2 Configure URL and Content Filter).

6.2.2 Configuration using the URL / Content Filter dialogue

You can use the *URL / Content Filter* dialogue box to

- edit, delete or add categories
- add or delete terms on the black or whitelists
- import and export black and whitelists

You can reach this dialogue box from the Rules Editor as follows:

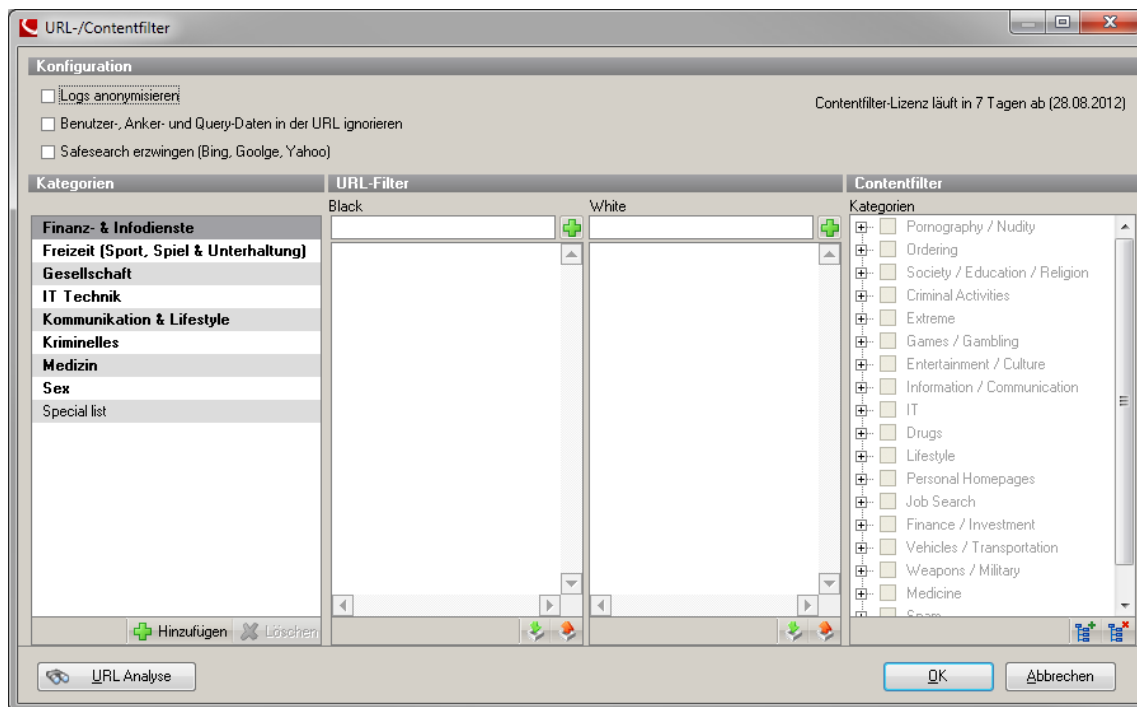
Step 1

Click on the *URL / Content Filter* tab in the Rules Editor.

Step 2

Click on the *URL / Content Filter Settings* button to configure existing categories and URL lists.

The *URL / Content Filter* dialogue box is displayed.



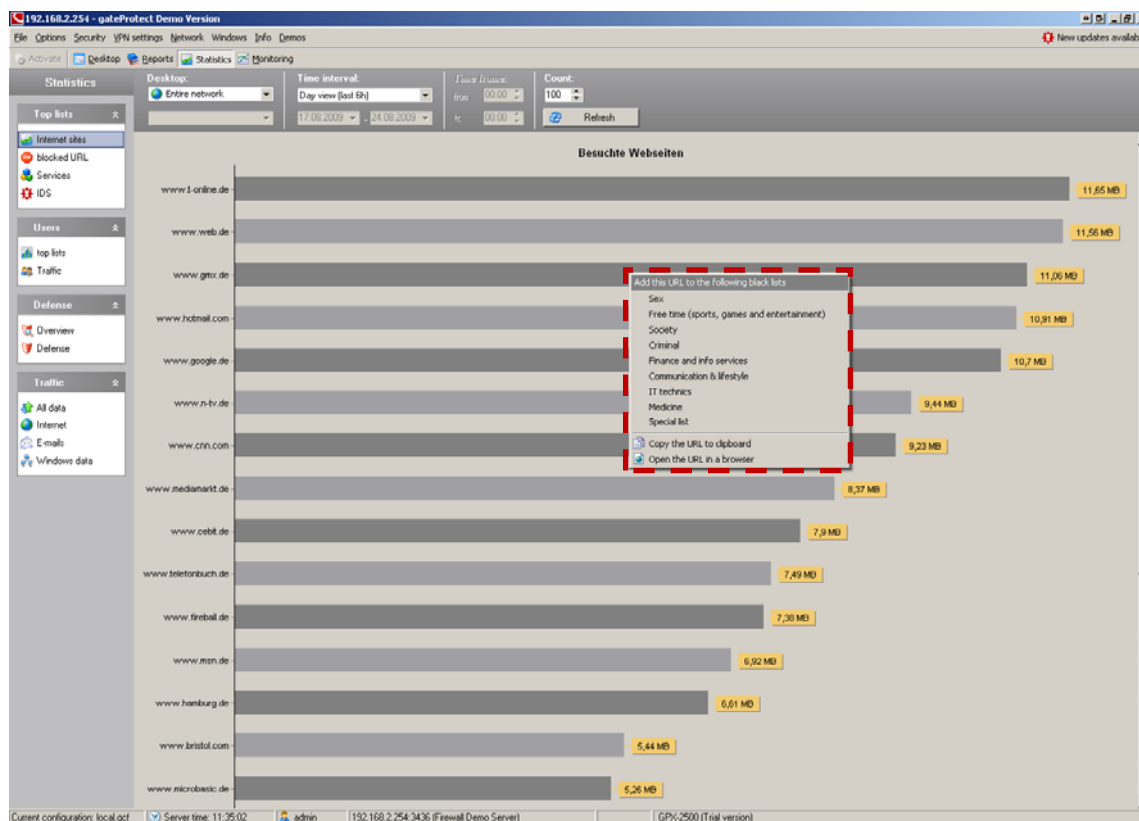
| Setting | Description |
|----------------|--|
| Anonymize logs | Tick this box if you don't want to log user names of users logged on to the web interface. The statistic for users in user administration will then be switched off. However, statistics on IP levels are continued. |
| SafeSearch | If SafeSearch is activated, image search in search engines is automatically set (SafeSearch="Strict" and should not be changed. |
| Categories | In "categories" you find a list of categories given by gateprotect as well as categories that you have created and edited individually. A category usually consists of a Blacklist, a Whitelist and a selection of content groups. |
| URL Filter | The <i>URL Filter</i> section displays all entries of the black and white lists of each selected category. |
| Black | You can enter your own terms in the <i>Black</i> text box and add them to the blacklist by clicking on the + button. |
| White | You can enter your own terms in the <i>White</i> text box and add them to the whitelist by clicking on the + button. |
| Content Filter | The Content Filter groups are provided by Commtouch and cannot be amended. |
| URL Search | If you have a specific URL that was blocked you can quickly find the terms in the URL lists, which lead to a block with this search. |

6.2.3 Adding URLs using the Administration Client or Statistic Client

You can create or edit your own URL lists either in the *URL / Content Filter* dialogue box or directly from the Statistics window of the Administration Client and Statistic Client.

Step 1

Right-click on the appropriate entry to do this.



Step 2

Select the category to which the entry is assigned from the context menu

6.3 Application Filter

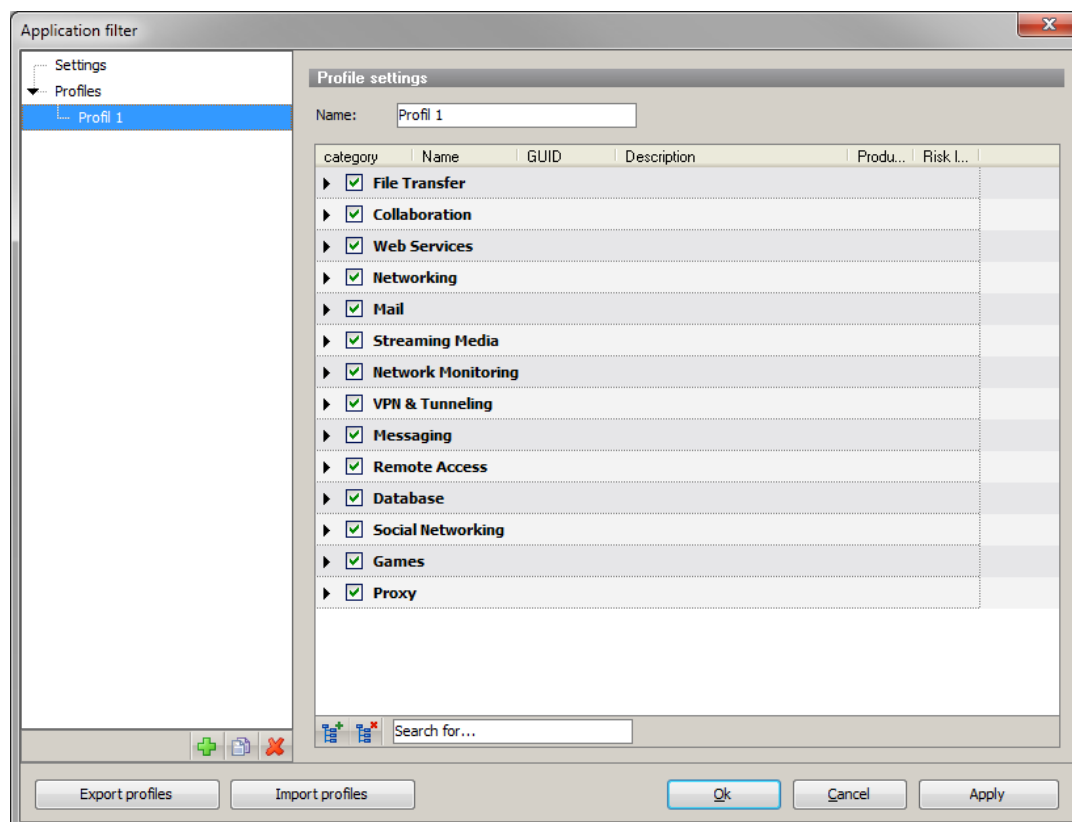
To improve the security in the company network, it is absolutely necessary to combine all filters – URL, Content and Application Filter.

Due to the easy handling of the URL and Content Filter you are able to filter all not allowed data from the whole traffic very fast and secure. Furthermore you can use the Application Filter to filter the content of the remaining and necessary services and websites very accurately.

The Application Filter can be found in the menu item *Security*.

6.3.1 Create profiles

First at least one profile with a selection of protocols that should be blocked need to be created.



- IT IS POSSIBLE THAT THE APP FILTER CLASSIFIES SOME LOGS ONLY AFTER SEVERAL PACKAGES. THEREFOR A FIRST CONTACT E.G. WITH SKYPKA CAN NOT ALWAYS BE PREVENTED. AFTER THATTHE FOLLOWING PACKAGES PACKAGES WILL BE BLOCKED.

6.3.2 How to set up the Application Filter for connections

The Application Filter will be configured for each connection in the rules editor in the same way as the URL- & Content-Filter.

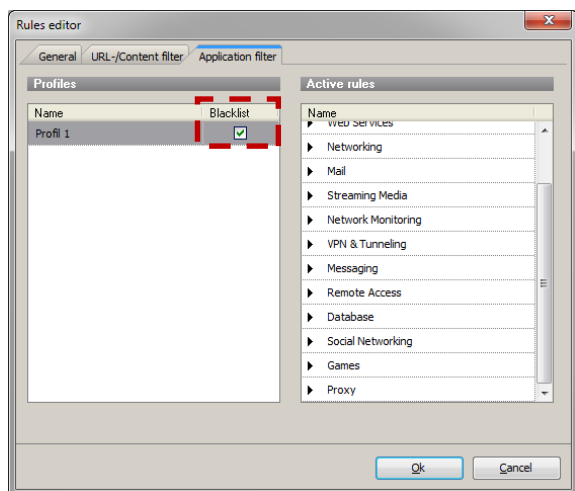
i YOU CAN JUST USE THE APPLICATION FILTER FOR IP BASED CONNECTIONS. IT IS NOT POSSIBLE FOR USERS OR USER GROUPS.

Step 1

Double click on a connection on the *Configuration Desktop*.

Step 2

Click on the *Application Filter* tab in the *Rules Editor*.



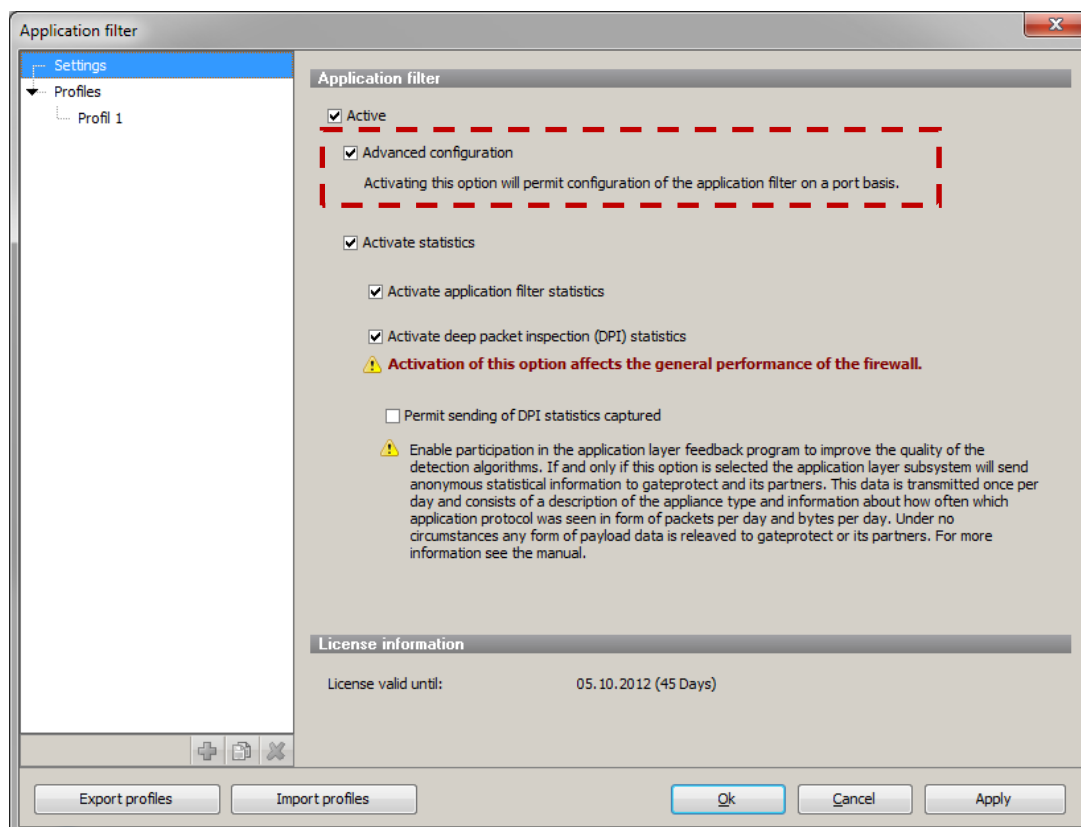
Step 3

In this tab you find the different *profiles* on the left and *Active rules* for this profile on the right.

Activate or deactivate the corresponding profiles by checking *Blacklist*.

6.3.3 Common settings of the Application Filters

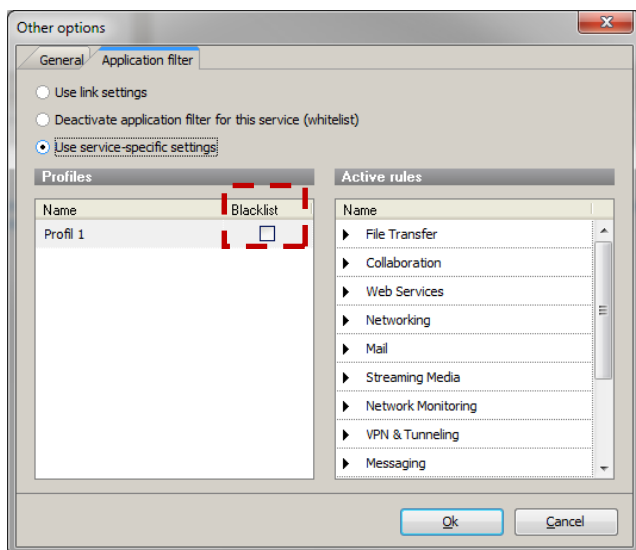
In addition, you can enable various other features of the app filter in this settings.



6.3.3.1 Advanced configuration

„*Advanced configuration*“ activates the Application Filter settings for single services.

Click in the Other Options column to apply Application Filter Profiles to individual services in the rule editor



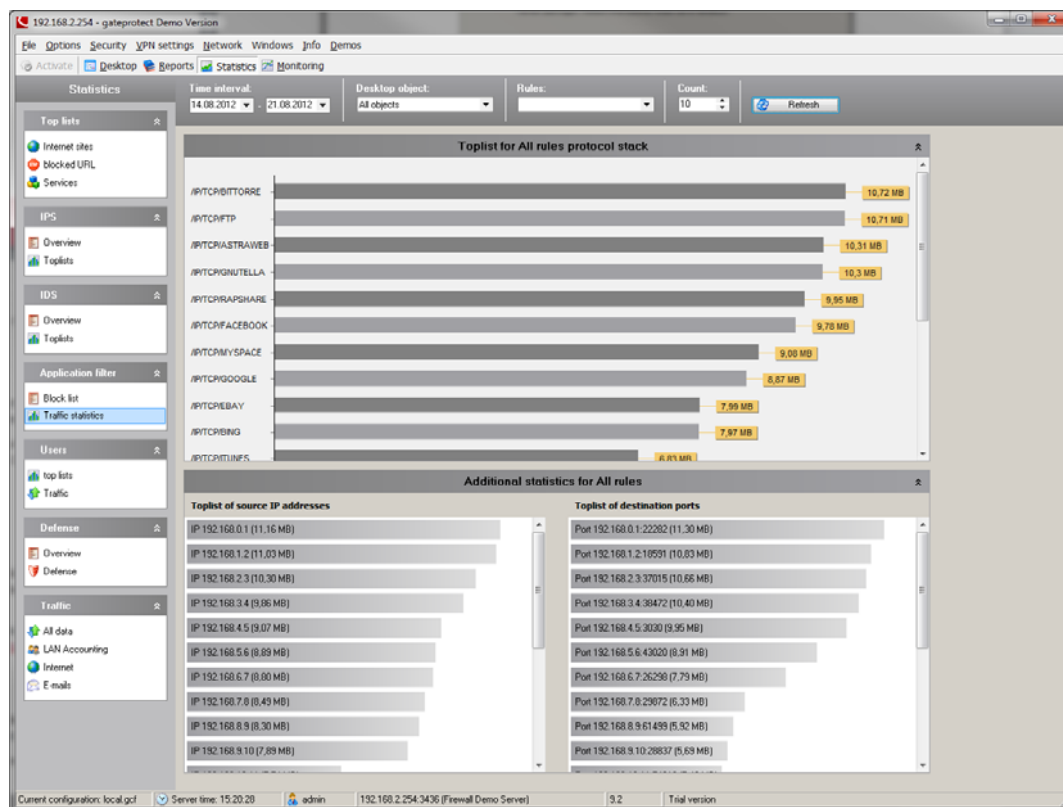
In this tab you find the different *profiles* on the left and *Active rules* for this profile on the right.

Activate or deactivate the corresponding profiles by checking *Blacklist*.

6.3.4 Statistics

If „*Statistics*“ is activated in the Application Filter settings, the system will generate statistics about the App-Filter. These can be evaluated in the Statistics module

„*Deep packet inspections statistics*“ allow more detailed information about used and blocked protocols; however they have a strong impact on the Firewall



7 LAN ACCOUNTING

7.1 Lan Accounting Introduction

Accounting is the customer related data acquisition of the network service usage. Generally the collected data contains the duration and the quantity of the network service utilization.

This data helps to develop systems to account and restrict the provided services.

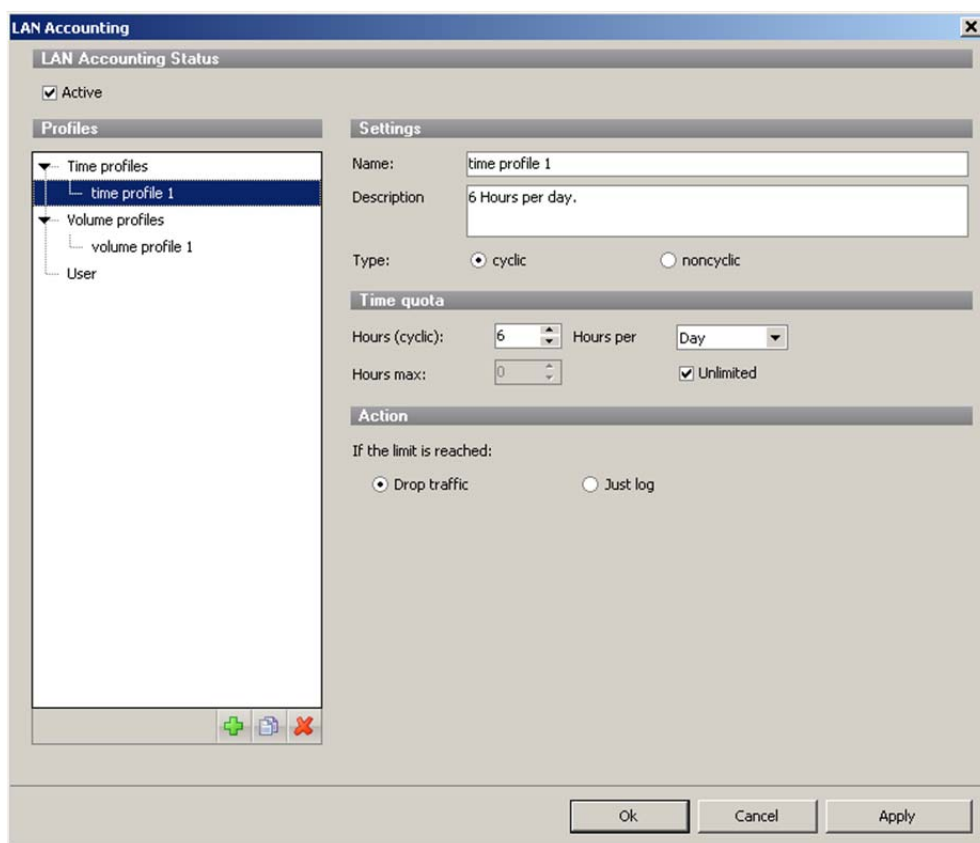
The gateprotect Lan Accounting offers the possibility to control the users network time and network traffic. It enables the configuration of time- and volume profiles.

7.2 Lan Accounting Configuration

To access the Lan Accounting dialog choose Options from the main menu and click on Lan Accounting.

