



# Getting started with gateprotect **First Installation Guide**

Installation and First Configuration of  
Next Generation UTM and Firewall Appliances

May 2013

Thank you for choosing a

## gateprotect Next Generation Firewall

IT security is an indispensable foundation for smoothly running business processes - regardless of the size of business and the particular industry. The number of daily cyber-attacks is constantly increasing. Almost every device is connected with others, and the flow of information is difficult to control. The widespread use of mobile terminal devices has only served to increase the threat. Loss of data can have devastating operational, financial and legal consequences, may cause considerable damage to a company's image, and could even jeopardise its continued existence.

This is why a committed, international team of top-quality, experienced specialists at gateprotect works on innovative solutions: to provide optimum support for our customers' business processes and to reliably protect their data. gateprotect solutions set new standards in operability, and in the configuration of complex security systems, providing a competitive advantage through dependable security.

gateprotect AG Germany has been a leading, globally acting provider of IT Security solutions in the area of network security for more than ten years. These solutions comprise **Next Generation Firewalls** with all commonly used UTM functionalities, managed security as well as VPN client systems. To minimize the risk of operator errors in highly complex security functions, gateprotect has developed the eGUI® interface concept. The **patented eGUI® technology** (ergonomic Graphic User Interface) and the Command Center based thereon for the configuration and administration of firewall systems for managed security service providers (MSSPs) increase the factual security in companies and allow for an efficient ongoing maintenance of the systems.

Reputable companies and institutions in more than 80 countries are among the users of about 24,000 installed appliances worldwide. Since 2010, gateprotect has been listed in the renowned **Gartner "Magic Quadrant"** for UTM firewall appliances in the SMB market. For the easy handling and comprehensive security of the UTM firewall solutions, gateprotect was the first German company to be honored with **the Frost & Sullivan Excellence Award**.



*„With an impressive range of features, gateprotect offers security appliance management that will avoid the pitfalls of misconfiguration.“*

**Dave Mitchell, SC Magazine UTM review**

The Next Generation UTM and Next Generation Firewall Appliances by gateprotect combine state-of-the-art security and network features such as firewalls, bridging, VLAN, single sign-on, traffic shaping, QoS, IPSec/SSL (X.509), IDS/IPS, web filters and application control, virus filters, real-time spam detection and a real HTTPs proxy, in a single unified system.

All Security Appliances from gateprotect are characterized by optimal scalability, security and performance. Thanks to a unique and patented eGUI<sup>®</sup> technology, gateprotect sets standards when it comes to the configuration of modern security systems. gateprotect's eGUI<sup>®</sup> technology raises operating security and efficiency to a previously unattained level.

**This guide will walk you through the very first steps of the firewall installation & setup:**



## 1. Installation of the latest Firmware



Your firewall appliance arrived pre-installed with gateprotect firewall firmware. To ensure you have the latest up-to-date security solution (including all the latest security patches), we recommend upgrading the firmware before you go ahead with the configuration.

**The latest firmware version is available here:**

<http://start.gateprotect.com>

### Step 1 | Preparation

To upgrade the firewall firmware, you will need:



- Blank USB flash drive (suggested size is between 512MB and 4GB)

The following are not required if you are performing an unattended install:

- *Serial cable (or a serial to USB converter cable if your workstation does not have a serial port available)*
- *Workstation with terminal software installed (e.g. PuTTY or Hyperterm)*

Insert the USB flash drive to your workstation.

#### **Important Note**

*Please make sure that no important data is left on this USB flash drive. It will be formatted and all data will be lost.*

## Step 2 | Download the USB installer

The "USB installer" is an executable file containing the latest firmware, and is available for download here:  
[start.gateprotect.com](http://start.gateprotect.com)



### Step 3 | Run the USB installer

By running the USB installer program, a wizard will guide you to create a bootable USB flash drive.

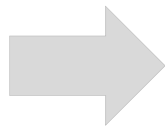
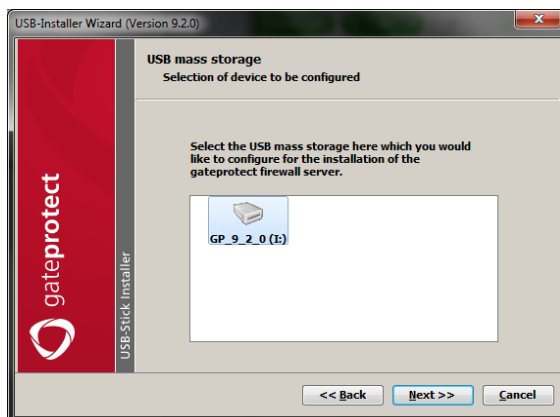
#### **Important Note**

*Please make sure that you do not restart your workstation with the newly created bootable USB flash drive connected, as it could wipe your workstation and replace it with the gateprotect firewall firmware!*

- With your USB flash drive inserted to your workstation, run the downloaded “USB installer” file. Select your language and click next.
- Review and accept the license agreement

#### **Select your USB flash drive**

The USB installer will scan your PC for available flash drives to install to.



#### **and confirm**

Please check that the drive letter is correct if you have multiple flash drives connected. You will receive a warning that all data on the flash drive will be deleted. Confirm and click **Next**.



## Step 4 | Backup files and unattended installations

With an unattended installation you can add previously created backup files.

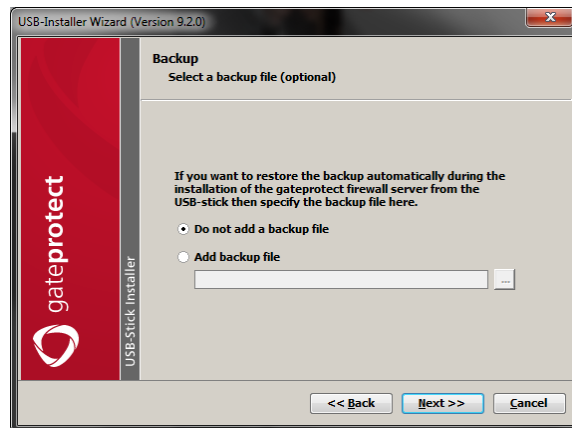
Adding the backup file will automate this installation to include the settings of the previous configuration so no additional interaction will be needed for the installation.

