Manual
Workshops (Excerpt)

IP Workshops

Legal Notice

Warranty

This publication is subject to modifications.

bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH is not liable for the information in this manual. bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH accepts no liability for any direct, indirect, incidental, consequential or other damages associated with the distribution, provision or use of this manual.

Table of Contents

Chapter 1 IP - Network Address Translation (NAT)

1.1 Introduction

The configuration of Network Address Translation (NAT) is described in the chapters below.

Network Address Translation (NAT) is a function on your device for defined conversion of source and destination addresses of IP packets. If NAT is activated, IP connections are still only allowed by default in one direction, outgoing (forward) (= protective function). Exceptions can be configured in the **NAT Configuration** menu.

You have a permanent 2-Mbps connection to the Internet with 8 IP addresses. Your Ethernet interface **ETH** is connected to the access router. This has the IP address `62.10.10.1/29`, whereas the remaining IPs from `62.10.10.2` to `62.10.10.6` are entered on Ethernet interface **ETH**.

You configure NAT enables for accessing your gateway over HTTP. You also want to access your terminal server and the corporate web server over the Internet.

Configuration in this scenario is carried out using the **GUI** (Graphical User Interface).

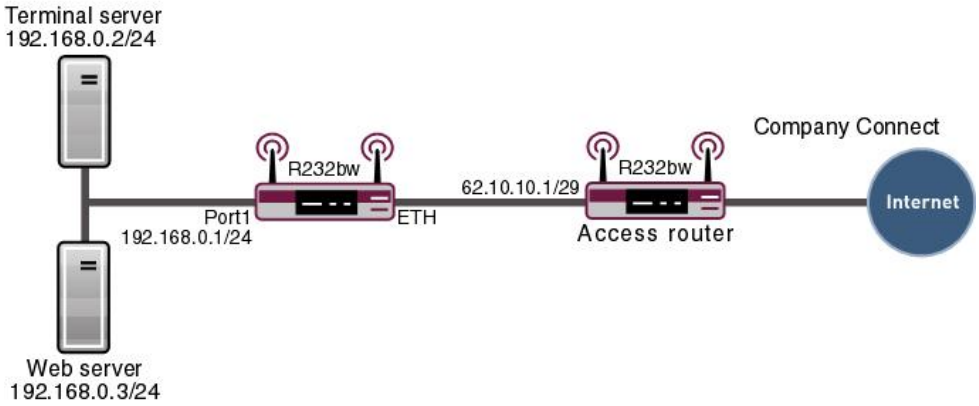


Fig. 1: Example scenario NAT

Requirements

The following are required for the configuration:

- Basic configuration of the gateway
- A boot image of version 7.10.1
- A working Internet access. For example, **Company Connect** with 8 IP addresses.

1.2 Configuration

1.2.1 Enable NAT

A list of all NAT interfaces is displayed in the NAT interface menu.

Go to the following menu to enable NAT for your interface:

(1) Go to **Network** -> **NAT** -> **NAT Interfaces**.

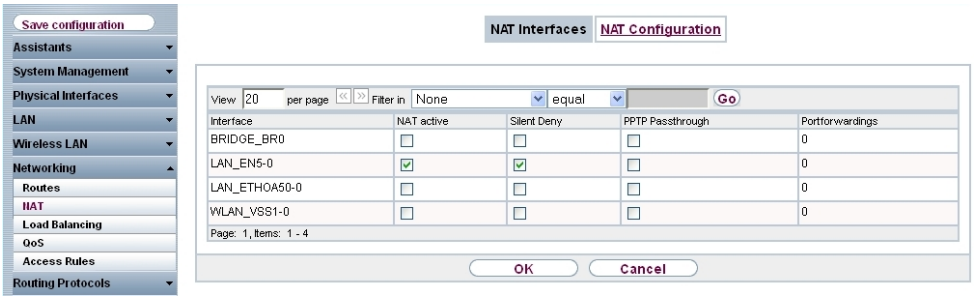


Fig. 2: **Network** -> **NAT** -> **NAT Interfaces**

Proceed as follows:

(1) Select **NAT active** for the `LAN_EN5-0` interface. This is how the NAT feature is enabled for the interface.

(2) Select **Silent Deny** for the `LAN_EN5-0` interface. If this function is enabled, no ICMP packets are answered.

(3) Confirm with **OK**.

1.2.2 Configuring NAT enables

NAT enable for the GUI

It should be possible to administer your gateway using HTTP over the Internet with the permanent IP address `62.10.10.2`. For security reasons use external port `8080`, for ex-

ample, instead of port *80*.

Go to the following menu to configure NAT entries.

(1) Go to **Network** -> **NAT** -> **NAT Configuration** -> **New**.

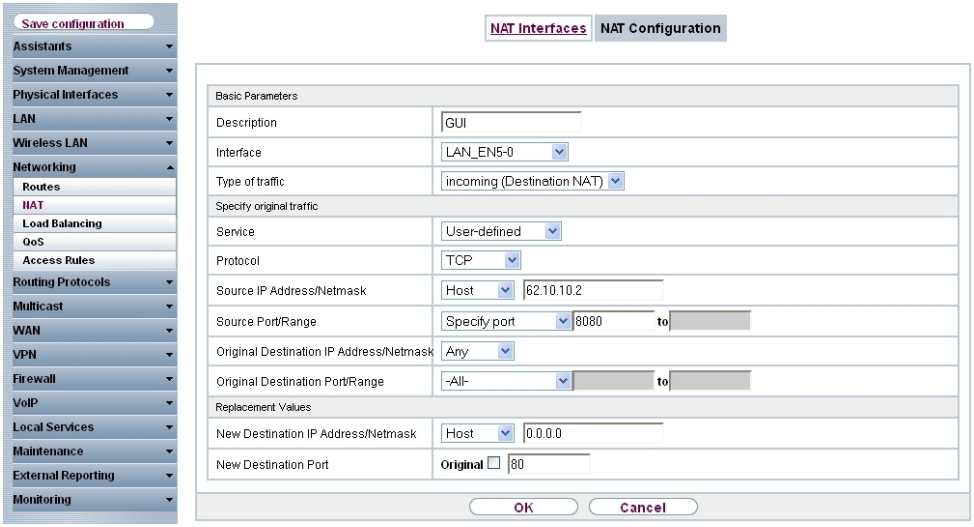


Fig. 3: **Network** -> **NAT** -> **NAT Configuration** -> **New**

Proceed as follows:

(1) Enter a **Description** for the NAT configuration, e. g. *GUI*.

(2) Select the **Interface** for your NAT enable, e. g. *LAN_EN5-0*.

(3) For the **Type of traffic** , select *incoming (destination NAT)*.

(4) Leave the **Service** set to *User Defined*.

(5) Set **Protocol** to *TCP*.

(6) Under **Source IP Address/Netmask** enter the gateway's external IP address, e. g. *62.10.10.2*.

(7) Set the **Source Port/Range** to *Specify Port* and enter *8080*, for example, in the first input field.

(8) Under **New Destination Port** disable **Original** and enter *80* in the input field.

(9) Leave the remaining settings unchanged and confirm them with **OK**.

NAT enable for Web Server

The internal Web server should be reached under the IP address *62.10.10.3*. External default port *80* is used as the Web server serves as a Web host for public websites.

(1) Go to **Network** -> **NAT** -> **NAT Configuration** -> **New**.

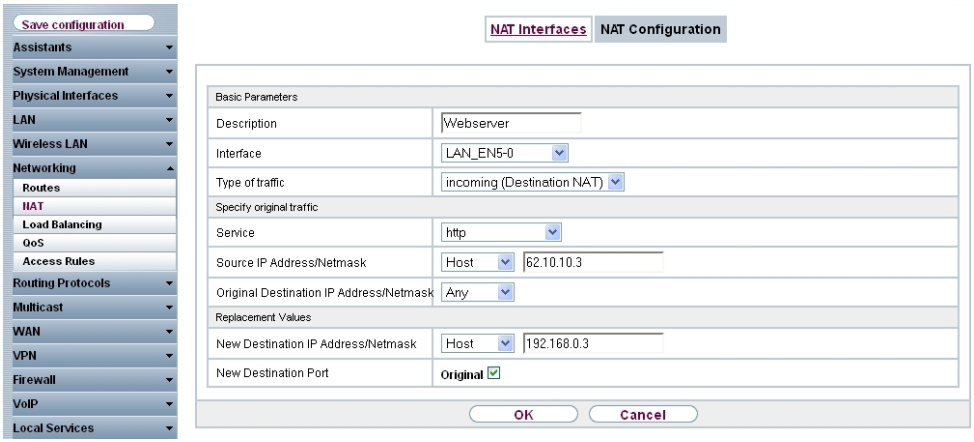


Fig. 4: **Network** -> **NAT** -> **NAT Configuration** -> **New**

Proceed as follows to configure the enable:

(1) Enter a **Description** for the NAT configuration, e. g. *Webserver*.

(2) Set the **Interface** to *LAN_EN5-0*.

(3) For the **Type of traffic** , select *incoming (destination NAT)*.

(4) Configure the **Service** to *http*.

(5) Under **Source IP Address/Netmask** enter the internal web server's IP address, e. g. *62.10.10.3*.

(6) Under **New Destination IP Address/Netmask** enter the internal IP address, for example *192.168.0.3*.

(7) Leave the remaining settings unchanged and confirm them with **OK**.

NAT Enable for Terminal Server

The internal terminal server should be reached under the IP address *62.10.10.4*. When port *3389* is open attackers can easily identify that you are using a terminal server. As a result, use a different port for external access using a remote desktop, for example port *5000*.

(1) Go to **Network** -> **NAT** -> **NAT Configuration** -> **New**.

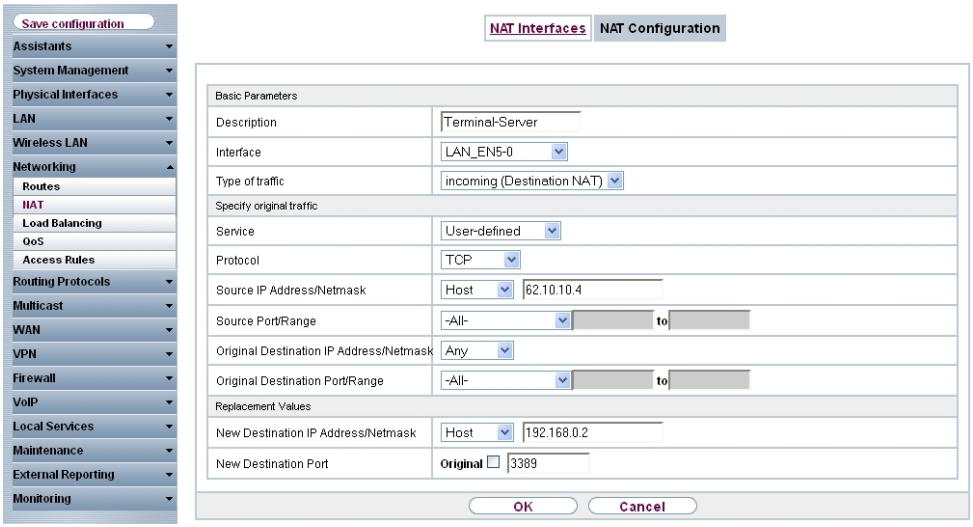


Fig. 5: **Network** -> **NAT** -> **NAT Configuration** -> **New**

Proceed as follows to configure the enable:

(1) Enter a **Description** for the NAT configuration, e. g. *Terminal-Server*.

(2) Set the **Interface** to *LAN_EN5-0*.

(3) For the **Type of traffic** , select *incoming (destination NAT)*.

(4) Leave the **Service** set to *User-defined*.

(5) Set **Protocol** to *TCP*.

(6) Under **Source IP Address/Netmask** enter the internal terminal server's IP address, e. g. *62.10.10.4*.

(7) Set the **Port** to *Specify Port* and enter *5000*, for example, in the first input field.

(8) Under **New Destination IP Address/Netmask** enter the internal IP address, for example *192.168.0.2*.

(9) For **New Destination Port** disable **Original** and enter *3389* in the input field.

(10) Leave the remaining settings unchanged and confirm them with **OK**.

1.3 Result

You have configured a NAT enable so that you can access the gateway with HTTP over the Internet. You also allow access to your internal Web server and the terminal server over the Internet.

1.4 Checking the connection

To check the settings, activate debug mode in the shell with the command `debug all&`. Call up the browser on an external computer on the Internet and enter the IP address of the gateway, e.g. *http://62.10.10.2:8080*.

The following message must appear if you are from the IP address *80.65.48.135*:

```
12:14:20 DEBUG/INET: NAT: new incoming session on ifc 5000
prot 6 127.0.0.1:80/ 62.10.10.2:8080 &lt;- 80.65.48.135:1024
```

1.5 Overview of Configuration Steps

Enable NAT

Field	Menu	Value
NAT active	**Network** -> **NAT** -> **NAT Interfaces**	Enabled for **LAN_EN5-0**
Silent Deny	**Network** -> **NAT** -> **NAT Interfaces**	Enabled for **LAN_EN5-0**

Configuring NAT enables

Field	Menu	Value
Description	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *GUI*
Interface	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*LAN_EN5-0*
Type of traffic	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*incoming (Destination NAT)*
Service	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*User-defined*
Protocol	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*TCP*
Source IP Address/Netmask	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *62.10.10.2*
Source Port/Range	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*Specify Port* with *8080*
New Destination Port	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*80*

Web server

Field	Menu	Value
Description	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *Webserver*
Interface	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*LAN_EN5-0*
Type of traffic	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*incoming (Destination NAT)*
Service	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*http*
Source IP Address/Netmask	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *62.10.10.3*
New Destination IP Address/Netmask	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *192.168.0.3*

Terminal Server

Field	Menu	Value
Description	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *Terminal-Server*
Interface	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*LAN_EN5-0*
Type of traffic	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*incoming (Destination NAT)*
Service	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*User-defined*
Protocol	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*TCP*
Source IP Address/Netmask	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *62.10.10.4*
Port	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*Specify Port* e. g. *5000*
New destination IP Address/Netmask	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *192.168.0.2*
New Destination Port	**Network** -> **NAT** -> **NAT Configuration** -> **New**	*3389*

Chapter 2 IP - Configuring a bintec router behind a provider router

2.1 Introduction

The configuration of a DMZ (Demilitarized Zone) with a **bintec RS232bw** is described in the following chapters.

Configuration is performed with the **GUI** (Graphical User Interface).

All FTP and HTTP/HTTPS requests from the Internet are to be forwarded to an FTP or Web server in the DMZ. The gateway has a leased Internet line with static public IP address, which is connected over the **ETH** port.

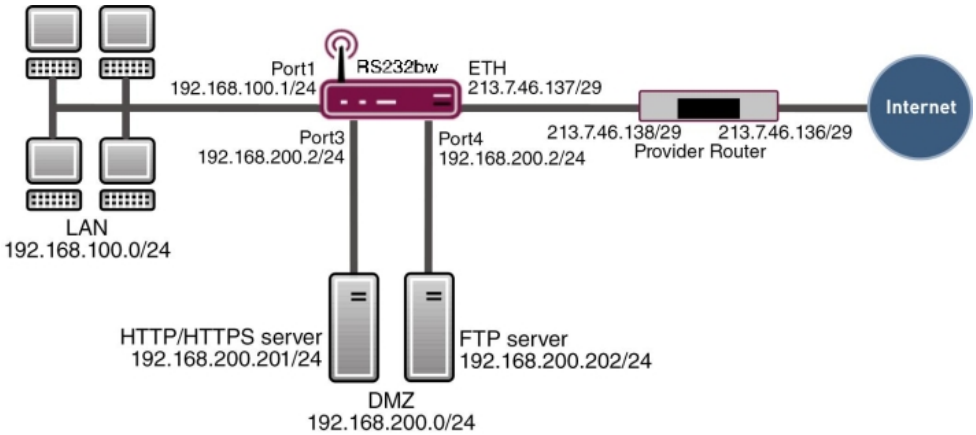


Fig. 6: Example scenario DMZ

Requirements

The following are required for the configuration:

- A **bintec RS232bw** gateway
- A boot image of version 9.1.5
- Internet access with static public IP address
- An FTP and web server in the DMZ
- Your LAN is connected to port **1** or **2** (interface `en1-0`) for the gateway.

- Your DMZ is connected to port **3** or **4** (interface `en1-1`) for the gateway.
- The leased Internet line is connected to port **ETH** (`en5-0`).

2.2 Configuration of the port

The DMZ is set up by dividing the four switch ports of the **bintec RS232bw** into two interfaces.

- Port **1** and **2** are assigned to the interface `en1-0`.
- Port **3** and **4** are assigned to the interface `en1-1`.

Go to the following menu to assign the ports to the interfaces:

(1) Go to **Physical Interfaces** -> **Ethernet Ports**-> **Port Configuration**.

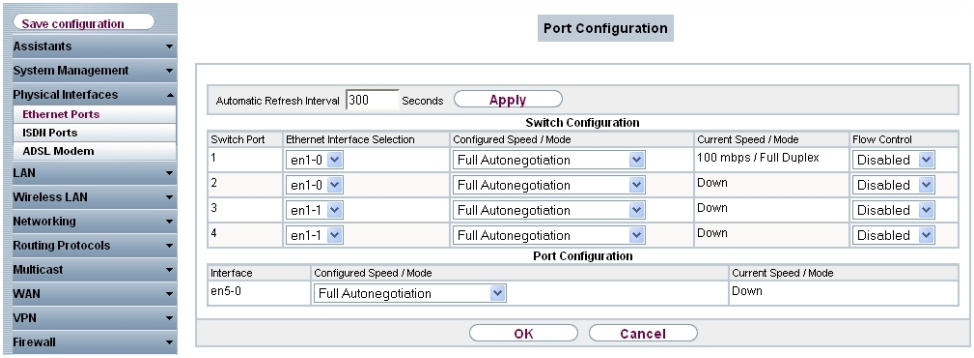


Fig. 7: **Physical Interfaces** -> **Ethernet Ports**-> **Port Configuration**

Proceed as follows to assign the ports to interfaces:

(1) Under **Ethernet Interface Selection** select `en1-0` for the **Switch Ports 1** and **2** from the dropdown menu.

(2) Select `en1-1` for the **Switch Ports 3** and **4**.

(3) Confirm with **OK**.

In the **IP Configuration** menu, you can assign IP addresses to the ports.

(1) Go to **LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>** .

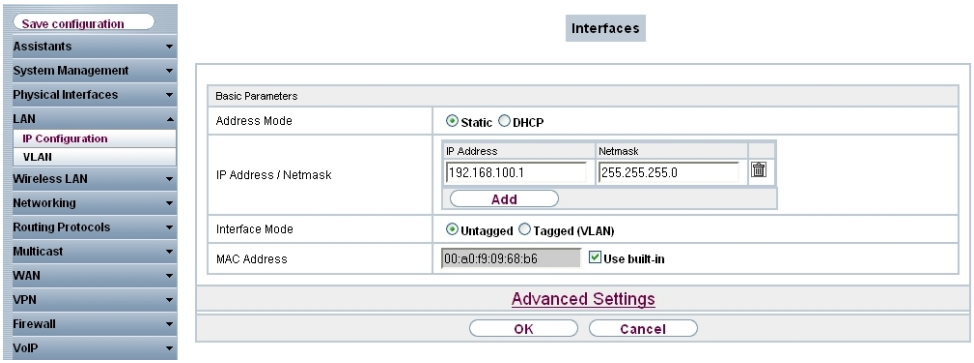


Fig. 8: **LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>** ->.

Proceed as follows:

(1) Leave **Address Mode** set to `Static`. The interface is assigned a static IP address.

(2) In **IP Address / Net Mask** enter the IP address and the subnet mask, here `192.168.100.1` and `255.255.255.0`.

(3) Leave **Interface Mode** set to `Untagged`. The interface is not assigned for a specific purpose.

(4) Confirm with **OK**.

Since your device can no longer be accessed by administration at the previous IP address, but only at the new IP address `192.168.100.1`, you must reconnect to the **GUI**. To do this, enter the new IP address `192.168.100.1` in the address bar of your browser and log in again.

Proceed as follows for interface `en1-1`:

(1) For `en1-1` go to **LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-1>**.

(2) Click the icon.

(3) Leave **Address Mode** set to `Static`.

(4) In **IP Address / Net Mask** enter the IP address and the subnet mask, here `192.168.200.2` and `255.255.255.0`.

(5) Leave **Interface Mode** set to `Untagged`.

(6) Confirm with **OK**.

If no IP address is entered, click **Add** for the IP address / Netmask. An input field appears for the IP address where you can assign the IP address and subnet mask.

2.3 Configuring Internet access

The gateway has a leased Internet line via the provider's router. Consequently, you must define the static public IP address for the gateway and configure a default route over the provider's router.

