gateprotect®

gateProtect Manual

Command Center

1 Setting up Command Center 5

1.1 Set up the Command Center firewall 5
1.2 Create the Command Center certificate 5
1.3 Import the Command Center certificate 5

2 Connect to the firewalls 6

2.1 Enter the Command Center key on the firewalls 6
2.2 Connect to the firewalls 6

3 Settings of the Command Center 7

3.1 Usermanagement 7
3.2 Backup 7
3.3 Certificates 8
3.4 Background 8

4 Settings of the firewalls 9

4.1 Firewall details 9
4.2 Firewall licensing 9
4.3 Auto-Backup settings 10
4.4 Updates 10

5 Dashboard (Firewall overview) 11

5.1 Firewall functions 11
5.2 Sorting and filtering 13

6 Map view 14

6.1 Symbols and lines 14
6.2 Zoom 14

7 VPN 15

7.1 Site-to-Site 15
7.2 Roadwarrior (Client-to-Site) 15

8 Licensing the Command Center 16

© 2011 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 handbook.

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.

You can reach us at:

support@gateProtect.com

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

From 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:

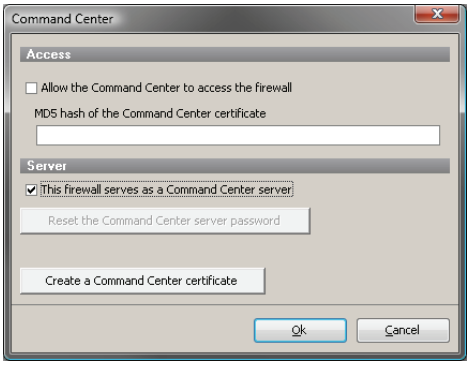
http://www.gateProtect.com

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

1 SETTING UP COMMAND CENTER

To start the Command Center the first time, some settings have to be made. This is only necessary for the first time. Later, you can always access the configured Command Center.

1.1 Set up the Command Center firewall

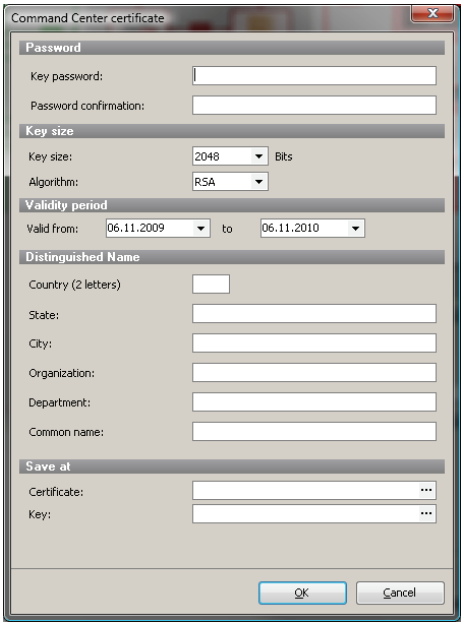


The Command Center needs a firewall as server for the Command Center. All files and settings of the Command Center will be stored on this firewall. To start the Command Center you have to connect to this firewall.

To define a firewall as server for the Command Center, connect to the firewall using the Administration Client and tick the "*This firewall serves as a Command Center server*" box in the *Options* > *Command Center* dialogue.

After you ticked the box, you have to enter the password for the Command Center.

1.2 Create the Command Center certificate



The Command Center needs its own certificate to establish a secured connection to the firewalls.

You can create this certificate on a firewall using the Administration Client. Connect to the firewall the usual way and open up the *Options* > *Command Center* dialogue. Create the Command Center certificate and save it on your administration computer.

1.3 Import the Command Center certificate

Start the Command Center and connect to the designated firewall. Choose "*Create new configuration*" in the configuration wizard and import the certificate you created in 1.2.

2 CONNECT TO THE FIREWALLS

If you followed the steps from 1., you are now connected to the firewall which serves the Command Center. At this moment, no firewalls are connected to the Command Center. This will be done now.