### If you wish to run an unattended installation

A “Default Configuration Backup” file is available here:

[start.gateprotect.com](http://start.gateprotect.com)

### Select “Add a backup”



Locate the backup file on your workstation and click **Next >>**

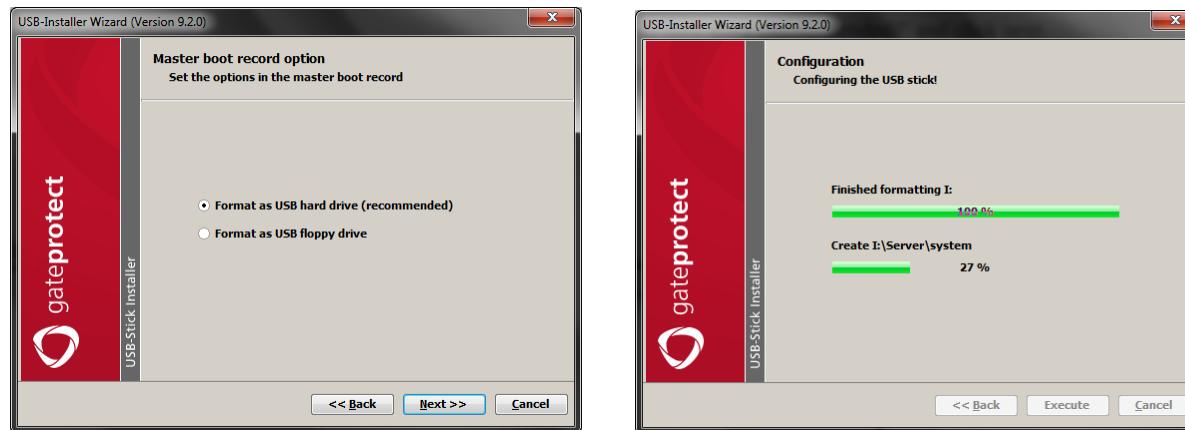
If you **DO NOT** wish to run an unattended installation:  
Select **“Do not add a backup”**

Click **Next >>**

## Step 5 | Format your USB flash drive

Select **format as USB hard drive (recommended)** and click **next**.

A quick format can be selected, click **next**. The USB installer will now format the USB flash drive and start creating the bootable installation.



After completion, click Finish and safely remove the USB flash drive from your workstation.

### ATTENTION

Please be aware that the USB flash drive will automatically boot on any computer and could install the firewall firmware, wiping the computer!

*If you chose an unattended installation, please skip directly to **Step 8***



## Step 6 | Connect your workstation to the firewall

After preparing the bootable USB flash drive, use the serial cable to connect your workstation to the serial port of the gateprotect appliance which is labeled "**CONSOLE**".

Start the terminal program (PuTTY or Hyperterm) using the following parameters:

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

- Select connection type to be **Serial**
- Select the com port number the serial cable is connected to.

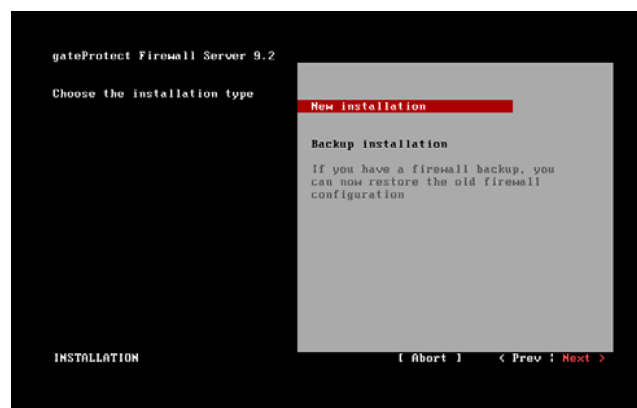
## Step 7 | Complete installation

Insert the newly created bootable USB flash drive into your gateprotect appliance and reboot (power-cycle). After a few seconds the installation dialogue will appear within the dialogue of the terminal program on your workstation. Using the keyboard, you can now define the settings and complete your gateprotect appliance firmware upgrade.

### 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.

Choose your keyboard layout → Accept Licence Agreement → Select new installation

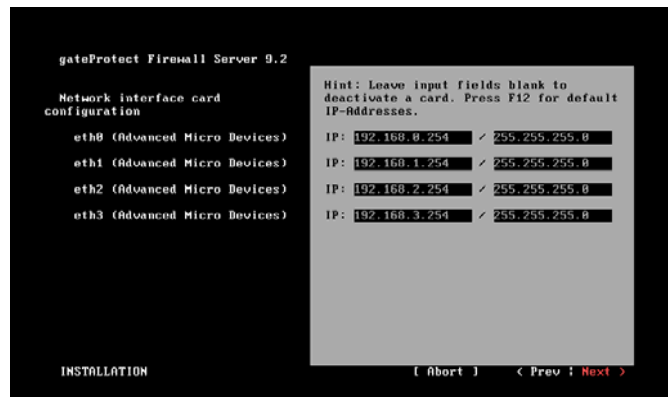


### Installing a Backup Configuration

If you did not opt for the **unattended installation** outlined above, you can restore a backup of a previous gateprotect firewall configuration now. Place the backup file on a separate USB flash drive and connect it to the appliance. Alternatively, you can also skip the backup at this point and apply it after installation, using the **Administration client**.

## Step 7 |

## Interface addresses



At the next screen you will be asked to insert the IP address for each interface. For the default configuration you can hit F12 and the default IP addresses will be loaded.

Select **Next >**

**NOTE**

DHCP cannot be selected in the installation. On completion you would need to configure your PC to match the interface settings to which you will be connected.

Leaving the fields empty, will deactivate the interface.

## Set Hostname and Domain name and Password.



Hostname and domain name are especially important if you plan to use the SSO feature, these settings can be changed later via the Administration client and can be left default for factory default installations.

The password created here is for the user **root**, on the console. This password will be changed.

Step 7 |

**The hard disk will be formatted**

At the next screen you will be prompted that the hard disk will be formatted.

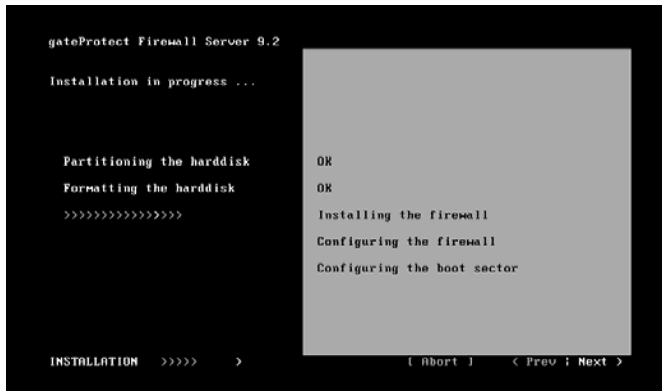


Select **[Yes]** to continue.

The setup will start to partition and format the hard disk after which the firewall will be installed and configured.

**Confirmation of completed steps**

Once completed you will see all steps listed as OK.



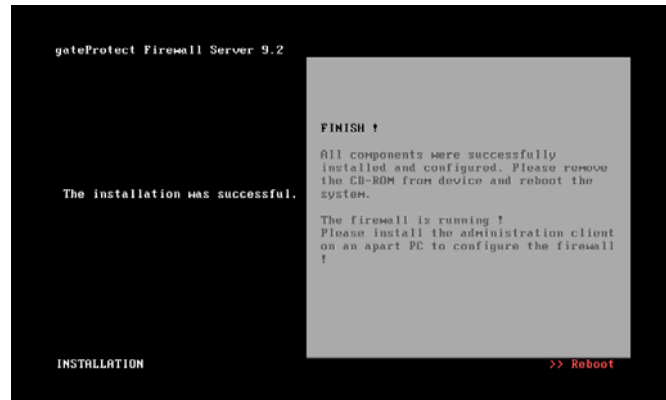
Select **Next >** to continue.