Configure the static public IP address for the interface `en5-0` in the same way as configuring the ports in the previous section:

(1) For `en5-0` go to **LAN** -> **IP Configuration** -> **Interfaces** -> **<en5-0>**.

(2) Click the icon.

(3) Leave **Address Mode** set to `Static`.

(4) In **IP Address / Net Mask** enter the IP address and the subnet mask, here `213.7.46.137` and `255.255.255.248`.

(5) Leave **Interface Mode** set to `Untagged`.

(6) Confirm with **OK**.

Set up a default route over the provider's router.

(1) Go to **Network** -> **Routes** ->**IPv4 Route Configuration**-> **New** .

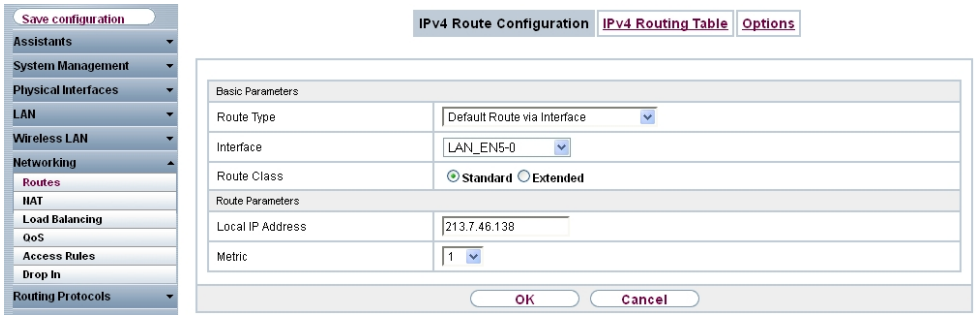


Fig. 9: **Network** -> **Routes**-> **IPv4 Route Configuration** -> **New**

Proceed as follows:

(1) For **Route Type** select `Default Route via Interface`. Default Route is used if no other suitable route is available.

(2) Select the **Interface** that is to be used for this route, e. g. `LAN_EN5-0`.

(3) Under **Gateway** enter the IP address of the Internet gateway, in this example `213.7.46.138`.

(4) For **Metric**, select the route's priority, e. g. `1`. The lower the value, the higher the priority of the route.

(5) Press **OK** to confirm your entries.

2.4 Configuration of DMZ

2.4.1 Enabling NAT on the DMZ interface

NAT must be enabled on the interface used to provide the Internet connection.

Go to the following menu to enable NAT for the DMZ interface:

(1) Go to **Network** -> **NAT** -> **NAT Interfaces**.

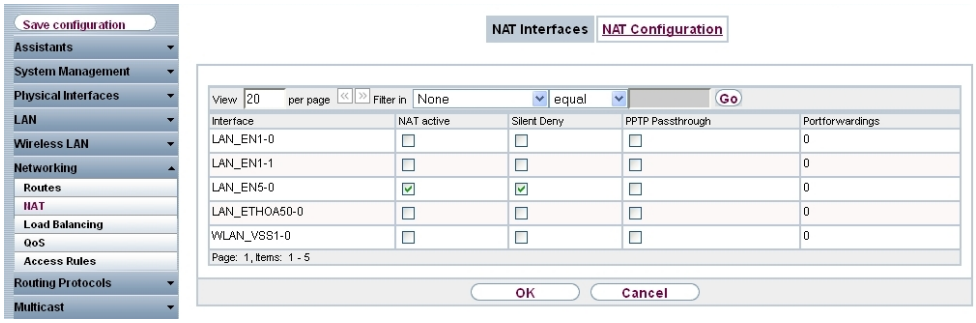


Fig. 10: **Network** -> **NAT** ->**NAT Interfaces**

Proceed as follows:

(1) Select **NAT Active** for the *LAN_EN5-0* interface. This is how the NAT feature is enabled for the interface.

(2) Select **Silent Deny** for the *LAN_EN5-0* interface. If this function is enabled, there is no feedback for dropped packets to the sender.

(3) Confirm with **OK**.

2.4.2 Configuring portforwarding

As NAT as been enabled on the interface for the Internet connection, it is no longer possible to access internal computers from the Internet. External users must be authorised to access the FTP server over FTP and the Web server over HTTP or HTTPS. Consequently, you must set up portforwarding for these services.

Go to the following menu to forward the required ports to the FTP or Web server:

(1) Go to **Network** -> **NAT** -> **NAT Configuration** -> **New**.

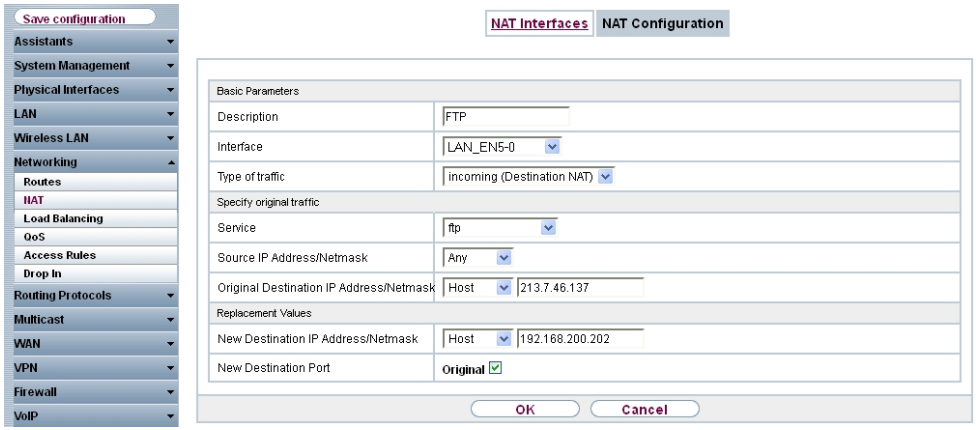


Fig. 11: **Network** -> **NAT** ->**NAT Configuration** -> **New**

Proceed as follows to set up portforwarding for FTP:

(1) Enter a **Description** for the NAT configuration, e. g. `FTP`.

(2) Set **Interface** to `LAN_EN5-0`.

(3) For the **Data Traffic Type** , select `incoming (destination NAT)`.

(4) For **Service**, select `ftp`.

(5) Under **Original Destination IP Address/Netmask**, enter the static public IP address of the gateway, here `213.7.46.137`.

(6) Under **New Destination IP Address/Netmask** enter the FTP server's IP address, for example `192.168.200.202`.

(7) Confirm with **OK**.

Proceed as follows to set up portforwarding for HTTP:

(1) Go to **Routing** -> **NAT** -> **NAT Configuration** -> **New**.

(2) Enter a **Description** for the NAT configuration, e. g. `HTTP`.

(3) Set **Interface** to `LAN_EN5-0`.

(4) For the **Data Traffic Type** , select `incoming (destination NAT)`.

(5) For **Service**, select `http`.

(6) Under **Original Destination IP Address/Netmask**, enter the static public IP address of the gateway, here `213.7.46.137`.

(7) Under **New Destination IP Address/Netmask** enter the HTTP server's IP address, for example `192.168.200.201`.

(8) Confirm with **OK**.

Proceed as follows to set up portforwarding for HTTPS:

(1) Go to **Routing** -> **NAT** -> **NAT Configuration** -> **New**.

(2) Enter a **Description** for the NAT configuration, e. g. `HTTPS`.

(3) Set **Interface** to `LAN_EN5-0`.

(4) For the **Data Traffic Type** , select `incoming (destination NAT)`.

(5) For **Service**, select `http (SSL)`.

(6) Under **Original Destination IP Address/Netmask**, enter the static public IP address of the gateway, here `213.7.46.137`.

(7) Under **New Destination IP Address/Netmask** enter the HTTPS server's IP address, for example `192.168.200.201`.

(8) Confirm with **OK**.

2.5 Checking the configuration

2.5.1 Checking portforwarding

The list of configured portforwarding should appear as follows:

(1) Remain in the **Network**-> **NAT** -> **NAT Configuration** menu.

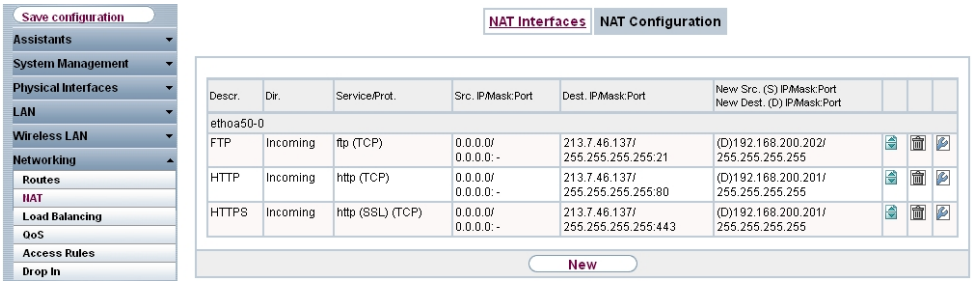


Fig. 12: **Network** -> **NAT** ->**NAT Configuration**

This list is used as a basis to forward all FTP requests on the public IP address of your gateway to your FTP server. HTTP and HTTPS requests are forwarded to your Web server accordingly. All other requests are rejected by the gateway.

Click **Save Configuration** and confirm with **OK** to save the configuration as the startup configuration.

2.5.2 Checking the functionality

Functionality can only be checked from the shell. To do this, enter the `debug all` command and confirm with **Return**.

```
r232bw:&gt; debug all
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80 &lt;- 62.137.56.89:1050
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80  &lt;- 62.137.56.89:1051
01:36:27 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.201:80/213.7.46.137:80  &lt;- 62.137.56.89:1052
01:36:33 DEBUG/INET: NAT: new incoming session on ifc 5000 prot 6
192.168.200.202:21/213.7.46.137:21 &lt;- 84.135.23.189:1053
```

As the debug extract shows, the HTTP requests (port 80) have been forwarded from IP address 62.137.56.89 to IP address 192.168.200.201. An FTP request (port 21) has also been forwarded from IP address 84.135.23.189 to IP address 192.168.200.202.

2.6 Overview of Configuration Steps

Configuration of the port

Field	Menu	Value
Ethernet Interface Selection	**Physical Interfaces** -> **Ethernet Ports**-> **Port Configuration**	Switch Port 1 and 2 to *en1-0*
Ethernet Interface Selection	**Physical Interfaces** -> **Ethernet Ports**-> **Port Configuration**	Switch Port 3 and 4 to *en1-1*
IP Address / Netmask	**LAN** -> **IP Configuration**-> **Interfaces** -> **<en1-0>** ->	*192.168.100.1* and *255.255.255.0*
IP Address / Netmask	**LAN** -> **IP Configuration**-> **Interfaces** -> **<en1-1>** ->	*192.168.200.2* and *255.255.255.0*

Configuring Internet access

Field	Menu	Value
IP / Netmask	**LAN** -> **IP Configuration** ->**Interfaces** -> **<en5-0>** ->	*213.7.46.137* and *255.255.255.248*
Route Type	**Network** -> **Routes**-> **IPv4 Route Configuration**-> **New**	*Default Route via Interface*
Interface	**Network** -> **Routes**-> **IPv4 Route Configuration**-> **New**	*LAN_EN5-0*
Gateway	**Network** -> **Routes**-> **IPv4 Route Configuration**-> **New**	*213.7.46.138*

NAT

Field	Menu	Value
NAT active	**Network** -> **NAT** ->**NAT Interfaces**	Enabled for **LAN_EN5-0**

Field	Menu	Value
Silent Deny	**Network -> NAT ->NAT Interfaces**	Enabled for **LAN_EN5-0**

Portforwarding

Field	Menu	Value
Description	**Network -> NAT -> NAT Configuration -> New**	e. g. *FTP*
Interface	**Network -> NAT -> NAT Configuration -> New**	*LAN_EN5-0*
Data Traffic Type	**Network -> NAT -> NAT Configuration -> New**	incoming (destination NAT)
Service	**Network -> NAT -> NAT Configuration -> New**	*ftp*
Original Destination IP Address / Netmask	**Network -> NAT -> NAT Configuration -> New**	e. g. *213.7.46.137*
New destination IP address/netmask	**Network -> NAT -> NAT Configuration -> New**	e. g. *192.168.200.202*
Description	**Network -> NAT -> NAT Configuration -> New**	e. g. *HTTP*
Interface	**Network -> NAT -> NAT Configuration -> New**	*LAN_EN5-0*
Data Traffic Type	**Network -> NAT -> NAT Configuration -> New**	incoming (destination NAT)
Service	**Network -> NAT -> NAT Configuration -> New**	*http*
Original Destination IP Address / Netmask	**Network -> NAT -> NAT Configuration -> New**	e. g. *213.7.46.137*
New destination IP address/netmask	**Network -> NAT -> NAT Configuration -> New**	e. g. *192.168.200.201*
Description	**Network -> NAT -> NAT Configuration -> New**	e. g. *HTTPS*
Interface	**Network -> NAT -> NAT Configuration -> New**	*LAN_EN5-0*
Data Traffic Type	**Network -> NAT -> NAT Configuration -> New**	incoming (destination NAT)
Service	**Network -> NAT -> NAT Configuration -> New**	*http (SSL)*
Original Destination	**Network -> NAT -> NAT Configur-**	e. g. *213.7.46.137*

Field	Menu	Value
IP Address / Netmask	**ation** -> **New**	
New destination IP address/netmask	**Network** -> **NAT** -> **NAT Configuration** -> **New**	e. g. *192.168.200.201*

Chapter 3 IP - IPTV on xDSL (ADSL / VDSL) T-Home Entertainment connection

3.1 Introduction

This solution shows how to configure a bintec router on one of the latest generation of xDSL T-Home Entertainment connections. On ADSL and new generation VDSL T-Home connections, the Internet data and IPTV multicast data are transmitted via separate VLAN interfaces.

The table below shows the main technical information for configuring the two accesses:

Internet data access	
VLAN ID	7
Network protocol	PPPoE
IP assignment done via	IPCP (Internet Protocol Control Protocol)
Routing	Default route must be configured
NAT	Active (Network Address Translation)
IPTV Multicast data access	
VLAN ID	8
IP assignment done via	DHCP (Dynamic Host Configuration Protocol)
IGMP Proxy	Active (Internet Group Management Protocol)
Routing	Required routes are learned via DHCP (no other configuration required)
NAT	Not mandatory, enabled in the example for security reasons (Network Address Translation)

A VDSL connection is used in this example. The ADSL/VDSL modem is connected to the physical Ethernet port *ETH5*. If you have a device with an integrated DSL modem, you can also use the internal modem, of course.

Note

Please note that this configuration can only work if the attached modem or internal modem behaves as a pure modem (this is a given with internal modems in bintec devices). If you only want to put a router that may have also been supplied in a state where it will function like a modem, problems can arise.

The **GUI** (Graphical User Interface) is used for configuration here.

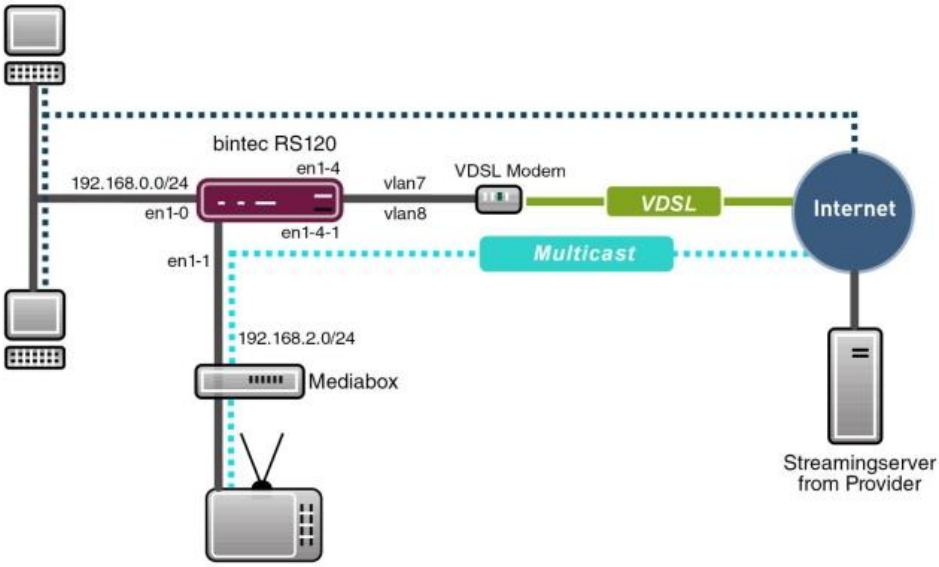


Fig. 13: Example scenario

Requirements

Provider specific:

- T-Home ADSL/VDSL connection of the latest generation with T-Home Entertainment pack
- Media Box (T-Home X301T) or similar device (usually supplied by the provider)

bintec elmeg specific:

- In this example, a **bintec RS120** with software version 7.9.4 Patch 5 was used.
- The configuration is the same as for other bintec router types. The list below shows the minimum requirement for the software versions that are to be used here:

TR200: 7.9.1 Patch 5

RS12x: 7.9.1 Patch 5

RS23x: 7.9.1 Patch 5

R120x: 7.9.1 Patch 5

R300x: 7.9.1 Patch 5

R400x: 7.9.1 Patch 5

- The configuration is done using the **GUI** Web configuration tool.

3.2 Configuration

3.2.1 Configuring the bintec RS120

For configuration, open an Internet browser and start a web (HTTP) connection to the **bintec RS120** router. Unless otherwise configured, use the standard IP address `192.168.0.254`. Once the HTTP connection has been established, log in using the following access data.

User `admin` **Password** `funkwerk` (default password unless otherwise configured).

Configuring VDSL Internet access

The GUI comes with a wizard for configuring VDSL Internet access. To do this, go to the following menu:

(1) Go to **Assistants** -> **Internet Access**-> **Internet Connections** -> **New**.

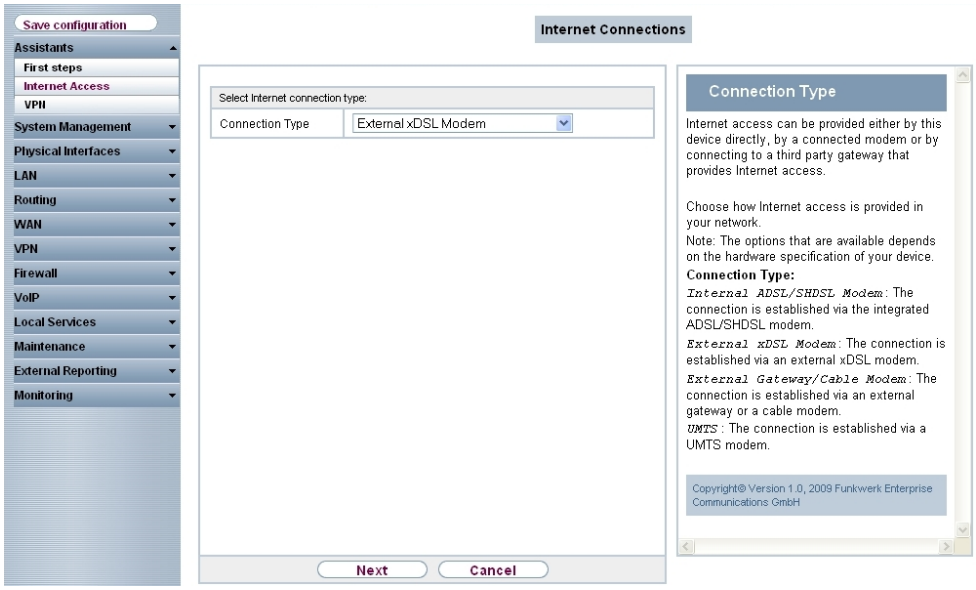


Fig. 14: **Assistants** -> **Internet Access** -> **Internet Connections** -> **New**

Proceed as follows:

(1) For **Connection Type**, select `External xDSL Modem`.

(2) Click on **Next** to configure a new Internet connection.

Enter the required data for the Internet connection.