7.2.1 Creating a time profile

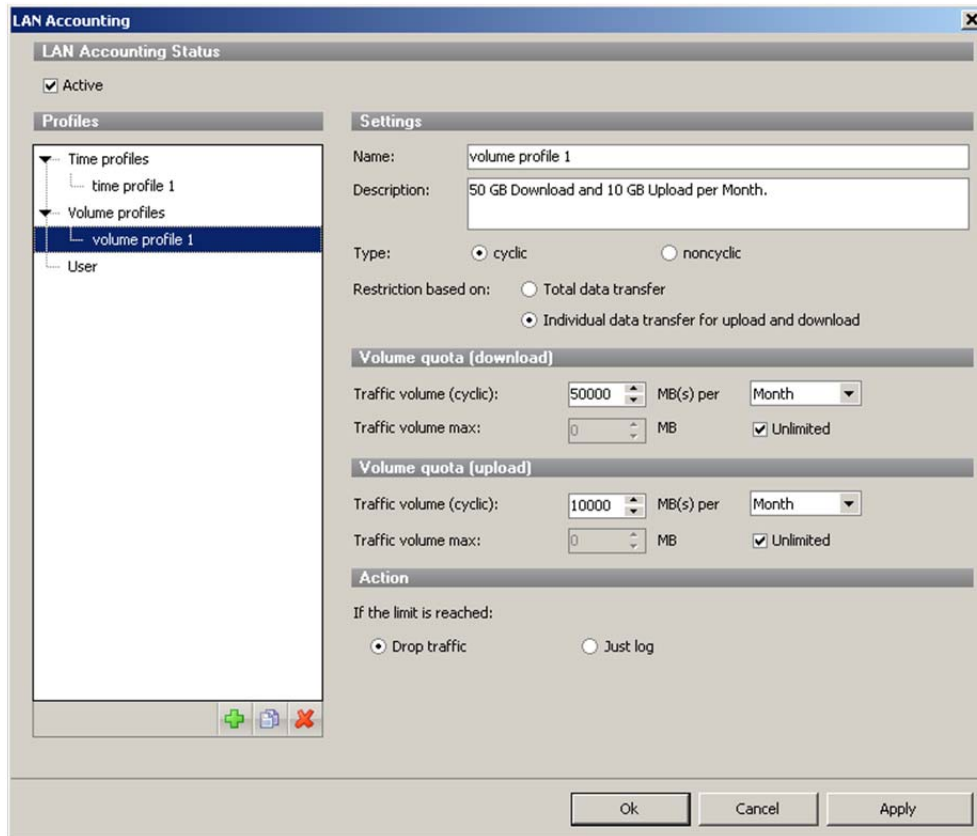
In the configuration dialog of the time profile you can choose the type of the profile to be cyclic or non-cyclic. The cyclic profile defines a time quota in a certain periodic cycle. (e.g. 6 hours per day)



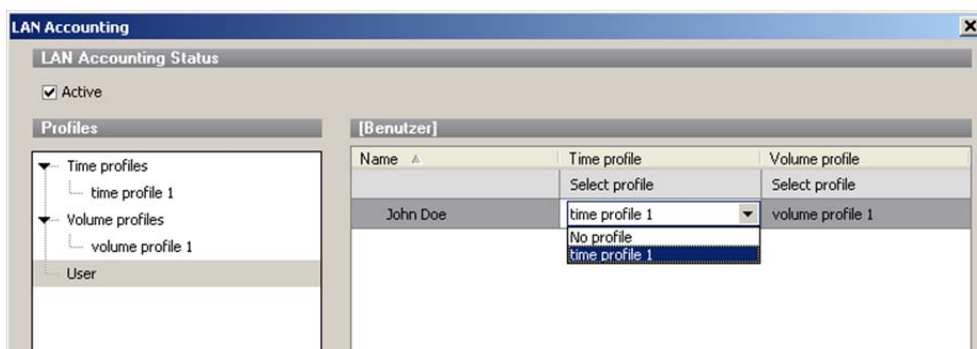
The non-cyclic profile sets a defined total time frame for the user to access the network services.

7.2.2 Create a volume profile

In the configuration dialog of the volume profile you can also choose the type of the profile to be cyclic or non-cyclic. The cyclic profile defines a volume quota in a certain periodic cycle. (e.g. per day/week/month) and in the non-cyclic profile you can set a fixed value.



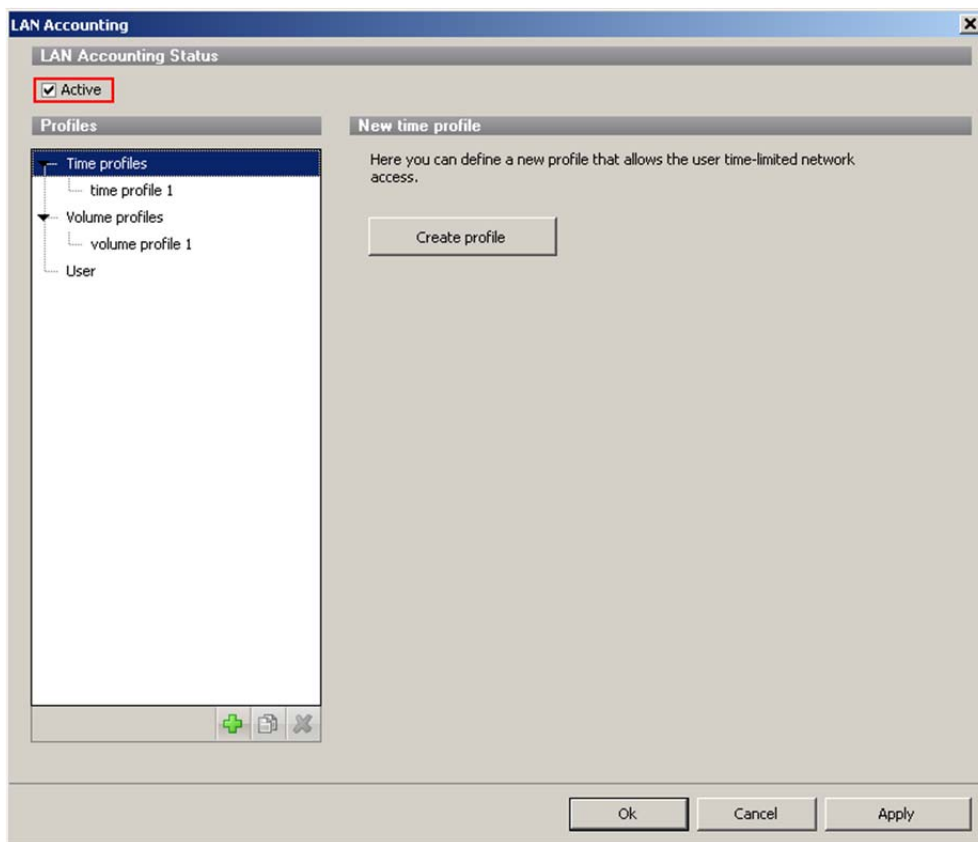
Both profile types offer the possibility to differentiate between up- and download traffic.



After the configuration the profiles have to be applied to the users.

7.3 Activate Lan Accounting

The Lan Accounting settings will only be activated when the corresponding the Lan Accounting status is set to active.



To control the utilization of the network services at specific time frames per day you can use the rules editor.

8 TRAFFIC SHAPING & QUALITY OF SERVICE

8.1 Introduction

8.1.1 Target

The aim of traffic shaping is either to reserve bandwidth on the lines for important services or preferred users, or, conversely, to limit bandwidth to certain users, computers or services. The gateprotect Firewall Server offers two methods to achieve this; the actual Traffic Shaping and Quality of Services (QoS). The two methods can be used individually and jointly.



NOTE

ACTUAL TRAFFIC SHAPING IS ONLY AVAILABLE IN THE X-SERIES OF THE GATEPROTECT FIREWALL SERVER, THE A- AND O-SERIES OF THE GATEPROTECT FIREWALL SERVERS JUST OFFERS QUALITY OF SERVICE.

8.1.2 Technical background

Traffic Shaping and Quality of Service are realized using different queues in the Linux Kernel. Within this, IP packets are sorted according to certain rules.

Without Traffic Shaping and Quality of Service the packets are simply transferred in the sequence of their arrival and sent further down the line (*FIFO*, first in first out).

With Quality of Service, gateprotect Firewall realizes a so-called *Prio-Qdisc* on all network cards and VPN tunnels for incoming and outgoing network traffic. A prerequisite of Quality of Service is that applications or devices, such as VoIP telephone systems, position the TOS field (Type of Service) in IP data packets.

The Firewall Server then sorts the packets according to the value of the TOS field and thus, by specified important into several queues with different priority. Data packets from the queue with the highest priority are forwarded immediately. Data packets from queues with lower priority are only forwarded when all queues with higher priority are empty. You can freely configure which data packets are treated with which priority.

The gateprotect Firewall Server only controls Traffic Shaping on the lines to the Internet. It is a prerequisite that the bandwidths of the lines in the up and download are correctly set up. If the bandwidth is set too low, Traffic Shaping stops more than the set bandwidth from being used.

However, if the bandwidth is set too high, the line capacity acts as a limiting factor and overrides Traffic Shaping before it can engage and regulate.

The Traffic Shaping in the gateprotect Firewall Server works according to the HTB model (Hierarchical Token Bucket) with up to two hierarchy levels.

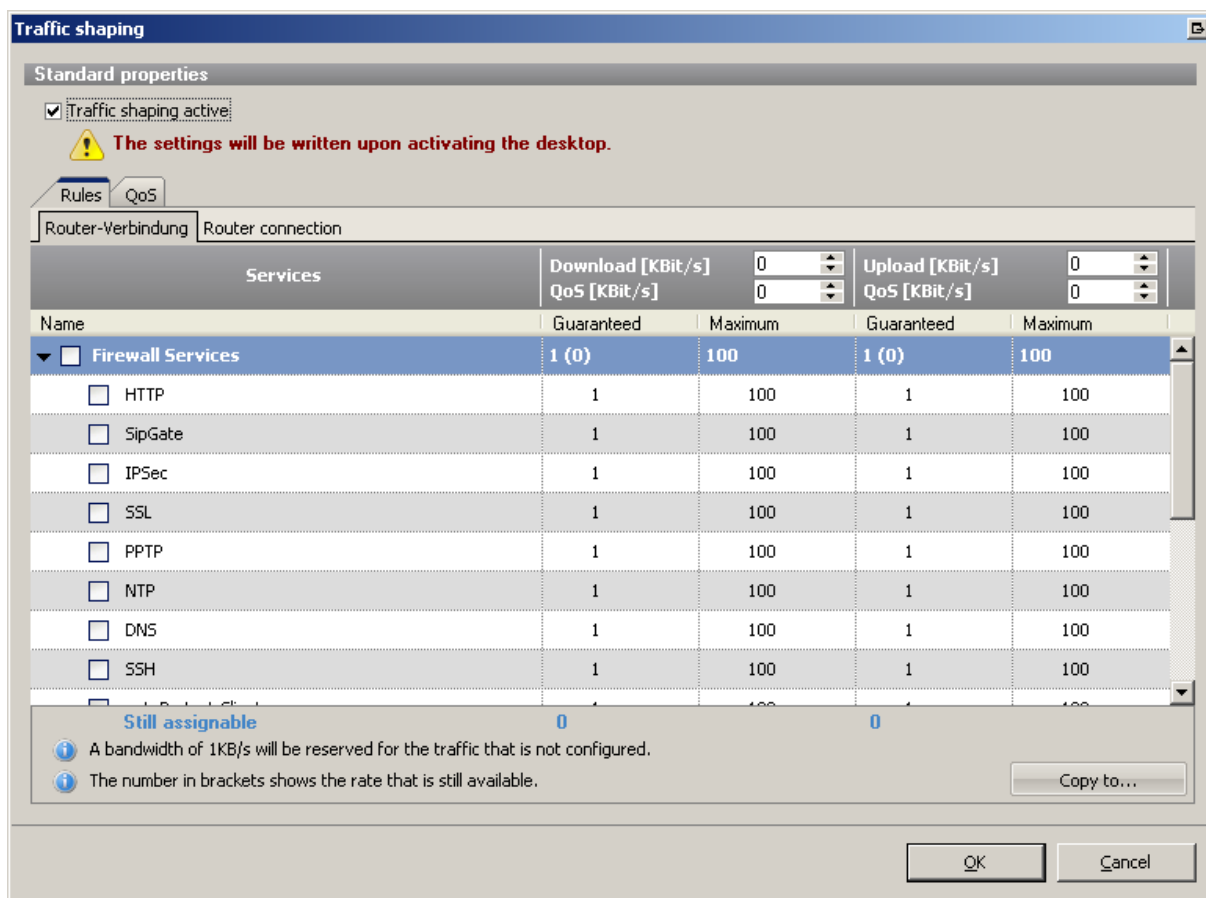
On the top level guaranteed minimum bandwidths or limiting maximum bandwidths for up and download can be specified separately for individual objects set up on the Administration Client desktop. If no maximum bandwidths are set, which are lower than the entire capacity of the line, bandwidth unused by other objects, even above the guaranteed minimum bandwidth, is made available to other objects that would like to use it.

Below the object level the bandwidth assigned to an object can be passed to different services by the same method, i.e. a minimum bandwidth can be guaranteed for the individual services for the relevant object, or services are limited by a maximum bandwidth. These values must lie within the framework of the bandwidths configured for the object. All bandwidths for the Traffic Shaping are specified on the gateprotect Firewall Server in Kbit per second.

If Traffic Shaping and Quality of Service are used at the same time, it remains on the internal network cards in the intranet with the *Prio-Qdisc*. In contrast, the Quality of Service behaves according to the HTB model on the interfaces to the Internet lines. The Firewall Server defines its own HTB class on the top level for data packets with set TOS field according to the set configuration. Therefore, a minimum and maximum bandwidth must be reconfigured for this class, so that network traffic with TOS fields configured differently is forwarded appropriate to its priority.

8.2 Settings Traffic Shaping


Actual Traffic Shaping is only available in the X-Series and in the GPA 400. You can configure Traffic Shaping via *Settings > Traffic Shaping* on the *Rules* tab.



Traffic shaping

Standard properties

Traffic shaping active

 The settings will be written upon activating the desktop.


Rules QoS


Router-Verbindung Router connection

| Services | Download [KBit/s] | QoS [KBit/s] | Upload [KBit/s] | QoS [KBit/s] |
|----------|-------------------|--------------|-----------------|--------------|
| | 0 | 0 | 0 | 0 |

| Name | Guaranteed | Maximum | Guaranteed | Maximum |
|--|------------|---------|------------|---------|
| <input type="checkbox"/> Firewall Services | 1 (0) | 100 | 1 (0) | 100 |
| <input type="checkbox"/> HTTP | 1 | 100 | 1 | 100 |
| <input type="checkbox"/> SipGate | 1 | 100 | 1 | 100 |
| <input type="checkbox"/> IPSec | 1 | 100 | 1 | 100 |
| <input type="checkbox"/> SSL | 1 | 100 | 1 | 100 |
| <input type="checkbox"/> PPTP | 1 | 100 | 1 | 100 |
| <input type="checkbox"/> NTP | 1 | 100 | 1 | 100 |
| <input type="checkbox"/> DNS | 1 | 100 | 1 | 100 |
| <input type="checkbox"/> SSH | 1 | 100 | 1 | 100 |

Still assignable 0 0

 A bandwidth of 1KB/s will be reserved for the traffic that is not configured.

 The number in brackets shows the rate that is still available.

Copy to...

OK Cancel

To use Traffic Shaping first tick the *Traffic Shaping active* box.

There is a tab for each Internet connection (e.g. a router connection) with the corresponding Traffic Shaping settings for each connection.

You must first detail the correct up and download rate for the line in Kbit/s. You can find these values in the information from your Internet service provider for example.

There is a line for each item on the desktop and you can enter settings for the guaranteed and the maximum rate of the Internet traffic for this object in the up and download. If you tick the box the object is included in the Traffic Shaping.

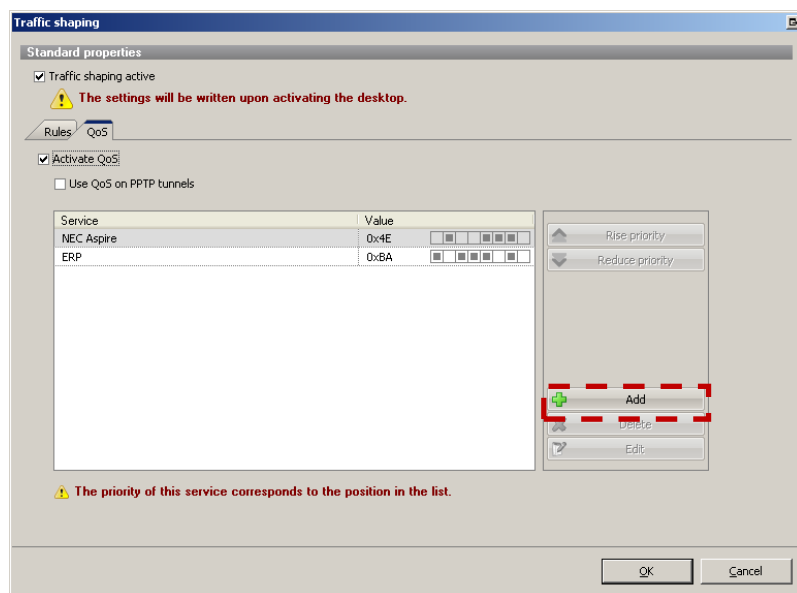
Each line can be expanded if you click on the arrow before the box. Then further lines appear under the object for the individual services allowed for the object.

These services can be included in the Traffic Shaping as a second hierarchy level. The rates for these individual services are always a proportion of the rate of the superior object.

The first line in the window is reserved for Firewall services. They are handled together like an object on the desktop. If you activate Traffic Shaping for the Firewall Services, then you can specify rates for the individual services on the Firewall in turn, as for each object on the desktop. It can for example be a rate for the network traffic, which is produced on the Firewall by a Proxy.

8.3 Settings Quality of Service

Depending on your Appliance, you will find the Settings for Quality of Service via *Options > Traffic Shaping* under the *QoS* tab or via *Options > Quality of Service*.



- Using the *Add* button you can define new services, for which the Quality of Service should be set up.
- Enter the name and hexadecimal value of the TOS field into the appropriate fields, which the application or device positions for the service. You will find information on this in the documentation for the application or device, or ask your manufacturer about this value.
As administrator you can also record the network traffic produced by the application and remove the corresponding data packets.
- With several entered services the allocation of the services in the window corresponds to their priority. The top service has the highest priority.
Change the priority by clicking on a service and using the *Increase Priority* or *Reduce Priority* buttons.
- To use Quality of Service for the individual service, tick the *Activate QoS* box. As a further option you can also decide whether Quality of Service is also to be applied to PPTP Tunnel. Normally, you will not require this set-ting and leave this field deactivated.



NOTE

AN ACTIVATED OPTION *QUALITY OF SERVICE ON PPTP-TUNNELS* PUTS A SUBSTANTIAL LOAD ON THE FIREWALL SERVER WHEN ESTABLISHING AND CLOSING PPTP CONNECTIONS, WHICH CAN LEAD TO DELAYS IN ESTABLISHING AN INTERNET CONNECTION. IF YOU WANT TO USE QUALITY OF SERVICE AT THE SAME TIME AS TRAFFIC SHAPING, THE DATA RATE ON THE *RULES* TAB MUST BE GREATER THAN ZERO FOR THE QUALITY OF SERVICE FOR UP AND DOWNLOAD.

9 CERTIFICATES

9.1 Introduction

To secure encrypted connection, the gateprotect firewall uses digital certificates as described in the X.509 standard. This affects several sections: IPSec and VPN-SSL, the User Authentication on the firewall, the HTTPS proxy as well as the connections from the Command Center to the administrated firewalls.

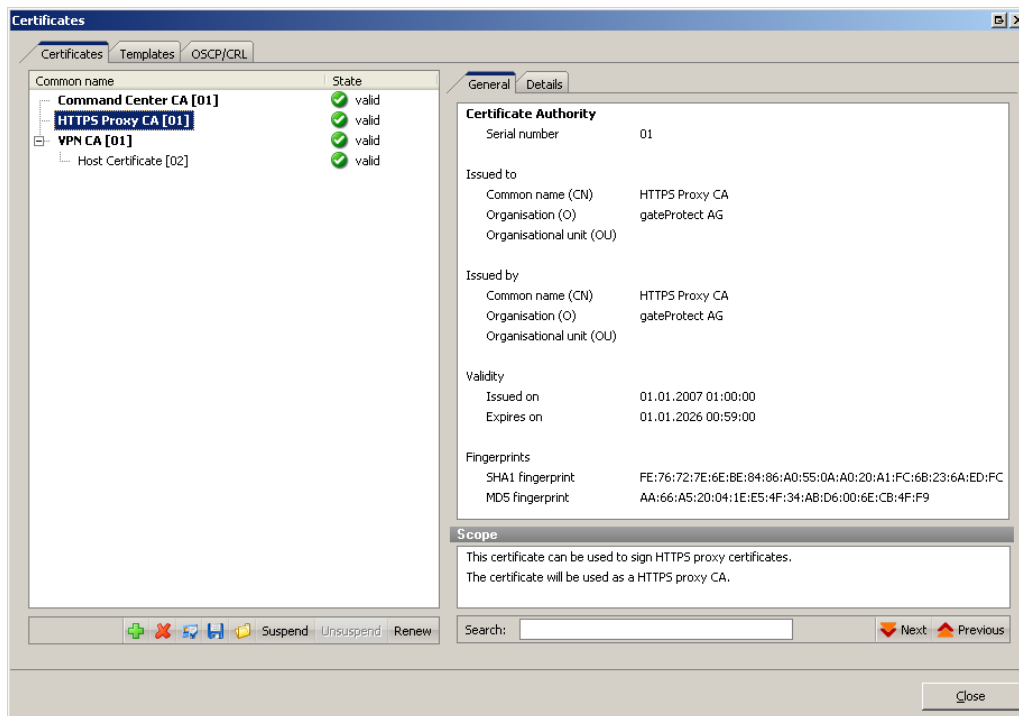
To manage the certificates for these purposes, the gateprotect firewall is equipped with an administration interface. The firewall itself acts as certification authority. To do this, a so-called CA-certificate is needed. To centralize the management of the certificates, it is advisable to create a CA-certificate on a central firewall and use it to sign every certificate used for the application directly. This is called a single-staged certification-chain.

All certificates for applications have to be signed by central firewall. If a certificate is needed for another firewall (an outpost), you have to create a request on it. This request has to be signed by the central firewall. The signed request you created has to be imported by the outpost firewall in order to use it.

If your outposts should have the ability to create certificates for mostly local purposes which are however recognized as valid to your whole organization, you can use multi-staged certification-chains. To achieve such a chain, you need a so-called Root-CA-certificate on your central firewall with which you sign the secondary CA-certificates. You need to create requests for these secondary CA-certificates on your outpost firewalls. After you imported the signed CA-certificates, the outpost firewalls themselves are able to sign certificates for applications. To display these connections clearly, the gateprotect firewall shows them in a tree-view.

9.2 Certificates

List of certificates.



The bold certificates are CAs which can sign other certificates.

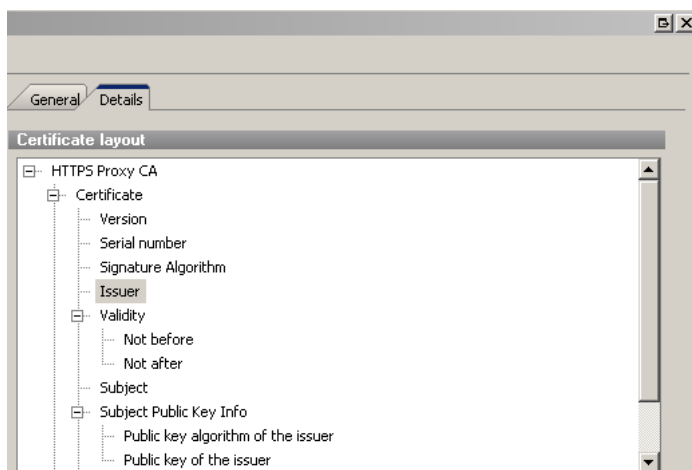
It is not possible to have more than one signing CA and one signing secondary CA besides the CAs for the Command Center and for the HTTPS proxy.