## Reboot

Disconnect all USB flash drives from the appliance.

On rebooting the appliance, the firmware upgrade and setup will be complete.



## Step 8 | Complete unattended installation

Insert the newly created bootable USB flash drive into your gateprotect appliance and reboot (power-cycle).

After some time your gateprotect appliance will beep.

### Beeps

The length of time before the beep depends on the appliance type and hardware specifications.

Completion of the installation process is indicated by a long beep whilst booting the firewall is indicated by a short beep.

Remove the USB flash drive and reboot the firewall.

Settings from the previous backup will be restored and the gateprotect firewall will be ready for use.

## 2. Installing the Administration Client

Step 1  
Download  
Administration Client

Step 2  
Install  
Administration Client

### Step 1 | Download the Administration Client

Please download the appropriate administration client version according to your installation.

The administration client software can be found at:

<http://start.gateprotect.com>

### Step 2 | Install the Administration Client

Execute the downloaded file on your PC.

#### NOTE

The Administration client can also be found on the USB flash drive created with the USB installer.



### 3. First Configuration

After the installation of the firewall appliance and the Administration Client, here are the steps for a basic configuration.



#### Step 1 | Run the Administration Client

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.

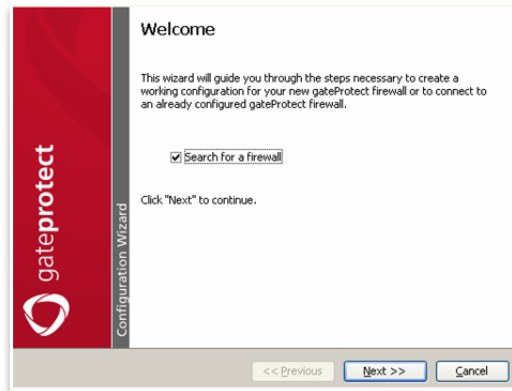
#### NOTE

The Administration Client is only compatible with a matching appliance version. For example, an Administration Client in version 9.2 can only connect to firewall appliances running version 9.2.

However, it is possible to have multiple versions of the Administration Client installed on the same Windows PC. You will be alerted if you try to connect with the wrong version of the Administration Client, and asked to start the correct version.



## Step 2 | Search for the firewall



The start window of the Configuration Assistant is displayed. You can search for a firewall appliance in your network by activating the **“Search for a firewall”** box.

The Configuration Assistant will only search for the firewall appliance in the network of the computer on which the Administration Client was installed. It will try the first (xxx.xxx.xxx.1) and last IP address (xxx.xxx.xxx.254) in this subnet.

If the Configuration Assistant finds the firewall appliance on one of the two addresses, you can skip directly to *Step 4 - First configuration in quick mode.*

If the Configuration Assistant does not find the firewall appliance on either of the two addresses, you must enter the address of the firewall appliance manually as described in *Step 3.*



## Step 3 | Firewall server's IP address

If the Configuration Assistant was not able to find the firewall, it will ask you to enter the IP address manually.

The login dialogue opens in order to create a manual connection. Clicking on the **Add** button, will open a new dialogue as shown below.

- Enter the name and address of the firewall appliance in the appropriate fields. Leave the Port unchanged (Port 3436) and click on Apply.
- The Login dialogue is displayed again. Enter the appropriate values for access to the firewall appliance in the user name and password fields. Then click on **Login**.

### Default Username & Password

When accessing the firewall appliance the first time, the default username is **admin** and default password is **admin**. You should change this as soon as possible. If you have installed the firewall appliance using a backup, use the user name and associated password set up for this backup.

The connection to the firewall appliance is now established and the Configuration Assistant continues with the selection of the configuration mode.

## Step 4 | First configuration in quick mode

First Configuration in Quick Mode creates a basic setup, which must be refined later on. The Quick Mode involves the configuration of an Internet connection and



gives access to some basic services into the Internet.

Choose the Quick start option and click the **Next** button.



Choose desired functions.

This will create some basic rules for all of your local networks attached to your firewall appliance, i.e. permitting HTTP, HTTPS and DNS access into the Internet.

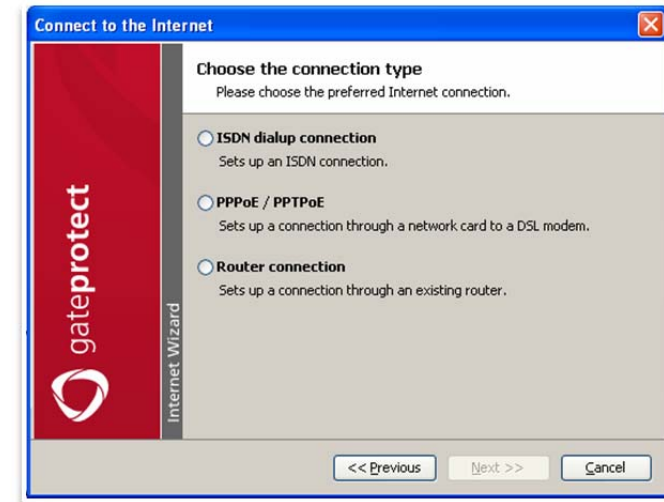
Click **Next >>**

## Step 5 | Connect to the Internet

The gateprotect firewall appliance supports the following connections to the Internet:

- A - PPPoE/PPTPoE
- B - Router connection
- C - ISDN dialup

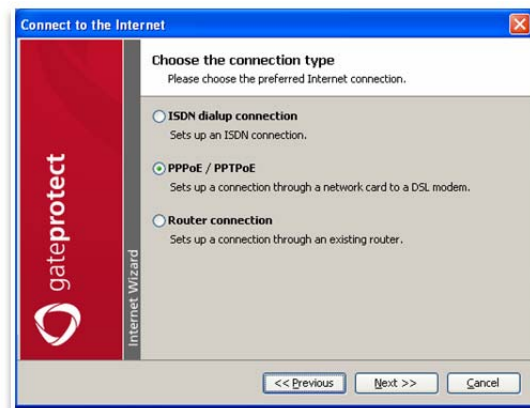
Depending on which Internet connection you use, please follow the corresponding configuration steps in the next chapters.



### A. Setting up a PPPoE connection

The following steps will setup an Internet connection using a DSL modem directly attached to one of the interfaces of the firewall appliance. If you have a DSL modem with an integrated router, please make sure, the router functionality is deactivated.

- Select the option **PPPoE / PPTPoE** in the dialogue box.
- Select the network card the DSL modem is connected to.



### STATIC IP ADDRESS

The network card the DSL modem is connected to must have been assigned with a static IP address. If you have not configured your interfaces during the installation, you will still need to do that after finishing the initial configuration.

Step 5 | Enter the User data given by your Internet service provider.