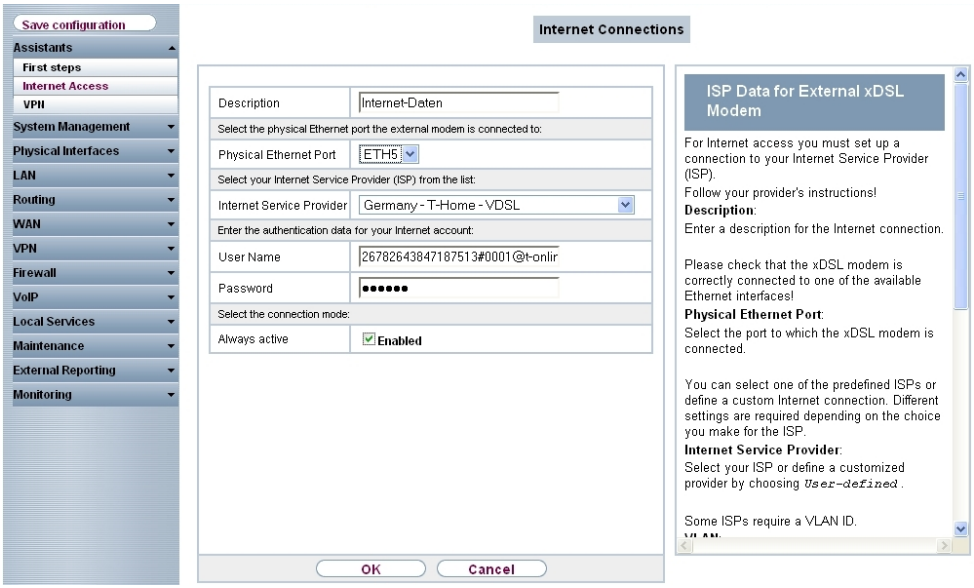


Fig. 15: **Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**

Proceed as follows to configure a new Internet connection:

(1) Under **Description**, enter a name for the Internet connection, e. g. `Internet Data`.

(2) Under **Physical Ethernet Port** select the physical Ethernet port to which the xDSL modem is connected, in this case `ETH5`.

(3) Under **Internet Service Provider** select the profile `Germany - T-Home - VDSL` for our VDSL connection.

(4) Under **User Name** enter the access data you received from your provider.

(5) Enter the **Password** you received from your provider.

(6) In the **Always active** field, specify whether or not the Internet connection should always be on. Only activate this option if you have Internet access with a flatrate.

(7) Press **OK** to confirm your entries.

3.2.2 Configuring the IPTV Multicast data access

To configure the virtual LAN interfaces for the Multicast access, go to the following menu:

(1) Go to **LAN** -> **IP Configuration** -> **Interfaces** -> **New**.

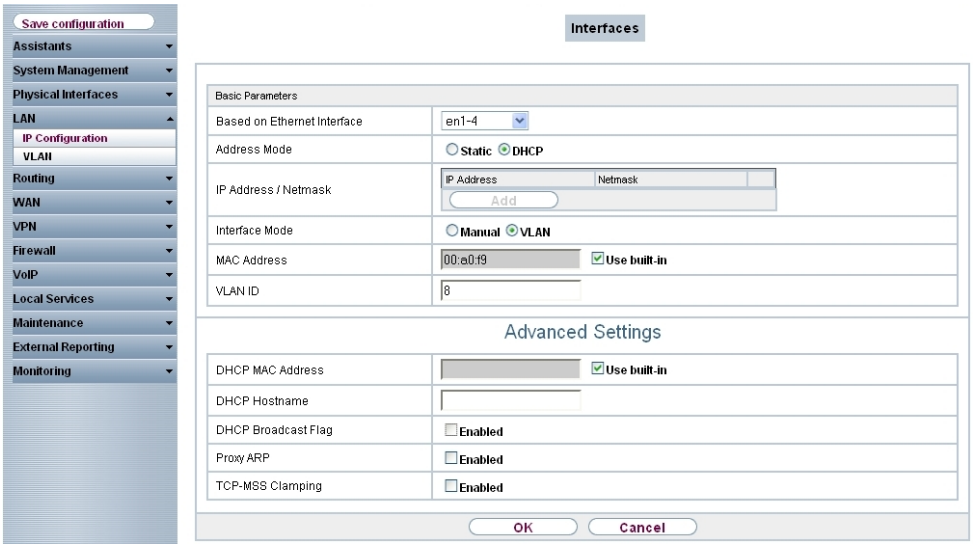


Fig. 16: **LAN->IP Configuration ->Interfaces-> New**

Proceed as follows:

(1) Under **Based on Ethernet Interface**, select the logical Ethernet interface that has been assigned to the physical Ethernet port used above. For Ethernet port ETH5, this is the `en1-4` interface (on this, see the explanation below).

(2) Set the **Address Mode** to `DHCP`. An IP address is assigned to the interface dynamically via DHCP.

(3) Set the **Interface Mode** to `VLAN`. You use this option to assign the interface to a VLAN.

(4) In the **VLAN-ID** input field, enter the VLAN ID `8` which is to be used.

(5) Click **Advanced Settings**.

(6) Disable the **DHCP Broadcast Flag** option.

(7) Leave the remaining settings unchanged and confirm your entries with **OK**.

Explaining the assigning of physical Ethernet ports and logical Ethernet interfaces

The assignment between the physical Ethernet port and the logical Ethernet interface can be flexibly configured in the routers with an integrated switch. Ex works, the following assignment usually applies:

Physical Ethernet Port	Logical Ethermet Interface
ETH1 to ETH4	en1-0

Physical Ethernet Port	Logical Ethermet Interface
ETH5	en1-4

For detailed information on the assigned that has been configured in your case, go to the **Physical Interfaces** menu. For the **bintec RS120** router that is used in the workshop, it looks like this ex works:

(1) Go to **Physical Interfaces** ->**Ethernet Ports**->**Port Configuration**.

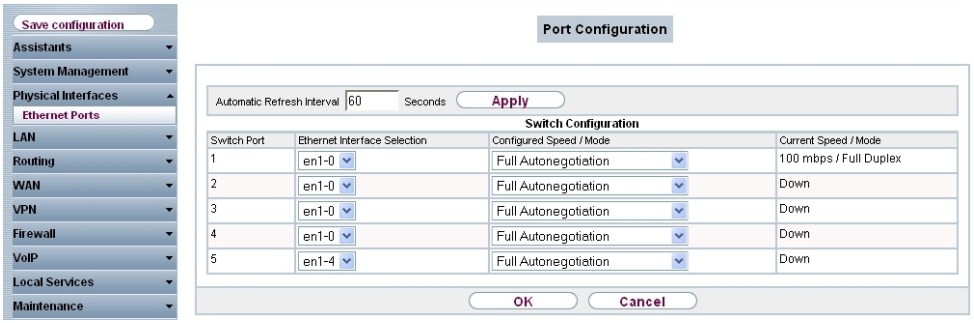


Fig. 17: **Physical Interfaces**->**Ethernet Ports**->**Port Configuration**

Configuring the IGMP (Internet Group Management Protocol) proxy

Now you will configure the IGMP proxy required to receive the IPTV Multicast data.

(1) Go to **Routing** -> **Multicast** -> **IGMP**-> **New** .

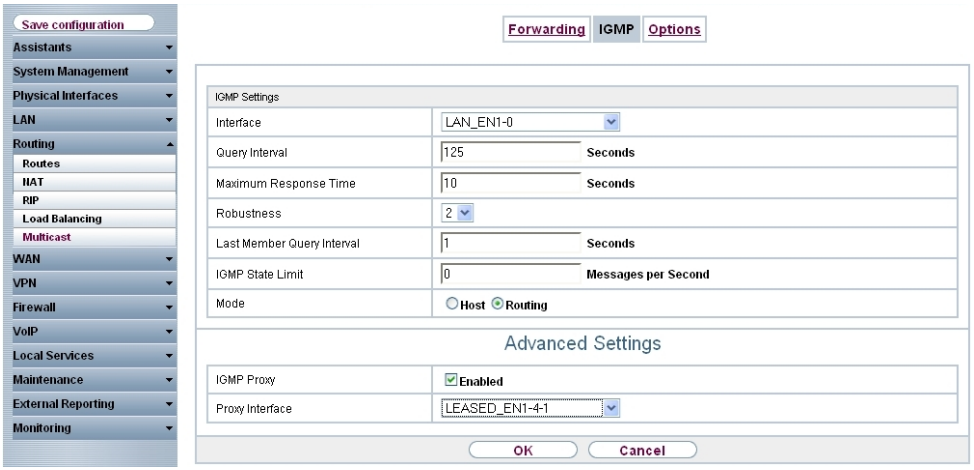


Fig. 18: **Routing** -> **Multicast** -> **IGMP** -> **New**

Proceed as follows to configure the IGMP proxy.

(1) Under **Interface**, select the logical Ethernet interface which the Media Box or client PCs are connected to. In our example, they are Ethernet ports ETH1 to ETH4. Based on the above assignment, the logical Ethernet interface `LAN_EN1-0` needs to be selected.

(2) Select `Routing` for **Mode**.

(3) Click **Advanced Settings**.

(4) Enable the **IGMP Proxy** option.

(5) As the **proxy interface**, select the generated VLAN interface `LEASED_EN1-4-1`.

(6) Leave the remaining settings unchanged and confirm your entries with **OK**.

The completed configuration looks as follows (the entry for the IGMP proxy interface (`en1-4-1`) is generated automatically):

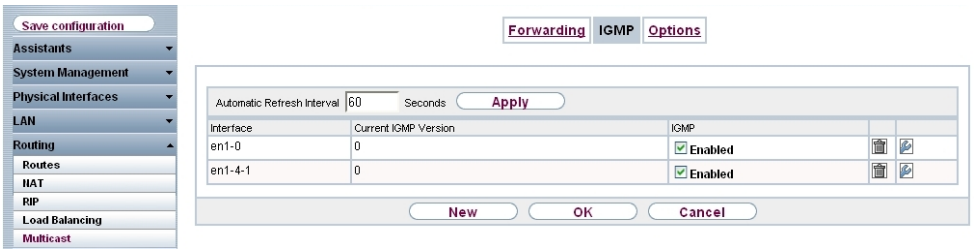


Fig. 19: **Routing** -> **Multicast** -> **IGMP**

Activating the Multicast Routing function

The routing of IP Multicast packets to the bintec router is disabled by default. In the following configuration step, you enable the Multicast routing function on the router. To do this, go to the following menu:

(1) Go to **Routing** ->**Multicast** ->**Options**.

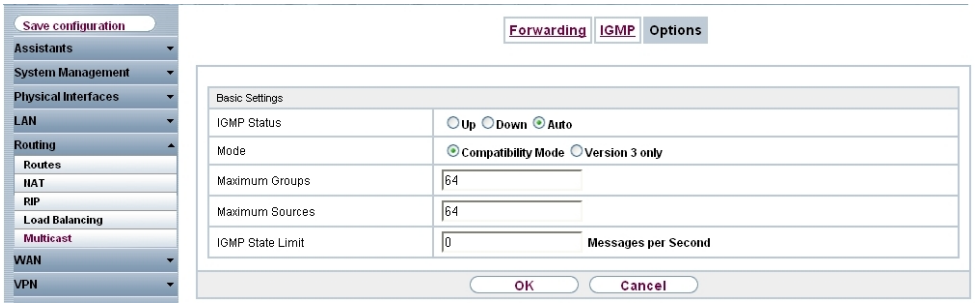


Fig. 20: **Routing** -> **Multicast** -> **Options**

Proceed as follows:

(1) Set the **IGMP status** to `Active` or `Auto`.

(2) Confirm your entry with **OK**.

Note

A one-off confirmation of the configuration page through **OK** is essential. This also applies if the **IGMP Status** has already been set to `Auto` or `Active` .

Enabling NAT on the IGMP proxy interface

For security reasons, and to ensure that video on-demand services work, the NAT function needs to be disabled.

(1) Go to **Routing** -> **NAT** -> **NAT Interfaces**.

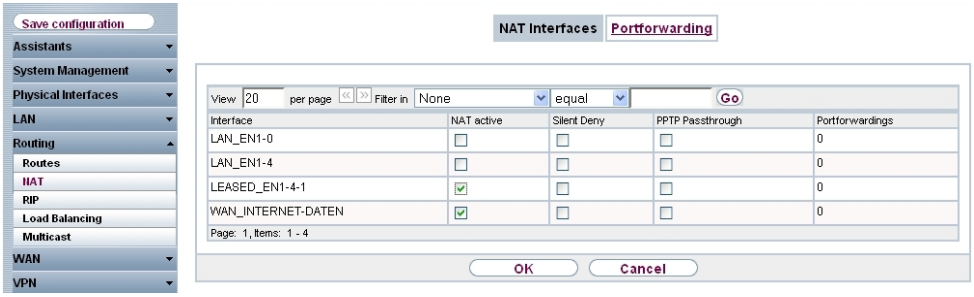


Fig. 21: **Routing** -> **NAT** -> **NAT Interfaces**

Proceed as follows:

(1) Under **NAT Active**, enable the `LEASED_EN1-4-1` interface.

(2) Confirm with **OK**.

3.2.3 Configuring a DHCP IP address pool on the LAN interface

The T-Home Media Box requires the IP address settings to be assigned dynamically via DHCP. For this purpose, a DHCP IP address pool needs to be configured on the LAN interface. In our case, this is the `en1-0` interface.

Note

Only carry out this configuration step if there is no other DHCP server in your local network. In this case, enter the LAN IP address of the **bintec RS120** router as the **Router** on the DHCP server. In our example, the LAN IP address of the **bintec RS120** is `192.168.0.254`.

If there is no DHCP server in your local network, proceed as follows:

(1) Go to **Local Services** -> **DHCP Server** -> **DHCP Pool** -> **New**.

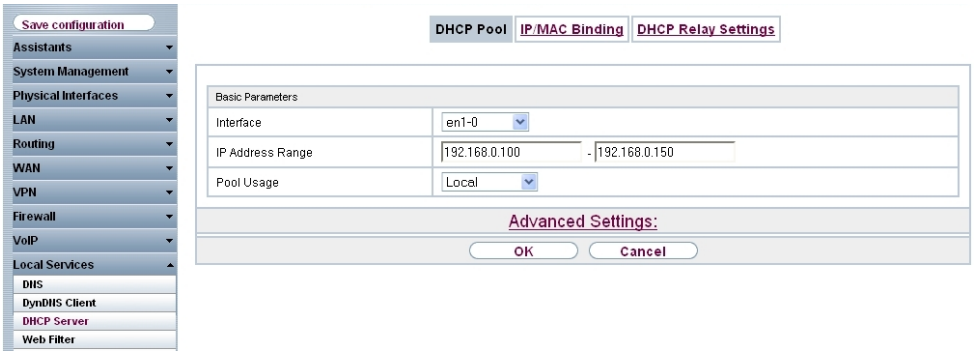


Fig. 22: **Local Services** -> **DHCP Server** -> **DHCP Pool** -> **New**

Proceed as follows to set up an IP address pool:

(1) Under **Interface**, select the logical interface `en1-0`.

(2) Enter an **IP address range**. In our example, an IP address range from `192.168.0.100` to `192.168.0.150` is configured.

(3) Press **OK** to confirm your entries.

Note

The IP address range must lie within the IP network range configured on the LAN interface.

3.2.4 Making a bootable backup of the configuration

This concludes the configuration. If the devices are connected correctly, the Internet data connection and the reception of IPTV data should work correctly. To create a bootable backup of the configuration, exit the **GUI** with **Save configuration** and confirm with **OK**.

3.3 Overview of Configuration Steps

Select the connection type

Field	Menu	Value
Interface	**Assistants** -> **Internet Access**-> **Internet Connections**	*External xDSL Modem*

Setting up an internet connection

Field	Menu	Value
Description	**Assistants** -> **Internet Access**-> **Internet Connections** ->**Next**	e. g. *Internet Data*
Physical Ethernet Port	**Assistants** -> **Internet Access**-> **Internet Connections** ->**Next**	*ETH5*
Internet Service Provider	**Assistants** -> **Internet Access**-> **Internet Connections** ->**Next**	e. g. *Germany-T-Home-VDSL*
User Name	**Assistants** -> **Internet Access**-> **Internet Connections** ->**Next**	e. g. *123456789#0001@t-online.de*
Password	**Assistants** -> **Internet Access**-> **Internet Connections** ->**Next**	e. g. *secret*
Always Active	**Assistants** -> **Internet Access**-> **Internet Connections** ->**Next**	*Enabled*

Configuring the VLAN interface

Field	Menu	Value
Based on Ethernet Interface	**LAN** -> **IP Configuration**-> **Interfaces** -> **New**	*en1-4*
Address mode	**LAN** -> **IP Configuration**-> **Interfaces** -> **New**	*DHCP*
Interface Mode	**LAN** -> **IP Configuration**-> **Interfaces** -> **New**	*VLAN*
VLAN ID	**LAN** -> **IP Configuration**-> **Interfaces** -> **New**	*8*
DHCP Broadcast flag	**LAN** -> **IP Configuration**-> **Interfaces** -> **New**	Disabled

Configure IGMP proxy

Field	Menu	Value
Interface	**Routing** -> **Multicast**-> **IGMP** -> **New**	*LAN_EN1-0*
Mode	**Routing** -> **Multicast**-> **IGMP** -> **New**	*Routing*
IGMP Proxy	**Routing** -> **Multicast**-> **IGMP** -> **New**	*Enabled*
Proxy Interface	**Routing** -> **Multicast**-> **IGMP** -> **New**	*LEASED_EN1-4-1*

Enable Multicast routing function

Field	Menu	Value
IGMP Status	**Routing** -> **Multicast**-> **Options**	*Active* or *Auto*

Activating NAT

Field	Menu	Value
Interface LEASED_EN1-4-1	**Routing** -> **NAT** ->**NAT Interfaces**	NAT active *Enabled*

Configuring the DHCP IP address pool

Field	Menu	Value
Interface	**Local Services** -> **DHCP Server**-> **DHCP Pool** -> **New**	*en1-0*
IP Address Range	**Local Services** -> **DHCP Server**-> **DHCP Pool** -> **New**	e. g. *192.168.0.100* - *192.168.0.150*
Pool Usage	**Local Services** -> **DHCP Server**-> **DHCP Pool** -> **New**	*Local*

Chapter 4 IP - OSPF Routing Protocol over IPSec Connection

4.1 Introduction

This solution shows the star-shaped linking of three locations by IPSec connections in which the OSPF routing protocol is used to transmit the IP network areas configured in the branch locations. Using a routing protocol is particularly beneficial in the case of more complex network structures (more IP network areas), because changes in the network structure are automatically propagated to all the routers involved in the network via the routing protocol.

The GUI is used to do the configuration.

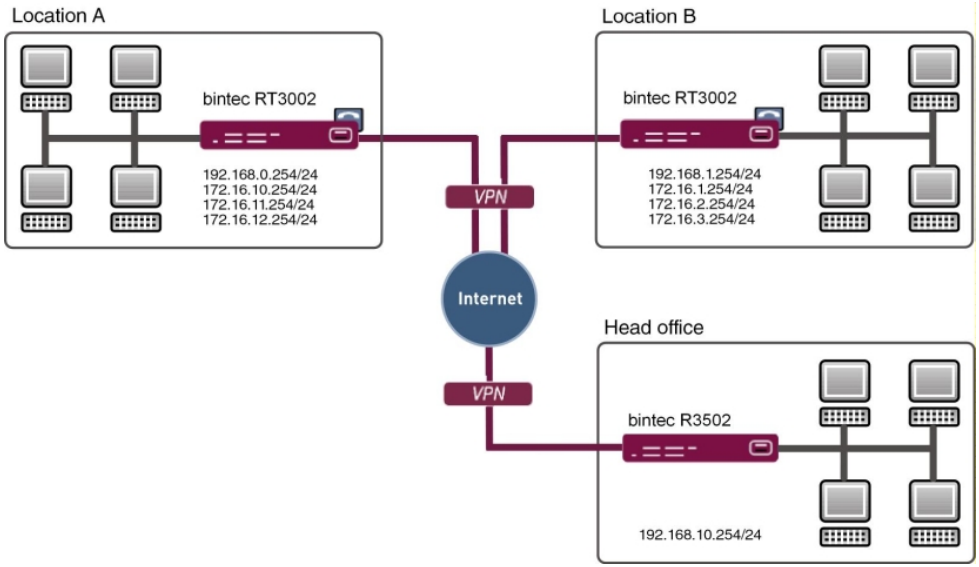


Fig. 23: Example scenario

In our example, more than one network is used at Locations A and B. With statically configured routing the result of this would be that all the networks of all the locations in all the VPN gateways would need to be configured. This is not the case if a routing protocol is used. In such a case, the only configuring required is that of a VPN tunnel which enables the communication to the head office gateway.

Specifically, when doing the VPN configuration, the administrator only needs to tend, in

each case, to the first network in the LAN interface for the relevant VPN gateway. The routing protocol takes care of the rest. In this example, the routing protocol propagates all the networks for Locations A and B to the head office gateway. Which means that all the locations can communicate with one another. If a LAN IP address is modified, or if a new network is added to one of the gateways, the routing information is automatically forwarded to the other gateways. The VPN gateways support the use of routing protocols, including in connection with IPSec connections.

Requirements

- A bintec VPN gateway from the Rxxx2- or RTxxx2 series at each location
- All the gateways require an independent connection to the Internet
- At least one IP address or a DynDNS account to make the head office gateway accessible

4.2 Configuration

4.2.1 Configure the gateway at head office

Configure the Internet access at the head office gateway

The Internet access at the head office gateway can be configured using the **Assistant**. In this workshop, an Internet access with a static IP address is used at the head office location.