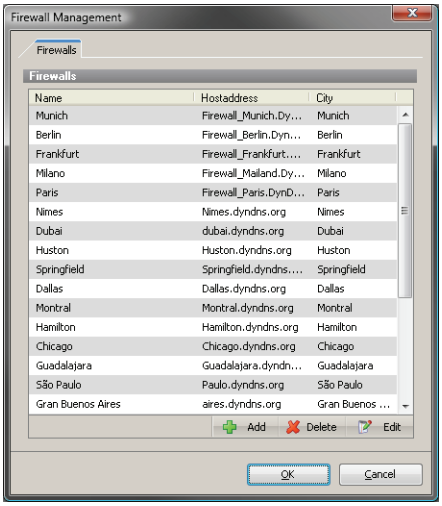
2.1 Enter the Command Center key on the firewalls

The Command Center certificate is still unknown to your firewalls. The firewalls require a unique hash (fingerprint) for the certificate to make sure that it is really the Command Center that wants to connect. The fingerprint can automatically be entered on the firewall on which the Command Center certificate was created (confirm the dialogue with "yes"). On all other firewalls, the fingerprint has to be entered by hand. In the *Command Center* > *Certificate* dialogue, you can copy the fingerprint into your clipboard by clicking the copy-icon.

Now connect to the firewalls you want to connect to the Command Center using the Administration Client. Open up the Command Center > Certificate dialogue. Here you can paste the fingerprint out of your clipboard. Of course you can enter it manually.

NOTE
IF YOU WANT TO CONNECT A FIREWALL WITH THE COMMAND CENTER THROUGH THE INTERNET, YOU HAVE TO ALLOW THE EXTERNAL CLIENT ACCESS IN YOUR SERVER SETTINGS.

2.2 Connect to the firewalls



At least, you have to connect your Command Center to the firewalls. In the *Firewalls* > *Firewall Management* dialogue, you can add as many firewalls as you want (only limited by your Command Center license).

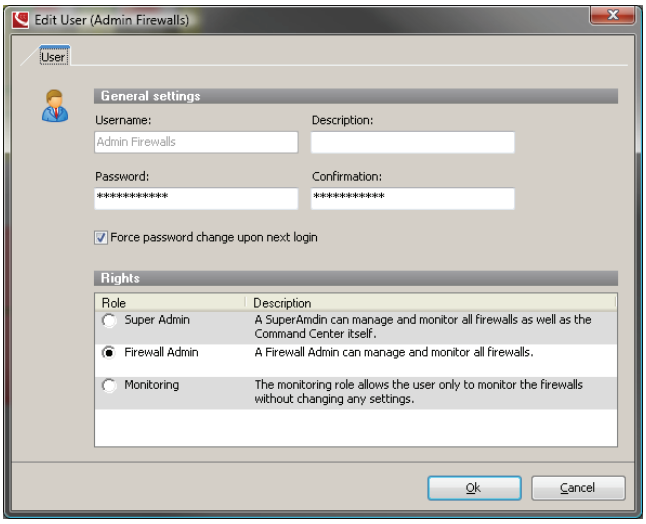
If you entered the Command Center fingerprint correctly, just enter the firewall's data in the corresponding fields.

3 SETTINGS OF THE COMMAND CENTER

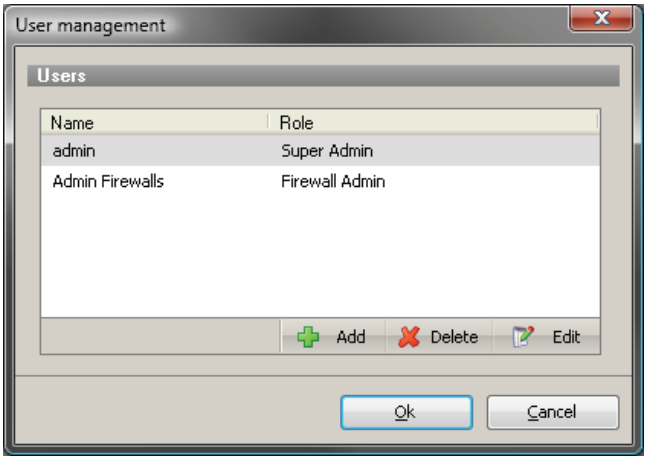
3.1 User management

Administrators which are allowed to connect to the Command Center can be separated in groups.
Three typical rules are predefined:

- Super Admin (Is allowed to administrate everything.)
- Firewall Admin (Is allowed to administrate firewalls.)
- Monitoring (Is allowed to read information.)



You can add as much users as you want.