The screenshot shows the 'Connect to the Internet' wizard window. The title bar reads 'Connect to the Internet'. The main content area is titled 'User data' and contains the instruction 'Enter the user data received from your provider.' Below this, there is a text input field for 'Username' with the placeholder text 'username@provider.com' and a password input field with masked characters '\*\*\*\*\*'. A checkbox labeled 'Show password unencrypted' is located below the password field. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Through the Timeout function, choose whether you wish the DSL line to always stay online, or if it should be disconnected after a specific idle time without any data sent on the line.



The screenshot shows the 'Connect to the Internet' wizard window at the 'Dial-up settings' step. The title bar reads 'Connect to the Internet'. The main content area is titled 'Dial-up settings' and contains the instruction 'Make additional settings here.' Under the 'Timeout' section, there are two radio buttons: 'Stay always online' (which is selected) and 'Disconnect the unused connection after the timeout has expired.' Below these is a spin box for 'Idle time (sec.):' set to '300'. Under the 'Connection type' section, there are two radio buttons: 'PPPoE' (which is selected) and 'PPTPoE'. Below this is a text input field for 'IP address of the modem:' with three dots '...' as a placeholder. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

This is especially useful, if you have a time based contract with your ISP.

The connection type should usually be set to **PPPoE**. ISPs use **PPTPoE** only in some cases. Please contact your ISP, if you are unsure, which protocol to use.

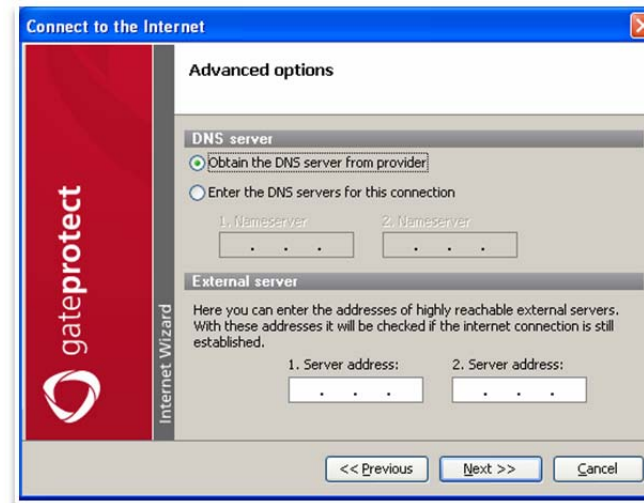
#### NOTE

If you set the Timeout function to disconnect after a specific idle time, please do not set any external servers and deactivate the NTP service on the firewall appliance.

## Step 5 | DNS Servers

If you don't want to use the DNS servers from your Internet provider, you can manually add two DNS servers in the advanced option. Otherwise, the firewall appliance will use the DNS server provided during the dial-up process.

The **External servers** are used for monitoring the state of this Internet connection. You should only enter IP addresses here, when you have a dedicated backup Internet connection. The servers entered here, should be hosted by different providers and must answer on ping requests. The firewall appliance will send out those ping requests on a regular basis and will switch to your backup Internet connection when both ping requests fail.



### Name your DSL connection

Enter a clear and meaningful name for the DSL connection, e.g. "Internet connection via DSL modem" and click on **Finished**.

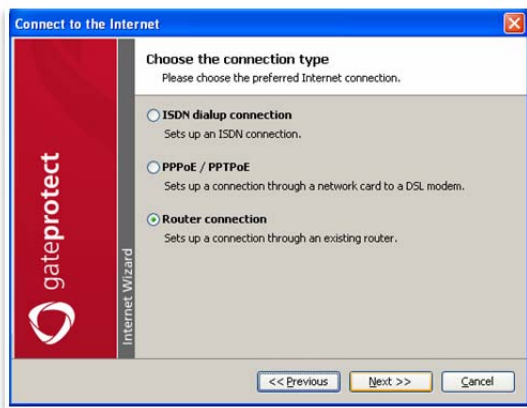
Now skip directly to

*Step 6 - Changing the Administration Client Password.*

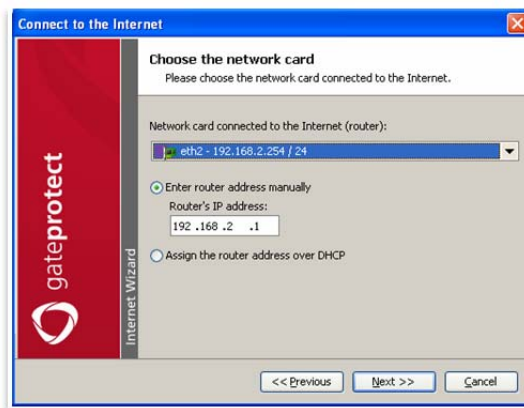
## Step 5 | B. Setting up a Router connection

The following steps describe the setup of an Internet Connection using a router. Please make sure, you know the local subnet which is used on the connection between the firewall appliance and the router. If you have been provided with a range of fixed IP addresses by your ISP, please have a look at *Step 7 - Setting up an Internet connection with fixed IP addresses*

Select the option **Router connection** in the dialogue box.



Please select the network card the router is connected to and specify the IP address of the router.



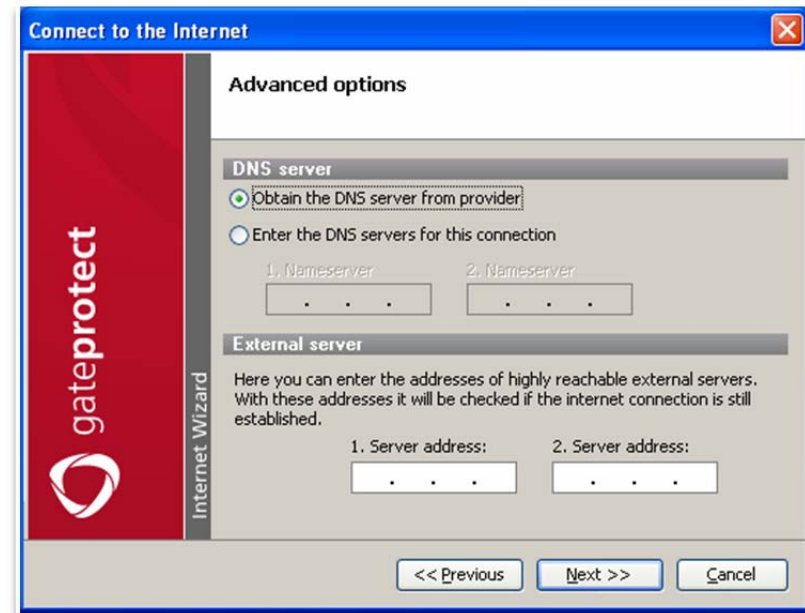
If the router is set to provide addresses via DHCP, you can select **Assign the router address over DHCP**.

### NOTE

The interface you select here must have been assigned an IP address in the same subnet as your router. You can change the subnet later through the Administration client.

**Step 5 |** When you set the DNS server option to **Obtain the DNS server from provider** please make sure, your router is providing valid DNS server addresses through DHCP. Of course you can also manually provide two DNS servers here.