(1) Go to **Assistants** -> **Internet Access**-> **Internet Connections** -> **New**.

(2) For **Connection Type**, select `Internal ADSL Modem`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

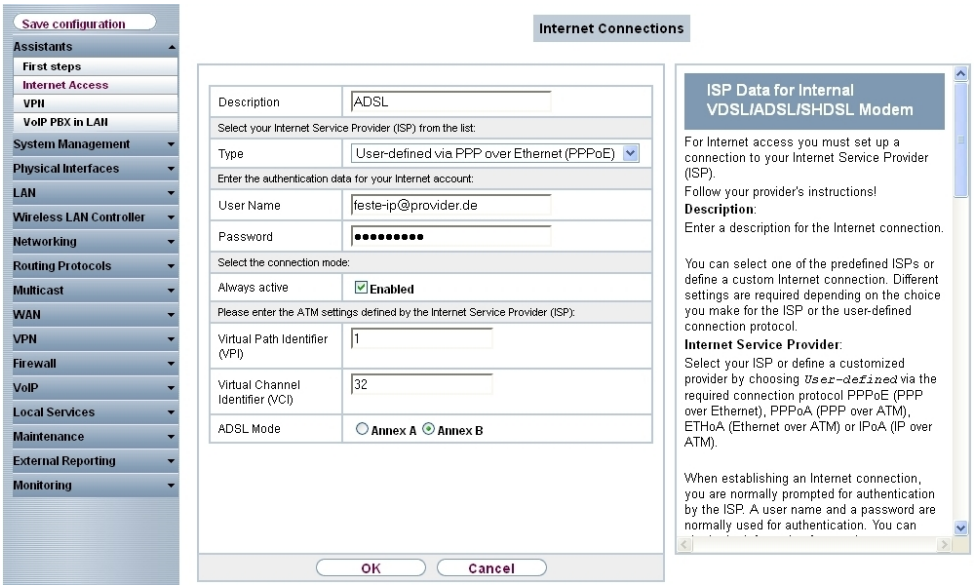


Fig. 24: **Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**

Proceed as follows to configure an Internet access:

(1) Under **Description** enter e. g. `ADSL`.

(2) For **Type**, select `User-defined via PPP over Ethernet (PPPoE).`

(3) As the **User** , enter the name which your provider has given you, e. g. `feste-ip@provider.de`.

(4) Enter the **Password** that your provider has given you, e. g. `test12345`.

(5) Enable the **Always active** option.

(6) For **ADSL Mode**, select `Annex B` for applications in Europe (provider-dependent).

(7) Press **OK** to confirm your entries.

Configure the VPN IPSec connections at the head office gateway

In our example, the VPN tunnels are always set up from the branch gateways to the head office gateway. For this reason, there is no need to configure the IPSec peer address at the head office gateway. In this workshop, the VPN IPSec tunnels for Location A and Location B will be configured using the **Assistant**.

(1) Go to **Assistants** -> **VPN** -> **VPN Connections** -> **New**.

(2) For **VPN Scenario** select `IPSec-LAN-LAN Connection`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

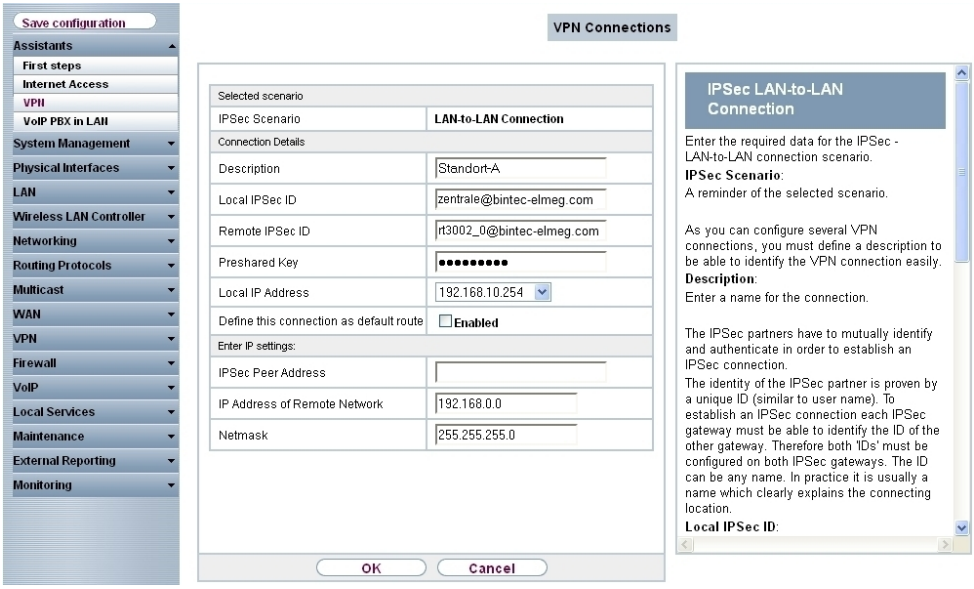


Fig. 25: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

To add the VPN connection to Location A, proceed as follows:

(1) For **Description**, enter a description of the peer which identifies it, e. g. `Location A`.

(2) For **Local IPsec ID**, enter the IPSec ID of the head office gateway, e. g. `zentrale@bintec-elmeg.com`.

(3) For **Remote IPSec ID**, enter the IPSec ID of the gateway at Location A, e. g. `rt3002-0@bintec-elmeg.com`.

Note

This ID must be unique.

(4) In the **Preshared Key** field, enter a password for the encrypted connection (e. g. `test12345`.

(5) The **Local IP address** specifies the IP address of the IPSec interface, e. g. `192.168.10.254`.

(6) For **IPSec Peer Address**, nothing needs to be entered because the VPN tunnel is always set up from the branch gateway to the head office gateway.
For **IP Address of Remote Network**, the network address of one of the IP networks used at Location A must be configured, e. g. `192.168.0.0` and the **net mask** `255.255.255.0`.

(7) Confirm with **OK**.

Now add the VPN connection to Location B.

(1) Go to **Assistants** -> **VPN** -> **VPN Connections** -> **New**.

(2) For **VPN Scenario** select *IPSec-LAN-LAN Connection*.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

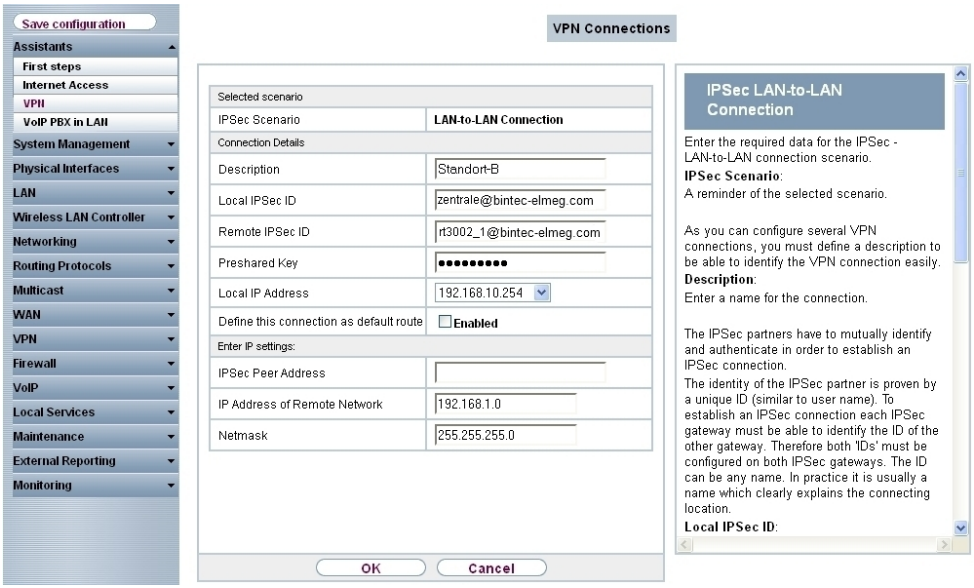


Fig. 26: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

To add the VPN connection to Location B, proceed as follows:

(1) For **Description**, enter a description of the peer which identifies it, e. g. *Location B*.

(2) For **Local IPSec ID**, enter the IPSec ID of the head office gateway, e. g. *zentrale@bintec-elmeg.com*.

(3) For **Remote IPSec ID**, enter the IPSec ID of the gateway at Location B, e. g. *rt3002-1@bintec-elmeg.com*.

Note

This ID must be unique.

(4) In the **Preshared Key** field, enter a password for the encrypted connection (e. g. *test12345*.

(5) The **Local IP address** specifies the IP address of the IPSec interface, e. g. *192.168.10.254*.

(6) For **IPSec Peer Address**, nothing needs to be entered because the VPN tunnel is always set up from the branch gateway to the head office gateway.
For **IP Address of Remote Network**, the network address of one of the IP networks used at Location B must be configured, e. g. `192.168.1.0` and the **net mask** `255.255.255.0`.

(7) Confirm with **OK**.

In the next step, the OSPF routing protocol is enabled. This propagates the routing entries via the VPN IPSec tunnel at the locations.

(1) Go to **Routing Protocols** -> **OSPF** -> **Global Settings**.

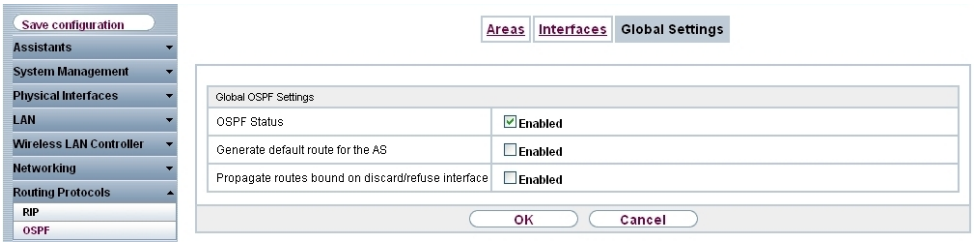


Fig. 27: **Routing Protocols** -> **OSPF** -> **Global Settings**.

Proceed as follows:

(1) Enable the **OSPF Status** option.

(2) Confirm with **OK**.

You specify which interface IP routing information is propagated on in the **Interfaces** menu.

(1) Go to **Routing Protocols** -> **OSPF** -> **Interfaces** -> **<Location A/Location B>** .

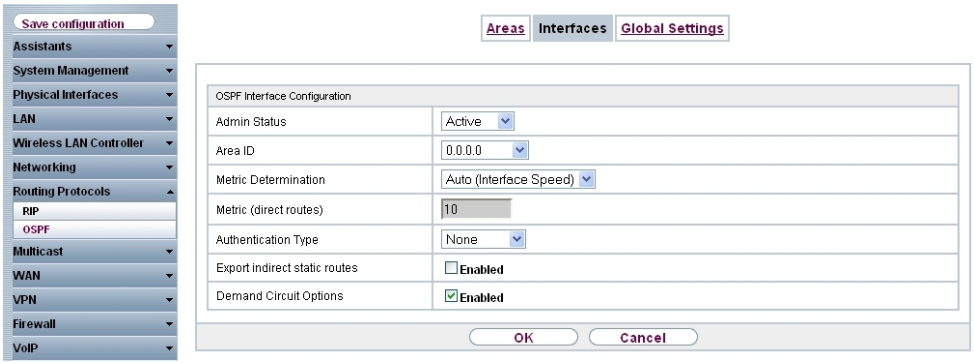


Fig. 28: **Routing Protocols** -> **OSPF** -> **Interfaces** -> **<Location A/Location B>** .

Proceed as follows:

(1) Set the OSPF **Admin Status** for the VPN IPSec interfaces to `Active` in order to propagate routing information on these interfaces. For all the other interfaces, the default value `Passive` is used to provide their routing information to the two VPN IPSec interfaces.

(2) Confirm with **OK**.

The complete configuration looks like this:

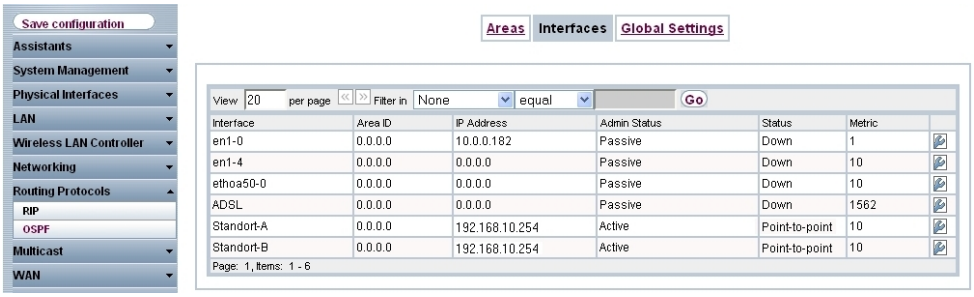


Fig. 29: **Routing Protocols** -> **OSPF** -> **Interfaces** .

4.2.2 Configure the gateway at Location A

Configure the Internet access at the Location A gateway

The Internet access at the Location A gateway can be configured using the **Assistant**.

(1) Go to **Assistants** -> **Internet Access**-> **Internet Connections** -> **New**.

(2) For **Connection Type**, select `Internal ADSL Modem`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

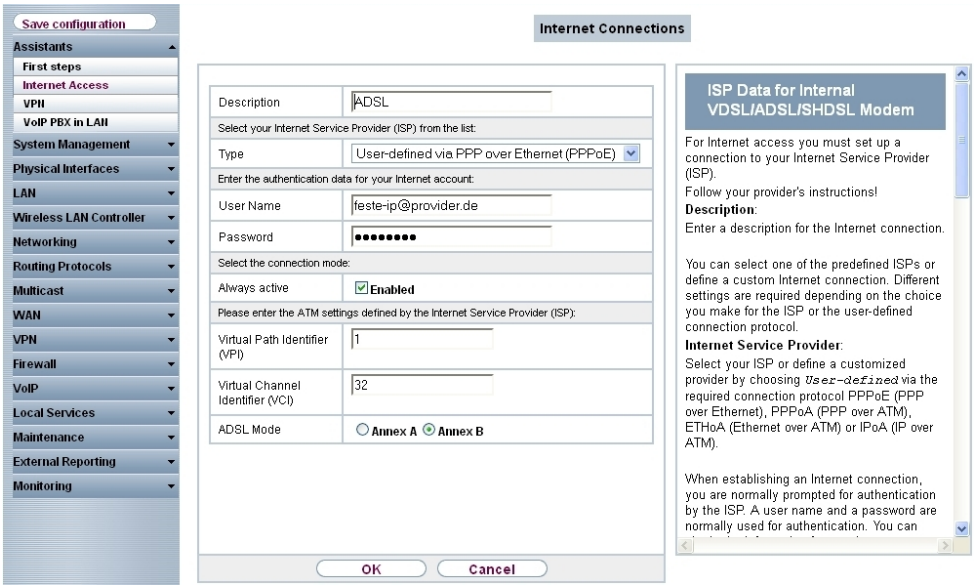


Fig. 30: **Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**

Proceed as follows to configure an Internet access:

(1) Under **Description** enter e. g. `ADSL` .

(2) For **Type**, select `User-defined via PPP over Ethernet (PPPoE).`

(3) As the **User** , enter the name which your provider has given you, e. g. `feste-ip@provider.de` .

(4) Enter the **Password** that your provider has given you, e. g. `test12345`.

(5) Enable the **Always active** option.

(6) For **ADSL Mode**, select `Annex B` for applications in Europe (provider-dependent).

(7) Press **OK** to confirm your entries.

Configure the VPN IPSec connection at the Location A gateway

In our example, the VPN tunnels are always set up from the branch gateway to the head office gateway. The VPN IPSec configuration is configured using the assistant.

(1) Go to **Assistants** -> **VPN** -> **VPN Connections** -> **New**.

(2) For **IPSec Scenario** select `IPSec-LAN-LAN Connection`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

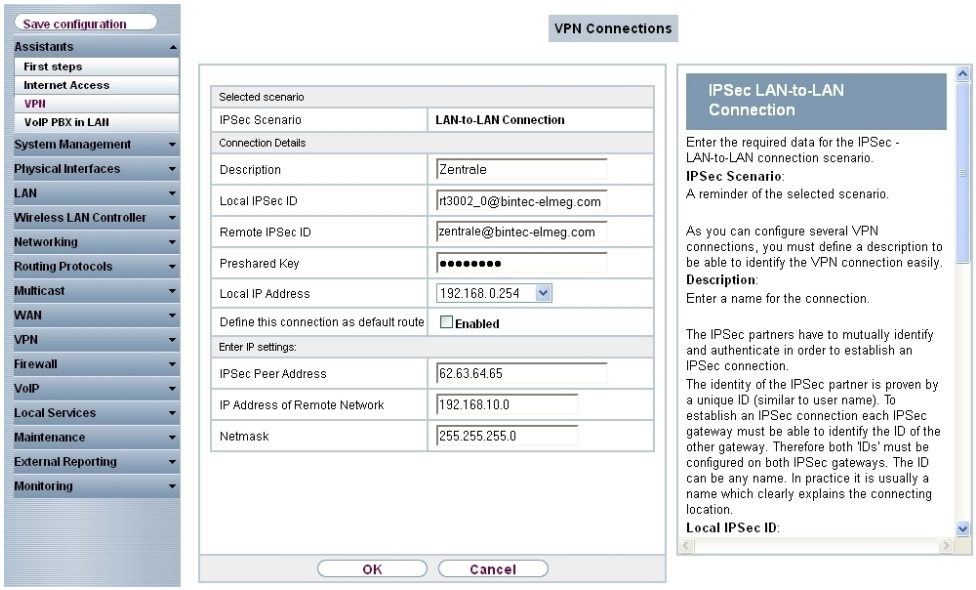


Fig. 31: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

To add the VPN connection to the head office gateway, proceed as follows:

(1) For **Description**, enter a description of the peer which identifies it, e. g. *Head Office*.

(2) For **Local IPSec ID**, enter the IPSec ID of the Location A gateway, e. g. *rt3002_0@bintec-elmeg.com*.

(3) For **Remote IPSec ID**, enter the IPSec ID of the head office gateway, e. g. *zentrale@bintec-elmeg.com*.

Note

This ID must be unique.

(4) In the **Preshared Key** field, enter a password for the encrypted connection (e. g. *test12345*.

(5) The **Local IP address** specifies the IP address of the IPSec interface, e. g. *192.168.0.254*.

(6) For **IPSec Peer Address**, the IP address or the DNS name that will be used to access the head office gateway must be entered. In our example, we shall use the head office gateway's static WAN IP address, e. g. 62.63.64.65.

(7) For **IP Address of Remote Network**, the network address of one of the IP networks used at head office must be configured, e. g. *192.168.10.0* and the **net mask** *255.255.255.0*.

(8) Confirm with **OK**.

In the next step, the OSPF routing protocol is enabled. This propagates the routing entries via the VPN IPSec tunnel at the locations.

(1) Go to **Routing Protocols** -> **OSPF** -> **Global Settings**.

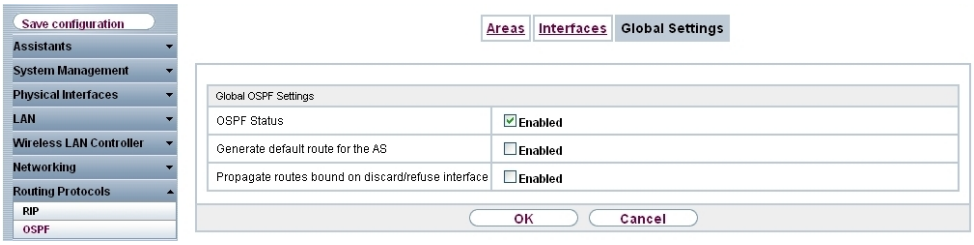


Fig. 32: **Routing Protocols** -> **OSPF** -> **Global Settings**.

Proceed as follows:

(1) Enable the **OSPF Status** option.

(2) Confirm with **OK**.

You specify which interface IP routing information is propagated on in the **Interfaces** menu.

(1) Go to **Routing Protocols** -> **OSPF** -> **Interfaces** -><**head office**> .