3.2 Backup

All settings you have made in the Command Center can also be saved in the Command Center backup.
(*File* > *Create Backup*)

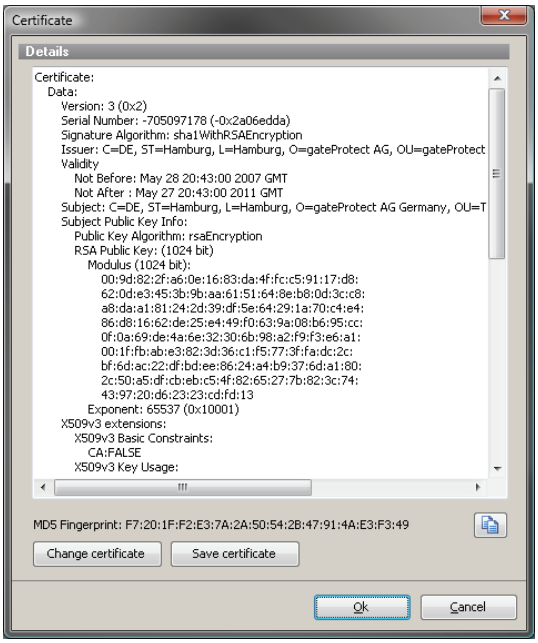
This file can also be imported. (*File* > *Import Backup*)

NOTE

YOU DO NOT NEED THE BACKUP TO SET UP THE COMMAND CENTER ON ANOTHER PC. BECAUSE THE SETTINGS ARE STORED ON THE COMMAND CENTER FIREWALL YOU CAN CONNECT FROM EVERY COMMAND CENTER AND SEE ALL SETTINGS AS USUAL.

3.3 Certificates

The Command Center certificate which you imported in 1.3 can be edited or saved again using the Command Center - Certificate dialogue.



Here you will always find the fingerprint you used in 2.1.

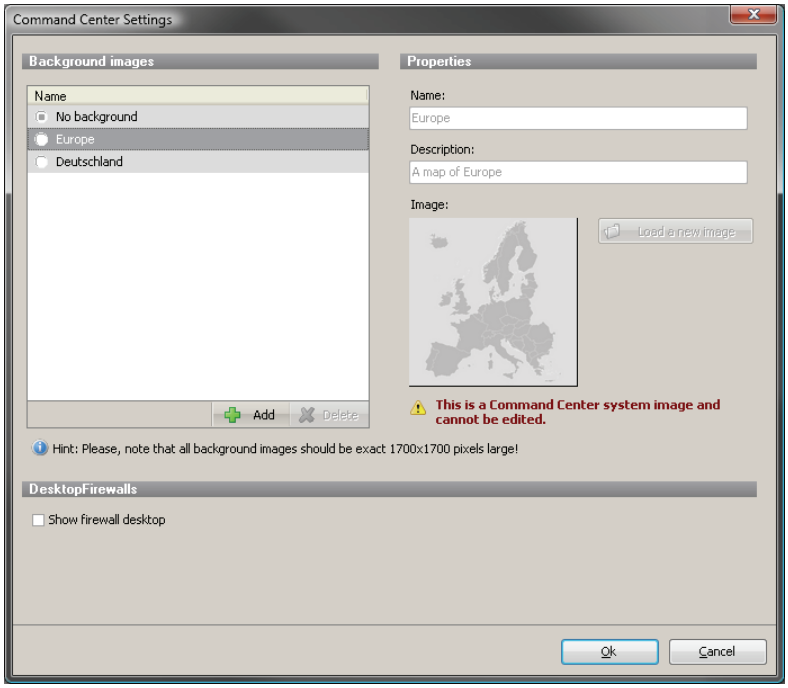
3.4 Background

You can change the background shown in the map-view in the Command Center > Background dialogue.

A map of Germany and Europe are included.

NOTE

IF YOU WANT TO USE YOUR OWN BACKGROUND, IT HAS TO BE 1700X1700 PIXELS.



4 SETTINGS OF THE FIREWALLS

4.1 Firewall details

Because the Command Center directly connects to the firewalls, many functions can be accessed as with the Administration Client.

A click on Details opens up the detailed mode of a selected firewall. Alternatively you can reach this mode by double-clicking on a firewall in the map-view or in the group-view.

In the detailed mode of a firewall, the buttons of the dark-grey bar are also available but have only an effect on the selected firewall.

In the detailed mode, following sections are available:

- Common - Overview over the license and the firewall
- System - System information and history
- Hardware - Overview hardware
- Resources - Monitoring
- Threats - Threats (IDS, denied accesses, …)
- Certificates - VPN certificates of the firewall
- VPN connections - VPN connections (SSL and IPSec)
- Report - Report with filter function
- IDS Report - IDS Report as in the Administration Client

NOTE
IN A GPO-75 FIREWALL, NOT ALL TABS ARE SHOWN BECAUSE THIS VERSION DOES NOT HAVE ALL FUNCTIONS.