If you create a CA, it is automatically the signing one. You will also see the requests created by the firewall. They were automatically deleted if you import the corresponding signed certificate. Below the list, you will find buttons to create or delete certificates. Furthermore a button to sign requests, to import/export, to suspend/unsuspend and to renew certificates.

On the General tab to the right, you can see general information of the selected certificate. This information can be searched using the *Search* input box below. In the lower box *Scope*, you can see for what purposes a certificate can be used and, if applicable, where it is used at the moment. The name of the certificate is always formatted in this way: "Common Name [Serial Number]" .

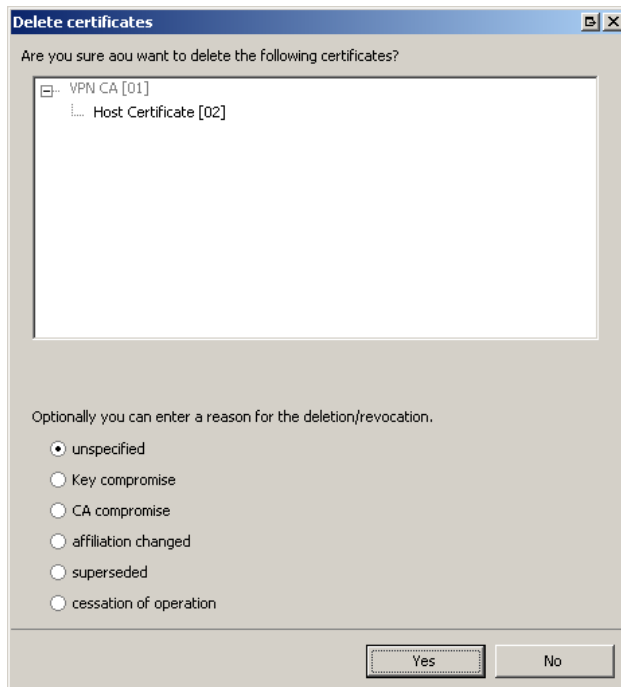
Certificates dialogue - Details

In this tab you will find more information about the selected certificate.



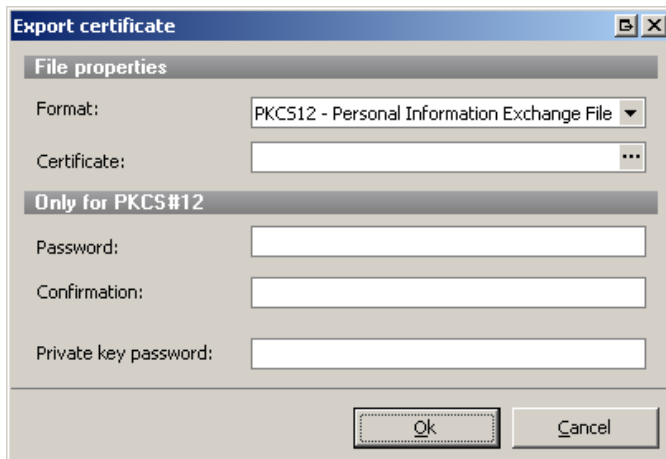
Delete dialogue

This list shows all certificates which are either selected or are affected by the delete action. You can additionally select a reason. It is not possible to delete a certificate which is currently in use.



Export dialogue

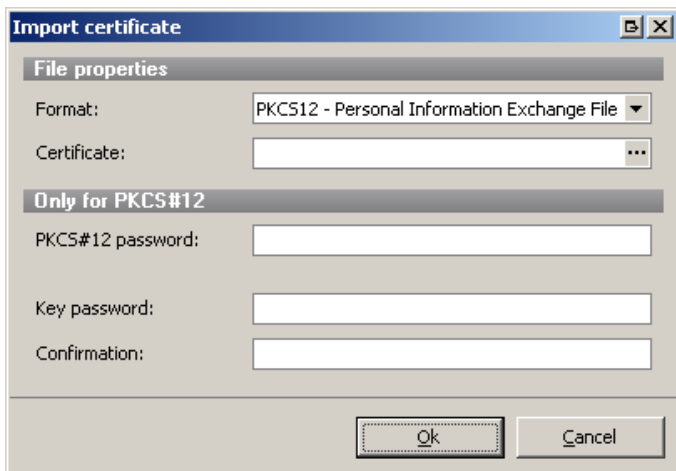
It is possible to export certificates using the PEM or the PKCS12 format. If you use PEM, you can only export the public key.



The name of the export file has to be given. If you use PKCS12, the password for the PKCS12 file and the password to encrypt the private key has to be given, too. In both formats, the whole certification-chain (public keys) will be exported.

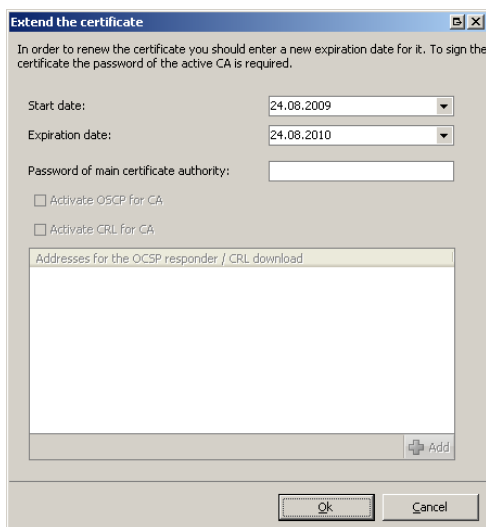
Import dialogue

It is possible to import certificates the same way as exporting them.



The PEM format only imports public keys. However, it imports the whole certification-chain so you don't have to import CA and certificate separately. Using PKCS12, you need the password to decrypt the file itself. The key password encrypts the private key again on the firewall.

Renew dialogue

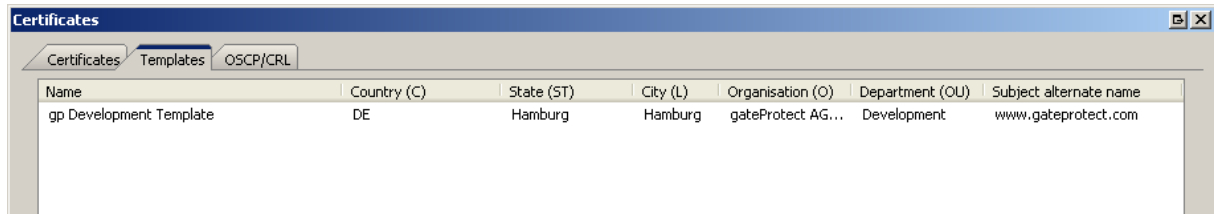


The selected certificate gets renewed. To do this, the firewall creates a new certificate using the same private key and data.

9.3 Templates

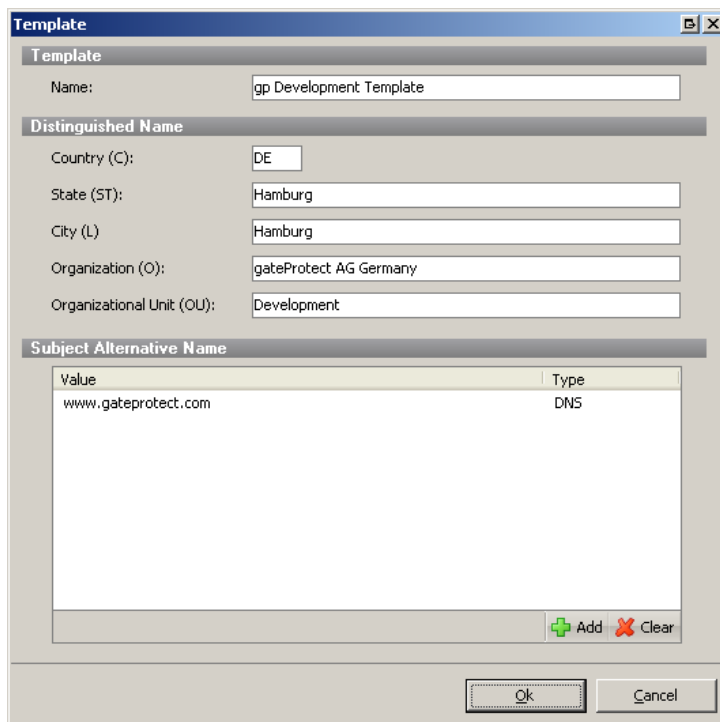
Using templates is a way to simplify the process of creating certificates which use the same data again and again. After you created a template, you can use it to fill in data in every certificate automatically. You can create as many templates as you like to and choose a suitable one of them every time.

The Templates tab in the Certificates dialogue. All templates are listed here.



| Name | Country (C) | State (ST) | City (L) | Organisation (O) | Department (OU) | Subject alternate name |
|-------------------------|-------------|------------|----------|-------------------|-----------------|------------------------|
| gp Development Template | DE | Hamburg | Hamburg | gateProtect AG... | Development | www.gateprotect.com |

Add/Edit a Template



Template

Name:

Distinguished Name

Country (C):

State (ST):

City (L):

Organization (O):

Organizational Unit (OU):

Subject Alternative Name

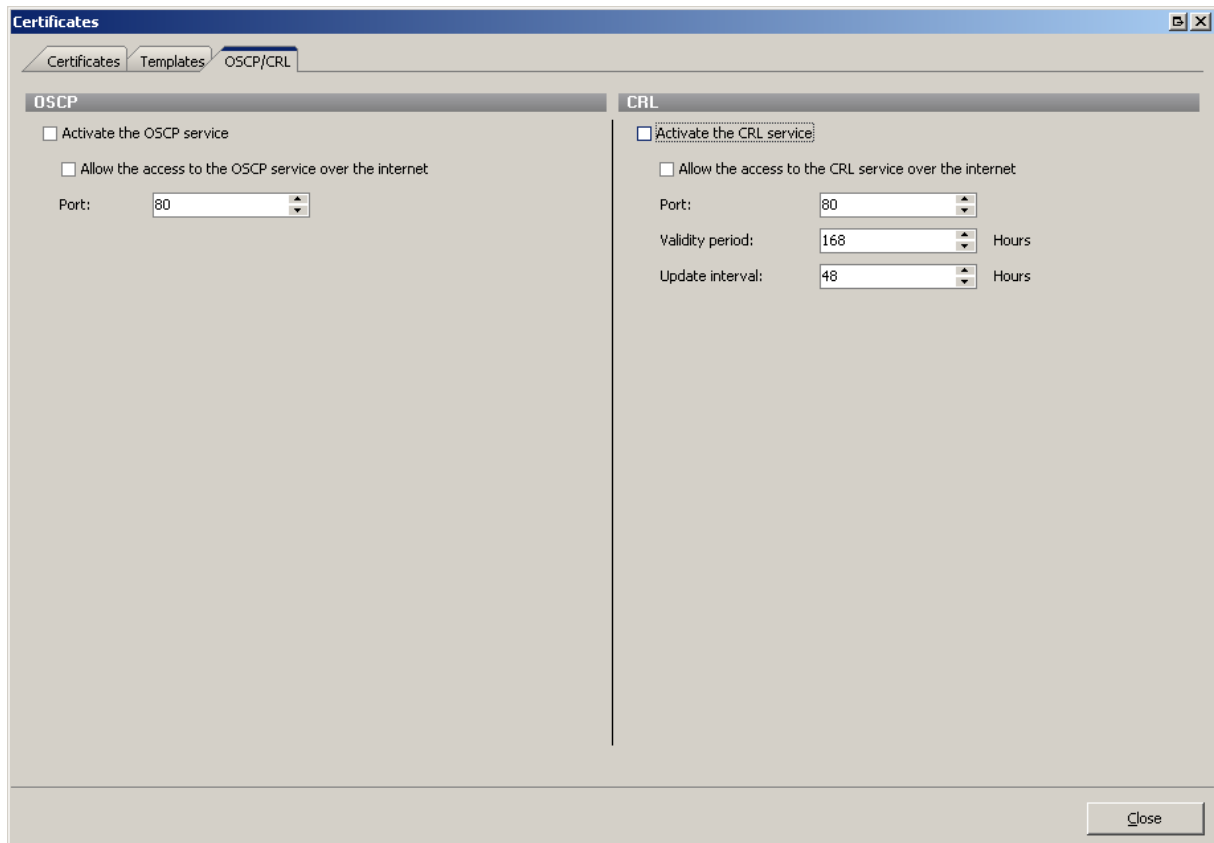
| Value | Type |
|---------------------|------|
| www.gateprotect.com | DNS |

9.4 OCSP / CRL

In cases like quitting of a co-worker or the lost of a private key, the corresponding certificate must be blocked to assure the company's security. This takes part on the firewall which issued the certificate. The deletion of the certificate on the issuing firewall always includes the revocation of the certificate. To make the status of a certificate accessible to other firewalls, the gateprotect firewall implements two distinct mechanisms. Using the Online Certificate Status Protocol (OCSP), the remote firewall requests the status of the certificate from the issuing firewall at the moment the certificate is needed. In addition the firewall is able to expose revocation lists (CRLs, Certificate Revocation Lists) in predefined intervals, which can be downloaded by remote firewalls. Now the application only has to check if the current and appropriate CRL listed the certificate as blocked. VPN-SSL currently only supports CRL.

To use CRL and/or OCSP, the service in general has to be activated one time with necessary settings (particularly the port for online requests). While creating or renewing a CA, you have to declare if CRLs and/or OCSP requests should be created/signed and under which address (URL) this service should be offered. These options were stored in the certificates themselves so applications or remote firewalls know where to check the status of a certificate.

Settings of OCSP/CRL



The screenshot shows the 'Certificates' configuration window with the 'OCSP/CRL' tab selected. The window is divided into two main sections: 'OCSP' and 'CRL'.

OCSP Section:

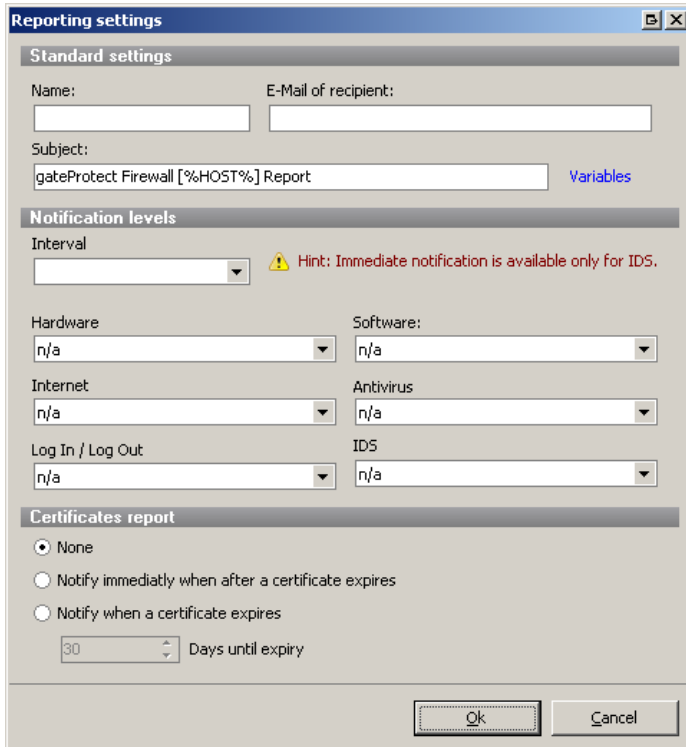
- Activate the OCSP service
- Allow the access to the OCSP service over the internet
- Port:

CRL Section:

- Activate the CRL service
- Allow the access to the CRL service over the internet
- Port:
- Validity period: Hours
- Update interval: Hours

A 'Close' button is located at the bottom right of the window.

9.5 Reports for certificates



The image shows a 'Reporting settings' dialog box with the following sections:

- Standard settings**
 - Name: [text box]
 - E-Mail of recipient: [text box]
 - Subject: gateProtect Firewall [%HOST%] Report [text box] [Variables](#)
- Notification levels**
 - Interval: [dropdown menu] ⚠ Hint: Immediate notification is available only for IDS.
 - Hardware: n/a [dropdown menu]
 - Software: n/a [dropdown menu]
 - Internet: n/a [dropdown menu]
 - Antivirus: n/a [dropdown menu]
 - Log In / Log Out: n/a [dropdown menu]
 - IDS: n/a [dropdown menu]
- Certificates report**
 - None
 - Notify immediatly when after a certificate expires
 - Notify when a certificate expires
 - 30 [dropdown menu] Days until expiry

Buttons: Ok, Cancel

It is possible to receive an E-Mail to get informed when a certificate is going to get expired or is already expired.

This is configurable via *Options > Reporting*.

10 VIRTUAL PRIVATE NETWORKS (VPN)

10.1 Introduction

VPN – Virtual Private Network

VPNs are used to connect several locations through the Internet with the highest possible level of security. Using encoded connections means that you or your external team also have direct access to your corporate network. Moreover, you can connect other branches or offices with your company headquarters.

With the gateprotect Firewall you can use the three most widespread protocols PPTP, IPSec and SSL (OpenVPN) for a secure connection. The following types of connection are available to you:

Client-to-Server connection (PPTP/IPSec/SSL)

With a client-to-server connection a connection is made to the corporate network from outside.

Authentication is either effected using a user name / password combination (PPTP) or with IPSec using issued certificates or so-called PSK (preshared key). Additionally with SSL (Open VPN) with certificates.



ATTENTION !

SEPARATE CLIENT SOFTWARE (E.G. GATEPROTECT VPN-CLIENT) IS REQUIRED FOR AN IPSec CLIENT-TO-SERVER CONNECTION.

Server-to-Server connection (IPSec/SSL)

With a server-to-server connection two locations are connected using an encoded tunnel to a virtual network and can exchange data through this. The two locations can have fixed IP addresses. Alternatively, the connection also supports DynDNS host names. It is also possible to set up IPSec connections between two dynamic IP addresses using DynDNS.

PPTP

The PPTP protocol was designed for client-to-server use. The security of the protocol depends essentially on the selected password (a password is only considered secure if it consists of at least six, or better eight characters and includes special characters, numbers, upper- and lowercase letters).

A PPTP connection is very easy to set up, as the Client is already integrated in newer versions of Windows (2000/XP/VISTA/7).

IPSec

IPSec has a higher security level than PPTP and also meets highest requirements. You need two VPN IPSec capable servers for an IPSec server-to-server connection. For a client-to-server connection, as described above, you will need separate client software. The configuration of the connections is described on the following pages.

The gateprotect firewall is able to create and use secured connections using the IPSec protocol suite. This is based on ESP in tunnel mode.

The key exchange can be accomplished using version 1 of the IKE protocol or using the newer IKEv2, selectively using Preshared Keys or using X.509 compliant certificates. Using IKEv1, it is possible to authenticate using XAUTH. The firewall server is also capable of serving IPSec-secured L2TP.

SSL (OpenVPN)

This type of VPN offers a fast and secure opportunity to tie down a Roadwarrior. The biggest advantage of SSL (OpenVPN) is the fact that all the data traffic runs over a TCP or UDP port and no special protocols are required in contrast to PPTP or IPSec.

10.2 PPTP connections

It is possible to create a PPTP-VPN connection using the VPN Wizard (*VPN Settings > VPN Wizard*). Because this is self-explanatory, this manual only describes the manual creation of a PPTP connection.

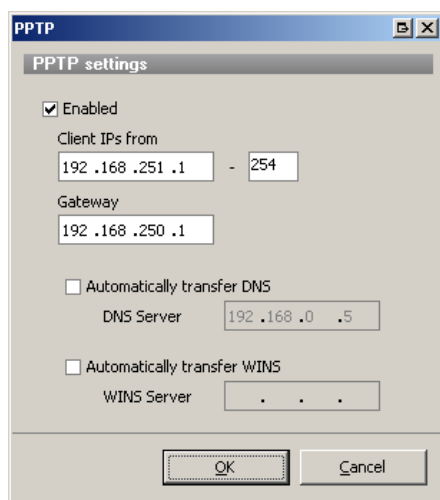
10.2.1 Setting up PPTP Client-to-Server connection manually

Create PPTP connection

You require a PPTP client to be able to use a PPTP connection (in Windows 2000/XP/VISTA/7 a PPTP client is already integrated).

To set up a PPTP connection, select *PPTP...* from the *VPN Settings* menu.

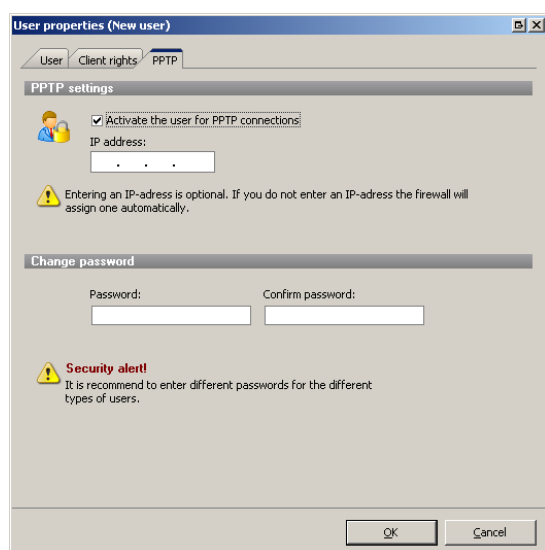
The following dialogue box appears:



Tick the *Active* box. Normally, you do not need to adjust the Client IP addresses this also applies to the Gateway. If you want a name resolution of your Active Directory domain, you must enter the DNS server (normally your AD server) here. If you are working with WINS, you can also enter the WINS server here. You can now confirm this dialogue with OK.

Create PPTP users

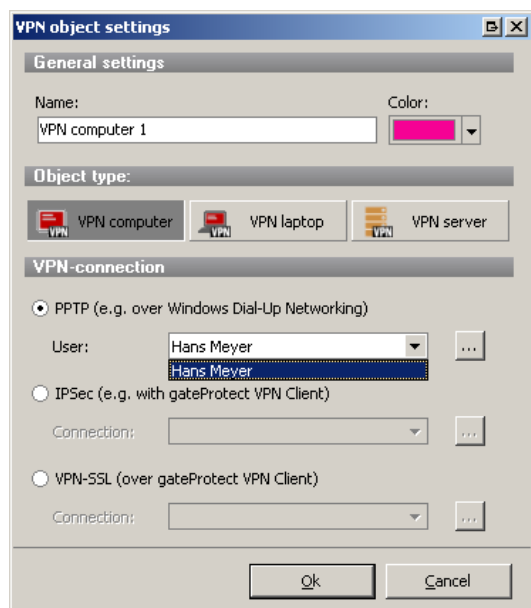
The Firewall is ready to accept PPTP tunnel and to produce the corresponding rules. In the next step you will create PPTP user accounts for dial in by PPTP. Open the user administration.



- Click on *User Administration* in the *Settings* menu.
- Click on *Add* to create a new user.
- Enter a user name and optionally a description. Make sure there are no empty spaces in the user name.
- Select the PPTP tab.
- Tick the *Enable user for PPTP connections* box on the PPTP tab.
- Assign the user an *IP address*, or leave the field blank so that an IP address from the address pool is used.
- Enter a password for the PPTP log-on and click on *OK*.

The set-up of the user account is now complete.

Create a VPN object (PPTP)



- Drag a new VPN computer from the toolbar to the Configuration Desktop.
- Enter a description for the new object in the dialogue box.
- Tick the *PPTP* box and choose a user from the box.