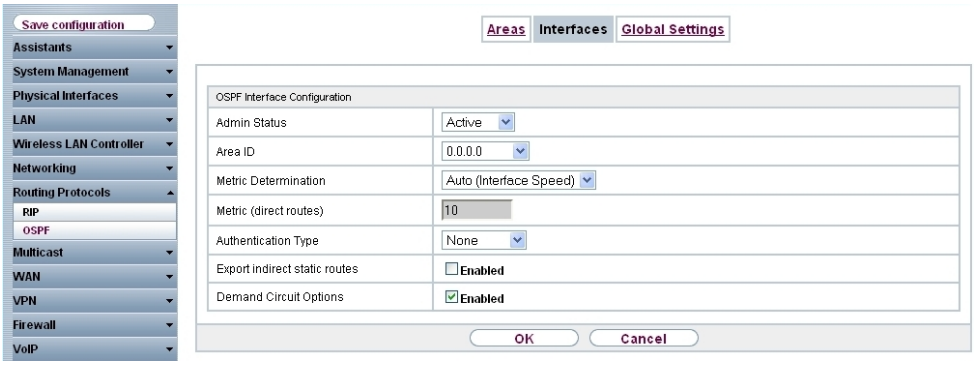


Fig. 33: **Routing Protocols** -> **OSPF** -> **Interfaces** -> <**head office**>

Proceed as follows:

(1) Set the OSPF **Admin Status** for the two newly configured VPN IPSec interfaces to `Active` in order to propagate routing information on these interfaces. For all the other interfaces, the default value `Passive` is used to provide their routing information to the two VPN IPSec interfaces.

(2) Confirm with **OK**.

The complete configuration looks like this:

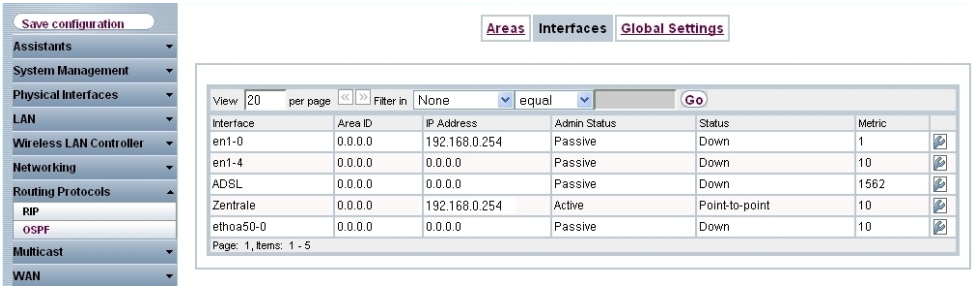


Fig. 34: **Routing Protocols** -> **OSPF** -> **Interfaces** .

4.2.3 Configure the gateway at Location B

Configure the Internet access at the Location B gateway

The Internet access at the Location B gateway can be configured using the **Assistant**.

(1) Go to **Assistants** -> **Internet Access**-> **Internet Connections** -> **New**.

(2) For **Connection Type**, select `Internal ADSL Modem`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

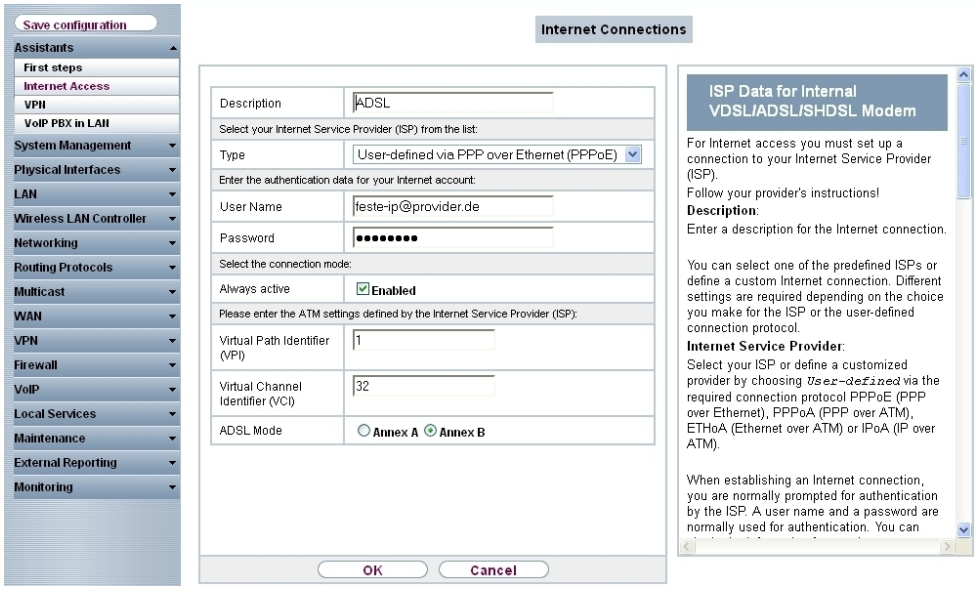


Fig. 35: **Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**

Proceed as follows to configure an Internet access:

(1) Under **Description** enter e. g. `ADSL`.

(2) For **Type**, select `User-defined via PPP over Ethernet (PPPoE).`

(3) As the **User** , enter the name which your provider has given you, e. g. `feste-ip@provider.de`.

(4) Enter the **Password** that your provider has given you, e. g. `test12345`.

(5) Enable the **Always active** option.

(6) For **ADSL Mode**, select `Annex B` for applications in Europe (provider-dependent).

(7) Press **OK** to confirm your entries.

Configure the VPN IPSec connection at the Location B gateway

In our example, the VPN tunnels are always set up from the branch gateway to the head office gateway. The VPN IPSec configuration is configured using the assistant.

(1) Go to **Assistants** -> **VPN** -> **VPN Connections** -> **New**.

(2) For **IPSec Scenario** select `IPSec-LAN-LAN Connection`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

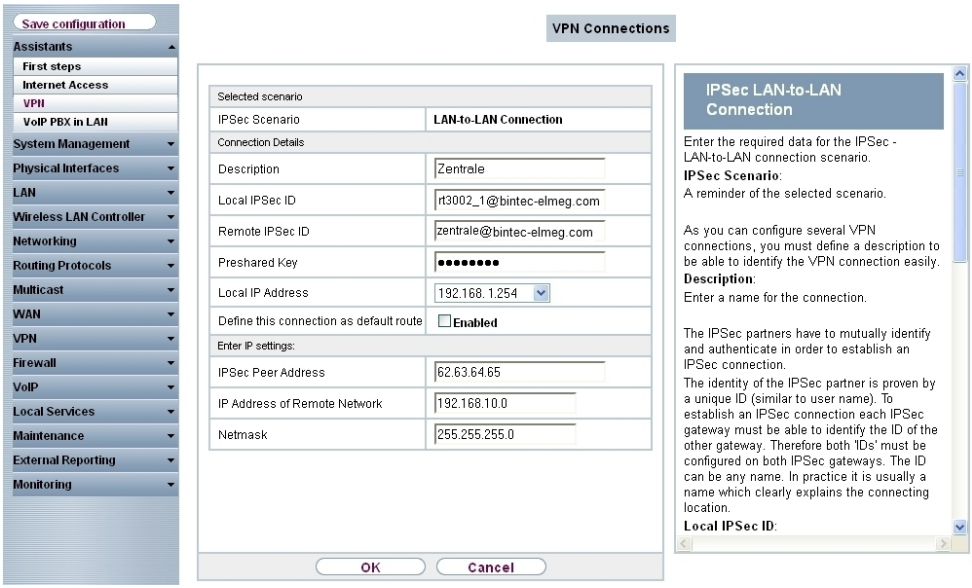


Fig. 36: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

To add the VPN connection to the head office gateway, proceed as follows:

(1) For **Description**, enter a description of the peer which identifies it, e. g. *`Head Office`*.

(2) For **Local IPSec ID**, enter the IPSec ID of the Location B gateway, e. g. *`rt3002_1@bintec-elmeg.com`*.

(3) For **Remote IPSec ID**, enter the IPSec ID of the head office gateway, e. g. *`zentrale@bintec-elmeg.com`*.

Note

This ID must be unique.

(4) In the **Preshared Key** field, enter a password for the encrypted connection (e. g. *`test12345`*.

(5) The **Local IP address** specifies the IP address of the IPSec interface, e. g. *`192.168.1.254`*.

(6) For **IPSec Peer Address**, the IP address or the DNS name that will be used to access the head office gateway must be entered. In our example, we shall use the head office gateway's static WAN IP address, e. g. 62.63.64.65.

(7) For **IP Address of Remote Network**, the network address of one of the IP networks used at head office must be configured, e. g. *`192.168.10.0`* and the **net mask** *`255.255.255.0`*.

(8) Confirm with **OK**.

In the next step, the OSPF routing protocol is enabled. This propagates the routing entries via the VPN IPSec tunnel at the locations.

(1) Go to **Routing Protocols** -> **OSPF** -> **Global Settings**.

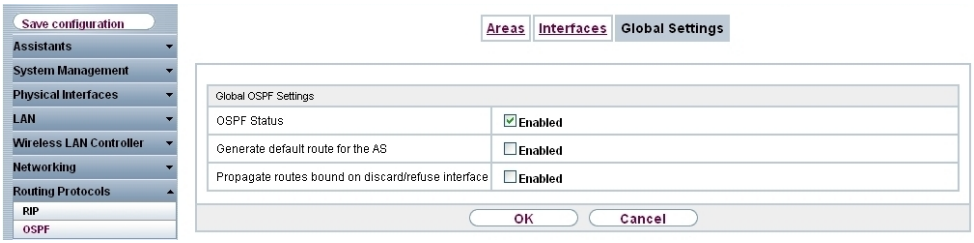


Fig. 37: **Routing Protocols** -> **OSPF** -> **Global Settings**.

Proceed as follows:

(1) Enable the **OSPF Status** option.

(2) Confirm with **OK**.

You specify which interface IP routing information is propagated on in the **Interfaces** menu.

(1) Go to **Routing Protocols** -> **OSPF** -> **Interfaces** -><**head office**> .

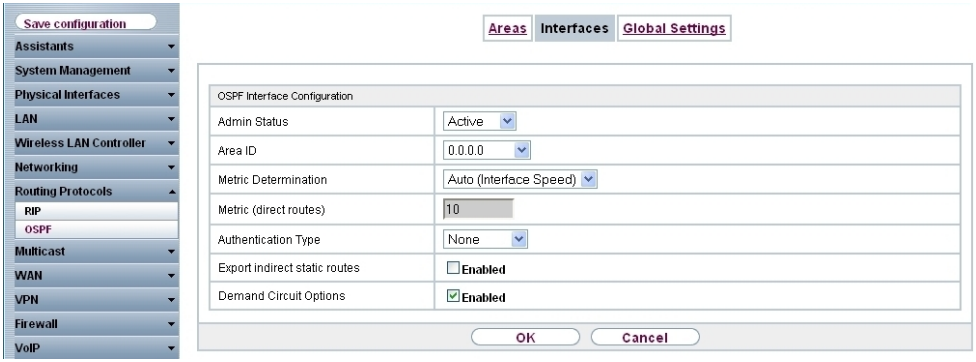


Fig. 38: **Routing Protocols** -> **OSPF** -> **Interfaces** -> <**head office**>

Proceed as follows:

(1) Set the OSPF **Admin Status** for the VPN IPSec interfaces to `Active` in order to propagate routing information on these interfaces. For all the other interfaces, the default value `Passive` is used to provide their routing information to the two VPN IPSec interfaces.

(2) Confirm with **OK**.

The complete configuration looks like this:

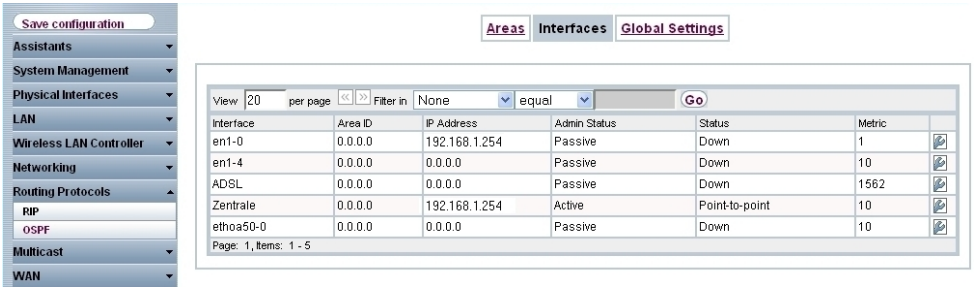


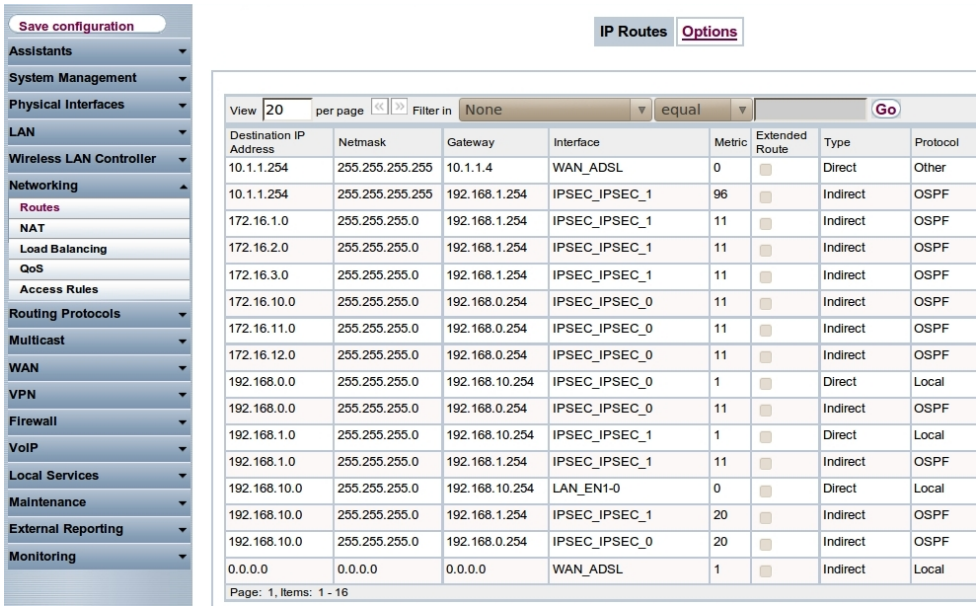
Fig. 39: **Routing Protocols** -> **OSPF** -> **Interfaces** .

4.3 OSPF monitoring

With the VPN IPSec configuration, the head office network (192.168.10.0/24) has been connected to the two Locations A and B (192.168.0.0/24 and 192.168.1.0/24). As shown in the example scenario, other IP networks, (e. g. 172.16.1.0/24 or 172.16.10.0/24 and others) are used at the two branch locations. To enable communication between Location A and Location B, and to make all the other networks accessible from every location, the gateways share all the routing information by means of the OSPF routing protocol. Using the VPN IPSec tunnel, this routing information is sent encrypted and updated periodically.

The **Protocol** column indicates whether the routing entry was configured manually or whether a routing entry was generated using the OSPF routing protocol.

(1) Go to **Network** -> **Routes** ->**IP Routes**.



Destination IP Address	Netmask	Gateway	Interface	Metric	Extended Route	Type	Protocol
10.1.1.254	255.255.255.255	10.1.1.4	WAN_ADSL	0		Direct	Other
10.1.1.254	255.255.255.255	192.168.1.254	IPSEC_IPSEC_1	96		Indirect	OSPF
172.16.1.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11		Indirect	OSPF
172.16.2.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11		Indirect	OSPF
172.16.3.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11		Indirect	OSPF
172.16.10.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11		Indirect	OSPF
172.16.11.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11		Indirect	OSPF
172.16.12.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11		Indirect	OSPF
192.168.0.0	255.255.255.0	192.168.10.254	IPSEC_IPSEC_0	1		Direct	Local
192.168.0.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	11		Indirect	OSPF
192.168.1.0	255.255.255.0	192.168.10.254	IPSEC_IPSEC_1	1		Direct	Local
192.168.1.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	11		Indirect	OSPF
192.168.10.0	255.255.255.0	192.168.10.254	LAN_EN1-0	0		Direct	Local
192.168.10.0	255.255.255.0	192.168.1.254	IPSEC_IPSEC_1	20		Indirect	OSPF
192.168.10.0	255.255.255.0	192.168.0.254	IPSEC_IPSEC_0	20		Indirect	OSPF
0.0.0.0	0.0.0.0	0.0.0.0	WAN_ADSL	1		Indirect	Local

Page: 1, Items: 1 - 16

Fig. 40: **Network** -> **Routes** ->**IP Routes**

The OSPF status information can be viewed with the GUI.

(1) Go to **Monitoring** -> **OSPF** -> **Status**.

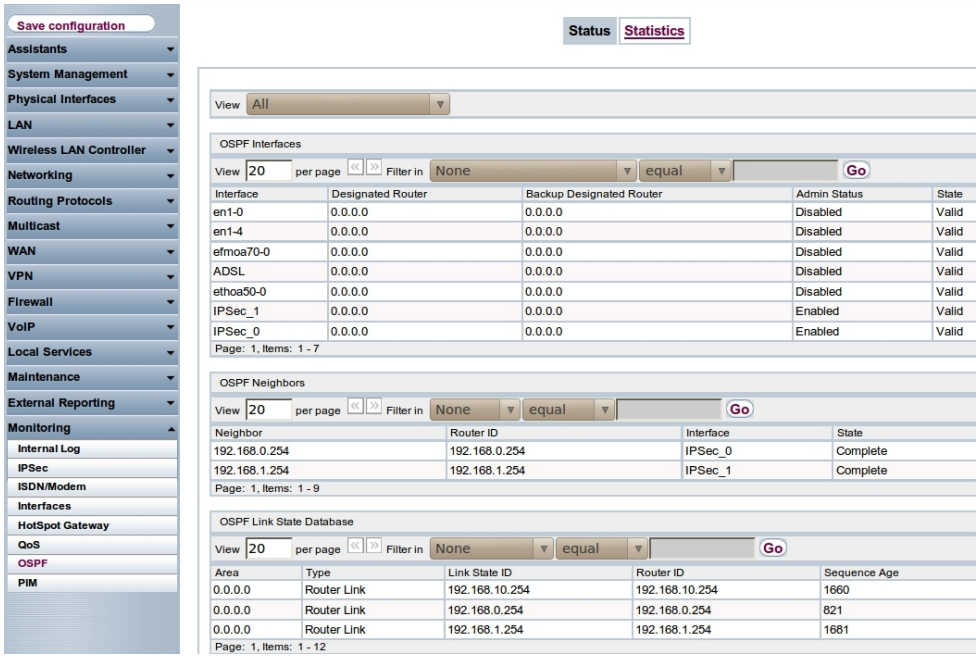


Fig. 41: **Monitoring** -> **OSPF** -> **Status**

The OSPF status information can be viewed using a console command.

```
Datei  Bearbeiten  Ansicht  Terminal  Hilfe
Welcome to R3502 version V.7.10 Rev. 1 (Patch 3) IPSec from 2011/08/26 00:00:00
systemname is r3502, location

Login: admin
Password:
Password not changed. Call "setup" for quick configuration.

r3502:> ospfmon db
    Area 0.0.0.0

    Router Link Age 861 Options 0x22 LsId 192.168.0.254
    RtrId 192.168.0.254 Seq 0x8000001f Checksum 0x917d Len 108
        options 0x0 links 7
        Point to Point id 192.168.10.254 data 192.168.0.254 metric 10
        Stub Network id 192.168.10.0 data 255.255.255.0 metric 10
        Stub Network id 10.1.1.254 data 255.255.255.255 metric 164
        Stub Network id 172.16.12.0 data 255.255.255.0 metric 1
        Stub Network id 172.16.11.0 data 255.255.255.0 metric 1
        Stub Network id 172.16.10.0 data 255.255.255.0 metric 1
        Stub Network id 192.168.0.0 data 255.255.255.0 metric 1

    Router Link Age 1721 Options 0x22 LsId 192.168.1.254
    RtrId 192.168.1.254 Seq 0x8000002a Checksum 0xe583 Len 108
        options 0x0 links 7
        Point to Point id 192.168.10.254 data 192.168.1.254 metric 10
        Stub Network id 192.168.10.0 data 255.255.255.0 metric 10
        Stub Network id 10.1.1.254 data 255.255.255.255 metric 86
        Stub Network id 172.16.3.0 data 255.255.255.0 metric 1
        Stub Network id 172.16.2.0 data 255.255.255.0 metric 1
        Stub Network id 172.16.1.0 data 255.255.255.0 metric 1
        Stub Network id 192.168.1.0 data 255.255.255.0 metric 1

    Router Link Age 1700 Options 0x22 LsId 192.168.10.254
    RtrId 192.168.10.254 Seq 0x8000000b Checksum 0xa9bf Len 96
        options 0x0 links 6
        Point to Point id 192.168.0.254 data 192.168.10.254 metric 10
        Stub Network id 192.168.0.0 data 255.255.255.0 metric 10
        Point to Point id 192.168.1.254 data 192.168.10.254 metric 10
        Stub Network id 192.168.1.0 data 255.255.255.0 metric 10
        Stub Network id 10.1.1.254 data 255.255.255.255 metric 92
        Stub Network id 192.168.10.0 data 255.255.255.0 metric 1

r3502:>
```