The **External servers** are used for monitoring the state of this Internet connection. You should only enter IP addresses here, when you have a dedicated backup Internet connection. The servers entered here, should be hosted by different providers and must answer on ping requests. The firewall appliance will send out those ping requests on a regular basis and will switch to your backup Internet connection when both ping requests fail.



#### **Name your Router connection**

Enter a clear and meaningful name for the router connection, e.g. "Internet connection via router" and click on **Finished**.

Now skip directly to  
*Step 6 - Changing the Administration Client Password.*

## Step 5 | C. Setting up an ISDN connection

- Select the option **ISDN Dial-Up Connection** in the dialogue box.
- A list of the available ISDN hardware is shown now. Choose one of the ISDN cards from the list.
- 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.
- Enter the access data for your ISDN Internet connection given by your internet service provider.
- 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.
- If you don't want to use the **DNS servers** from your Internet provider, you can manually add two DNS servers in the advanced option. Otherwise, the firewall appliance will use the DNS server provided during the dial-up process.

The **External servers** are used for monitoring the state of this Internet connection. You should only enter IP addresses here, when you have a dedicated backup Internet connection. The servers entered here, should be hosted by different providers and must answer on ping requests. The firewall appliance will send out those ping requests on a regular basis and will switch to your backup Internet connection when both ping requests fail.

### NOTE

When you set the **Timeout** setting to disconnect after a specific idle time, please make sure, you don't set any external servers and deactivate the NTP service on the firewall appliance.

- Select the corresponding options or enter the data in the appropriate fields and click on **Next**.
- 
- Enter a clear and meaningful name for the ISDN connection, e.g. "Internet connection via ISDN" and click on **Finished**.

Now skip directly to

*Step 6 Changing the Administration Client Password.*

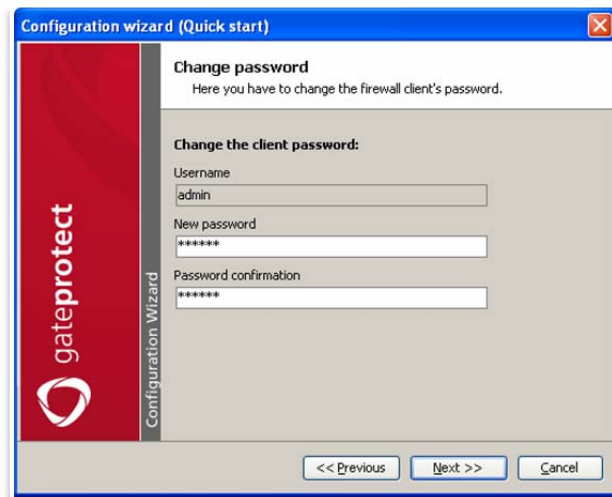


## Step 6 | Changing the Administration Client Password

After setting up your Internet connection through the Quick start wizard, you will get a warning from the wizard, asking for your confirmation.



After confirming you will be asked to change your Administration client password.



### The Administration client password

Must contain at least 6 characters, and may include upper and lower case letters, numbers and special characters.

## Step 7 | Setting up an Internet connection with fixed IP addresses

Setting up an Internet connection with fixed IP addresses is only possible after the initial configuration, as you have to change your interface configuration.

### An Example

Let's say that the following subnet details have been assigned to you by your ISP.

Subnet:	216.239.37.96 / 29 or 216.239.37.96 / 255.255.255.248
Network address:	216.239.37.96
Router of the provider:	216.239.37.97
Own use:	216.239.37.98 – 216.239.37.102
Broadcast address:	216.239.37.103

### Step A

This network is divided into the following sections

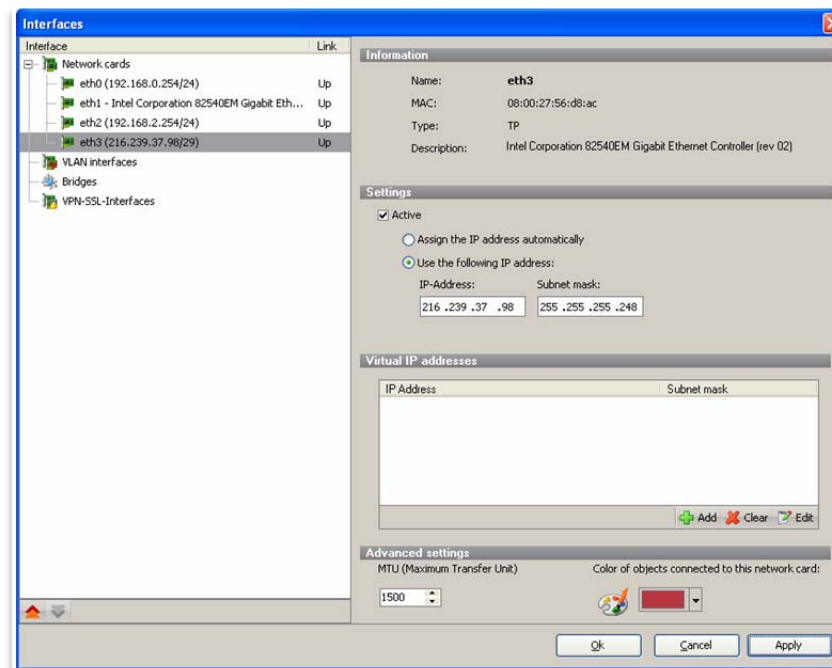
The given network is a 29Bit IP address range. You have eight IP addresses but you can only use five for addressing. Two of the eight addresses have been used for network logic (network address and broadcast address) and one IP address is assigned to the router of your provider. This is usually the first IP after the network address.

### Step B

To be able to set up an Internet connection through the router, the firewall has to be configured with one of the remaining addresses assigned by the provider.

Open the **Options** menu and click on **Interfaces**.

Select the interface which is connected to your router (we use eth3 for this example) and configure the IP address 216.239.37.98 with the subnet mask 255.255.255.248. Apply your settings and close the dialogue.



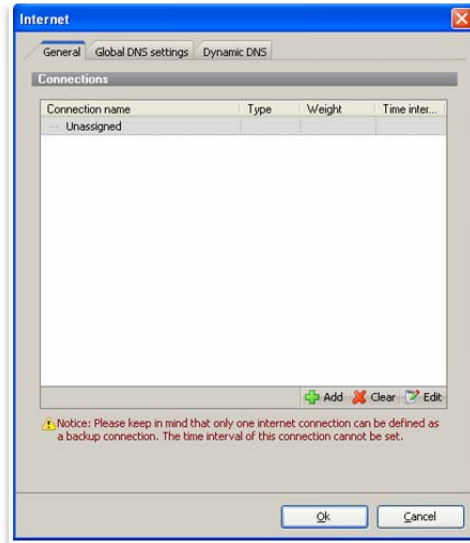
### NOTE

If you plan to use the other available IP addresses for DMZ configurations, you have to enter them as virtual IP addresses on the same interface.