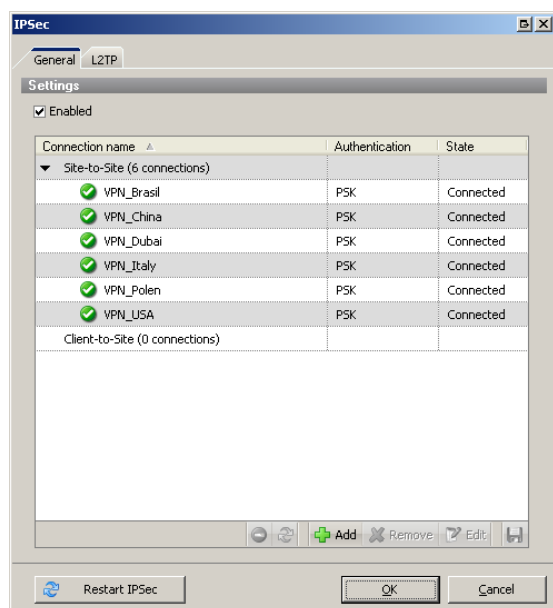
10.3 IPSec connections

It is possible to create an IPSec-VPN connection using the VPN Wizard (*VPN Settings > VPN Wizard*). Because this is self-explanatory, this manual only describes the manual creation of an IPSec connection.

10.3.1 Setting up an IPSec connection manually

IPSec connections / global Settings

This dialogue shows all IPSec connections, separated in server-to-server and client-to-server connections with information about authentication and connection status.



Possible options

Enabled

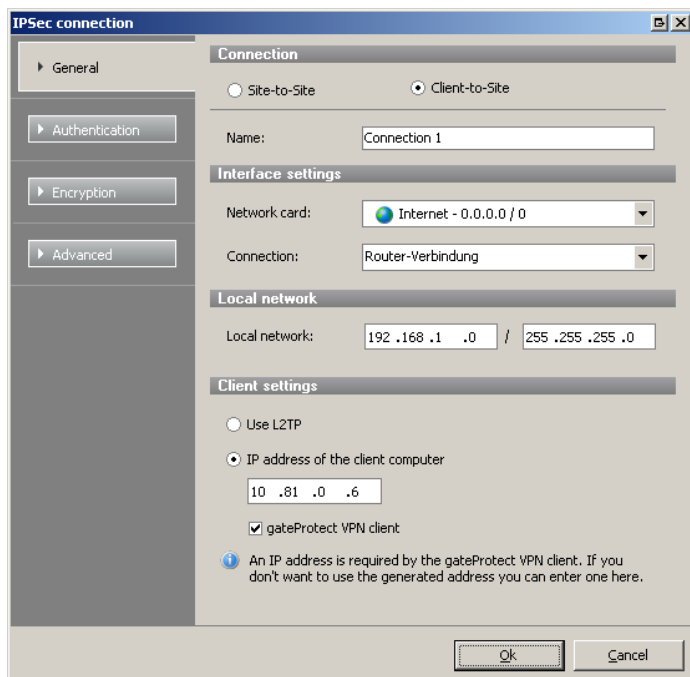
Allows turning IPSec on and off completely.

Restart IPSec

Restarts IPSec, which leads to a restart of all tunnels.

Button list with following actions (from left to right):

- Activate/Deactivate single connections.
- Restart single connections (the tunnel is going to be closed; it will initiate the connection if it is configured to)
- Add, remove, edit and export of the selected IPSec connection.

General – Client-to-Site


The screenshot shows the 'IPsec connection' dialog box with the 'General' tab selected. The 'Client-to-Site' radio button is chosen. The 'Name' field contains 'Connection 1'. Under 'Interface settings', 'Network card' is set to 'Internet - 0.0.0.0 / 0' and 'Connection' is 'Router-Verbindung'. The 'Local network' section shows '192.168.1.0' and '255.255.255.0'. In the 'Client settings' section, 'Use L2TP' is unselected, 'IP address of the client computer' is selected with the value '10.81.0.6', and 'gateProtect VPN client' is checked. A note at the bottom states: 'An IP address is required by the gateProtect VPN client. If you don't want to use the generated address you can enter one here.'

Name

User-defined Name for the connection.

Interface settings

Selection of the interface/internet connection to use for the IPsec tunnel.

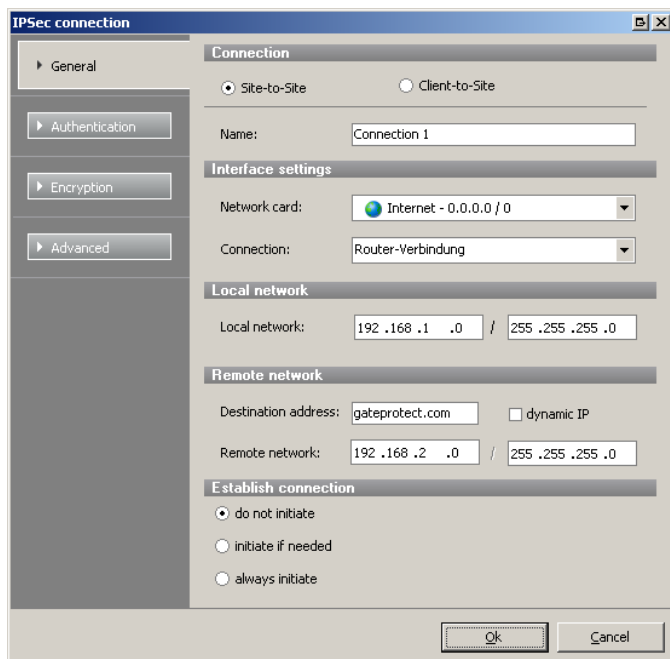
Local network

Local Network, which is accessible through the tunnel.

Client settings

L2TP activates the use of IPsec/L2TP. This way, the local network gets disabled, because the IPsec tunnel is only used to carry out L2TP packets and the actual data is tunneled on L2TP level. If you select this, a confirmation pops up which automatically activates IKEv1, deactivates PFS and sets the port and protocol restrictions to UDP/1701 to keep the compatibility to Windows clients.

Without L2TP, you can enter a virtual source address for the client under *IP address of the client computer*, which is needed for using the gateprotect VPN client.

General – Server-to-Server


Name, *Interface settings* and *local network* comply with the client-to-server settings.

The *Destination address* of the remote IPsec server can be an IP address or a FQDN.

Remote network describes which network is accessible through the tunnel.

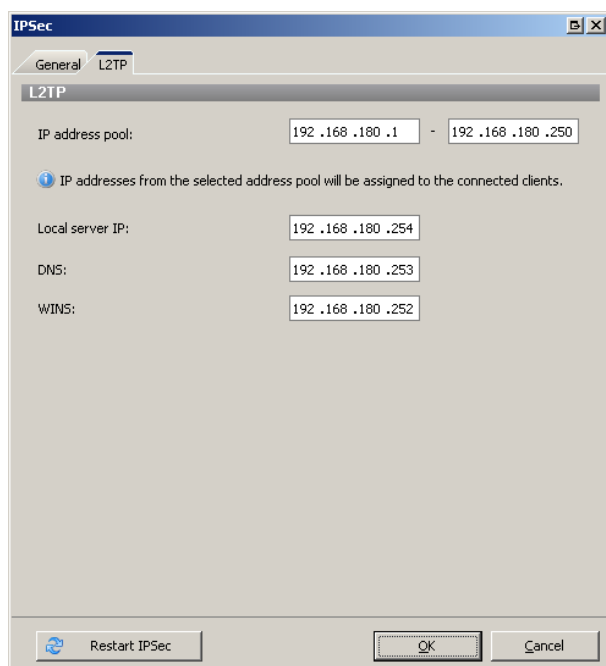
If *dynamic IP* is activated, the connection has to be initiated by the remote server. Using this, the *Destination address* is grayed out and it is not possible to initiate the connection by this server.

Following options are possible while establishing the connection:

- The local firewall should not initiate the connection – the remote server creates the tunnel.
- The local firewall should initiate the connection if needed – a trap in the kernel will be set up. The trap initiates the connection when a packet is to be sent / routed which, according to the network settings, has to be sent through the tunnel.
- The local firewall should always initiate the tunnel if it is currently not running.

10.3.2 L2TP / XAUTH

While IPsec client-to-server connections usually need client software, because few systems support IPsec by default, the L2TP feature assures the interoperability of miscellaneous systems (like Windows) without the client software. Using L2TP, you can just create a network connection. It is important that only PAP can be used to authenticate on PPP level, which eventually has to be activated in the client. PAP is often considered as unsecure because the password is sent in plaintext. In this case it is secure because the PPP connection gets established after the IPsec tunnel is created, which secures all PPP traffic.

Global L2TP settings

IP address pool

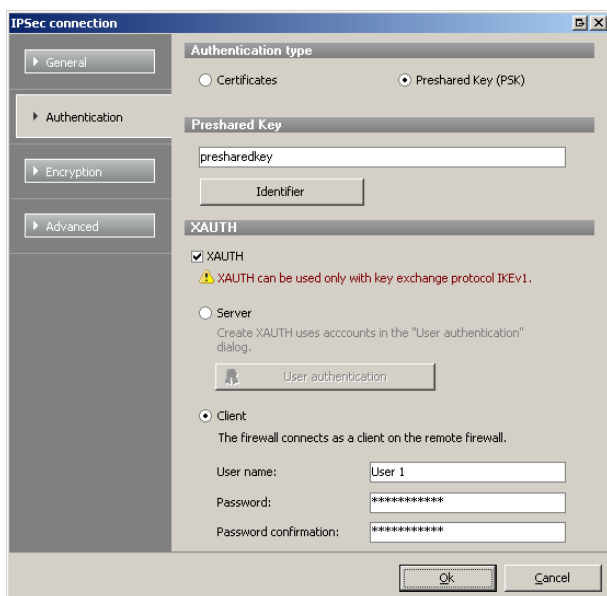
The IP address pool is an IP range from which the client gets his IP. This has to be set in order to use L2TP.

Local server IP

Address, which is used by the firewall as PPP address to communicate with the clients. This also has to be set in order to use L2TP

Optional DNS server address, which is told to the client while initiating the connection.

Optional WINS server address, which is told to the client while initiating the connection.

Authentication – PSK


Via *Identifier* you are able to define custom identifier, which were used instead of the IP address.

Here you have the choice to activate XAUTH (only with IKEv1):

With *XAUTH*, the firewall can be the server or the client part. If the firewall acts as server, you don't have to set up anything else here. This takes part in the user management. (See *chapter 5.3 – Users*).

Acting as client, you have to enter *Username* and *Password* in order to authenticate on the remote server.

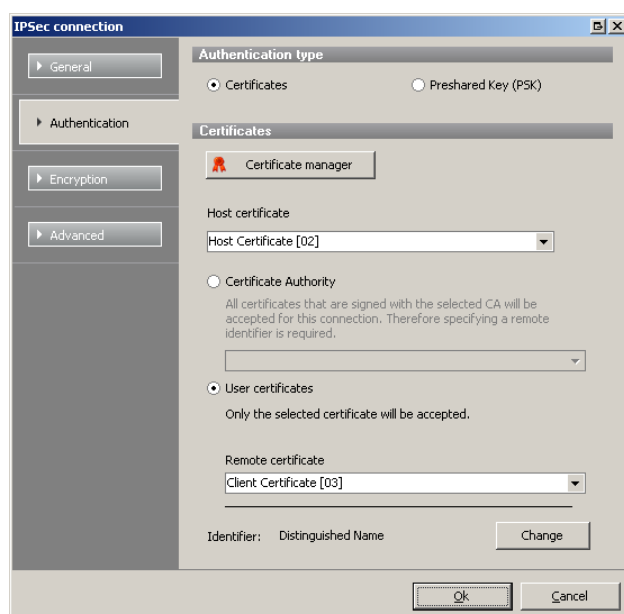
10.3.2.1 Rules

The rules, which define what services are accessible through a tunnel, were usually set up via VPN objects (VPN groups for server-to-server connections, VPN computer for client-to-server connections). Two exceptions are L2TP and XAUTH tunnel. VPN users and VPN groups were created to handle these types of objects.

Using the additional user data (username/password of XAUTH or PAP login of L2TP) the validation against the user authentication takes place. If this is successful, the rules of the configuration desktop will be applied to the specified users.

It is not important, which tunnel the user is using. Login is possible on every tunnel which has activated the corresponding authentication mechanism. You can deny the use of specified tunnels to specified users with the preceding ISAKMP authentication.

Authentication – Certificates



The own certificate has to be defined to authenticate against the remote client. For this certificate, the private key has to be available.

You can choose between a certificate authority and a single certificate for the remote client:

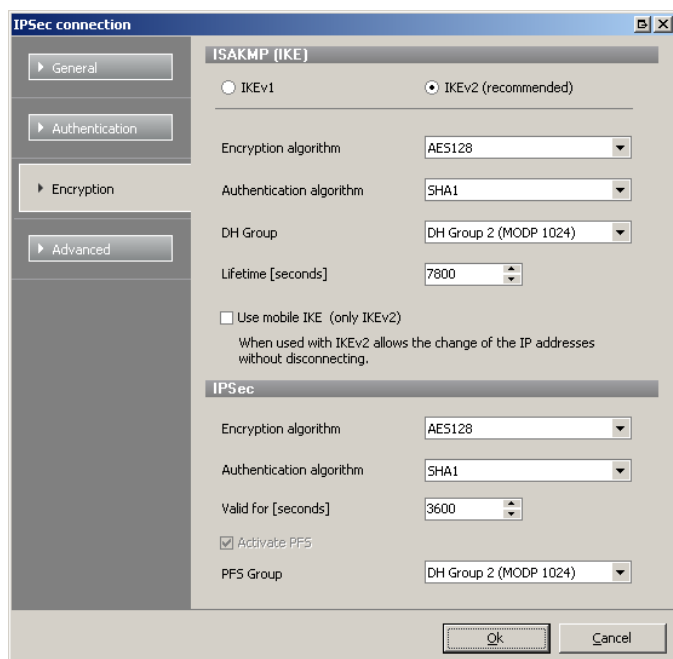
If you choose the CA, you need its public key. Now every certificate (which is signed by this CA) is accepted for this connection. In this case, there is no need to import a certificate for every remote client.

You can directly select a certificate as remote certificate. The remote client has to own the private key on initiation to authenticate.

It is possible to select the identifiers

Following options are available:

- You can use the *Distinguished Name* of the certificates, which is the usual way to connect gateprotect firewalls of version 8.1 and higher.
- *Subject Alternate Name* is the usual way, gateprotect firewalls before version 9.0 used to authenticate. If you want to connect to one of them, you have to use this option.
- *Userdefined Identifier* are possible. While it should be noted that the identifier entered here must be covered by the Distinguished Name or a Subject Alternate Name of the certificates so that a tunnel is possible, it may be useful for various reasons to edit it by hand. Besides the possibility to enter values, which were expected by third-party products as a peer, you can use wildcards. For example, you can choose a CA authentication but limit the peer by a remote identifier to all members of an OU (Organization Unit).

Encryption


You can choose between *IKEv1* (Internet Key Exchange) and its successor *IKEv2*. IKEv2 is faster while initiating the tunnel and rekeying. IKEv1 is kept for compatibility reasons; XAUTH is only possible with this version.

You can specify *encryption* and *authentication algorithms* as well as *DH groups* for IKE.

Also, you can specify the *Lifetime* of the ISAKMP-SA. This doesn't affect the rekeying directly. To prevent all tunnels from rekeying at the same time (which would lead to heavy system load), the actual moment is randomly chosen.

If IKEv2 is chosen, *Mobile IKE* can be activated. This allows changing the IP address on one side without abortion of the tunnel.

You can specify *encryption* and *authentication* algorithms for quick mode (for IPsec-SA negotiation) also.

A *Lifetime* for IPsec-SA also can be specified. As with ISAKMP-SA, the actual moment for rekeying is randomly chosen.

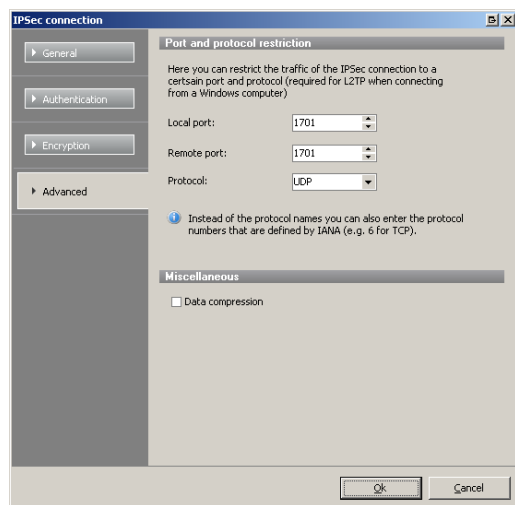
If you choose IKEv1, *PFS* (Perfect Forward Secrecy) can be activated. This feature enhances the security but has to be deactivated if the remote client doesn't support it (like Windows XP). Using IKEv2, PFS is always activated.

If PFS is activated, a Diffie-Helman group can be defined for PFS via *PFS Group*.

The following list shows all supported encryption and authentication algorithms as well as all DH groups:

| Encryption algorithms | Authentication algorithms | DH groups |
|-----------------------|---------------------------|-------------------------|
| AES 128 | SHA 1 | DH Group 1 (modp 768) |
| AES 196 | SHA 256 | DH Group 2 (modp 1024) |
| AES 256 | SHA 368 | DH Group 5 (modp 1536) |
| 3DES | SHA 512 | DH Group 14 (modp 2048) |
| Blowfish 128 | MD5 | DH Group 15 (modp 3072) |
| Blowfish 192 | | DH Group 16 (modp 4096) |
| Blowfish 256 | | DH Group 17 (modp 6144) |
| | | DH Group 18 (modp 8192) |

Advanced settings



Here you can specify *Port* and *Protocol* which IPsec has to use. This is useful, if you only want specific packets to be sent through the tunnel. To use L2TP, you have to select UDP and port 1701.

You can choose one of the predefined *Protocols* or type in one of the protocol numbers that are defined by IANA.

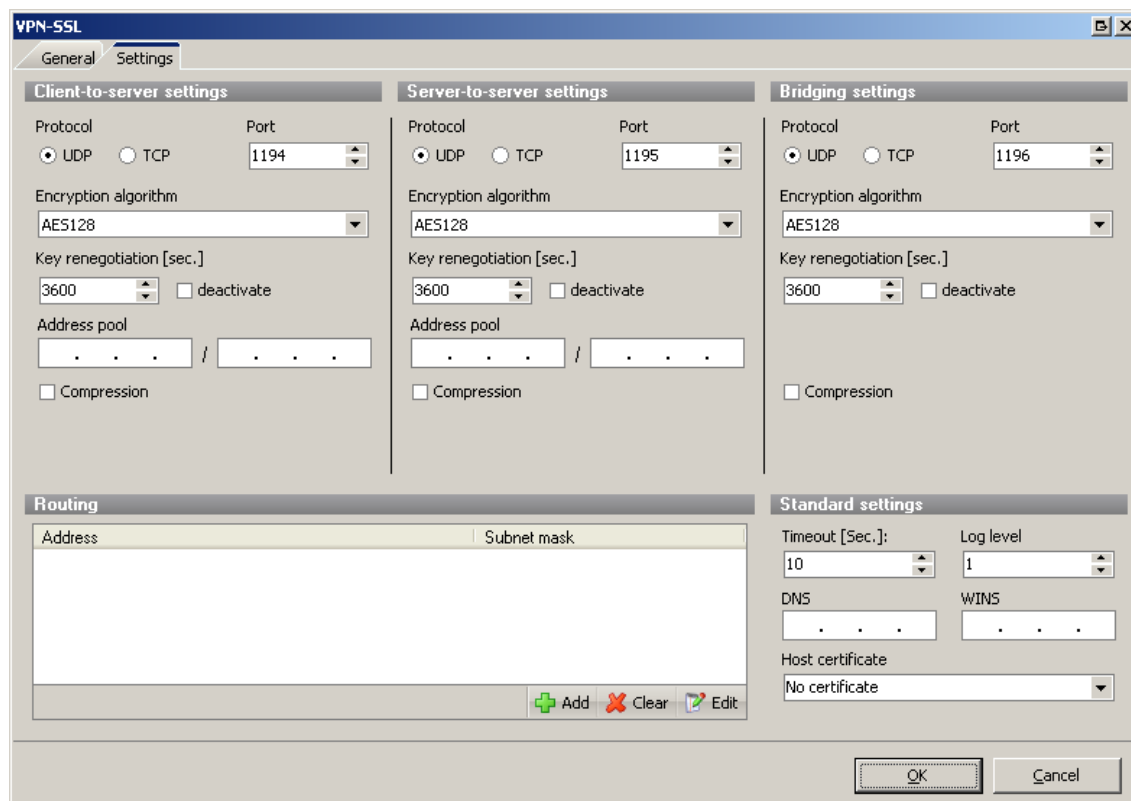
At last you can activate *Data compression* which uses IPComp.

10.4 VPN over SSL

It is possible to create a VPN over SSL connection using the VPN Wizard (*VPN Settings* > *VPN Wizard*). Because this is self-explanatory, this manual only describes the manual creation of a VPN over SSL connection.

VPN over SSL offers the possibility to create client-to-server connections, server-to-server connections and SSL bridges. This connection is always certificate based and depends on working certificate management.

You can set up general settings for *client-to-server* connections, *server-to-server* connections with *routing* and server-to-server connections with *bridging* via the *Settings* tab.



As with IPsec, the *encryption algorithm* can be chosen as well as *protocol* and *port* on which the firewall listens for incoming connections.

! PLEASE NOTE THAT ONLY THE TCP PROTOCOL WORKS RELIABLE IF YOU HAVE MORE THAN ONE INTERNET CONNECTION WITH LOAD BALANCING.

Similar to IPsec, a VPN over SSL connection also renews the session key while the connection is established to increase security. These intervals are freely configurable for each connection type.

In the *Routing* section of the dialogue, you can specify routes for the first two connection types which were added to the remote clients/firewalls routing table. These routes apply for all connections. It is also possible to enter routes separately for each connection.

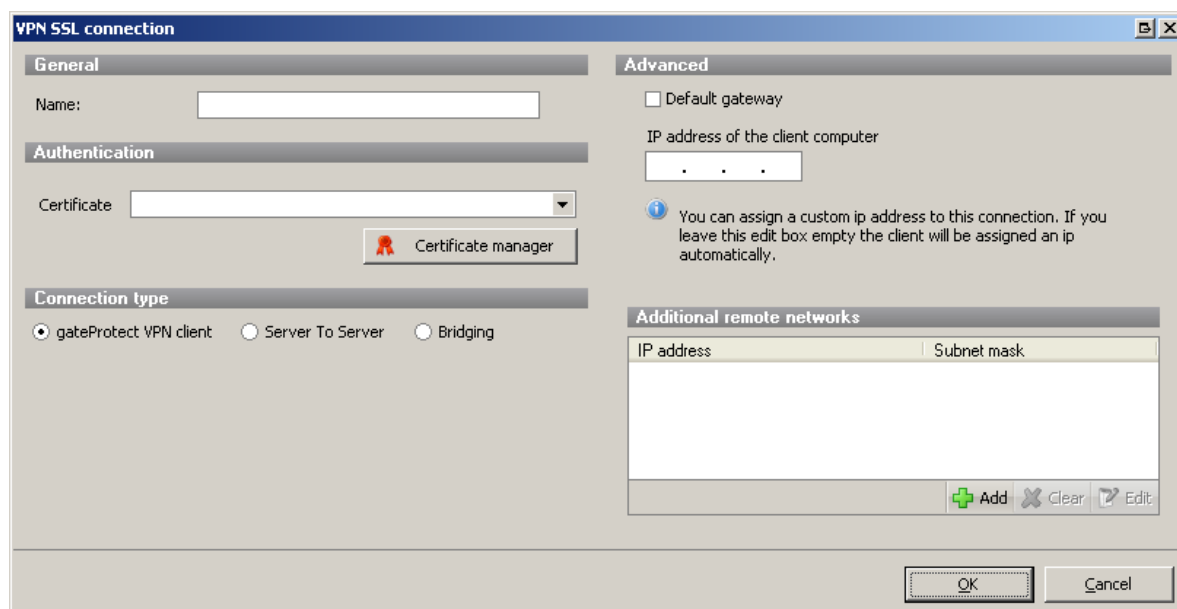
The *Timeout* option defines after what idle time the connection gets closed. 0 means it will never be closed.