The sections are accessible through different tabs.

If more information or functions are needed, click the *Configure* button. The Administration Client opens up (if installed) with the IP (or hostname) of the firewall.

4.2 Firewall licensing

As user of the Command Center you can receive licenses in a group license file. This .gplf-file is XML-formatted and contains several licenses.

Select a license-file to get a list of all included licenses. It is possible to combine licenses with or without antivirus, content filter and spam but the bundle itself can only be assigned to one firewall. In the right column you can select one of the firewalls using a drop-down-menu. Now you can assign the selected license to the selected firewall with clicking Apply Licenses. The license will now be submitted to the firewall.

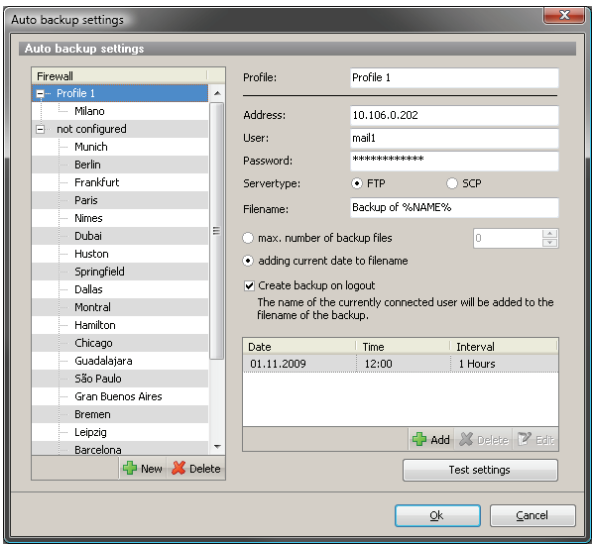
A double-click on a license-line opens a window with further information.

4.3 Auto-Backup settings

Automated backups with the Command Center can be created using "profiles".

For a task like "upload a daily backup to a SCP-server", a profile has to be created. All firewalls which should take part in this procedure should be assigned to it.

These settings are like the settings in the Administration Client.



First, enter the data of the server to which the backups should be sent. You have to choose if the backup should be transmitted using FTP (attention: without encryption!) or SCP.

Second, define how the backup files should be named. If you select "*max number of backup files*", the backup number is added to the end of the filename. If the maximum is reached, the oldest backup gets overwritten automatically.

The option "*adding current date to filename*" creates files named based on the defined filename and the current date. Because the filenames will never be repeated, the older backups will never be overwritten and more files were created.

Only one of these options can be selected.

If you select "*Create backup on logout*", a backup will be created if you close the Administration Client. These backups are marked by the username of the Administrator at the end of the filename.

Also, timed backup-jobs can be created.

The button "*Test settings*" tries to upload a testfile (called "filename_test") on the just created server. If the test succeeds you can delete the file and a window containing a positive response pops up.

If you already have created auto-backups in the Administration Client, they will appear here.

4.4 Updates

The Command Center allows updating multiple or even all firewalls at the same time. Besides the known feature of updating one firewall in its detailed view, a new dialogue is reachable via *Command Center* > *Updates*. This dialogue shows the available updates, sorted by firewall versions.

This list is taken from the Command Center firewall. To update the list of available updates, you can just click on *Get new update list*.

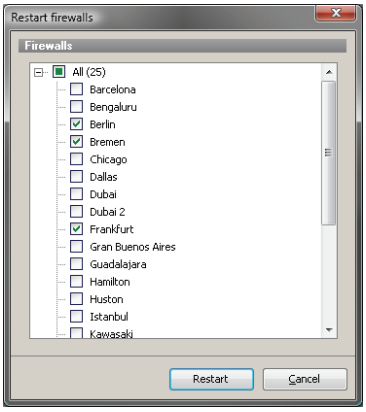
To install the updates on multiple firewalls, select the updates you want to install and click on Install updates. The next window shows your list of firewalls. You can use this list to select the firewalls which are supposed to install the update.

5 DASHBOARD (FIREWALL OVERVIEW)

5.1 Firewall functions

If you are in the overview, you can access several functions which you can use with one, multiple or all firewalls.

Reboot / Shutdown



The simultaneous reboot / shutdown of one or more firewalls is possible from the overview. Select one or more firewalls (using the shift-key) and click on reboot or shutdown.