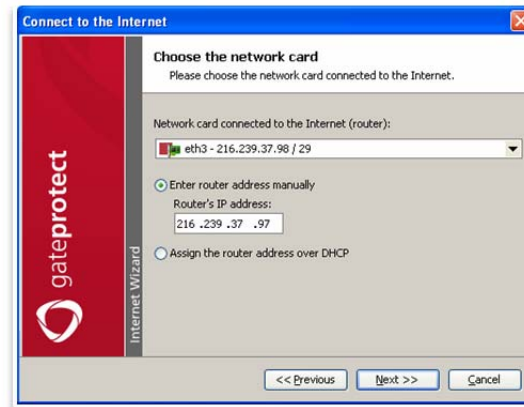
**Step 7 | Step C**

The interface is now ready to communicate with the router. However, we have not configured the firewall to use the router as a default gateway, yet. To do so, Drag & Drop an Internet connection symbol from the toolbar to the desktop of the Administration client.

This will open up the Internet connection dialogue.

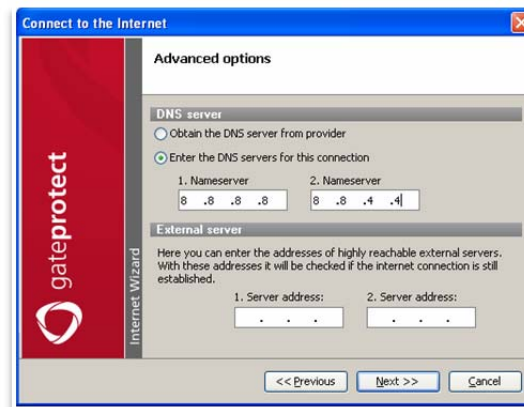


Clicking on the **Add** button will open the Internet connection wizard. Select Router connection and click on **Next**.



From the list of interfaces select the one which is connected to the router and has been configured with a static IP address before.

In the field **Enter router address manually** you have to specify the IP address of the router of your provider. In our example: 216.239.37.97.



Click on the **Next** button and enter two DNS servers.

If you don't have the IP addresses of your providers DNS servers, you can use the google DNS servers 8.8.8.8 and 8.8.4.4.

**Step 7** | The External servers are used for monitoring the state of this Internet connection. You should only enter IP addresses here, when you have a dedicated backup Internet connection. The servers entered here, should be hosted by different providers and must answer on ping requests. The firewall appliance will send out those ping requests on a regular basis and will switch to your backup Internet connection when both ping requests fail.

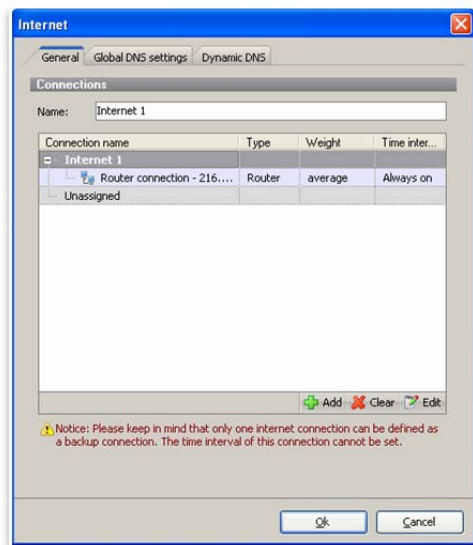
#### NOTE

If you want to use the option **Obtain the DNS server from provider**, you have to make sure the router of your provider is supplying these information using DHCP. If you're not sure about this, use the above mentioned publicly available DNS servers.

In the last step, provide a meaningful name for you Internet connection and click on **Done**.



You will get back to the Internet connection dialogue, where you have to make sure, the newly created Internet connection has been assigned correctly as shown below.




Clicking on **OK** will save you settings and activate the Internet connection.

## Step 8 | DMZ & Port Forwarding

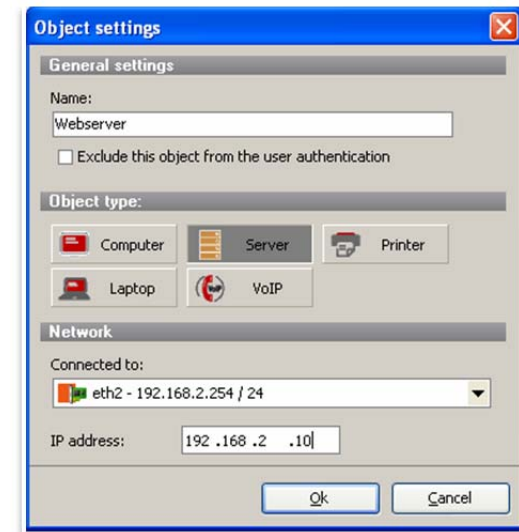
### A. Simple Port Forwarding

In most cases, forwarding of a single or a few ports is desired to provide access to a web server from the internet.

#### Step A

Drag & Drop a server symbol  from the toolbar to the configuration desktop.

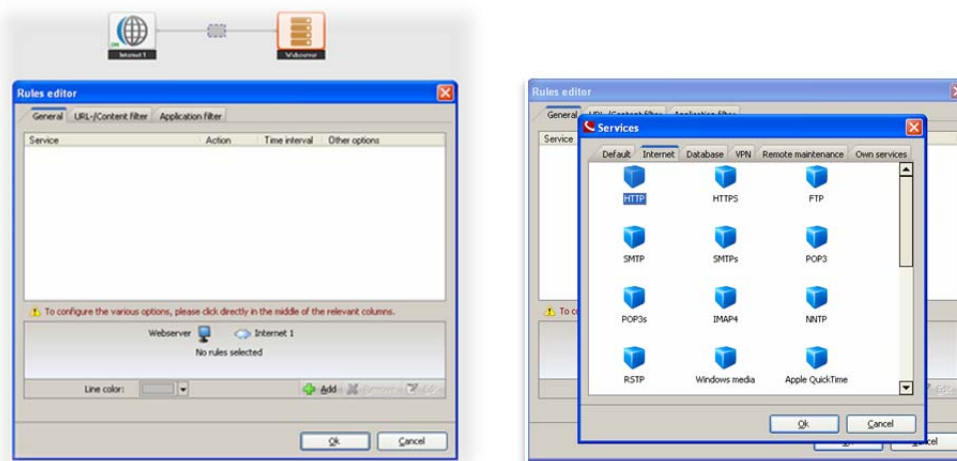
This will open the Object settings dialogue. Provide a name, select the network card the local server is connected to, enter the local IP address of the server, and click **OK**.



#### Step B



Back on the configuration desktop, select the Connection tool, click on the new symbol for the web server, and click on the Internet symbol. This will open up the Rules editor.