If clients should use defined *DNS* and/or *WINS server*, you can enter them here.

The *Log level* defines how detailed the messages in the reporting should be.

It is also possible to select a Host certificate for VPN over SSL connections. Unlike IPsec, this is not for just one connection; it is for the whole service.

To create a connection for the gateprotect VPN Client, you have to choose the connection type *gateprotect VPN Client* in the add *VPN over SSL connection* dialogue.



The *Name* of the connection is arbitrary. The certificate has to be a certificate for the client which you created before. If you didn't create one, you can do this now using the *Certificate manager* button.

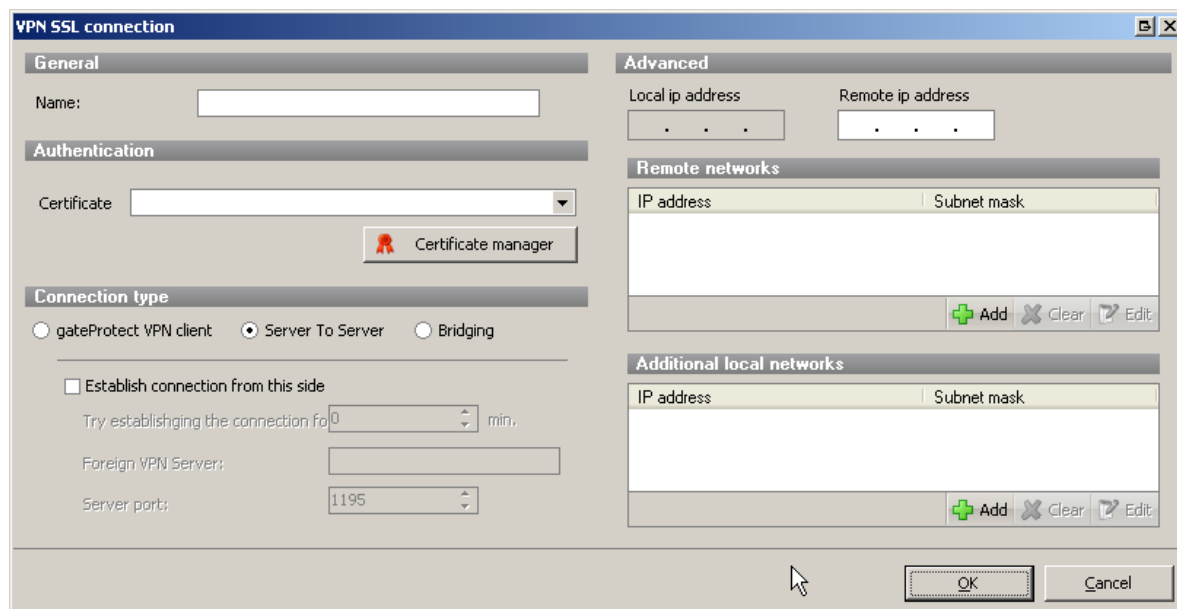
In the *Additional remote networks* field, you can specify (additional to the general routes) routes for this connection as mentioned before. The IP address of the client computer can but doesn't have to be given.

The option *Default gateway* defines, whether the VPN client should use the tunnel as default gateway or not. If this option is not ticked, concrete routes have to be sent to the client.

If the connection type *server-to-server* is chosen, you can specify *Additional local networks* which were handled like *Additional remote networks* before. This means that the remote firewall adds routes for these networks.

Networks, which are available via the remote firewall, have to be entered in *Remote networks*.

If the connection should be initiated by this firewall, you have to enter a *DNS name* or an *IP address* in the *Foreign VPN Server* field as well as the *Server port*. *Try establishing the connection for* defines how long the firewall should try to connect to the remote server. 0 means that the firewall will try it forever.



If you choose the connection type *Bridging*, you are able to assign the connection to an existing bridge or to a new one.

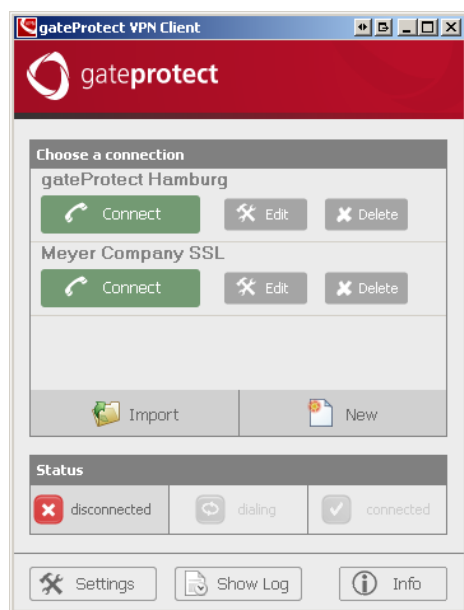
10.5 VPN over SSL without default gateway

Using VPN over SSL it is possible to force the client to use the VPN tunnel as default gateway. This option enhances security and should therefore be used in most cases because malware on the client isn't able to send data through the additional available internet connection anymore.

If you don't want to use this option (e.g. for a support co-worker), following steps are required:

- Disable the *Default gateway* option in the gateprotect Administration client using *VPN Settings > VPN SSL* and the appropriate connection.
- If the gateprotect VPN Client now connects to the firewall, no additional routes were added to the client's routing table. This also means that the client computer doesn't know the way to the company's network. Because of that you have to assure that you have set up routes via *Additional remote networks* or in the general VPN over SSL settings.

10.6 The gateprotect VPN Client



The gateprotect VPN Client offers an easy and secure method to create VPN tunnels via VPN over SSL or IPSec.

If you have created a VPN connection on the gateprotect firewall server using the VPN client-to-server wizard (with VPN over SSL or IPSec), you should be able to save a VPN configuration file on your hard disk or on a removable device.

If you installed the gateprotect VPN Client before, double-clicking on the configuration file automatically adds the connection to the client. After prompting for the password, the VPN tunnel gets established. When you remove the device on which the configuration file, the client disconnects automatically.

10.6.1 Automatic creation of a VPN connection using a configuration file

The easiest way to create a VPN connection is using a configuration file. While setting up a VPN connection on the firewall server using the VPN Wizard, you are able to save the connection in a password protected configuration file.

Step 1

Transfer the configuration file via E-Mail or via a removable device to the client.

Step 2

Open this file via double-clicking on it.

This starts the associated gateprotect VPN Client.

Step 3

Enter the password for the configuration file.

Step 4

The VPN connection gets established and the configuration is done.

Optionally it is possible to import the configuration file into the gateprotect VPN Client using the *Import* button.

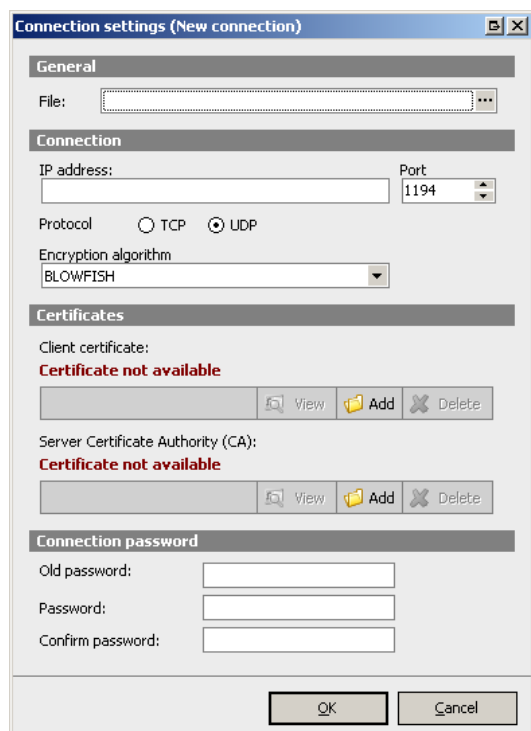
10.6.2 Manual creation or edit a VPN connection

To manually create a VPN connection on the gateprotect VPN Client, you need the client certificate and the public key of the server's Certificate Authority (Root-CA). These files can be created and exported using the firewall's Certificate management. Please export the client certificate using the PKCS#12 format.

- To create a connection, click the *New* button in the main window of the gateprotect VPN Client and choose between *SSL connection* and *IPSec connection*.
- To edit an existing connection, click on the *Edit* button next to the connection's name. After you entered its password, the settings dialogue opens.

 PLEASE NOTE THAT ALL MODIFICATIONS WERE DIRECTLY SAVED IN THE CONFIGURATION FILE (.GPCS).

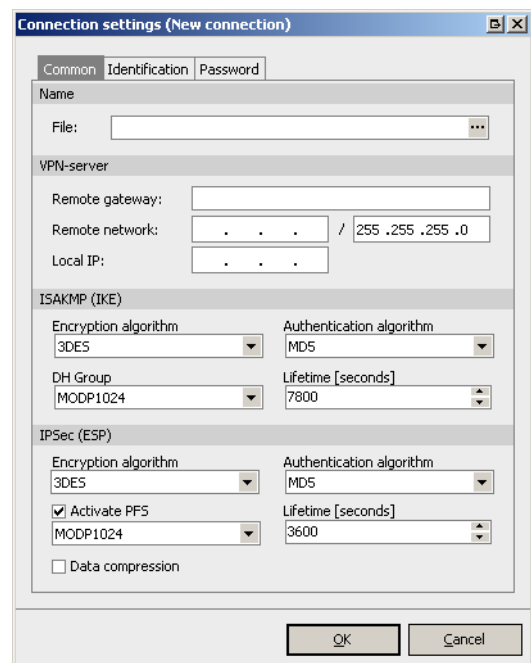
10.6.2.1 Settings of a VPN over SSL connection



- *File* is the .gpcs-file (gateprotect Connection Settings), where all connection settings get saved to.
- The hostname / IP address of the VPN server has to be entered into the *IP address* field.
- *Port*, *Protocol* and *Encryption* algorithm have to match the settings on the VPN server.
- Add the exported certificates to the connection.
- You may add a password to the connection file or change it. If you add a new connection, leave the *Old password* field empty.

10.6.2.2 Settings of a IPSec connection

Tab *Common*



- *File* is the .gpcs-file (gateprotect Connection Settings), where all connection settings get saved to.
- The hostname / IP address of the IPSec server has to be entered into the *Remote gateway* field.
- *Remote network* and *Local IP* have to match the routing configuration of the IPSec server.
- The settings belonging to IKE (Internet Key Exchange) and IPSec have also to match the settings of the IPSec server.

Tab *Identification*

- You can use a *Preshared Key* (PSK) to secure the connection but we recommend using certificates because of some restrictions and better authentication methods.
- In the *Certificates* section, you can add the exported certificates to the connection.
- Some remote clients need (mostly in conjunction with PSK authentication) a *Local identifier*.

Tab *Password*

- Optionally, you can add a password to the connection file or edit it.
- If you create a new connection, leave the *Old password* field empty.

11 HIGH AVAILABILITY

11.1 Functionality

High Availability (HA) is used for providing the services of the firewall within the shortest time without manual intervention in case of a hardware failure.

The technique consists of a primary and a secondary firewall connected in a cluster monitoring each other and synchronizing the configurations and statuses. If the primary firewall malfunctions, the secondary firewall takes over the tasks; this is called failover. If the secondary firewall fails, a warning will be printed in the report of the primary firewall.

In case of a fail-over the secondary firewall becomes the new primary. The new primary firewall takes over the whole configuration, including IP and MAC addresses of the failed firewall.

After repairing it, the firewall can be reconnected to the HA-Cluster. For this procedure special mechanisms ensure the new integrated firewall gets the secondary IP and MAC addresses and only one firewall is labelled primary at all times. This eliminates the risk of an IP address conflict.

It is recommended to use dedicated network interfaces, because the monitoring and synchronization causes high data traffic. Additionally the use of cross-cables is recommended, because the data is not encrypted.

If you use only one dedicated link for monitoring and synchronization and this one fails for some kind of reason, the firewalls are unable to monitor the other one. As a result, both firewalls would think the other one failed. In this situation both firewalls would switch into primary mode. To avoid such a scenario it is recommended to use two dedicated links.

11.2 Downtime while failover

Downtimes of direct data connections depend on your type of internet connection and whether or not they go through a proxy.

The current version has the following specifications:

- Direct data connections via router connection are halted for a maximum of 4 seconds. Indirect connections (which go through a proxy) are completely disconnected but can be re-established after a maximum of 4 seconds.
- Data connections via dial-up connection are completely disconnected but can be re-established after a maximum amount of 10 seconds.

11.3 Configuration

General

- To set up High Availability, you need two identical gateprotect firewall servers with different IP addresses. It is important that they have the same number of network interfaces.
- Both firewalls need the same licensing.
- The primary and secondary firewall need to have the same host name.

11.3.1 IP addresses of the network interfaces

As mentioned before, you should use at least two (maximum four) dedicated links for monitoring and synchronization. The firewalls are shipped with identically configured network interfaces and they need to be reconfigured.

- IP addresses on the primary and secondary have to be different. The primary firewall has to have the first IP address of the used network (e.g. 192.168.0.1) and the secondary IP address has to be the second of the used network (e.g. 192.168.0.2).
- IP addresses of the dedicated network interfaces have to be in the same subnet.
- IP addresses of the primary firewalls network interface which is connected to the local network has to be identical with the configured gateway address of all hosts.

11.3.2 Connecting the firewalls via dedicated links

Network interfaces for the same dedicated link have to be named identically. For example if you want to use eth3 and eth4 on the primary firewall, you have to connect them to the same network interfaces on the secondary firewall. It is recommended to use crossover cables for the dedicated links.

11.3.3 Activating the High Availability

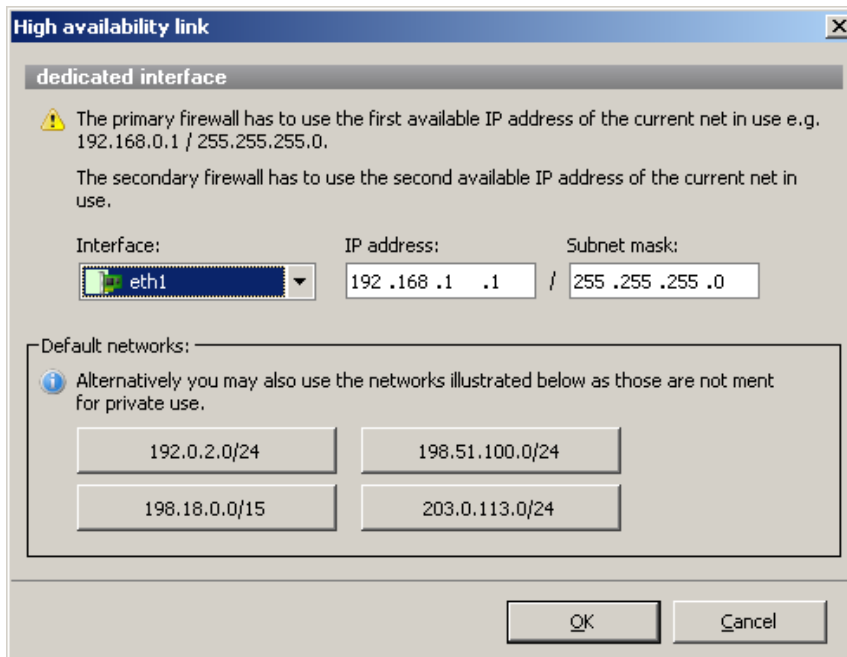
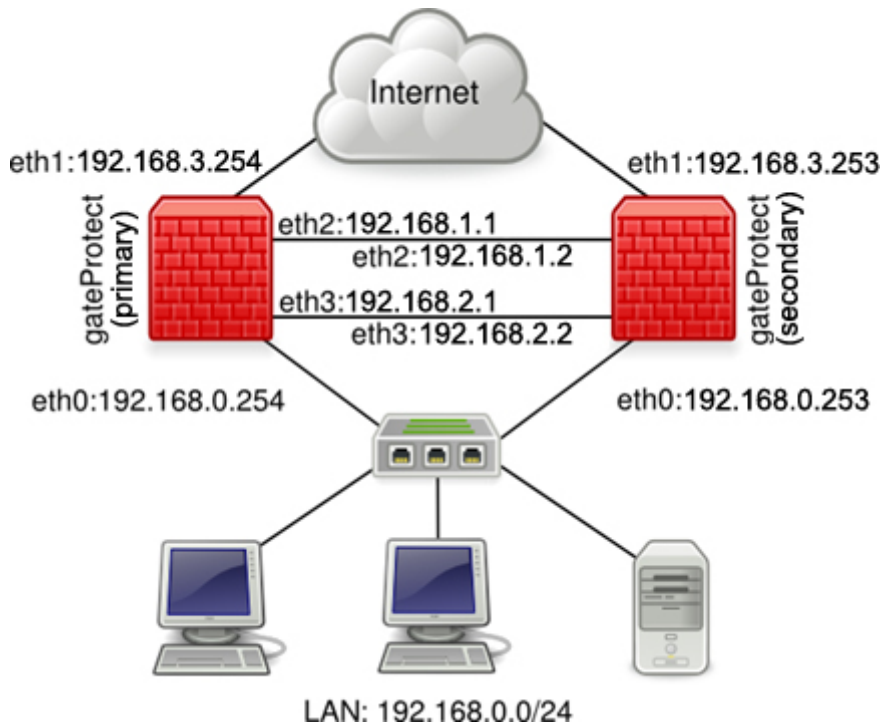
Connect to the primary firewall using the Administration Client. Open up the High Availability menu via *Options > High Availability*. Now tick the *Active* box and choose the Primary role for the firewall. Choose the network interfaces for monitoring and synchronization. You can define whether statistic data should be synchronized or not. Confirm your settings with OK. Now, connect to the secondary firewall and configure it similar to the primary firewall. About 60 seconds after both firewalls were configured, High Availability is in operational mode.



NOTE

IF THE FIREWALLS ARE IN OPERATIONAL MODE, A MESSAGE APPEARS IN THE REPORT. IF THE FIREWALLS REACH THIS MODE, IT IS RECOMMENDED TO CREATE A BACKUP OF THE PRIMARY FIREWALL. IF ONE FIREWALL FAILS, YOU NEED THE BACKUP TO GET THE FAILED FIREWALL OPERATIONAL. PLEASE CONSIDER THAT YOU CANNOT CONNECT TO THE SECONDARY FIREWALL USING THE ADMINISTRATION CLIENT.

Following illustrations show an example configuration and the High Availability dialogue.



11.4 Edit the settings of High Availability

While the firewalls are in operational mode, you can edit the settings for High Availability. To do this, connect to the primary firewall using the Administration Client. Open up the High Availability dialogue via *Options > High Availability*. In this dialogue, you can choose whether or not statistic data should be synchronized. Affirm your settings with *OK*.

NOTE
CHANGES IN THE SETTINGS WILL CAUSE A RESTART OF HIGH AVAILABILITY ON BOTH FIREWALLS.

11.5 Deactivating High Availability

If the operational mode is already established, connect to the primary firewall using the Administration Client. Open up the dialogue *High Availability* in the *Options* menu. Now deactivate the *Active* box. HA automatically gets deactivated on the secondary Firewall. If the operational mode isn't established, connect to each firewall using the Administration Client and deactivate High Availability.

11.6 Role change

The takeover of the primary firewall's tasks is called a role change. This happens automatically if the primary firewall fails. It is also possible to change roles while the firewalls are in operational mode. To do this, connect to the primary firewall using the Administration Client and open up the High Availability dialogue. Now, click on the Role Change button.

WARNING:
WHEN APPLYING TWO AND MORE HA LINKS THE FIRST HA LINK IS USED FOR THE DATA SYNCHRONIZATION. WHILE SWITCHING THE ROLES (MANUALLY OR AUTOMATICALLY) THIS LINK HAS TO BE ACTIVE, SINCE THIS ASSURES THAT THE CONFIGURATION ON THE SECONDARY IS UP TO DATE.
PLEASE CHECK THE REPORT OF THE ADMINISTRATION CLIENT THAT THE LINK WAS NOT DISCONNECTED FOR AT LEAST 5 MINUTES BEFORE SWITCHING THE ROLES.

NOTE
ROLE CHANGE CANNOT TAKE PLACE BEFORE HIGH AVAILABILITY IS IN OPERATIONAL MODE. AS WITH FAILOVER, THE ROLE CHANGE LEADS TO A DISRUPTION OF RUNNING SERVICES.

11.7 Commissioning a firewall after the failure

If one of the two firewalls fails so that the firewall software does not have to be reinstalled after the repair, no special actions are required after rebooting: The firewall automatically determines its HA role as well as its MAC and IP addresses. If the failure of a firewall and its repair are combined with reinstallation of the firewall software, you have to set up High Availability in following way: Put the firewall into a separate network and install the firewall software with the backup of the primary firewall. Finally, put the firewall back into the High Availability cluster and reboot it. The firewall then determines its HA role as well as its MAC and IP addresses automatically.

NOTE
BEFORE BOOTING THE REPAIRED FIREWALL IN THE CLUSTER MAKE SURE THE DEDICATED NETWORK INTERFACES ARE CONNECTED TO THE PRIMARY FIREWALL IN THE SAME WAY AS BEFORE THE FAILURE.

11.8 Restoring backup or performing a software Update

Connect to the primary firewall using the Administration Client. Open the High Availability dialogue via the Options menu. Now deactivate High Availability, this makes the secondary firewall accessible via Administration Client.

Restore the backup or apply a software update on both firewalls and dismiss the questions for rebooting. Now reactivate High Availability on both firewalls. After the operational mode is reached, perform two role changes: Trigger a role change on the primary firewall, now the secondary firewall becomes the new primary firewall. After HA reached operational mode, trigger the second role change on the new primary firewall. Some updates require a reboot of the firewalls. If a reboot is necessary is displayed in the patch description in the update menu.

NOTE
THIS DOUBLE ROLE CHANGE ENSURES THAT THE BACKUP OR SOFTWARE UPDATES WERE APPLIED CORRECTLY.

11.9 Report messages

The workflow of High Availability is documented in the report. Normally, following messages appear in the report after activating HA:

- High availability started, this firewall is primary
- High availability started, this firewall is secondary
- High availability entered discovery state
- High availability entered handshake state
- High availability entered heartbeat state
- High availability is operational

Following messages may appear in the report after activating HA if an error occurs:

- High availability started, this firewall is primary
- High availability started, this firewall is secondary
- High availability entered discovery state
- High availability terminates, because roles primary/secondary set incorrectly
- High availability terminates, because dedicated links configured incorrectly
- High availability terminates, because not all heartbeat connections could be established

Following messages may appear in operational mode:

- High availability detected dedicated link eth3 has failed
- High availability detected dedicated link eth3 is operational again
- High availability detected all dedicated links have failed
- High availability detected primary firewall failed, making failover
- High availability detected secondary firewall failed, restarting with old settings
- High availability detected harddisk failure on peer firewall

Following messages appear, if an administrator edits settings on High Availability in its dialogue:

- High availability is not ready to change settings, try again later
- High availability restarts with new settings
- High availability temporarily unable to change roles, try again later
- High availability reboots this firewall to change roles, as ordered by admin
- High availability terminates, as ordered by admin

12 INTRUSION DETECTION AND PREVENTION SYSTEM (IDS/IPS)

The Intrusion Detection System (IDS) and the Intrusion Prevention System (IPS) are systems to recognize and prevent attacks.