Fig. 42: Status information

4.4 Overview of Configuration Steps

Configure the gateway at head office

Field	Menu	Value
Connector Type	**Assistants** -> **Internet Access** -> **Internet Connections** -> **New**	*Internal ADSL Modem*
Description	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *ADSL*
Type	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*User-defined via PPP over Ethernet (PPPoE)*
User Name	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *feste-ip@provider.de*
Password	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *test12345*
Always Active	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*Enabled*
ADSL Mode	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*Annex B*
VPN scenario	**Assistants** -> **VPN** -> **VPN Connections** -> **New**	*IPSec - LAN-to-LAN connection*
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *Location A*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *zentrale@bintec-elmeg.com*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *rt3002_0@bintec-elmeg.com*
Preshared key	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *test12345*
Local IP Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.10.254*
IP Address of Remote Network	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.0.0*
Netmask	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *255.255.255.0*

Field	Menu	Value
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *Location B*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *zentrale@bintec-elmeg.com*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *rt3002_1@bintec-elmeg.com*
Preshared key	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *test12345*
Local IP Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.10.254*
IP Address of Remote Network	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.1.0*
Netmask	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *255.255.255.0*
OSPF status	**Routing Protocols** -> **OSPF** -> **Global Settings**.	*Enabled*
Admin Status	**Routing Protocols** -> **OSPF** -> **Interfaces** -> **<Location A>**	*Active*
Admin Status	**Routing Protocols** -> **OSPF** -> **Interfaces** -> **<Location B>**	*Active*

Configure the gateway at Location A

Field	Menu	Value
Connector Type	**Assistants** -> **Internet Access** -> **Internet Connections** -> **New**	*Internal ADSL Modem*
Description	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *ADSL*
Type	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*User-defined via PPP over Ethernet (PPPoE)*
User Name	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *feste-ip@provider.de*
Password	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *test12345*
Always Active	**Assistants** -> **Internet Access** -> **Inter-**	*Enabled*

Field	Menu	Value
	net Connections -> **Next**	
ADSL Mode	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*Annex B*
Connector Type	**Assistants** -> **VPN** -> **VPN Connections** -> **New**	*Internal ADSL Modem*
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *Head Office*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *rt3002_0@bintec-elmeg.com*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *zentrale@bintec-elmeg.com*
Preshared key	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *test12345*
Local IP Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.0.254*
IPSec Peer Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *62.63.64.65*
IP Address of Remote Network	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.10.0*
Netmask	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *255.255.255.0*
OSPF status	**Routing Protocols** -> **OSPF** -> **Global Settings**.	*Enabled*
Admin Status	**Routing Protocols** -> **OSPF** -> **Interfaces** -> **<head office>**	*Active*

Configure the gateway at Location B

Field	Menu	Value
Connector Type	**Assistants** -> **Internet Access** -> **Internet Connections** -> **New**	*Internal ADSL Modem*
Description	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *ADSL*
Type	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*User-defined via PPP over Ethernet (PPPoE)*

Field	Menu	Value
User Name	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *feste-ip@provider.de*
Password	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	e. g. *test12345*
Always Active	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*Enabled*
ADSL Mode	**Assistants** -> **Internet Access** -> **Internet Connections** -> **Next**	*Annex B*
Connector Type	**Assistants** -> **VPN** -> **VPN Connections** -> **New**	*Internal ADSL Modem*
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *Head Office*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *rt3002_1@bintec-elmeg.com*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *zentrale@bintec-elmeg.com*
Preshared key	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *test12345*
Local IP Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.1.254*
IPSec Peer Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *62.63.64.65*
IP Address of Remote Network	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *192.168.10.0*
Netmask	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e. g. *255.255.255.0*
OSPF status	**Routing Protocols** -> **OSPF** -> **Global Settings**.	*Enabled*
Admin Status	**Routing Protocols** -> **OSPF** -> **Interfaces** -> **<head office>**	*Active*

Chapter 5 IP - RIPv2 Routing Protocol over IPSec Connection

5.1 Introduction

This solution shows the linking of two locations by an IPSec connection in which the RIPv2 routing protocol is used to transmit the IP network areas configured in both locations. Using a routing protocol is particularly beneficial in the case of more complex network structures (more IP network areas), because changes in the network structure are automatically propagated to all the routers involved in the network via the routing protocol. The example that follows aims to explain the way it works.

The GUI is used to do the configuration.

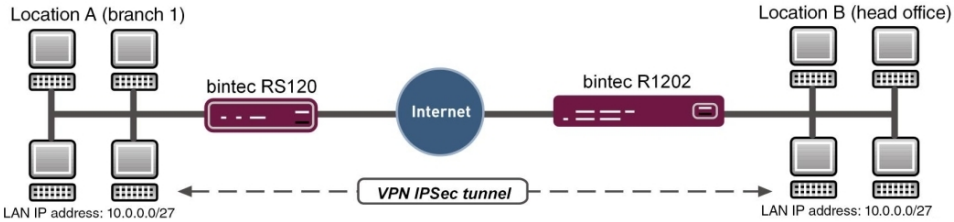


Fig. 43: Example scenario

In our example, an additional network is now to be added at Location A. With statically configured routing the result of this would be that the VPN gateway configuration at both locations would need to be changed. This is not the case if a routing protocol is used. In such cases, only the Location A VPN gateway needs to be configured. Specifically, the administrator only needs to configure the network on the LAN interface of the Location A VPN gateway. The routing protocol takes care of the rest.

The VPN gateways support the use of routing protocols, including in connection with IPSec connections. The following workshop aims to clarify this using a concrete example.

Requirements

The following are required for the configuration:

- A VPN gateway e. g. **bintec R1202** at head office
- A VPN gateway e. g. **bintec RS120** at the field office

- A boot image of Version 7.10.1 on both gateways
- Both gateways require an independent connection to the Internet

About the test setup

RS120 Location A (field office):	
System Name	RS120 field office 1 (used as local IPSec peer ID)
LAN IP address	10.0.0.30
LAN IP subnet mask	255.255.255.224
Public Internet IP address	62.146.1.1 (a host name can also be used here)
Standard gateway IP address	62.146.1.2
Local IP address of the IPSec interface	1.0.0.1 (Important: this IP address must be unique, i. e. may not be in the locations' LAN IP address range.)

R1202 Location B (head office):	
System Name	R1202 head office (used as local IPSec peer ID)
LAN IP address	100.0.0.30
LAN IP subnet mask	255.255.255.224
Public Internet IP address	62.147.1.1 (a host name can also be used here)
Standard gateway IP address	62.147.1.2
Local IP address of the IPSec interface	1.0.0.2 (Important: this IP address must be unique, i. e. may not be in the locations' LAN IP address range.)

5.2 Configuration

5.2.1 Configure the bintec R1202 at Location B (head office)

Configure the IPSec Connection

First set up a new connection. The IPSec Phase 1 / IPSec Phase 2 standard profiles are used in the example.

To do this, go to the following menu:

(1) Go to **VPN** -> **IPSec** -> **IPSec Peers** -> **New**.

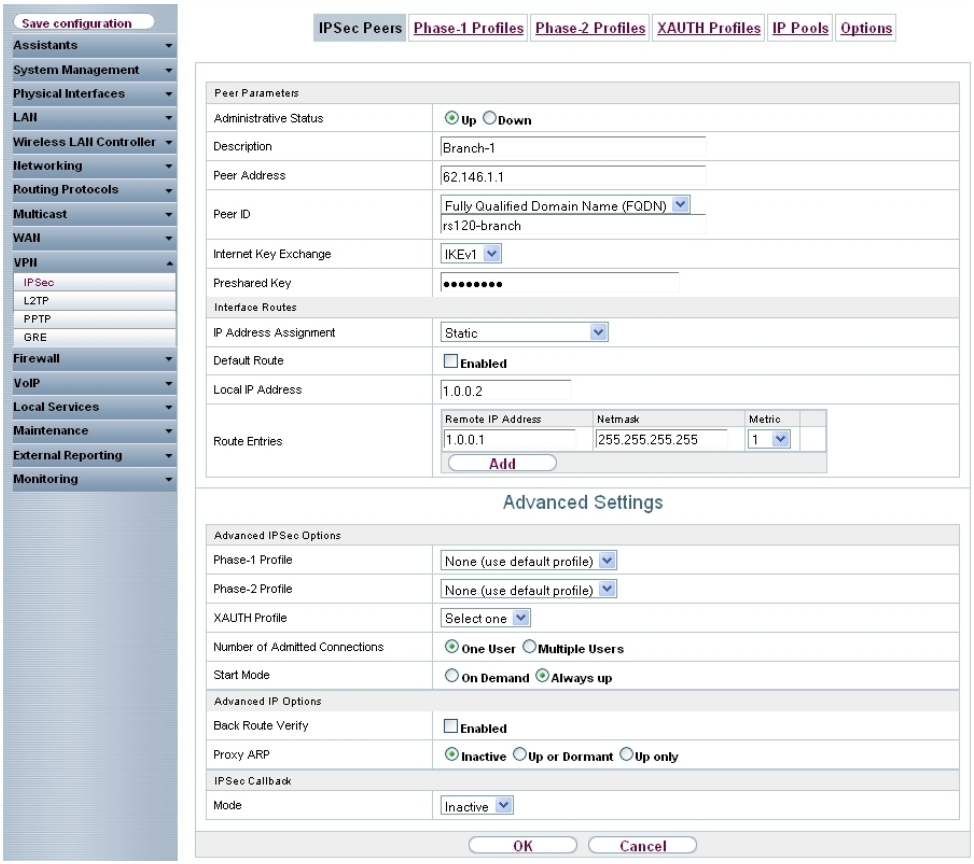


Fig. 44: **VPN**-> **IPSec**-> **IPSec Peers**-> **New**

To add a new connection, proceed as follows:

(1) For **Description**, enter a description of the peer which identifies it, e. g. `Field Office 1`.

(2) For **Peer Address**, enter the public Internet IP address, e. g. `62.146.1.1`.

(3) For **Peer ID**, enter the peer's ID, e. g. `RS120 field office 1`.

(4) For **Preshared Key**, enter the password for the encrypted connection (e. g. `test`.

(5) The **Local IP address** specifies the IP address of the IPSec interface, here e. g. `1.0.0.2`.

Note

Here, do NOT enter the LAN IP address of the **bintec R1202**, but use an IP address which is NOT within a location's LAN IP address range.

(6) The local IP address of the field office's IPSec interface should be configured as the **Route Entry**, here e. g. `1.0.0.1`. In this case, the subnet mask can be `255.255.255.255` (host route).

Note

Here, do NOT enter the actual network routes for accessing the remote location. The creating of the network routes that are required to access the locations concerned is done, in our case, by the RIP routing protocol.

(7) The **Start Mode** must be configured to `Always active` konfiguriert sein. In this mode, the IPSec connection is always established automatically, i. e. the connection is always active. This is needed so that RIP can transmit the routes to the relevant neighbour gateway.

(8) Leave the remaining settings unchanged and confirm them with **OK**.

Changing the Phase 1 profile

To configure the Phase 1 profile, open the profile that is indicated to be the default.

(1) Go to **VPN** -> **IPSec** -> **Phase 1 Profiles** ->.

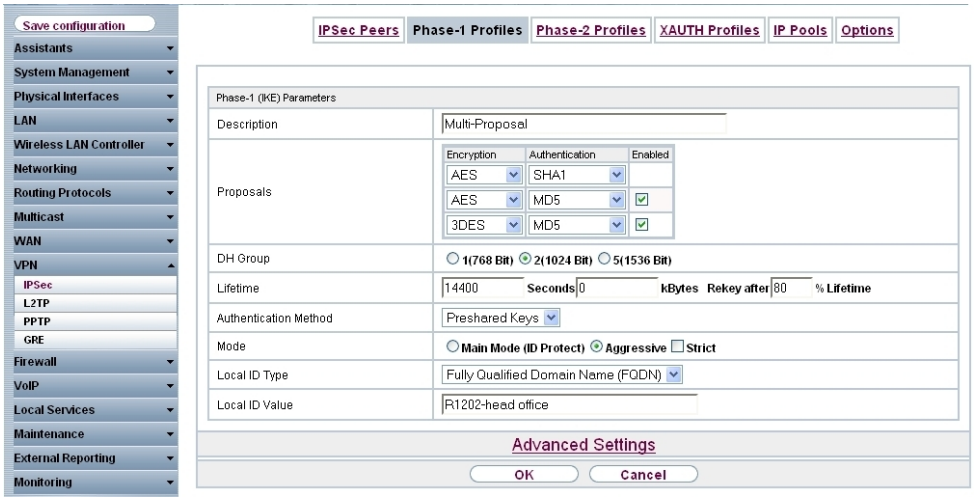


Fig. 45: **VPN** -> **IPSec** -> **Phase 1 Profiles** ->

Proceed as follows:

(1) For **Local ID value**, enter the your device's ID, here e. g. `R1202 head office`.

(2) Leave the remaining settings unchanged and confirm them with **OK**.

Configure the RIP routing protocol for the IPSec interface

The routing protocol is configured in the RIP Interfaces menu.

(1) Go to **Routing Protocols** -> **RIP** -> **RIP Interfaces** -><**field office 1**> .

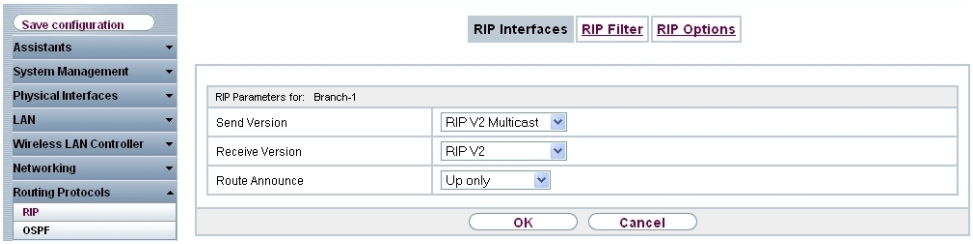


Fig. 46: **Routing Protocols** -> **RIP** -> **RIP Interfaces** -><**field office 1**> .

Proceed as follows:

(1) For the **Send Version**, select `RIP V2 Multicast`. The RIP protocol packets use the `224.0.0.9` multicast address as the target address. You may also use other RIP variants here. But it is important that the RIP version used (RIPv1/RIPv2) is the same on both VPN gateways.

(2) For the **Receive Version**, select `RIP V2`.

(3) For **Route Announce**, select `Active Only`.

(4) Press **OK** to confirm your entries.

In the last step in the configuration, the default route distribution is disabled.

(1) Go to **Routing Protocols** -> **RIP** -> **RIP Options**.

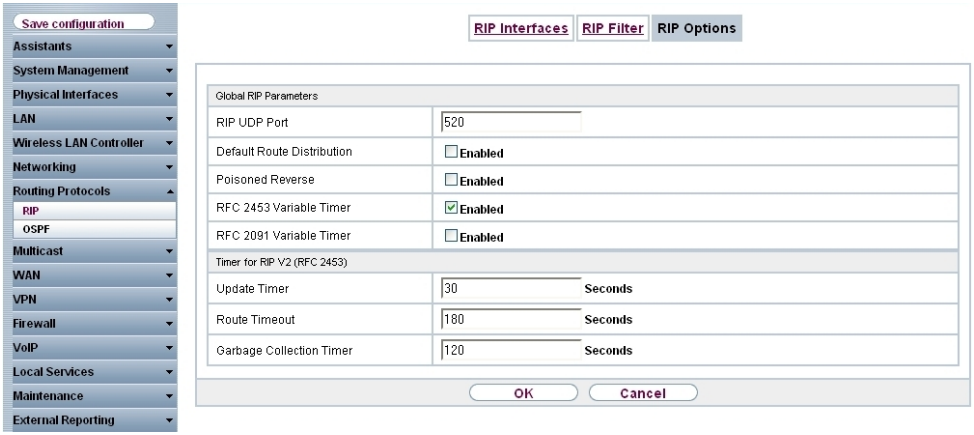


Fig. 47: **Routing Protocols** ->**RIP**->**RIP Options**

Proceed as follows:

(1) Disable the **Default Route Distribution** parameter. This prevents the configured default route being propagated via RIP.

(2) Confirm with **OK**.

This completes the configuration of the **bintec R1202** gateway.

5.2.2 Configure the bintec RS120 at Location B (field office)

Configure the IPSec Connection

First set up a new connection. The IPSec Phase 1 / IPSec Phase 2 standard profiles are used in the example.

To do this, go to the following menu:

(1) Go to **VPN** -> **IPSec** -> **IPSec Peers** -> **New**.

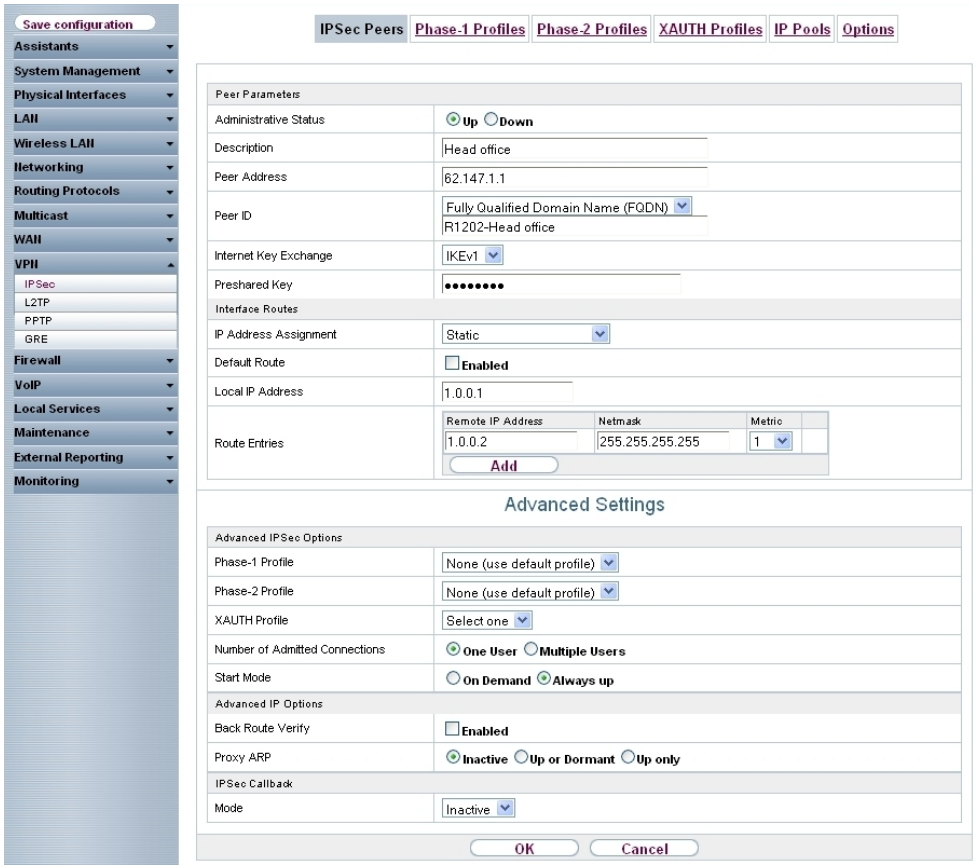


Fig. 48: **VPN**-> **IPSec**-> **IPSec Peers**-> **New**

To add a new connection, proceed as follows:

(1) For **Description**, enter a description of the peer which identifies it, e. g. *`Head Office`*.

(2) For **Peer Address**, enter the public Internet IP address, e. g. *`62.147.1.1`*.

(3) For **Peer ID**, enter the peer's ID, e. g. *`R1202 head office`*.

(4) For **Preshared Key**, enter the password for the encrypted connection (e. g. *`test`*.

(5) The **Local IP address** specifies the IP address of the IPSec interface, here e. g. *`1.0.0.1`*.

Note

Here, do NOT enter the LAN IP address of the **bintec RS120**, but use an IP address which is NOT within a location's LAN IP address range.

(6) The local IP address of the head office's IPSec interface should be configured as the **Route Entry**, here e. g. `1.0.0.2`. In this case, the subnet mask can be `255.255.255.255` (host route).

Note

Here, do NOT enter the actual network routes for accessing the remote location. The creating of the network routes that are required to access the locations concerned is done, in our case, by the RIP routing protocol.

(7) The **Start Mode** must be configured to `Always active` konfiguriert sein. In this mode, the IPSec connection is always established automatically, i. e. the connection is always active. This is needed so that RIP can transmit the routes to the relevant neighbour gateway.

(8) Leave the remaining settings unchanged and confirm them with **OK**.

Changing the Phase 1 profile

To configure the Phase 1 profile, open the profile that is indicated to be the default.

(1) Go to **VPN** -> **IPSec** -> **Phase 1 Profiles** ->.