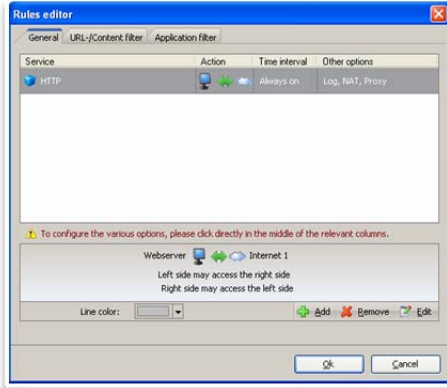


Clicking on the **Add** button will open the list of Services, where we select **HTTP** from the **Internet** tab and click on **OK**.

This will add the HTTP service to the rules editor.

### Step C

The rule added by the Administration client is not yet correct. As you can see from the symbols in the **Action** column, this rule allows new connections coming from the web server. However, we want new connections coming from Internet 1.

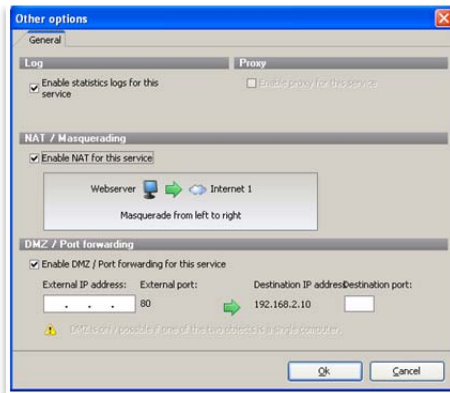


Clicking in the arrow will change the direction, so the server can be accessed from the Internet. Clicking a second time will create a double arrow, allowing both connections from the web server to the Internet and connections from the Internet to the server.

In our example, we allow bidirectional communication.

### Step D

Clicking on the **Log, NAT, Proxy** in the **Other options** column in the HTTP row, will open the Other options menu. First, deactivate the proxy setting, and then tick the box for **DMZ / Port forwarding**. Then re-enable the **NAT / Masquerading** option and make sure, the arrow is pointing to the Internet symbol.



Please leave the entry fields blank in this section.

Click on **OK** to accept the settings.

**Step E**

Once the Rules editor is confirmed with **OK** and configuration has been activated using **F9**, all data designated 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.

**B. Port Forwarding with Port Re-routing**

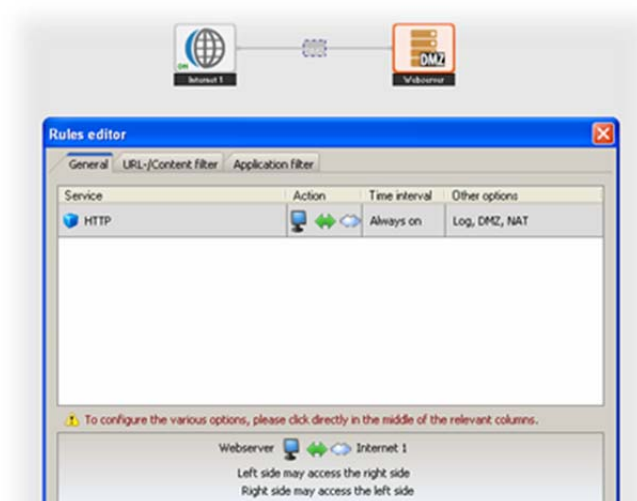
Port rerouting can be used to change the destination port of an IP packet.

**Step A**

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). Choose the externally accessible port 10022 which should be forwarded to the web server on port 22.

**Step B**

Click on the rectangle between the web server object and the Internet symbol to open the rules editor.



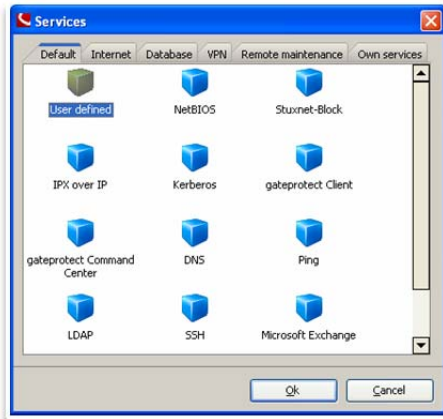
### Step C

Click on the **Add** button to open the Service dialogue.

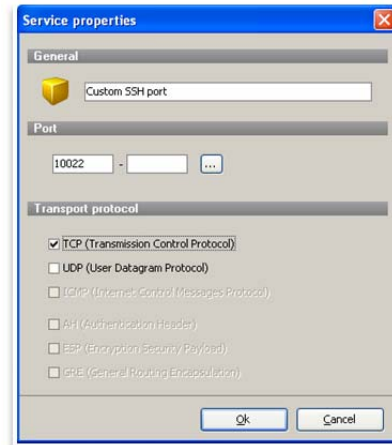
From our example, our connections coming from the Internet will have the destination port 10022, so we need to define a custom service.

Double click on **User defined** in the **Default** tab.

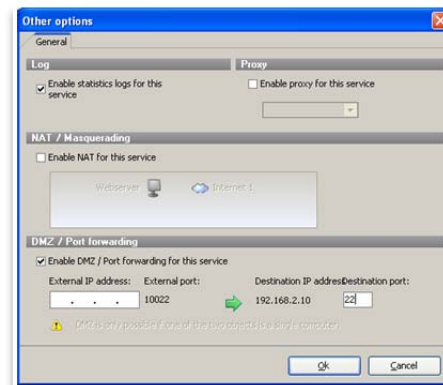
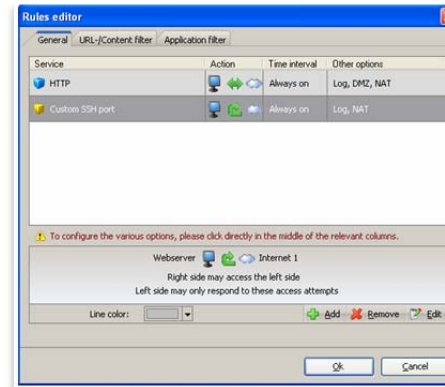
This will open the Service properties dialogue, where you can setup your own service now.



Enter the data as shown and click **OK**.



Back in the **Rules editor** you have to change the direction in the **Action** column, to allow access from the Internet to this internal server.



After changing the direction, double click into the **Other options** column for the newly defined SSH service. In the upcoming dialogue activate the option **Enable DMZ / Port forwarding for this service**, enter the port 22 in the **Destination Port** field, and click on **OK**.

Accept your changes to the Rules editor and activate your configuration using **F9** or the **Activate** button in the toolbar.

Step 4 described how to configure a static IP address for your Internet connection. The IP address belonged to a bigger subnet and for the following configuration we will use some additional IP addresses out of this subnet.