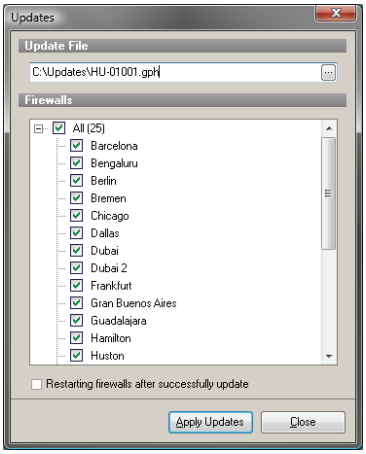
Now a new window pops up which asks you if you really want to reboot or shut down the selected firewall.

If you have more than one firewall selected, a menu for selecting the firewalls pops up.

Updates

Hotfixes and patches often have to be installed on multiple or all firewalls. To simplify that, the Command Center is able to install a patch on more than one firewall.

The hotfixes / patches are delivered as a gph-file for Command Center users.



Select one or more firewalls and click on "*Update*".

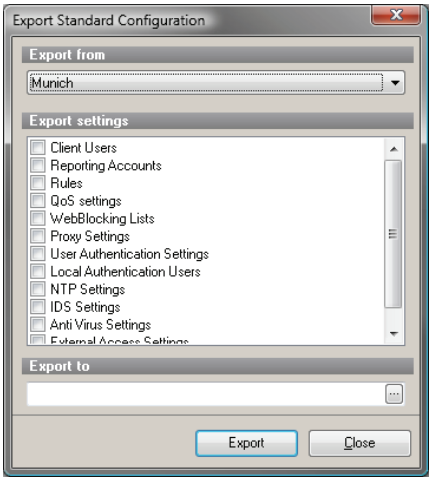
A window opens up in which you can select on which firewalls the update may be applied.

Some hotfixes / patches need a reboot of the firewall after installing. In this case, please tick the "*Restart firewalls after successful update*" box.

Import / export standard configuration

To clone parts of the firewall-configuration to several firewalls, you can use the export / import function for standard configuration.

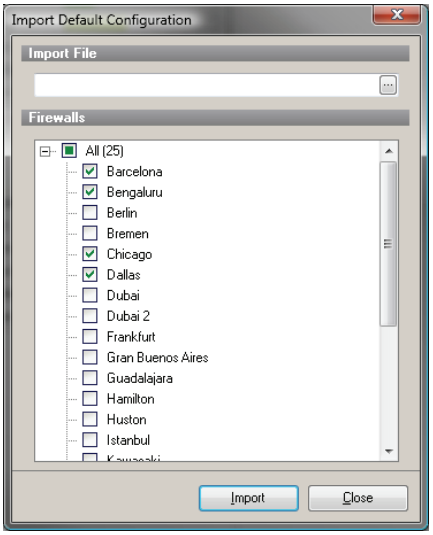
Example:
You want to have more administrator-accounts on the firewalls. Select the firewall on which the additional accounts are already created and click the *export config* button. A new window opens up:



Select Client Users. In the upper part of the window, the firewall is selected from which the configuration gets exported.

Now choose the target file under *export to* and click the *export* button. Your configuration is now saved to the file.

Now select all firewalls on which the user should be imported and click on import config. The following window pops up:



Select the file created in the previous step and select the firewalls. A click on *import* imports the configuration on the selected firewalls.

After the configuration is transferred, all firewalls have to be rebooted to recognize the new user list.

All firewalls now have the new account.

You can select following parts for your standard configuration:

- Client Users - User accounts of the administration client
- Reporting Accounts - Accounts for reporting mails
- Rules - Rules of the firewall (be careful!)
- QoS Settings - QoS Settings
- Webblocking Lists - Lists used for the URL-filter
- Proxy Settings - Configuration of the proxy
- User Authentication Settings - UA settings
- Local Authentication Settings - Local users of UA
- NTP Settings - Settings related to NTP
- IDS Settings - Settings related to IDS
- Antivirus Settings - Settings related to Antivirus
- External Access Settings - External access via Administration Client or SSH

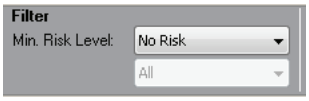
5.2 Sorting and filtering

Groups of firewalls are listed in the left part of the Command Center.

This groups can be separated by None (alphabetically), City, Country or Company.

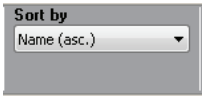
If the Command Center is used with many (> 10) firewalls, the overview can easily suffer. To get the overview back, the Command Center is able to sort the firewalls. This function can be activated using the filter-icon. If you activated the function, a new bar is displayed at the bottom. Here you can filter, sort and search.