They are based on the open source Intrusion-Detection-System Snort that analyses and monitors data communication with the Internet in both directions using predefined rule groups, which can recognize typical attacks.

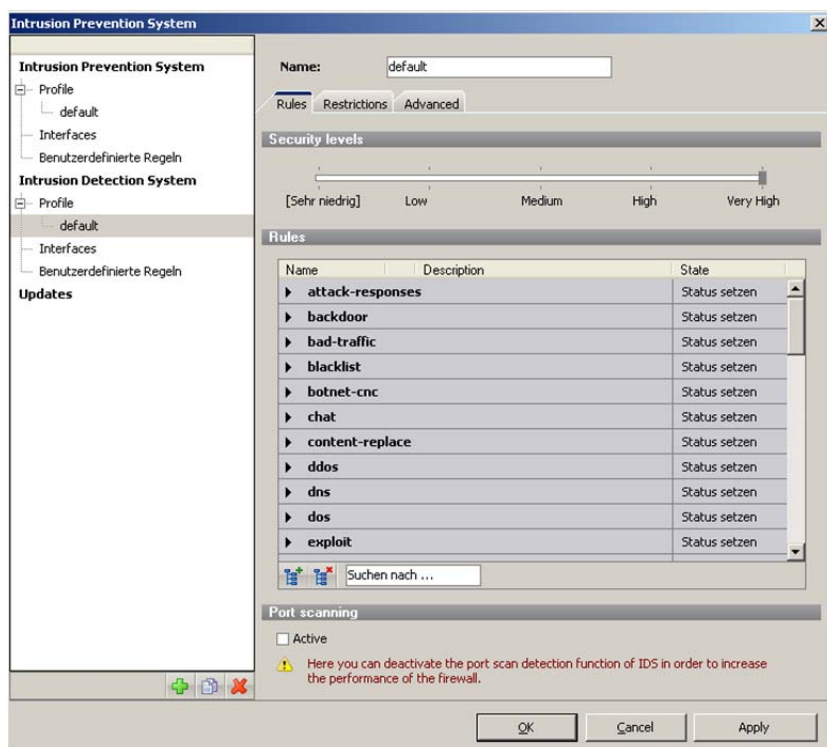
Each of the rule groups contain several individual rules (signatures), which correspond to typical attack patterns, e.g. a trojan, worm or other attack. These signatures are constantly changing and should be updated manually or automatically over the Internet.

To be able to perform the analyses of attack patterns in the shortest time and without delays, the system requires a lot of performance and there is a very heavy load on the system resources. You can save system resources through the number of rules and the number of computer systems to be monitored and, if necessary the amount of IDS/IPS reports or notifications.

12.1 Configuring IDS/IPS Profiles

You can reach the IDS/IPS configuration dialogue box by selecting *IDS/IPS* from the main *Security* menu.

To configure the IDS/IPS the gateprotect Firewall uses profiles. Every profile is customizable and can be assigned to a network interface. The rules of a profile can be set to different states. The IPS offers 5 different states, DISABLE, LOG, DROP, DROP_LOG and REJECT to configure rules individually, the IDS has 2 different states, LOG and DISABLE. The states define how traffic that matches the rules is dealt with.



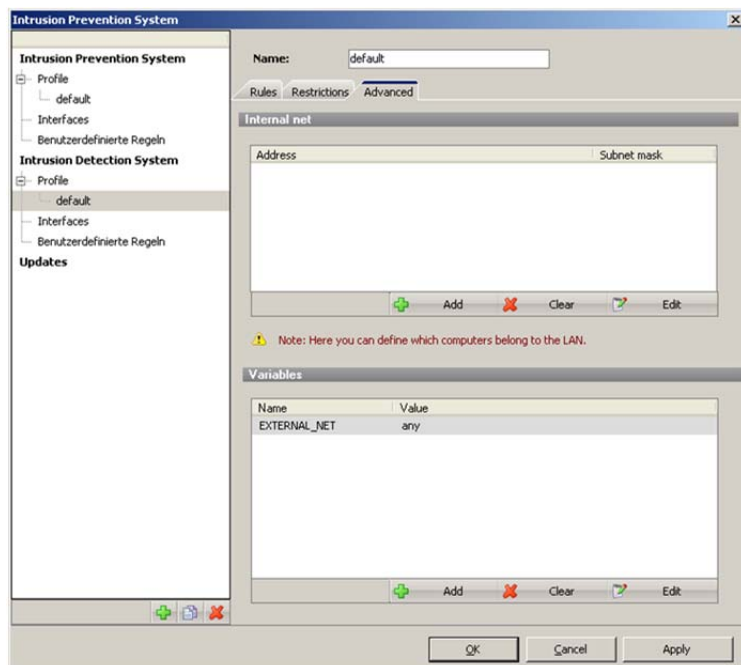
The IDS configuration also contains a slider that can be used to decrease and increase the amount of rules easily.

Port Scanning

Here you can deactivate the port scan detection of IDS in order to increase the performance of the firewall.

12.2 Configuring IDS/IPS Internal/External Network

The IDS/IPS only produces alarm reports if attacks are performed on IP addresses of a defined computer group. A computer group can consist of individual computers or whole networks, that are located in the protected area of the network.

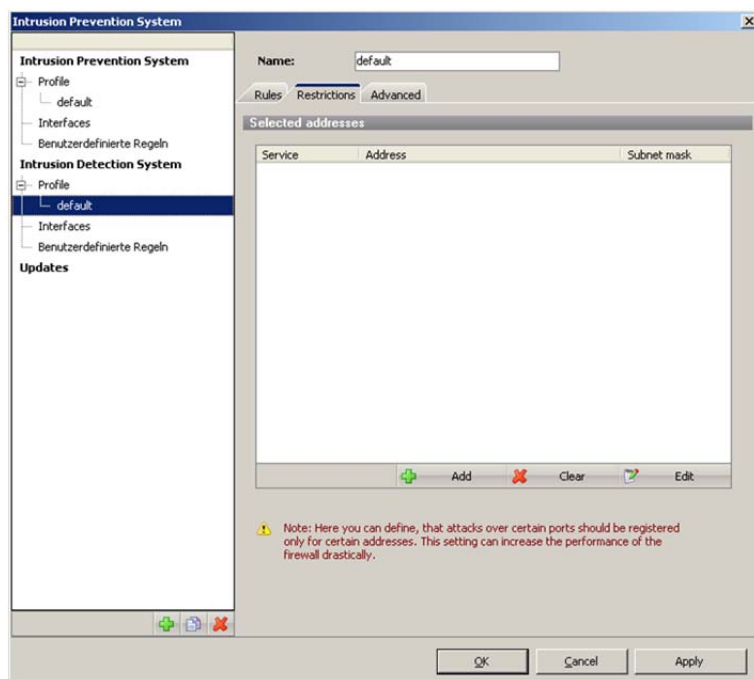


You can add or delete individual computers or local networks of the internal network to a computer group, or edit the computer groups using this dialogue box. The **Add** button opens an entry dialogue.

You can use this to add an IP address of a computer or a sub network with associated subnet mask to the list.

12.3 Configuring IDS/IPS Restrictions

The Intrusion Detection System should monitor special computer systems or networks, e.g. a web server, a mail server or a DMZ in particular. You can enter the services and IP addresses for this type of computer system or network in the **Restrictions** configuration window.



Selected addresses

Use the **Add**, **Delete** and **Edit** buttons to manage the services, which should only be monitored for certain computers.

Pressing the **Add** button opens the **Address** dialogue box and you can enter the service, the address and the subnet mask of a new entry.

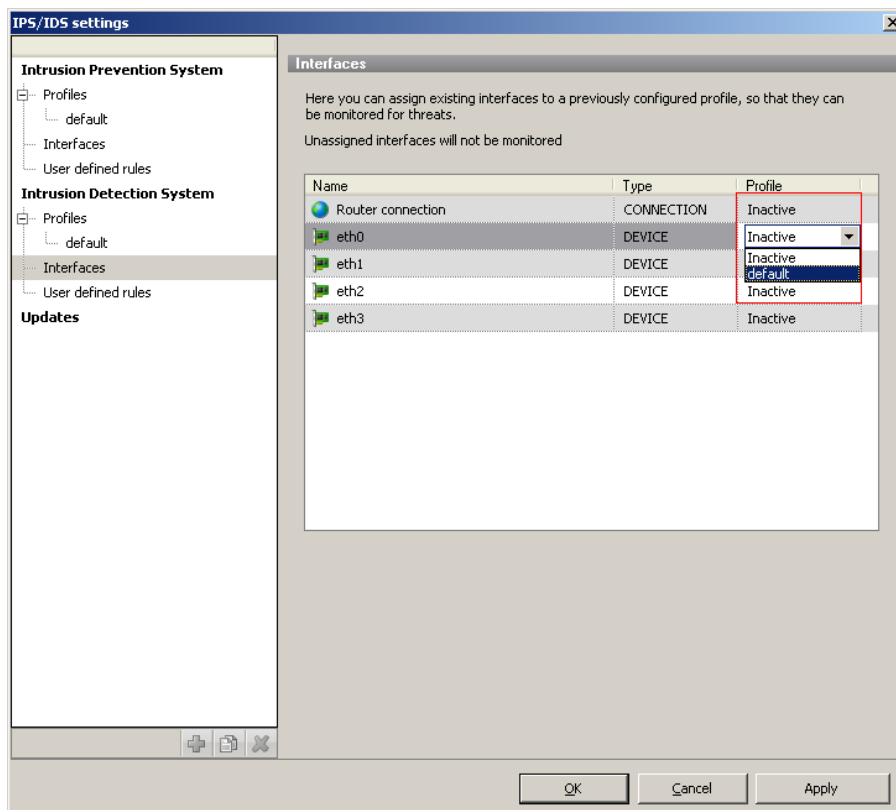
Expanded settings for services

If a service does not run on the standard port the IDS/IPS system can apply the rules to custom ports.

12.4 Activating the Intrusion Detection and Prevention System

You can reach the *IDS/IPS* configuration dialogue box by selecting *IDS/IPS* from the main *Security* menu.

To activate a chosen profile assign it to an interface.



12.5 The IDS and IPS rules can be extended with custom rules.

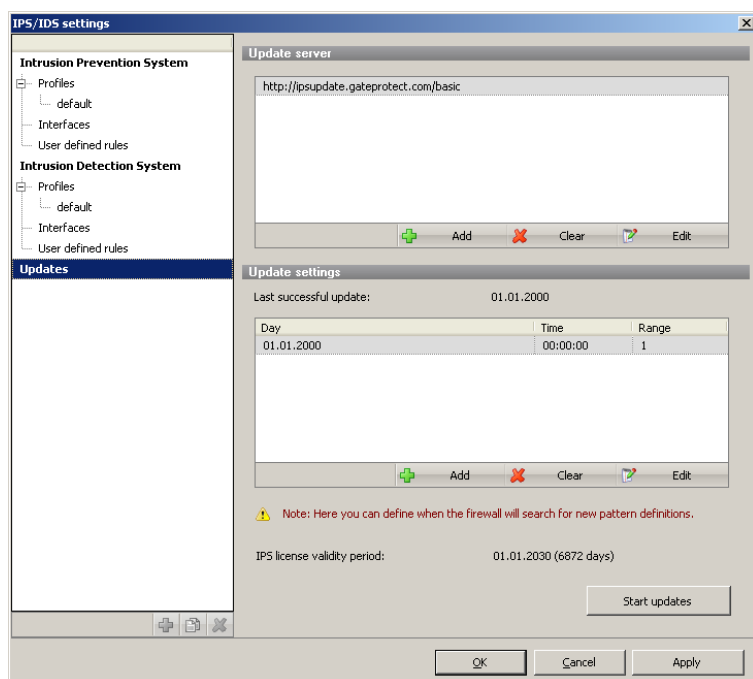
This feature should only be used by administrators who have a deep understanding of Snort based Intrusion Detection/Prevention Systems. Custom rules can potentially block all traffic and render the network infrastructure unusable.

12.6 Updating IDS/IPS Patterns

As the attack methods continually change, e.g. by exploiting new security loopholes, the signatures of the Intrusion Detection System and Prevention System must also be regularly updated to recognize such attacks. You will find the settings for these updates in the *IDS/IPS* configuration dialogue in the *Updates* window. By changing the update path to <http://ipsupdate.gateprotect.com/full> it is possible to switch from the basic set of rules to the full set of rules.



RECOMMENDED FOR EXPERTS ONLY



Manual updates

Click on the *Manual update* button to update the signatures of the IDS/IPS immediately. The Firewall Server connects to a signature server on the Internet and loads the current signatures from there.

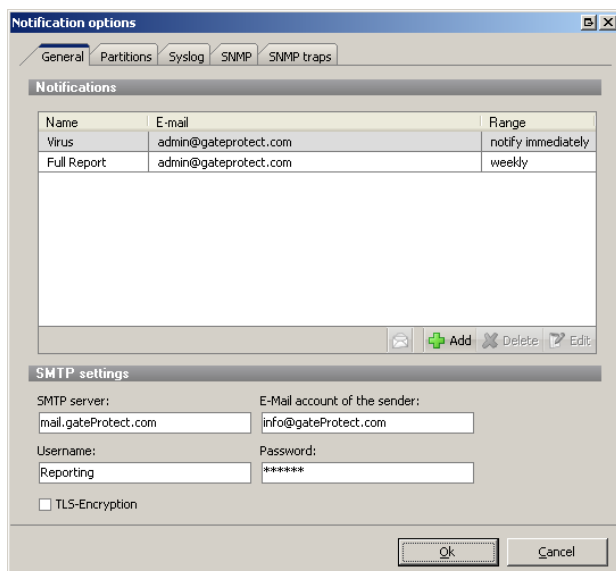
Automatic updates

You can specify a list of regular updates in the *Automatic Updates* section. Open the *Update Settings* dialogue box using the *Add* button. You can set date, time and intervals of the automatic update here.

13 REPORTING

13.1 General

You can have mails sent to yourself with log file extracts under *Settings* > Reporting Settings.



| Name | E-mail | Range |
|-------------|-----------------------|--------------------|
| Virus | admin@gateprotect.com | notify immediately |
| Full Report | admin@gateprotect.com | weekly |

SMTP settings

SMTP server: mail.gateProtect.com E-Mail account of the sender: info@gateProtect.com

Username: Reporting Password: *****

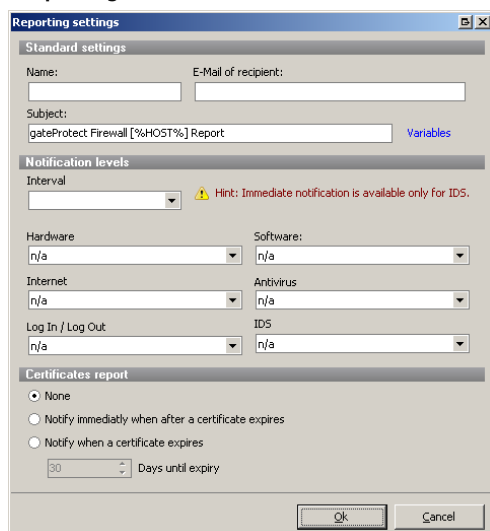
TLS-Encryption

First enter a valid e-mail account on an *SMTP server*, to which the reporting mails can be sent.

You can send a test mail with the *Letter* button. This tests whether the settings have all been made correctly. However, for this purpose at least one reporting task must be set up.

Create as many reporting tasks as necessary with the *Add* button.

Reporting characteristics



Standard settings

Name: E-Mail of recipient:

Subject: gateProtect Firewall [%HOST%] Report Variables

Notification levels

Interval: Hint: Immediate notification is available only for IDS.

Hardware: n/a Software: n/a

Internet: n/a Antivirus: n/a

Log In / Log Out: n/a IDS: n/a

Certificates report

None

Notify immediately when after a certificate expires

Notify when a certificate expires

90 Days until expiry

In addition to the general settings on recipient and content, it is possible to select different intervals and reporting levels.

You can choose the reporting level for all sections of the Firewall Server.

Errors and Warnings & Information is the most comprehensive reporting level.



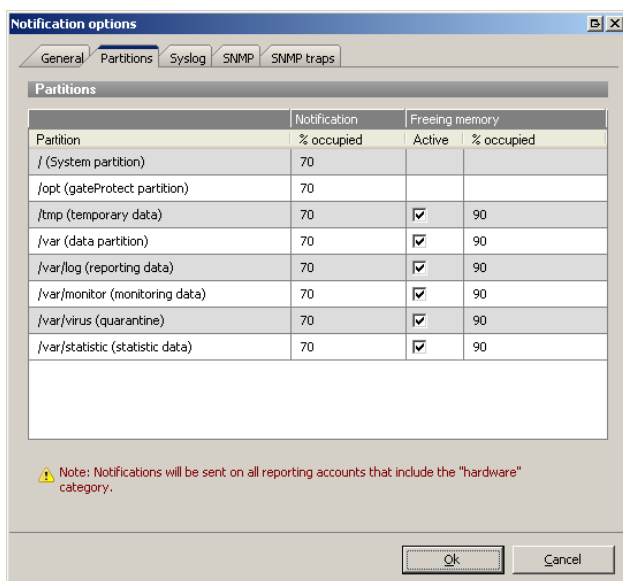
NOTE

MAILS CAN QUICKLY GROW TO A CONSIDERABLE SIZE USING THIS SETTING.

13.2 Partitions

All partitions on the Firewall are listed here. The Firewall monitors the level of the individual partitions independently. If a partition exceeds a critical level, you can be informed by e-mail. If a further limit is exceeded, the Firewall can release disk space, by compressing or deleting old log entries for example.

You can change these settings:



| Partition | Notification | | Freeing memory | |
|---------------------------------|--------------|-------------------------------------|----------------|----|
| | % occupied | Active | % occupied | |
| / (System partition) | 70 | | | |
| /opt (gateProtect partition) | 70 | | | |
| /tmp (temporary data) | 70 | <input checked="" type="checkbox"/> | | 90 |
| /var (data partition) | 70 | <input checked="" type="checkbox"/> | | 90 |
| /var/log (reporting data) | 70 | <input checked="" type="checkbox"/> | | 90 |
| /var/monitor (monitoring data) | 70 | <input checked="" type="checkbox"/> | | 90 |
| /var/virus (quarantine) | 70 | <input checked="" type="checkbox"/> | | 90 |
| /var/statistic (statistic data) | 70 | <input checked="" type="checkbox"/> | | 90 |

Note: Notifications will be sent on all reporting accounts that include the "hardware" category.

Reports

Here you can enter the level in percent, at which you want to receive a report. The reporting mails are sent to every recipient of the hardware information. Set up the reporting mails as described in Chapter 13.1.

Release storage

Enter the percentage, at which disk space should be released. In this event, only old and insignificant data are deleted. You receive a mail with information on the partition cleaning with the reporting mails from the *Hardware* category.

No storage space can be released for partitions with program data. However, these partitions cannot be fully written either.

13.3 Syslog-export

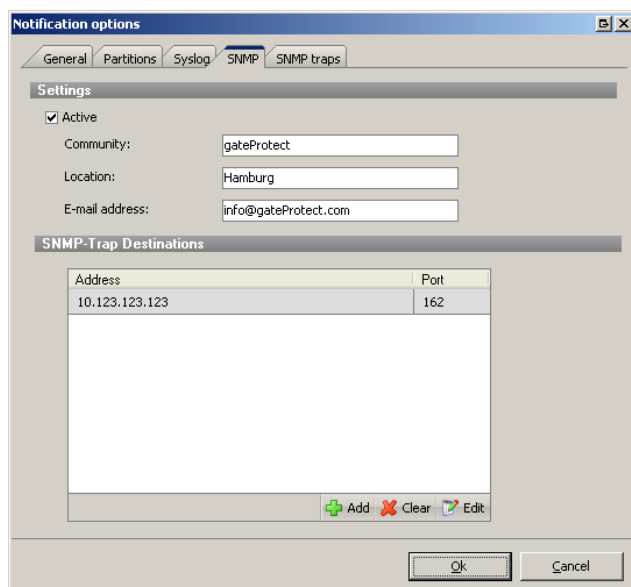
Syslog is a TCP/IP based protocol for transmission of log messages. The firewall logging can be expanded to one or more Syslog servers. Enter the Syslog servers in the Syslog Dialog under *Reporting Settings* for this. The firewall logs will then also be exported to the servers entered here.

13.4 SNMP

Since 8.0 SNMP has its own (gateprotect) MIBs and is able to send SNMP-traps.

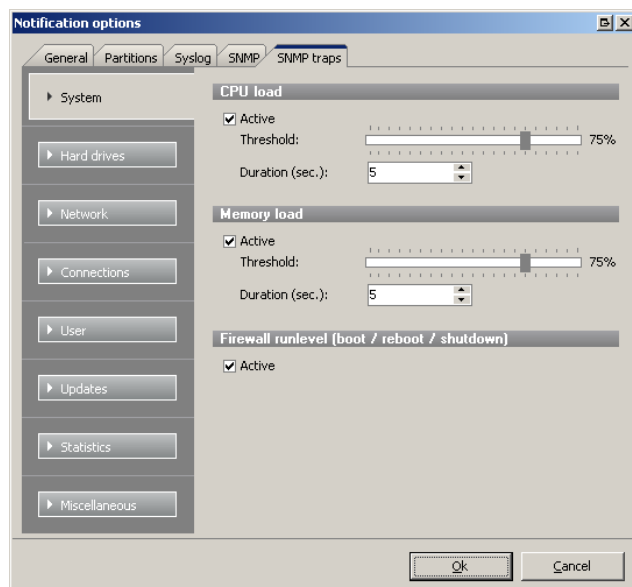
To use the new gateprotect MIBs you should first install your SNMP-software and then install the new MIBs which are located:

<http://www.gateprotect.de/snmp/>



The SNMP-settings are located in *Options > Reporting settings > SNMP*. Here you can set the community string and a list of hosts which will receive the SNMP traps.

On the tab *SNMP-traps* you can select which traps will be sent.

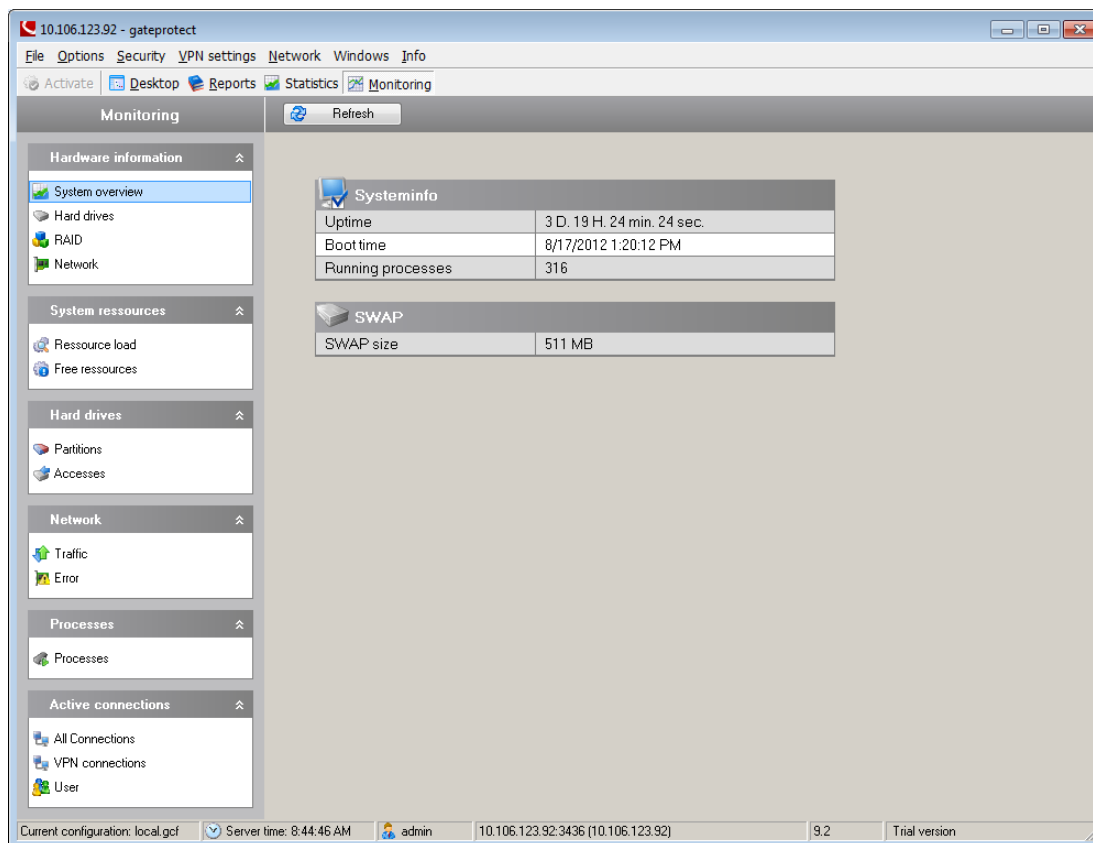


HINT
BETWEEN AN EVENT AND THE SNMP-TRAP THERE MIGHT BE UP TO 60 SECONDS.