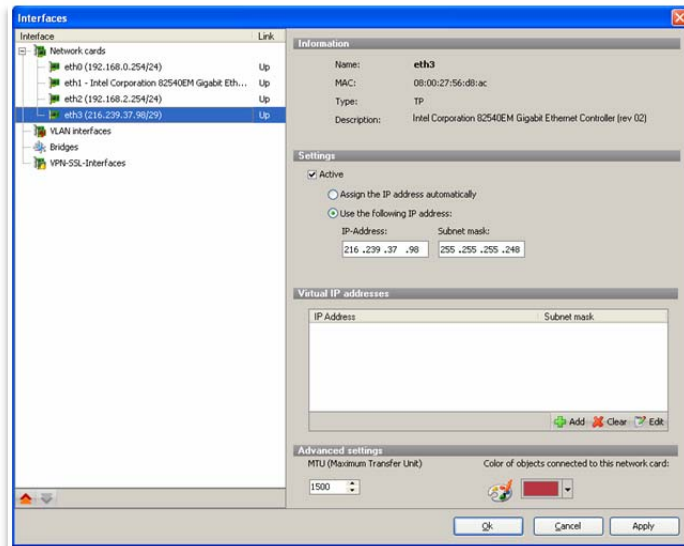


## DMZ by Source IP

We will add two additional IP addresses to the firewall configuration to make the appliance aware of these IP addresses, so she can handle the traffic, e.g. forward it to internal servers.

### Step A

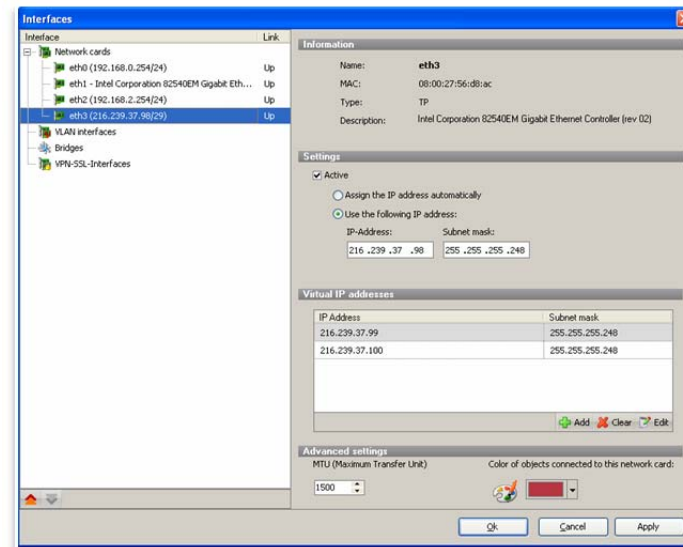
Open the menu **Options** and click on **Interfaces**.



Select the interface which has been configured with the static IP address (eth3 in our example).

Now click on the **Add** button and enter the additional IP addresses, e.g. 216.239.37.99/255.255.255.248.

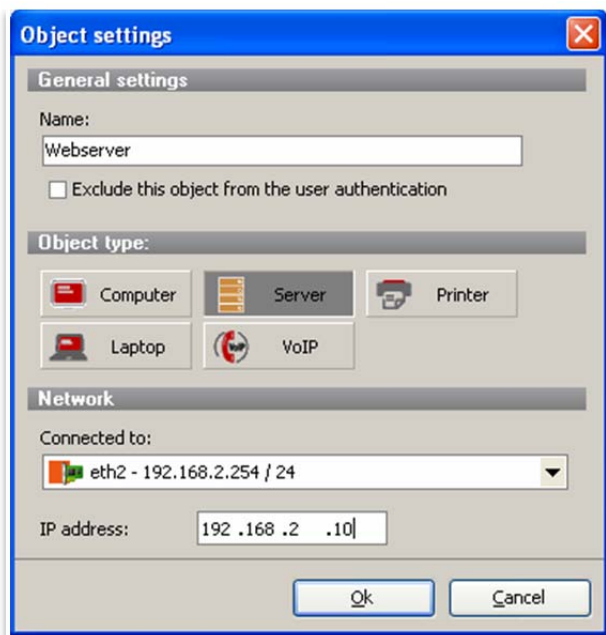
For our example we will also add 216.239.37.100/255.255.255.248.



Save your settings by clicking on **OK**.

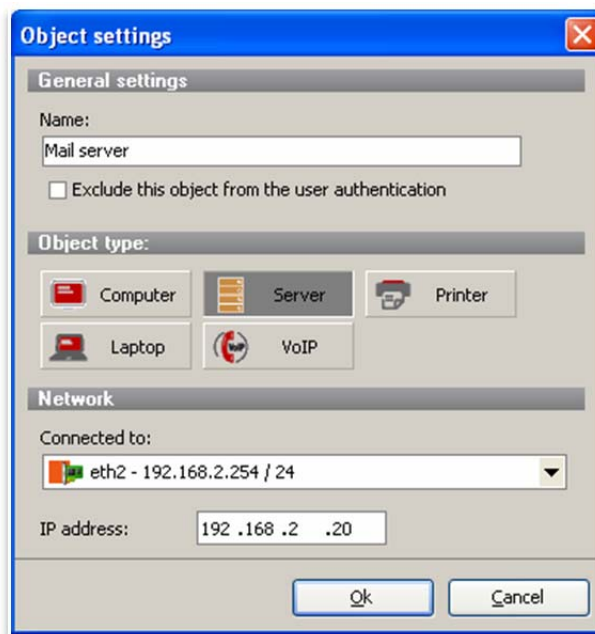
The gateprotect firewall is now configured for these additional IP addresses.

## Step B



Drag a server symbol from the tool bar to the configuration desktop, select the network card the server is connected to, and enter the internal IP address of the server (192.168.2.10 in our example).

We create a second server object on the configuration desktop, this time for our mail server (IP address 192.168.2.20).



For a better overview on the configuration desktop, clear names have been assigned to the symbols (e.g. web server and mail server).

## Web server

### Step A

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 B

By 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!

#### ATTENTION

When connecting the two symbols, you must first click on the internal computer and then on the external computer

### Achieve separate access to the web server internally using the DNS name

If a web server has been set up like the above example, this can still only be internally accessed from using its internal IP address.

However, some applications demand the host name of the computer, e.g. [www.your-company.com](http://www.your-company.com).

To avoid service or changing the name server entries, it is possible to realize this with the gateprotect firewall.

You can do this by creating 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

A mail server normally acts like an HTTP-DMZ. However, there are special cases where it is necessary 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 A

For this purpose, the internal mail server is set up as an individual server symbol.

### Step B

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.

### Step C

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.



### **Congratulations!**

You finished the first configuration of your gateprotect Next Generation UTM and Firewall successfully.

If you need any further assistance please contact your next certified gateprotect partner or get in contact with us:

[sales@gateprotect.com](mailto:sales@gateprotect.com)

For more Information please also visit our website:

[www.gateprotect.com](http://www.gateprotect.com)

gateprotect is security  
that you can  
really see



#### *Headquarter*

**gateprotect AG Germany**

Valentinskamp 24

20354 Hamburg / Germany

Phone +49 40 278 850

#### *North America*

**gateprotect Inc.**

5201 Great America Parkway,

Suite 320

Santa Clara, CA 95054 / USA

Phone +1 408 730 6858

#### *Africa*

**gateprotect South Africa**

Suite C, Nautica Building, The Water Club,

Granger Bay, Cape Town, 8001

South Africa

+27 21 405 3700