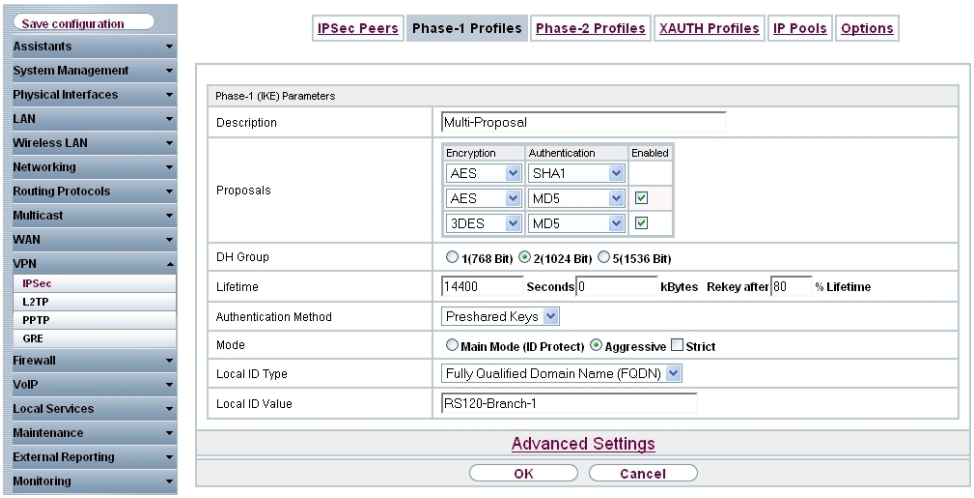


Fig. 49: **VPN** -> **IPSec** -> **Phase 1 Profiles** ->

Proceed as follows:

(1) For **Local ID value**, enter the your device's ID, here e. g. `RS120 field office 1`.

(2) Leave the remaining settings unchanged and confirm them with **OK**.

Configure the RIP routing protocol for the IPSec interface

The routing protocol is configured in the RIP Interfaces menu.

(1) Go to **Routing Protocols** -> **RIP** -> **RIP Interfaces** -><**head office**> .

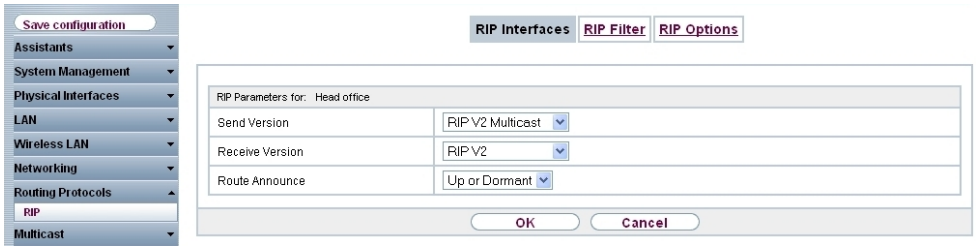


Fig. 50: **Routing Protocols** -> **RIP** -> **RIP Interfaces** -><**head office**> .

Proceed as follows:

(1) For the **Send Version**, select `RIP V2 Multicast`. The RIP protocol packets use the `224.0.0.9` multicast address as the target address. You may also use other RIP variants here. But it is important that the RIP version used (RIPv1/RIPv2) is the same on both VPN gateways.

(2) For the **Receive Version**, select `RIP V2`.

(3) For **Route Announce**, select `Up or Dormant`.

(4) Press **OK** to confirm your entries.

In the last step in the configuration, the default route distribution is disabled.

(1) Go to **Routing Protocols** -> **RIP** -> **RIP Options**.

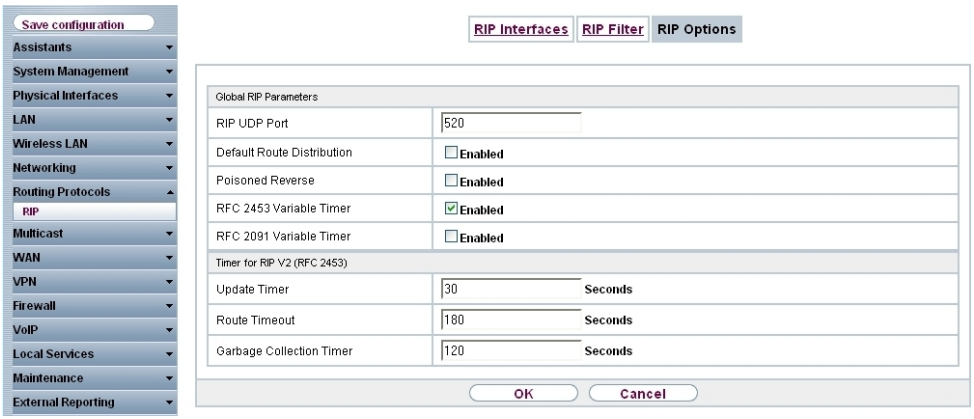


Fig. 51: **Routing Protocols** ->**RIP**->**RIP Options**

Proceed as follows:

(1) Disable the **Default Route Distribution** parameter. This prevents the configured default route being propagated via RIP.

(2) Confirm with **OK**.

This completes the configuration of the **bintec RS120** gateway.

5.3 Check functioning

If your Internet connection is working and the settings have been done in accordance with the instructions, the default connection should now work.

To check that it does, go to the **Network** -> **Routes** -> **IP Routes** menu.

Here you see, on both VPN gateways, the network routes to access the relevant location. The routes propagated via **RIP** are indicated in the table with the `RIP` protocol.

Results: Location B (head office)

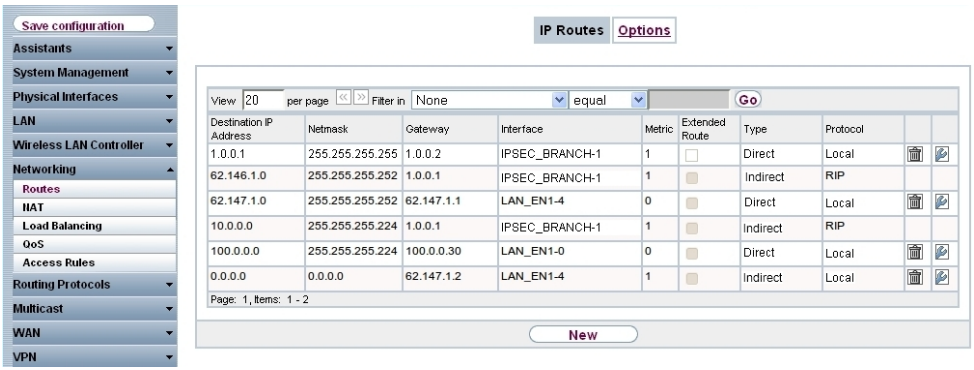


Fig. 52: **Network** -> **Routes** -> **IP Routes**

Results: Location A (field office)

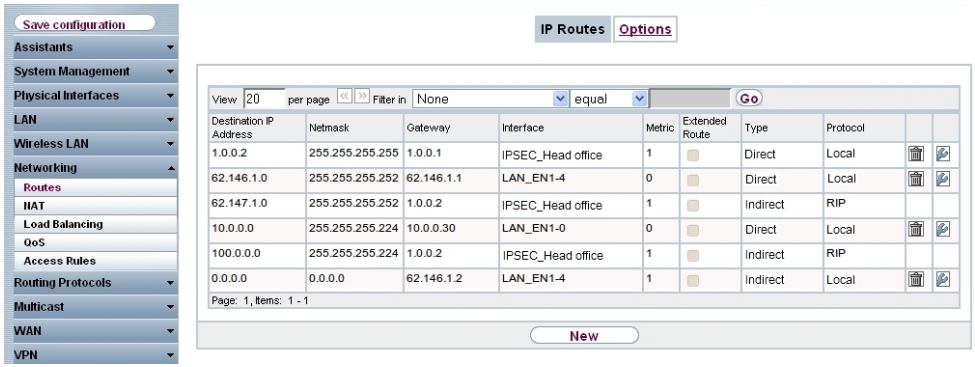


Fig. 53: **Network** -> **Routes** -> **IP Routes**

Now, any change made to the LAN IP configuration will automatically impact on the routing entries for both VPN gateways.

5.4 Overview of Configuration Steps

Configure IPSec connection (head office)

Field	Menu	Value
Description	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *Field Office 1*
Peer Address	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *62.146.1.1*
Peer ID	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *RS120 Field Office 1*
Preshared key	**VPN-> IPSec-> IPSec Peers-> New**	e.g. *test*
Local IP Address	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *1.0.0.2*
Route Entries	**VPN-> IPSec-> IPSec Peers-> New**	*1.0.0.1* and *255.255.255.255*
Start mode	**VPN-> IPSec-> IPSec Peers-> New**	*Always Active*

Changing the Phase-1 profile

Field	Menu	Value
Local ID Value	**VPN -> IPSec -> Phase 1 Profiles ->**	e. g. R1202 Head Office

Configure the routing protocol

Field	Menu	Value
Send Version	**Routing Protocols -> RIP -> RIP Interfaces -><field office 1>** .	*RIP V2 Multicast*
Receive Version	**Routing Protocols -> RIP -> RIP Inter-**	*RIP V2*

Field	Menu	Value
	faces -><field office 1> .	
Route Announce	**Routing Protocols** -> **RIP** -> **RIP Interfaces -><field office 1>** .	*Active Only*

Set up RIP options

Field	Menu	Value
Default Route Distribution	**Routing Protocols** ->**RIP**->**RIP Options**	*Disabled*

Configure IPSec connection (field office)

Field	Menu	Value
Description	**VPN**-> **IPSec**-> **IPSec Peers**-> **New**	e. g. *Head Office*
Peer Address	**VPN**-> **IPSec**-> **IPSec Peers**-> **New**	e. g. *62.147.1.1*
Peer ID	**VPN**-> **IPSec**-> **IPSec Peers**-> **New**	e. g. *R1202 Head Office*
Preshared key	**VPN**-> **IPSec**-> **IPSec Peers**-> **New**	e.g. *test*
Local IP Address	**VPN**-> **IPSec**-> **IPSec Peers**-> **New**	e. g. *1.0.0.1*
Route Entries	**VPN**-> **IPSec**-> **IPSec Peers**-> **New**	*1.0.0.2* and *255.255.255.255*
Start mode	**VPN**-> **IPSec**-> **IPSec Peers**-> **New**	*Always Active*

Changing the Phase-1 profile

Field	Menu	Value
Local ID Value	**VPN** -> **IPSec** -> **Phase 1 Profiles** ->	e. g. RS120 Field Office 1

Configure the routing protocol

Field	Menu	Value
Send Version	**Routing Protocols** -> **RIP** -> **RIP Interfaces -><field office 1>** .	*RIP V2 Multicast*
Receive Version	**Routing Protocols** -> **RIP** -> **RIP Interfaces -><field office 1>** .	*RIP V2*
Route Announce	**Routing Protocols** -> **RIP** -> **RIP Interfaces -><field office 1>** .	*Up or Dormant*

Set up RIP options

Field	Menu	Value
Default Route Distribution	**Routing Protocols** ->**RIP**->**RIP Options**	*Disabled*

Chapter 6 IP - ULA - Unique Local Addresses

6.1 Introduction

Internet Protocol Version 6 (IPv6) is needed to follow up IPv4 because the IPv4 address range is almost exhausted.

Note

But IPv4 addresses are still required! We recommend that you run the router as a perimeter system, without a router in front of it. This is due to using 6in4 and session timeouts.

In our example, we shall describe how to hook up IPv4 in the WAN and IPv4 in the LAN with ULA (Unique Local Addresses).

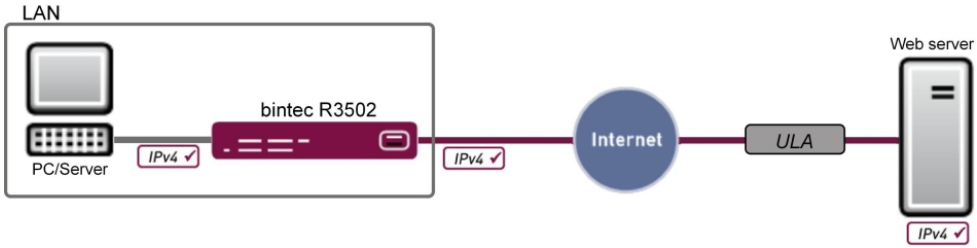


Fig. 54: Example scenario

WAN	LAN
WAN interface: en1-4	LAN interface: en1-0
IP address: 192.168.100.110/24	IP address: 192.168.0.254/24
Gateway IP address: 192.168.100.254	DHCP range: 192.168.0.10 - 192.168.0.39

The Graphical User Interface (GUI) is used for the configuration.

Requirements

The following are required for the configuration:

- A bintec gateway from the RS, Rxxx2 or RXL series, e. g. **bintec R3502** with system software 8.2.1

- A functioning Internet connection
- Internet Protocol Version 6 (IPv6) enabled on the relevant computers (IPv6 is enabled by default on Windows 7)
- All the necessary interfaces with their basic configuration
- Possibly a separate ULA range which can be requested from SixXS

6.2 Configuration

In the first step, the interface is configured; you will then create a prefix, and a subnet will automatically be created. A route will likewise be created automatically.

(1) Go to **LAN** -> **IP Configuration** -> **Interfaces** -> **New**.

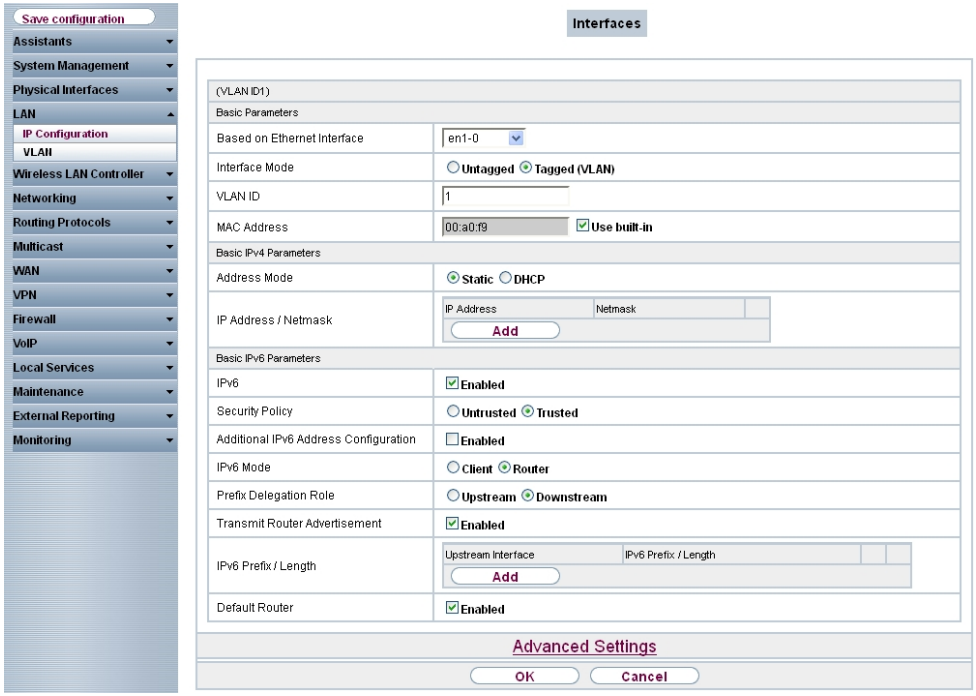


Fig. 55: **LAN** -> **IP Configuration** -> **Interfaces** -> **New**

Proceed as follows to configure an interface for IPv6:

(1) For **Based on Ethernet Interface**, select the interface which is used for IPv6, here e. g. `en1-0`.

(2) For **IPv6** select `Enabled`.

(3) For **Security Policy**, select `Trusted`. All IP packets are allowed through except for those which are explicitly prohibited.

(4) For **IPv6 Mode** leave the option `Router`.

(5) For **Prefix Delegation Role** leave the option `Downstream`.

(6) For **Transmit Router Advertisement**, select `Enabled`. Router advertisements are sent via the interface selected.

(7) In **IPv6 Prefix/Lenght**, click **Add** in order to create a prefix and automatically create a subnet.

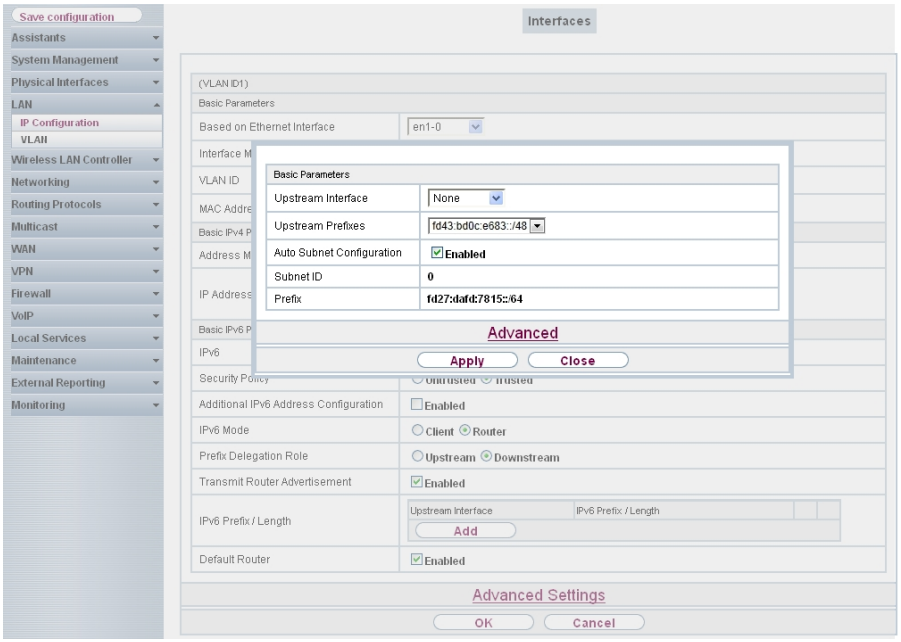


Fig. 56: **LAN** -> **IP Configuration** -> **Interfaces** -> **New** -> **Add**

(8) For **Upstream Interface**, select `None`.

Note

This setting is important because, for Unique Local Addresses (ULAs), there is no upstream interface which the packets can be transported to.

(9) For **Upstream Prefixes**, enter the prefix to specify the address range. For the ULA range in the GUI, that is the prefix `fd43:bd0c:e683::/48`.

(10) Leave **Auto Subnet Configuration** set to `Enabled`.
The automatically created **Subnet ID** `0` and the automatically created **Prefix** `fd43:bd0c:e683::/64`
for the subnet are displayed.

(11) Confirm with **Apply**.

(12) Leave the option **Default Router** *Enabled*.

(13) Confirm with **OK**.

A route has already been automatically created in **Networking** -> **Routes** ->**IPv6 Routes**. You cannot edit this route, and you need not create any further routes. All devices can be reached through this direct route.

6.3 Overview of Configuration Steps

Configure interface

Field	Menu	Value
Based on Ethernet Interface	**LAN** -> **IP Configuration** -> **Interfaces** -> **New**	e. g. *en1-0*
IPv6	**LAN** -> **IP Configuration** -> **Interfaces** -> **New**	*Enabled*
Security Policy	**LAN** -> **IP Configuration** -> **Interfaces** -> **New**	*Trusted*
IPv6 Mode	**LAN** -> **IP Configuration** -> **Interfaces** -> **New**	*Router*
Prefix Delegation Role	**LAN** -> **IP Configuration** -> **Interfaces** -> **New**	*Downstream*
Transmit Router Advertisement	**LAN** -> **IP Configuration** -> **Interfaces** -> **New**	*Enabled*
Default Router	**LAN** -> **IP Configuration** -> **Interfaces** -> **New**	*Enabled*

Assign address range

Field	Menu	Value
Upstream Interfaces	**LAN** -> **IP Configuration** -> **Interfaces**-> **New** -> **Add**	*None*
Upstream Prefixes	**LAN** -> **IP Configuration** -> **Interfaces**-> **New** -> **Add**	*fd43:bd0c:e683::/48*
Auto Subnet Configuration	**LAN** -> **IP Configuration** -> **Interfaces**-> **New** -> **Add**	*Enabled*

Chapter 7 IP - IPv6 LAN routing

7.1 Introduction

This examples describes the IPv6 routing between two networks with ULA prefixes. To do this, a ULA prefix with subnet ID is configured on a router to the two interfaces en1-0 and en1-4. It is important that no upstream interface is selected as there is no superordinate prefix in this scenario.