14 MONITORING

14.1 Introduction

Monitoring provides you with up-to-date hardware and system information.



You can use the list on the left to decide which system groups or system information is to be displayed on the right-hand side.

You can update the displayed data of a page using the *Update* button at the top and, if necessary, select additional options for the evaluation:

- specify the period or the interval for timed statistics,
- select additional components if available,
- show or hide sections of the graphic evaluation, etc.

14.2 Components displayed in monitoring

| Monitoring | Description |
|----------------------|--|
| Hardware information | Provides system information on the Firewall Server, the hard drives, the RAID system (if available) and the network, or network cards. |
| System resources | Provides information on the temporal capacity of the used and free system resources. |
| Hard drives | Provides temporal information on hard drive allocation and capacity. |
| Network | Provides information on the network capacity, the achieved traffic capacity and any error rates. |
| Processes | Shows the percentage and temporal application of the services configured in the Firewall. |
| Active connections | Shows a list of the active VPN connections and active users. |

15 ANTI-SPAM / MAILFILTER

15.1 Mailfilter

The mail filter is only usable in connection with the SMTP proxy. With the mail filter you can filter mails by their destination address. If filtered it does not reach the real mail server. You can configure the mail filter in *Security > AntiSpam / Mailfilter*.

Possible settings:

- *Active*
Activates the mail filter.
- *Whitelist mode*
Emails of all addresses in this list will be forwarded to the mail server.
- *Blacklist mode*
Emails of all addresses in this list will never be forwarded to the mail server.
- *Reject E-Mails*
Unwanted emails will be rejected with a RFC-conform answer.
- *Delete E-Mails*
Unwanted emails will be deleted. The sender believes the email reached the mail server.



ATTENTION !

THE SETTING „DELETE E-MAILS“ IS NOT RFC-CONFORM. MISCONFIGURATION MAY DELETE IMPORTANT EMAILS.

The email addresses in the mail filter list can contain wildcards.

- * For whole words
- ? For single characters

If you are connected to an Active Directory Server all known email addresses will be shown in the list on the right hand side.

15.2 Anti-Spam

A commercial spam filter is integrated in the gateprotect firewall. This can optionally be activated with its own license.

A 30-days trial is usually available for every firewall in order to test the effectiveness of the filter.

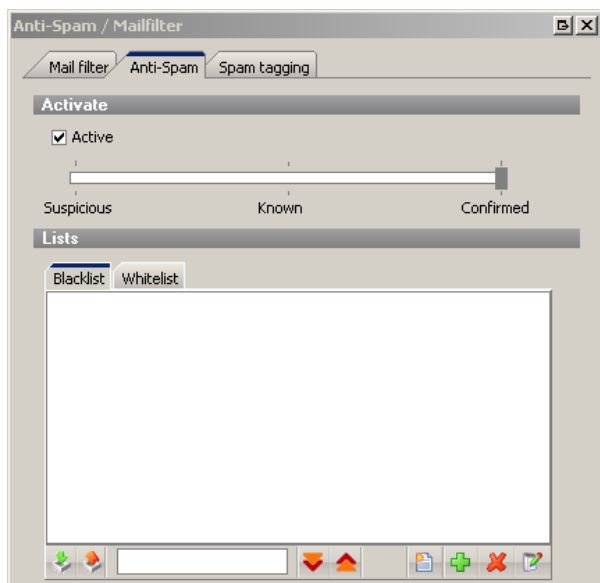
The spam filter has been developed by the company Commtouch and has a completely different functionality than Spamassassin for example.

If an email arrives at the firewall, a hash value of this email is generated. This hash value is sent to a central Commtouch server. This server determines the probability of this email being spam using a comprehensive database and complex algorithms. Different from conventional spam filters, not only is the content of the email analyzed here but also the frequency of the occurrence of this email on the Internet.

Commtouch has analysis programs installed at many email providers worldwide for this purpose.

This probability is then returned to the firewall which possibly flags the email as spam.

Using the slider, all emails with the category of the slider and all categories to the right of it are marked as spam.



Suspect

This email has already occurred frequently on the Internet but not so frequently to clearly classify it as spam (e.g. at the start of a spam campaign).

Known

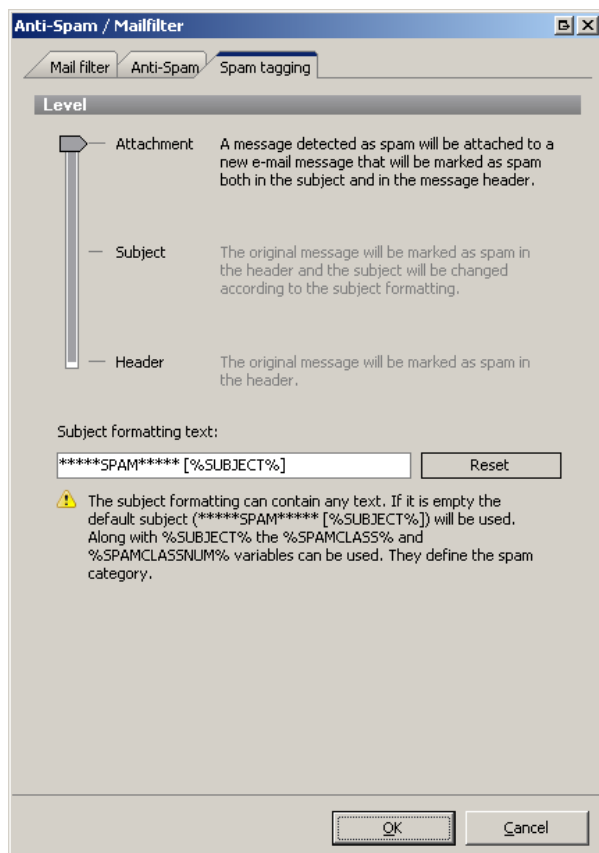
This email has already been seen so frequently on the Internet that it can be designated as spam. However, the sender is not a known spam address

Confirmed

This email comes from an address which is known as a spam mailer.

15.3 Spam-tagging

You are able to tag mails which are identified as spam.



Attachment

The original email will be attached to a new mail which describes the found spam. The spam-subject and X-Header are also added.

Subject

In this case only the subject of the original email will be replaced with the modified subject from the spam-tagging-dialog. X-Headers are also added.

Header

An email header will be added to detected Spam-Mails. These are the X-Header:

- X-Pimp-Spam-Class: This X-header can have the value "commtouch", if the spam is found by Commtouch. Or the value "spam", if the spam is caused by a blacklist entry.
- X-Pimp-Spam-Class-Num: This X-header describes the probability of spam.

Values can be „NONE, UNKNOWN, SUSPECT, BULK, CONFIRMED, BLACKLISTED“.

16 VIRUS PROTECTION

16.1 Introduction

The gateprotect Firewall Server protects your internal network from computer viruses using the integrated virus scanner from Kaspersky. As one of most well-known suppliers of virus protection solutions, Kaspersky offers the best possible protection from dangerous computer viruses with regular updates of the virus pattern and updated virus protection engine.

16.2 Licensing

The Antivirus Scanner of the gateprotect Firewall is not a component of the gateprotect firewall license. You must acquire a valid license for the virus scanner separately. Our sales department will be happy to help you further. If you have a valid license number for the Kaspersky virus scanner, you must license this in the Administration Client of the gateprotect Firewall.

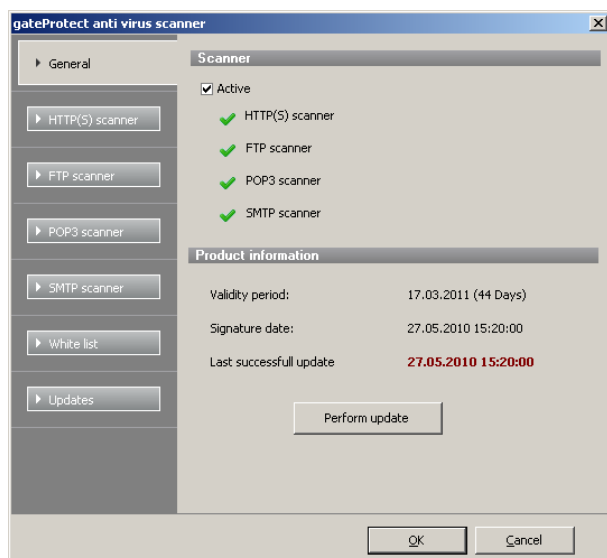


ATTENTION !

AFTER INSTALLATION OF THE FIREWALL SERVER, YOUR VIRUS SCANNER RUNS FOR 45 DAYS AS A TEST VERSION. ONCE THIS TIME HAS LAPSED, THE VIRUS SCANNER REMAINS ACTIVE, BUT NO MORE UPDATES ARE PERFORMED.

16.3 Settings

16.3.1 Antivirus settings: General



1. In the *Scanner* section this dialogue box provides you with an overview of the Internet protocols, which are monitored by the Virus scanner.

2. In the *Product Information* section you will find information on the validity of your Antivirus licence and the date of the last update.

3. The *Perform update* button allows you to manually update the virus definitions

16.3.2 Scanner

You can adjust settings for the relevant protocols in the dialogue boxes for the *HTTP Scanner*, *FTP Scanner*, *POP3 Scanner* and *SMTP Scanner*. You can switch the corresponding options on or off by ticking or clearing the boxes.

| Option | Meaning |
|----------------------------------|---|
| Scan archive files | Archive files (e.g. zip, tar, arc, rar) are "opened" by the Scanner and the individual components are checked for viruses. |
| Scan packed files | Packed files are unpacked and the individual components are checked for viruses. |
| Scan self-unpacking files | Self-unpacking files are unpacked and the individual components are checked for viruses. |
| Scan mail base | E-mail databases are stripped down and the individual components are checked for viruses. |
| Scan text mails | Simple texts in e-mails are checked for viruses. |
| Block files with viruses | Files with clearly identified viruses are blocked. |
| Block suspect files | Files that the Virus Scanner cannot allocate, unpack or analyse are blocked. |
| Block files with warnings | Files, in which a new variation of a virus may have been found, are blocked. |
| Activate scan heuristic | Binary data are checked for code, which has similar characteristics to a virus or could cause other damage. This method enables recognition of sub variations of viruses, which have no signature of their own under certain circumstances. |
| Expanded settings | Specify the maximum size of files in the expanded settings of the FTP and HTTP scanner, which are scanned directly in the main memory or are excluded from the scan process because of their size. |
| Maximum scan size (POP3- & SMTP) | Defines the size limit to which an attachment will be scanned. |

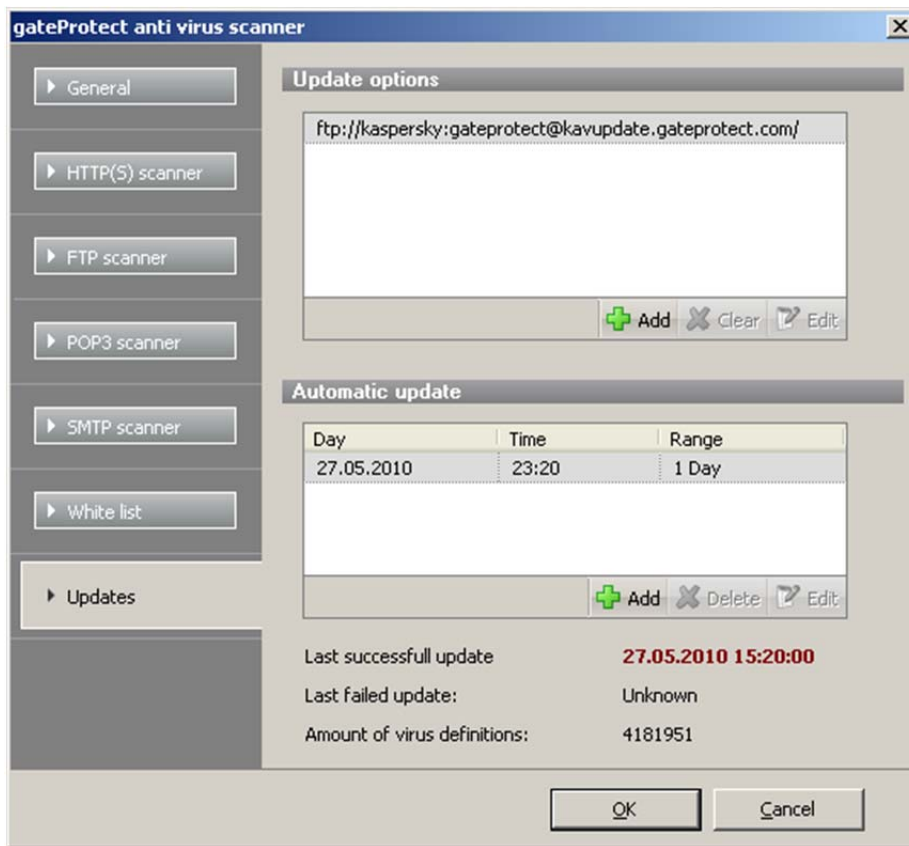
16.3.3 White list

You can enter trusted hosts or servers in a list in the *White List* dialogue box. Data transferred by HTTP or FTP from these hosts are not checked for viruses.

1. Click on the *Add* button to add a host to the White list.
The entry box for a trusted host is opened.
2. Enter the complete address of the host in the entry field and click on *OK*.

16.3.4 Updates

You can perform a manual update in the *Updates* dialogue box and edit settings for automatic updates.



Update options

Update-Server can be managed by adding new Server, clearing or editing existing ones.

Automatic update

Enter the date, time of the first update and intervals at which the update should be performed in the appropriate fields and click on the *OK* button.

17 UPDATES

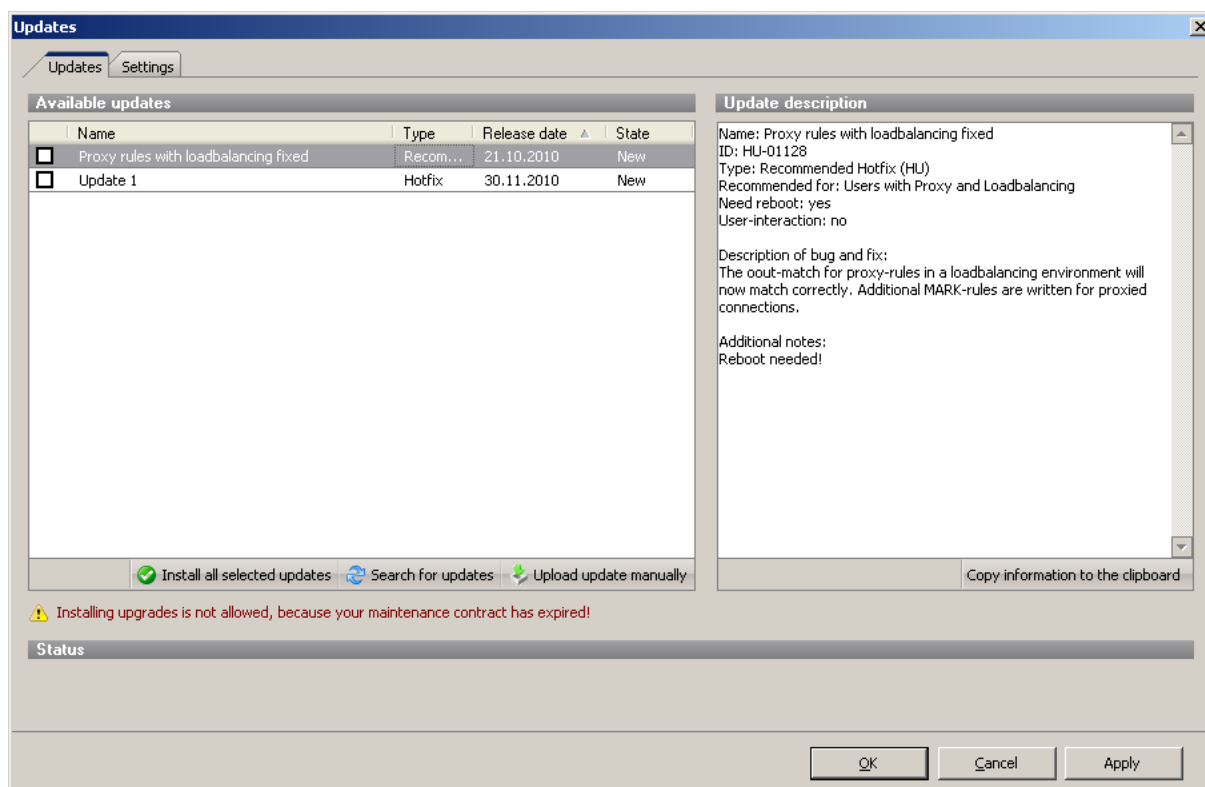
17.1 Introduction

The gateprotect update system offers the possibility of keeping your firewall always up to date. Hotfixes, security updates and new functions can be installed fast and straightforward on your firewall server. Furthermore, the update system is equipped with several functions to inform the administrator if new updates are available. A history of installed updates is also available.

To prevent the installation of denied or malicious updates on the firewall, all updates were digitally signed by gateprotect. Only updates with a valid signature were listed and applied. All others will be deleted by the system.

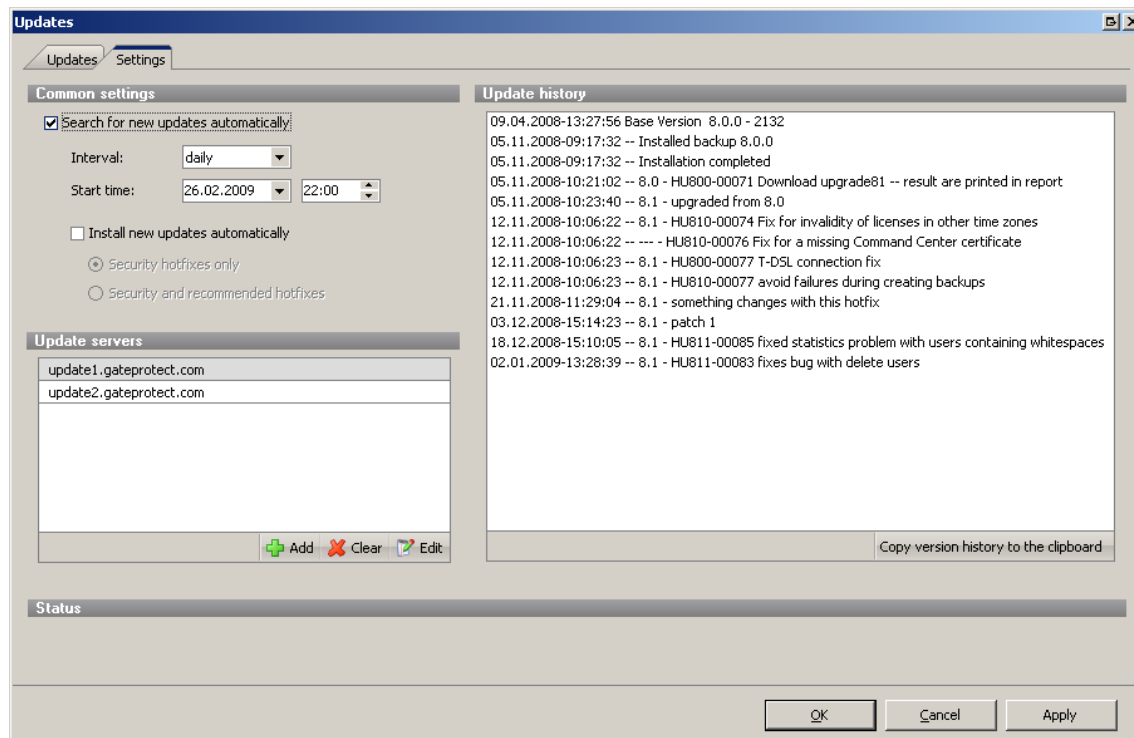
The updates can be downloaded automatically or manually from the update server. For the case that the firewall does not have an internet connection, it is possible to install updates using a local storage device.

You can reach the dialogue including the settings of the update system via *Options > Updates*.



The first tab in this window contains a list of known updates, a text field with detailed information of the selected update, buttons to download and install updates as well as a status area.

In the second tab, you can specify settings of the automated download of updates, edit the list of update servers and view the update history.



17.2 Updates

All available updates are listed in this dialogue. This list shows the name, the type, the release date and the status of the update. New updates were listed as well as already installed ones; they vary in the status. Furthermore, installed updates cannot be installed a second time.

The update system differentiates between four update types:

| Type | Description |
|--------------------|---|
| Security hotfix | Contains corrections which affects the security of the firewall |
| Recommended hotfix | Contains corrections, performance and stability optimizations |
| Hotfix | Eventually contains new functions besides corrections of firewall modules |
| Upgrade | Contains an upgrade to the next firewall version |

On the right to the update list, there is a text field with detailed information about the selected update.

This field shows following information:

| Information | Description |
|-------------|---|
| ID | An unique identification number |
| Name | Short description of the update |
| Description | Contains a detailed description of the update |

Furthermore, dependencies are listed if applicable.

17.3 Download updates automatically

The firewall is able to search for new updates automatically. To activate this function, open up the *Updates* dialogue, select the *Settings* tab and tick the *Search for new updates automatically* box. You can specify the *Interval* in which the firewall server should search for updates. You can choose between hourly, daily or weekly. In the *Start time* field, you can type in the date of the first search. All following actualizations take place in the entered time.

If the option *Install new updates automatically* is activated, new updates were automatically installed on the firewall server. This function is limited to security and recommended hotfixes.

17.4 Manually download updates

To search for updates manually, open the *Updates* dialogue and select the *Updates* tab. Click the button *Search for updates*. This process may take some time. You can watch the progress of the search in the status area. After the search has ended, the update list gets refreshed.

17.5 Install updates

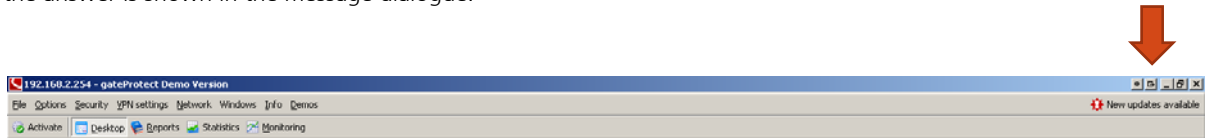
To install available updates, open the *Updates* dialogue and select the *Updates* tab. Select the updates you want to install and click the *Install all selected updates* button.