Filter



If you configure the filter as in the example, only firewalls which have problems with resources are shown in the overview. All other firewalls are hidden. If a firewall gets problems with their resources in the future, it will be shown in the overview. You can define the minimal risk level and select the source of the problem.

Sorting



With the sorting function, it is possible to list firewalls with problems first. If a firewall gets problems, it automatically gets on top of the list.

Search

If you have many firewalls, you can use the search to find the desired firewall faster.

6 MAP VIEW

The map view is an overview for the firewalls and administrators which can be displayed as icons on a configurable background. Maps of Germany and Europe are included but you can also define own images as background.

6.1 Symbols and lines

Like in the Administration Client, you will find icons of computers, users, regions and info-areas in the map view.

Arrow-icon is the selection tool.

If you have activated this tool, you can select a firewall with a single click (for example to move it) or open the details window with a double click. If you drag an area over more than one icon, all icons within the area were selected.

Connection-icon

This icon is a connection tool. If it is activated you can connect firewalls together or link users to firewalls. If you created a connection, the VPN-wizard opens up. The complete procedure is described in chapter 7.

Zoom-icon

With this tool, you can select areas of the map and zoom them in. Select an area from the upper left to the lower right and the selected area gets zoomed. If you select an area from the lower right to the upper left the map gets zoomed back to 100%. Double clicking on a firewall icon zooms in the firewall and shows its desktop.

The **red computer icons** symbolize firewalls.

You can drag one of the icons on the map and select a firewall in the following dialogue. Also you can drag a firewall from the list of firewalls on the map.

User-icons symbolize roadwarriors.

These icons are for users which connect to the firewalls using VPN (SSL or IPSec).

Region- and Info-icon

With these icons, you can create colored backgrounds or info-areas on the map as in the Administration Client.

6.2 Zoom

The map view offers the possibility to zoom in or out on different areas.

You can use the zoom tool as described in 6.1 or simply scroll using your mouse wheel on the map view.

In the lower left of the Command Center, you will find a thumbnail view of the map. You can also select the zoom level using the slider below. The blue border can be used to change the view on the map. If you zoom in very close on a firewall, the desktop of the firewall will be shown instead of the firewall icon.

7 VPN

7.1 Site-to-Site

Select a firewall and another one. The VPN-wizard opens up which leads you through the configuration of a Site-to-Site connection.

IPSec

Here you can choose between a PSK- (Pre Shared Key) or a certification based IPSec Site-to-Site connection.

The wizard leads you step by step through all relevant settings. If necessary, you have to create certificates. If all steps are done, the configuration and, if necessary, the certificates were transferred to all participating firewalls.

A new line between the firewalls is now visible on the map. This line may be red (connection has a problem or isn't already established) or green (connection is established and ready).

SSL

Like with IPSec, you can also create a SSL Site-to-Site connection. Again, the VPN-wizard leads you step by step through all important settings for a SSL-VPN connection. You have to create certificates (if you haven't done this already) and select the networks which should be connected.

If all steps are done, the configuration and, if necessary, the certificates were transferred to all participating firewalls.

Existing connection

If you already have an IPSec or SSL connection between the selected firewalls, it gets recognized automatically and a connection line is shown on the map.

7.2 Roadwarrior (Client-to-Site)

If you connect an user icon with a firewall, a wizard opens up which leads through the configuration of a Client-to-Site VPN connection.

IPSec and SSL-VPN are available like in a Site-to-Site connection.

IPSec

Here you can choose between a PSK- (Pre Shared Key) or a certification based IPSec Client-to-Site connection. If you choose the certification based connection and haven't already created certificates, the wizard leads you step by step through the creation of the certificates.

If all steps are done, the connection may be exported into a gpcs-file for use with the gateProtect VPN Client.

SSL

Like with the creation of an IPSec connection, the wizard leads you step by step through the setup of a certification based SSL-VPN connection.

If all steps are done, the connection may be exported into a gpcs-file for use with the gateProtect VPN Client.

Existing connections

If you already have a Client-to-Site connection, the Command Center recognizes them. You can export a gpcs-file for use with the gateProtect VPN Client.

If you have created the Client-to-Site connection, a connection line will be shown between the user icon and the firewall icon.

A *red* line implies that the connection isn't (already) established or a problem exists.

A *green* line implies that the connection is established and ready.

8 LICENSING THE COMMAND CENTER

To license the Command Center, click on *Info* > *Change license* and load your license file.

You will receive a license file when you buy one.