17.6 Install updates from local storage device

To install an update from a local storage device, open the *Updates* dialogue and select the *Updates* tab. Click the *Upload update manually* button which opens a file dialogue. Select the update file you want to load up and click *OK*. This file gets now transferred to the firewall. The firewall server now checks the signature of the file and shows the update in the update list from where it can be installed. This process may take some time. You can watch the progress in the status area.

17.7 Update interaction

The update system allows the firewall to show information or interact with the user while installing certain updates. This interaction can be a yes/no question or an input field with a question. As soon as the firewall gets the answer, the answer is shown in the message dialogue.



If an user interaction is needed, the client shows this in the status area. To respond, click the Answer question button. The client now shows a dialogue with the corresponding question which has to be answered. If you don't answer to the question, the firewall remains in standby and doesn't install further updates.

18 EXAMPLES

18.1 Introduction

This chapter concerns several problems that occur in practice as examples. To simplify matters the following configuration is used as the starting point each time and supplemented depending on the example. All data used are fictitious and only intended as an example.

There is a small company with three departments:

- Marketing
- Sales
- Technology

Every department has its own network and is separated physically from the others (network separation).

Furthermore, the company has an internal mail server, which collects mails from external mail servers and sends them to the employees internally.

The company has a central location for storage of corporate data in the network: a fileserver, which is located in the same network as the mail server.

There is a DSL dial-in connection without time limits for the internet connection.

The following rules have been configured using the Administration Client:

Marketing

The Marketing network (192.168.0.0/24) may always access the internet with the services HTTP (internet pages), FTP (file download), HBCI (home banking), SMTP (send e-mail) and POP3 (receive e-mail) without time limits or web blocking.

Sales

The Sales network (192.168.1.0/24) may access the internet with the services HTTP (internet pages) and FTP (file download) on weekdays between 8am and 8pm. Furthermore, the HTTP access is limited by web blocking and the "Sex" wordlist.

Technology

The Technology network (192.168.2.0/24) may access the internet with the services HTTP (internet pages), FTP (file download), POP3 (receive e-mail), SMTP (send e-mail), SSH (encoded remote access), PPTP (encoded remote access) and PING (network test) without time limits or web blocking.

General

Every internal network may access the internal mail server (via POP3 and SMTP) and the internal file server (via Net-BIOS, KERBEROS, LDAP and MySQL). The internal file server has the IP address 192.168.0.100 and the internal mail server has the IP address 192.168.4.6.

18.2 Setting up the internet connection with fixed IP address

18.2.1 Setting up a dedicated line with fixed IP addresses using a router

Step 1

You have received the following data from you provider:
 216.239.37.96 / 29 or 216.239.37.96 / 255.255.255.248

This network is divided into the following sections

Network address: 216.239.37.96

Router of the provider (gateway): 216.239.37.97

Own use: 216.239.37.98 – 216.239.37.102 (five addresses)

Broadcast address: 216.239.37.103

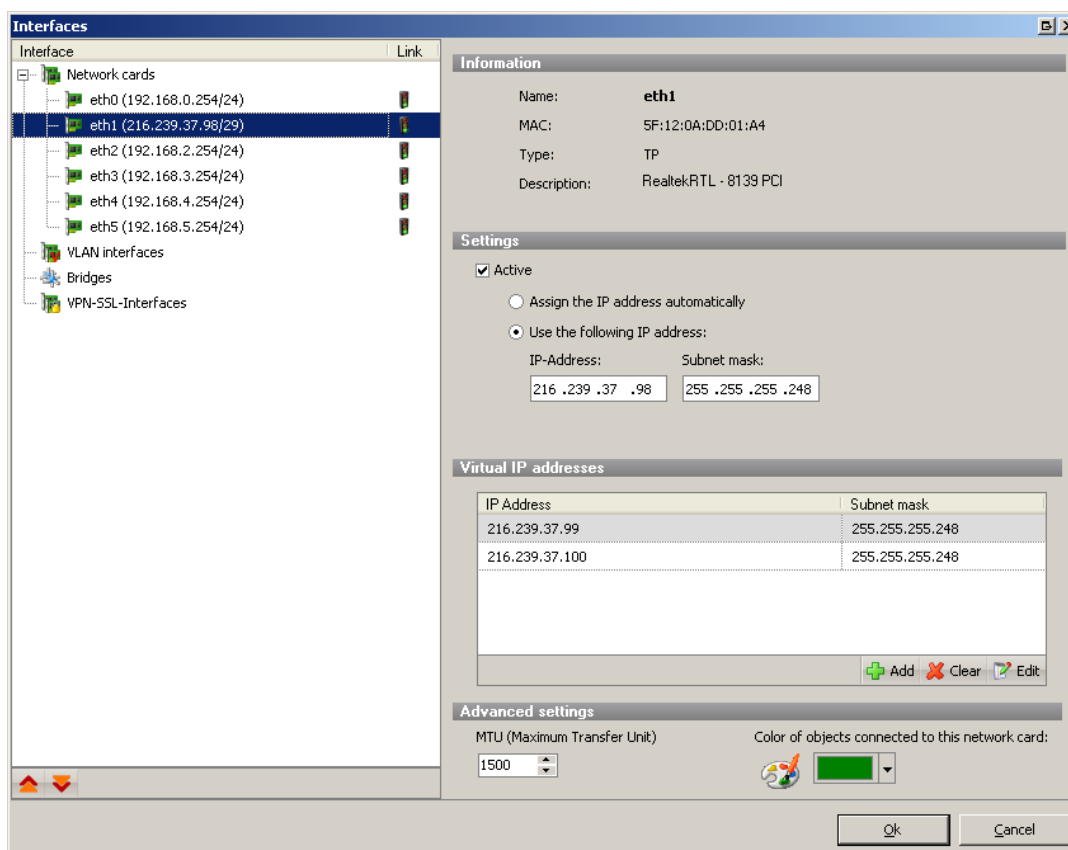
This is a typical 29bit IP address range, as supplied by most German providers. You have eight IP addresses but you can use only five for addressing.

Two of the eight addresses were used for network logic (network address and broadcast address) and one IP address is assigned to the router of the provider. This is usually the first IP after the network address.

Step 2

To be able to set up an internet connection through the router, the firewall has to get one of the usable addresses and the subnet mask assigned by the provider.

Firstly, a network card (we use eth0 for this example) gets the IP address 216.239.37.98 with the subnet mask 255.255.255.248 in the menu *Options -> Interfaces*



Step 3

In the next step, a router connection is set up using the internet connection assistant via *Options > Internet* using the *Add* button.

Step 4

Enter the IP address of the provider router as the router address (in this example 216.239.37.97).



NOTE

IF THE INTERNET CONNECTION DOES NOT WORK AT FIRST GO, PLEASE RESTART THE ROUTER. IF YOU WANT TO KNOW, HOW TO MAKE THE OTHER FOUR IP ADDRESSES USEABLE THROUGH THE FIREWALL, PLEASE READ SECTION 18.3.3 DMZ BY SOURCE IP.

18.2.2 Setting up a DSL connection with fixed IP address

Setting up a DSL connection with a static IP address (usually designated as SDSL, xDSL or DSL-Business) is like setting up a normal DSL connection.



NOTE

PLEASE DO NOT SET UP THE FIXED IP ADDRESS TO ONE OF THE NETWORK CARDS OF THE FIREWALL. BECAUSE YOU GET ALL CONNECTION DATA (INCLUDING THE IP ADDRESS) FROM YOUR PROVIDER, IT IS NOT NECESSARY TO CHANGE THEM ON THE FIREWALL. THIS COULD LEAD TO PROBLEMS WITH SOME SERVICES.

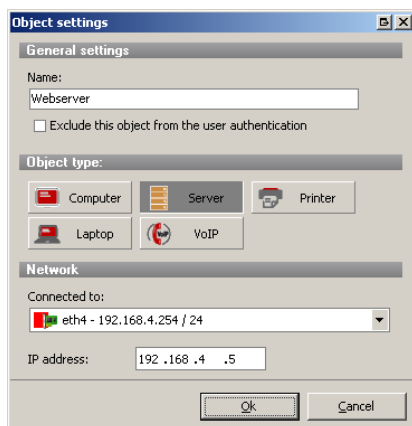
18.2.3 Setting up a cable connection with DHCP IP addresses

The interface the cable modem is connected to has to be set to "Assign the IP address automatically" in the Interface settings. When configuring the internet connection select "Router connection" and choose "*Assign the router address over DHCP*".

18.3 Demilitarized zone (DMZ)

18.3.1 Simple port forwarding

In most cases, forwarding of a single or a few ports is desired to facilitate access to a web server from the internet for example.



Step 1

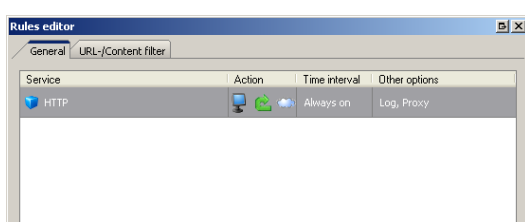
For this purpose, a server is dragged from the tool list to the configuration desktop and the IP address of the server is then entered in the open dialogue box (in this case 192.168.4.5) as well as the network interface to which the server is connected (here eth4).

For a better overview on the configuration desktop the symbol gets a clear name (e.g. web server).

Step 2

Now create a connection from the server to the internet cloud using the connection tool.

This opens the Rules editor. Use the Add button and select a service which should be forwarded to the server (in this case HTTP).

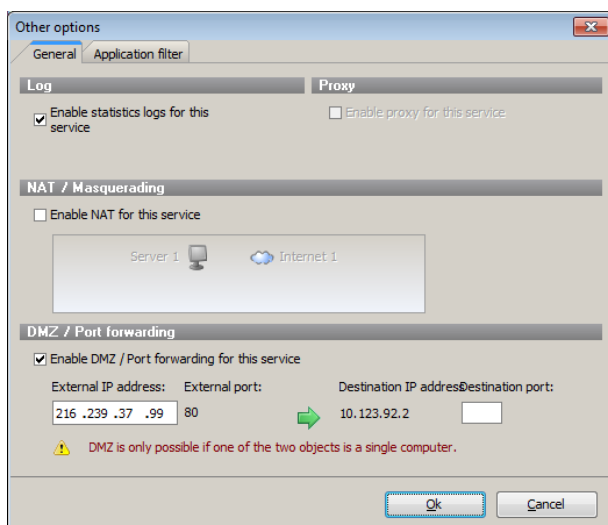


Step 3

In the column *Action* the arrow for *Stateful inspection* is set from the internet towards the computer and back to the internet. This settings means that the internal server can be accessed from the internet but cannot access the internet by itself. If you want the server to be able to access the internet, please set a *double arrow* here.

Step 4

Click on the last column *Additional options* and tick the *Activate DMZ / port forwarding for this service* box.


NOTE

PLEASE LEAVE THE ENTRY FIELDS BLANK IN THIS SECTION. THE FUNCTION OF THESE FIELDS IS EXPLAINED IN THE NEXT TWO CHAPTERS.

Step 5

Once the Rules editor is confirmed with *OK* and configuration has been activated using *F9*, all data that goes to your external IP address on port 80 is forwarded to the internal web server.

NOTE

PORT FORWARDING CAN ONLY BE TESTED FROM AN EXTERNAL ACCESS. YOU CANNOT REACH YOUR EXTERNAL IP ADDRESS FROM THE LOCAL NETWORK.

18.3.2 Port forwarding with port rerouting

Port rerouting can be useful if you want to be able to access the same service (e.g. HTTP) using one IP address. There are also security advantages if no standard ports are used for certain services (e.g. Telnet, SSH). You can re-route a port to realize this. This example refers to the settings and rules made in the previous section.

Step 1

In this example, we would like to be able to access the SSH service (for remote maintenance using a text console) of our web server (in this case 192.168.4.5) using a different port than the standard SSH port (22/tcp). We choose the externally accessible port 10022 which should be forwarded to the web server on port 22.

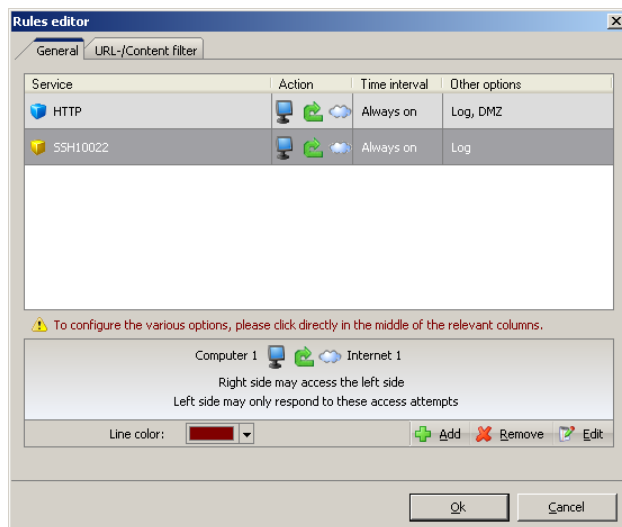
Step 2

For this purpose, double-click on the connection point between the internet cloud and the *web server* symbol. In the Rules editor, choose the service *Freely defined* using the *Add* button.

Step 3

In the dialogue box that now appears, enter a name for our service. We choose SSH 10022. Under Port enter 10022 in the first field. The second Port field is only needed if you want to define more than one port for this service (port range).

Under *Transport protocol*, select TCP (Transmission Control Protocol).


Step 4

In the *Action* column, the arrow for *Stateful inspection* is set from the internet towards the computer and back to the internet. This setting means that the internal server can be accessed from the internet but the server cannot access the internet by itself.

Step 5

In the last column *Additional options*, tick the *Activate DMZ / port forwarding for this service* box. Because we want to reroute the starting port (10022) to the web server on port 22, enter *22* in the *Target port* field. NAT is not required for this freely defined service.

The web server now receives external queries on port 10022 on its port 22 (which is reserved for SSH).

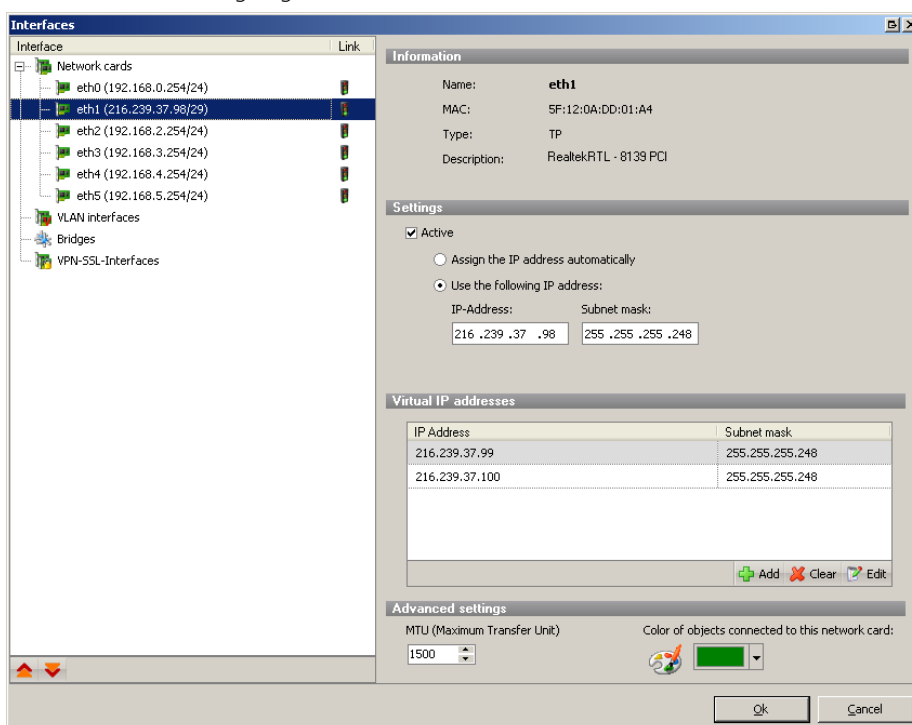
18.3.3 DMZ by source IP

If there is an internet connection with several fixed IP addresses, perhaps several mail servers or several web servers are operating behind the firewall with different external IP addresses.

- The web server with the internal IP address 192.168.4.5 should be accessible with the external IP address 216.239.37.99.
- The mail server with the internal IP address 192.168.4.6 should be accessible with the external IP address 216.239.37.100.

Step 1

First, we have to assign the external network card of the firewall (which is connected to the provider's router) with the IP address we are going to use.


Step 2

The corresponding network card connected to the router is selected under *Options > Interfaces*. The virtual IP address is added under *Virtual IP addresses*.

The gateprotect firewall is now configured for these additional IP addresses.

Step 3

Next, a server is dragged from the tool list to the configuration desktop and the internal IP address of the server is entered in the open dialogue box (in this case 192.168.4.5) and the network card is selected.

The same is done for the mail server with the internal IP address 192.168.4.6.

For a better overview on the configuration desktop, clear names were assigned to the symbols (e.g. web server and mail server).

Web server

Step 1

Now create a connection from the server to the internet cloud using the connection tool. In the Rules editor, use the *Add* button to select the service which should be forwarded to the server. The service *HTTP* is inserted between the web server and the internet.

Step 2

With ticking the Enable DMZ / Port forwarding for this service box in the Additional options, the DMZ gets created. It is crucial that the above configured IP address is also used now, that the official IP address of the web server is entered in the Source IP field.

This configuration is activated and the web server can be accessed under this IP address.



ATTENTION!
THE HTTP PROXY MUST NOT BE ACTIVATED IN A HTTP-DMZ!

Achieve separate access to the web server internally using the name

If a web server has been set up like the above example, this can still only be accessed from internally using its internal IP address.

However, some applications demand the host name of the computer, e.g. *www.your-company.com*.



NOTE

TO AVOID SERVICE OR CHANGING THE NAME SERVER ENTRIES, IT IS POSSIBLE TO REALIZE THIS WITH THE GATEPROTECT FIREWALL.

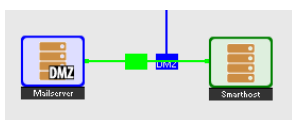
Create a connection from the web server symbol to the internal LAN using the connection tool. In the Rules editor, add the HTTP service and enter the official source IP address in the DMZ in the Additional options.

Mail server

With a mail server it normally behaves like an HTTP-DMZ. However, there are special cases where it is desired to allow certain mail servers to connect with the internal mail server (so-called smart hosts). Here the gateprotect firewall offers the opportunity to create a dedicated DMZ.

Step 1

For this purpose, the internal mail server is set up as an individual server symbol.



Step 2

Now a further server symbol is dragged to the desktop. In the configuration the internet is selected as the network card and the IP address is the external one.



ATTENTION !
WHEN CONNECTION THE TWO SYMBOLS, YOU HAVE TO CLICK ON THE INTERNAL COMPUTER FIRST AND THEN ON THE EXTERNAL ONE.

Step 3

SMTP is now set up as a service and the DMZ is activated in the Additional options. The official mail server IP address is entered as the source IP.

18.4 Examples for user authentication

18.4.1 Windows domain

If you have a Windows domain, you can connect user authentication to the Windows domain controller. Enter the data of your domain controller on the Settings tab of the Authentication server dialogue box. In the user list you will see all users of the domain. Then you can drag user icons to the configuration desktop and assign rules to them.

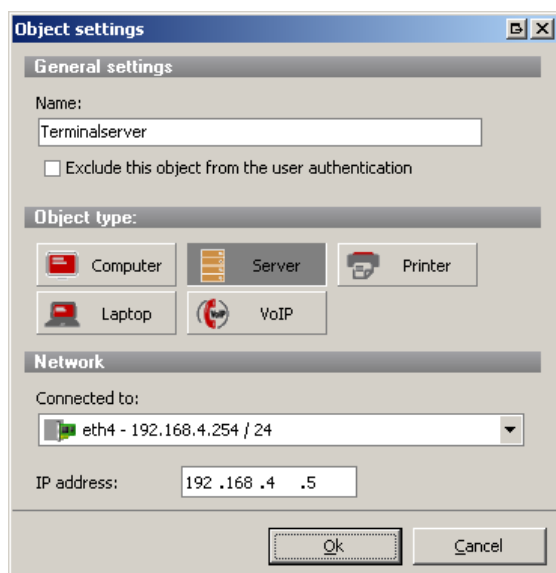
The users have to call up the IP address of the firewall server with https in their browsers to log on. If log-on is successful, the user's firewall rules are applied to the given IP address. If the browser window is closed, the session cookie lapses and the rules expire.

18.4.2 Terminal server

If you use a terminal server, it should be removed from the user authentication, as otherwise when one user has logged on, all further users will receive the same rights as the first one. To remove the terminal server from the user authentication, proceed as follows:

Step 1

Double-click on the terminal server symbol on the configuration desktop.



Step 2

Tick the *Exclude this object from user authentication* box.

For a terminal server, the intransparent HTTP-Proxy is advisable. Adjust the HTTP Proxy to intransparent for this purpose under *Options > Proxy*.



NOTE

THE BROWSERS HAVE TO ENTER THE HTTP-PROXY WITH THE IP ADDRESS OF THE FIREWALL IN THEIR SUB NETWORKS AND CONFIGURE PORT 10080. TO AVOID DOWNLOAD LOOPS, THE FIREWALL IP ADDRESS SHOULD BE ENTERED IN "EXCLUDE THIS IP ADDRESS FROM PROXY" SETTINGS OF THE BROWSER.

All users who now log on to the terminal server will first receive a notification when they open the browser asking for a username and password. As soon as they have authenticated against the local user authentication, the Active Directory or OpenLDAP/Krb5, they can use the terminal server to surf the internet.

The logged on users can surf until the last browser window is closed. When the browser is reopened, they have to log in again.

Logged-on users receive their own URL and content filter settings and are logged in the statistics individually under their names or their IP addresses.

19 STATISTICS

The statistics or the external Statistic Client portrays and evaluates the statistics functions of the firewall.



NOTE

1. YOU CAN ONLY LOG ONE ADMINISTRATION CLIENT INTO THE FIREWALL BUT AN UNLIMITED NUMBER OF EXTERNAL STATISTIC CLIENTS.
2. TO BE ABLE TO CONNECT A STATISTIC CLIENT WITH THE FIREWALL, YOU NEED AN USER ACCOUNT ON THE FIREWALL WHICH HAS RIGHTS TO START THE CLIENT AND TO DISPLAY STATISTICS.
3. TO DISPLAY THE STATISTICS FOR INDIVIDUAL USERS, YOU STILL REQUIRE THE DISPLAY RIGHTS STATISTICS BY USER. FOR TECHNICAL REASONS, THE RIGHTS OPEN / STORE CONFIGURATION IS ALSO SET.
4. IF YOU WOULD LIKE TO HAVE THE OPPORTUNITY TO EXPAND THE WEB BLOCKING LISTS FROM THE INTERNET TOP-LISTS WITH A SIMPLE RIGHT-CLICK, YOU WILL NEED THE RIGHT TO MANAGE WEB BLOCKING.

19.1 Using the Statistic Client / Statistics

19.1.1 Toolbar

You can use the toolbar in the Statistic Client to:

- Print out the current statistics,
- Change the language of the Statistic Client for menu and use,
- Obtain information on the Statistic client,
- End the Statistic Client.

19.1.2 Filter possibilities

You can filter the displayed results depending on the prepared statistics data in the upper part of the statistics window:

- Desktop: whole network, users or computers
- Period: 6, 12 or 24 hours, 7 or 14 days, 1, 3 or 12 months
- Self-defined period with date and time for start and end
- Time window: any time of day with start and end
- Blocked access: incoming or outgoing

Use the *Update* button to download the latest data from the firewall server.

19.1.3 Statistics

The statistics of the Statistic client have the same range of functions as the Administration Client described in 3.6.