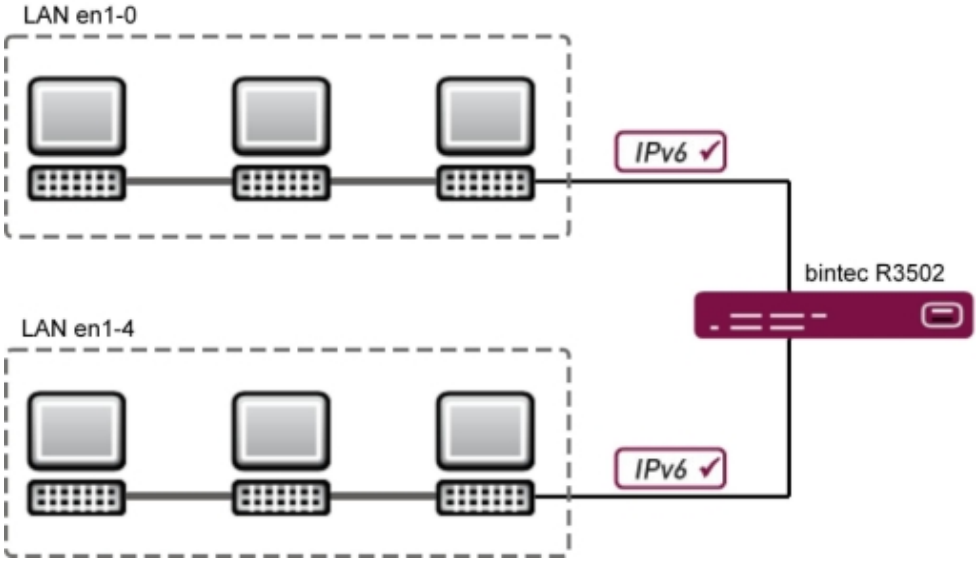


Fig. 57: Example scenario

The graphical user interface (GUI) is used for configuration.

The GUI is a web-based graphic user surface that you can use from any PC with an up-to-date Web browser via an HTTP or HTTPS connection.

To be able to configure your gateway with the GUI, you need to access the device via the serial interface, via LAN or via an ISDN connection. You need to start a web browser, enter the IP address of your device in the browser address bar, and log in with your user name and password.

Requirements

The following prerequisites for configuration must be met:

- A bintec gateway from the RS, Rxxx2 or RXL series, e.g. **bintec R3502** with system software 8.2.1
- Internet Protocol Version 6 (IPv6) enabled on the relevant computers (IPv6 is enabled by default on Windows 7)
- All the necessary interfaces with their basic configuration
- Potentially a separate ULA range; this can be requested from a tunnel broker, e.g. SixXS.

7.2 Configuration

For the configuration, a ULA prefix must be applied to the respective interface.

To create a ULA prefix for the **<en1-0>** interface, proceed as follows:

(1) Go to **LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>** .

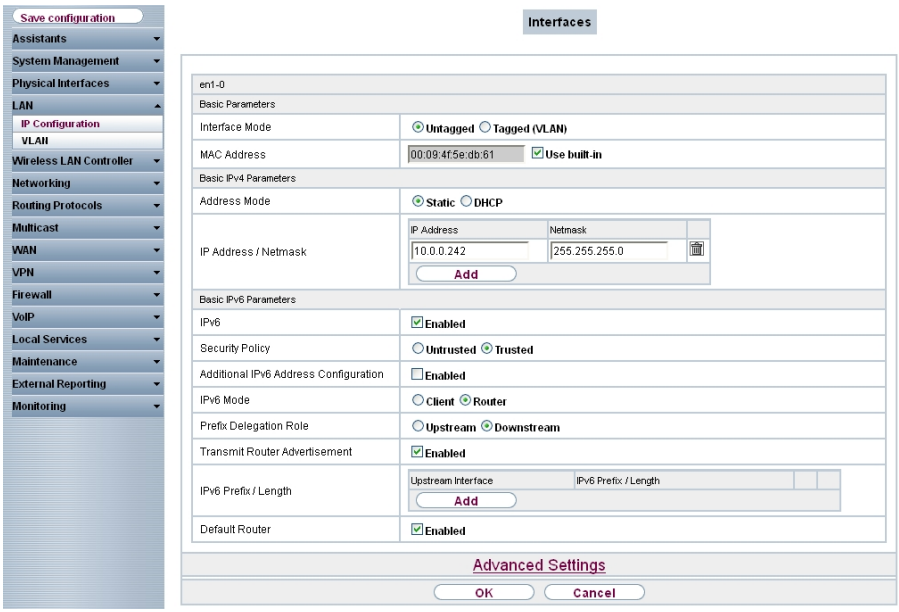


Fig. 58: **LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>**

(2) Select `Enabled` for **IPv6**.

(3) Leave **Security Policy** set to `Secure`. All IP packets are allowed through except for those which are explicitly prohibited.

(4) Leave **IPv6 Mode** set to `Router`.

(5) Leave **Prefix Delegation Role** set to `Downstream`.

(6) Leave **Transmit Router Advertisement** set to `Enabled`. Router advertisements are sent via the interface selected.

(7) Click **Add** under **IPv6 Prefix/Length** in order to automatically create a subnet.

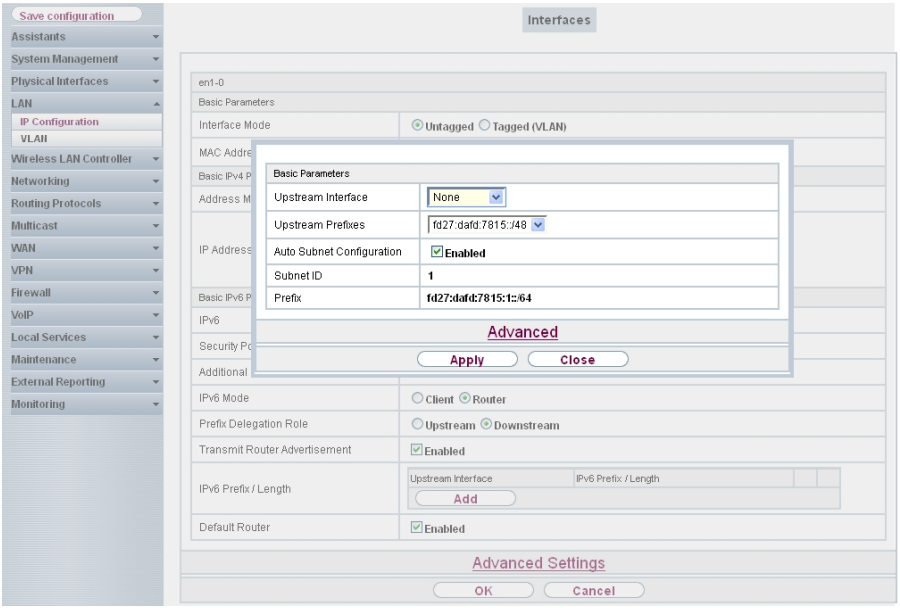


Fig. 59: **LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-0>** ->**Add**

(8) Select `None` for **Upstream Interface**.

(9) Select the displayed prefix `fd78:3491:5a32::/48` under **Upstream Prefixes**.

(10) Leave **Auto Subnet Configuration** set to `Enabled`.
The automatically created **Subnet ID** `0` and the automatically created prefix `fd78:3491:5a32::/64` are both displayed.

(11) Press **Apply** to confirm your entries.

(12) Leave **Standard Router** set to `Enabled`.

(13) Press **OK** to confirm your entries.

To create a ULA prefix for the **<en1-4>** interface, proceed as follows:

(1) Go to **LAN**-> **IP Configuration** ->**Interfaces**-> **<en1-4>** .

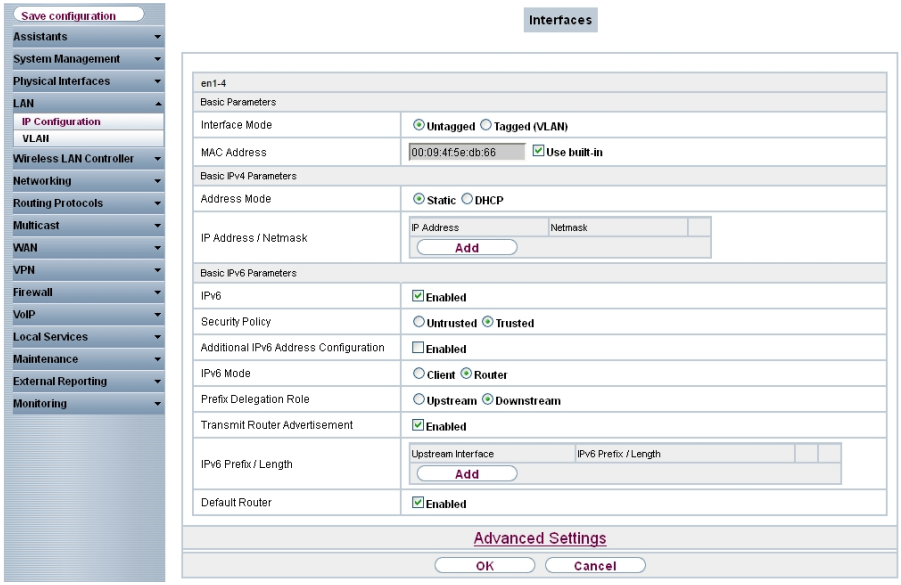


Fig. 60: **LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-4>**

(2) Select `Enabled` for **IPv6**.

(3) Leave **Security Policy** set to `Secure`. All IP packets are allowed through except for those which are explicitly prohibited.

(4) Leave **IPv6 Mode** set to `Router`.

(5) Leave **Prefix Delegation Role** set to `Downstream`.

(6) Leave **Transmit Router Advertisement** set to `Enabled`. Router advertisements are sent via the interface selected.

(7) Click **Add** under **IPv6 Prefix/Length** in order to automatically create a subnet.

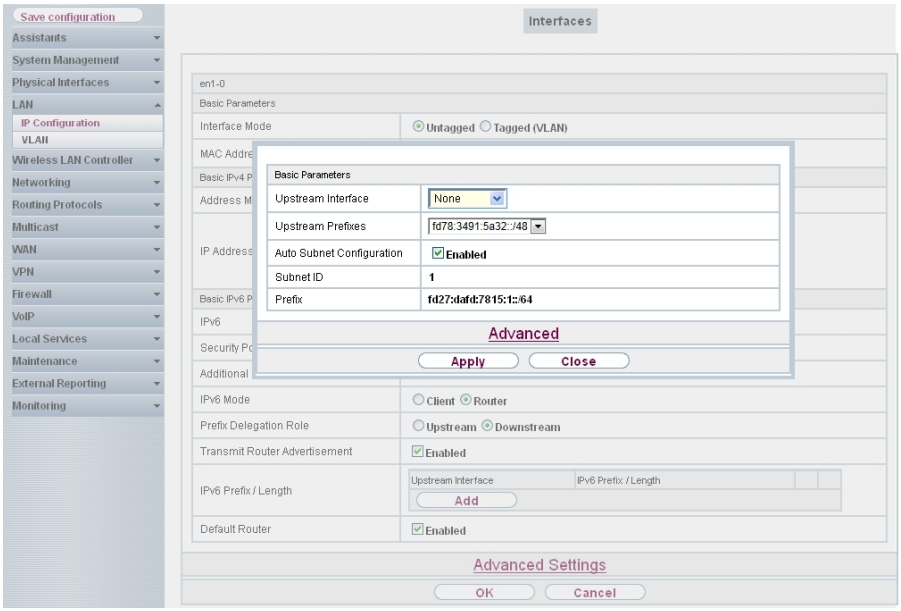


Fig. 61: **LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-4>** ->**Add**

(8) Select `None` for **Upstream Interface**.

(9) Select the displayed prefix `fd78:3491:5a32::/48` under **Upstream Prefixes**.

(10) Leave **Auto Subnet Configuration** set to `Enabled`.
The automatically created **Subnet ID** `1` and the automatically created prefix `fd78:3491:5a32:1::/64` are both displayed.

(11) Press **Apply** to confirm your entries.

(12) Leave **Standard Router** set to `Enabled`.

(13) Press **OK** to confirm your entries.

By configuring both prefixes, two new routers are automatically created enabling communication between both of the networks.

7.3 Overview of Configuration Steps

Interface <en1-0>

Configure Interface

Field	Menu	Value
IPv6	**LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>**	`Enabled`

Field	Menu	Value
Security Policy	**LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>**	*Secure*
IPv6 mode	**LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>**	*Router*
Prefix Delegation Role	**LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>**	*Downstream*
Transmit Router Advertisement	**LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>**	*Enabled*
Default router	**LAN** -> **IP Configuration** -> **Interfaces** -> **<en1-0>**	*Enabled*

Assign Address Range

Field	Menu	Value
Upstream interface	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-0>** ->**Add**	*None*
Upstream Prefixes	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-0>** ->**Add**	*fd78:3491:5a32::/48*
Auto Subnet Configuration	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-0>** ->**Add**	*Enabled*

Interface <en1-4>

Configure Interface

Field	Menu	Value
IPv6	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-4>**	*Enabled*
Security Policy	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-4>**	*Secure*
IPv6 mode	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-4>**	*Router*
Prefix Delegation Role	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-4>**	*Downstream*
Transmit Router Advertisement	**LAN** -> **IP Configuration** -> **Interfaces**-> **<en1-4>**	*Enabled*
Default router	**LAN** -> **IP Configuration** -> **Inter-**	*Enabled*

Field	Menu	Value
	faces-> <en1-4>	

Assign Address Range

Field	Menu	Value
Upstream Interface	**LAN** -> **IP Configuration** -> **Interfaces-> <en1-4>** ->**Add**	*None*
Upstream Prefixes	**LAN** -> **IP Configuration** -> **Interfaces-> <en1-4>** ->**Add**	*fd78:3491:5a32::/48*
Auto Subnet Configuration	**LAN** -> **IP Configuration** -> **Interfaces-> <en1-4>** ->**Add**	*Enabled*

Chapter 8 IP - SixXS IP tunnel broker with the ::/48 prefix

8.1 Introduction

This example describes how to hook up IPv4 in the WAN and IPv4/IPv6 in the LAN via a tunnel broker with the SixXS ::/48 prefix. With a tunnel and the appropriate prefix, the computer can supply itself with valid IPv6 addresses in its own LAN.

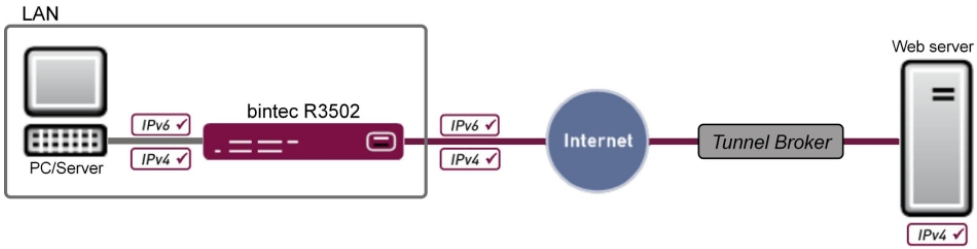


Fig. 62: Example scenario

WAN	LAN
WAN interface: Internet Service Provider via DSL	LAN interface: en1-0
IP address: Dynamic IP address	IP address: 192.168.0.254/24
	DHCP range: 192.168.0.10 - 192.168.0.39

The Graphical User Interface (GUI) is used for the configuration.

Requirements

The following are required for the configuration:

- A bintec gateway from the RS, Rxxx2 or RXL series, e. g. **bintec R3502** with system software 8.2.1
- A functioning Internet connection
- Internet Protocol Version 6 (IPv6) enabled on the relevant computers (IPv6 is enabled by default on Windows 7)
- All the necessary interfaces with their basic configuration
- Access plus a network prefix for a tunnel broker, e. g. SixXS

8.2 Configuration

In the first step, the interface is configured and the assigned prefix is specified.

To do this, go to the following menu:

(1) Go to **WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**.

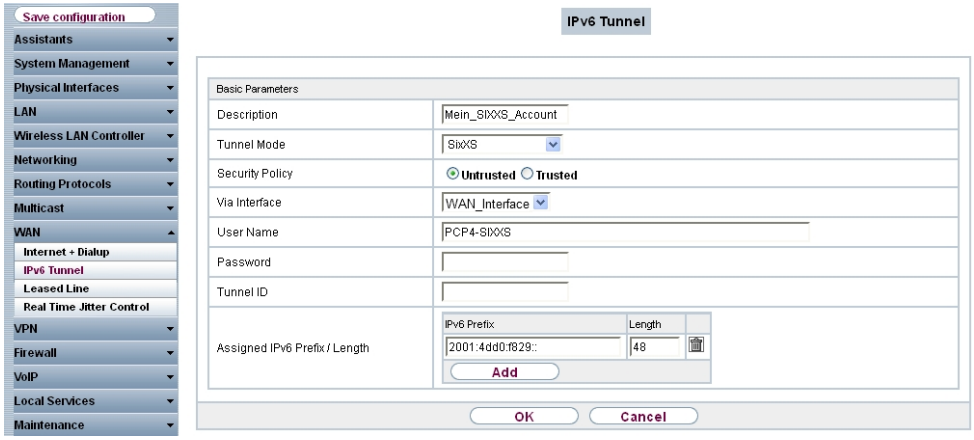


Fig. 63: **WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**

Proceed as follows to configure an interface for IPv6 with SixXS:

(1) For **Description**, enter any description you want for the interface e. g. `Mein_SIXXS_Account`.

(2) For **Tunnel Mode**, select `SixXS`. A SixXS tunnel (SixXS configuration profile for a 6in4 tunnel configuration) is used.

(3) For **Security Policy**, select `Untrusted`. IP packets are only allowed through if the connection has been initiated from "inside". Use this setting if you want to use IPv6 outside of your LAN.

(4) For **Via Interface** select the WAN-Interface, here `WAN_Interface`.

(5) For **User Name**, enter the SixXS username which you have received from SixXS, e. g. `PCP4-SIXXS`.

(6) For **Password**, enter the tunnel password that you configured through SixXS for your tunnel.

(7) Enter the **Tunnel ID** of your SixXS tunnel, which SixXS have given you.

(8) Click below to **Assigned IPv6 Prefix/Length** on **Add**.

(9) Specify the values for **IPv6 Prefix** and **Length** you have received from your service provider, e.g. `2001:4dd0:f829::` and `48`.

(10) Select **OK** to confirm your entries.

In the next step, the LAN interface is configured and the subnet automatically generated.

(1) Go to **LAN** -> **IP Configuration** -> **Interfaces** -> **New**.

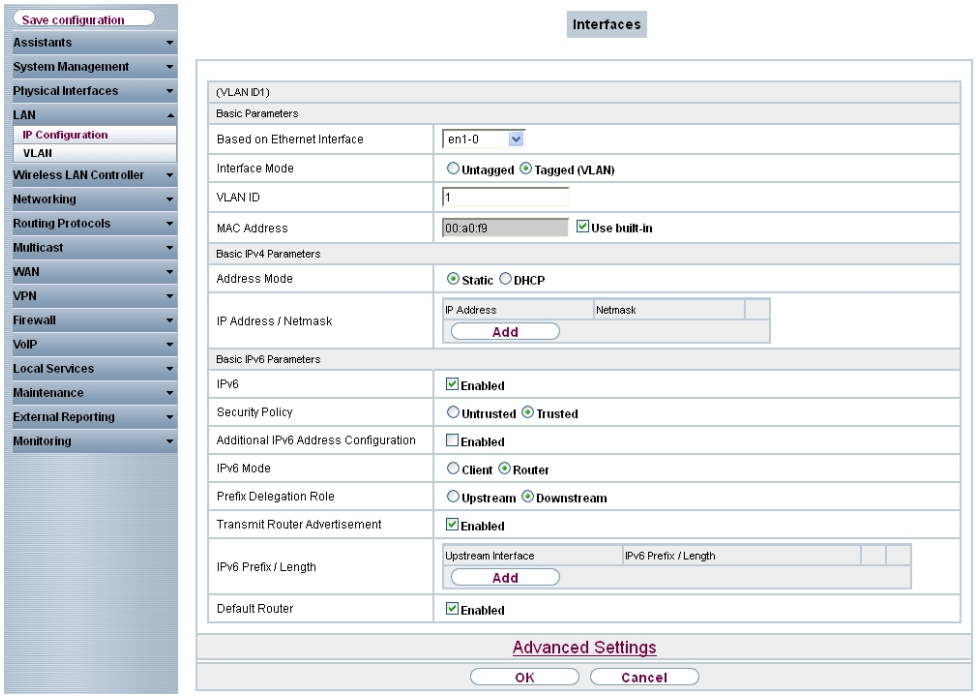


Fig. 64: **LAN** -> **IP Configuration** -> **Interfaces** -> **New**

Proceed as follows:

(1) For **Based on Ethernet Interface**, select the Interface, here e. g. `en1-0`.

(2) For **IPv6** select `Enabled`.

(3) For **Security Policy**, select `Trusted`. All IP packets are allowed through except for those which are explicitly prohibited.

(4) For **IPv6 Mode** leave the option `Router`.

(5) For **Prefix Delegation Role** leave the option `Downstream`.

(6) For **Transmit Router Advertisement**, select `Enabled`. Router advertisements are sent via the interface selected.

(7) In **IPv6 Prefix/Length**, click **Add** in order to automatically create a subnet.

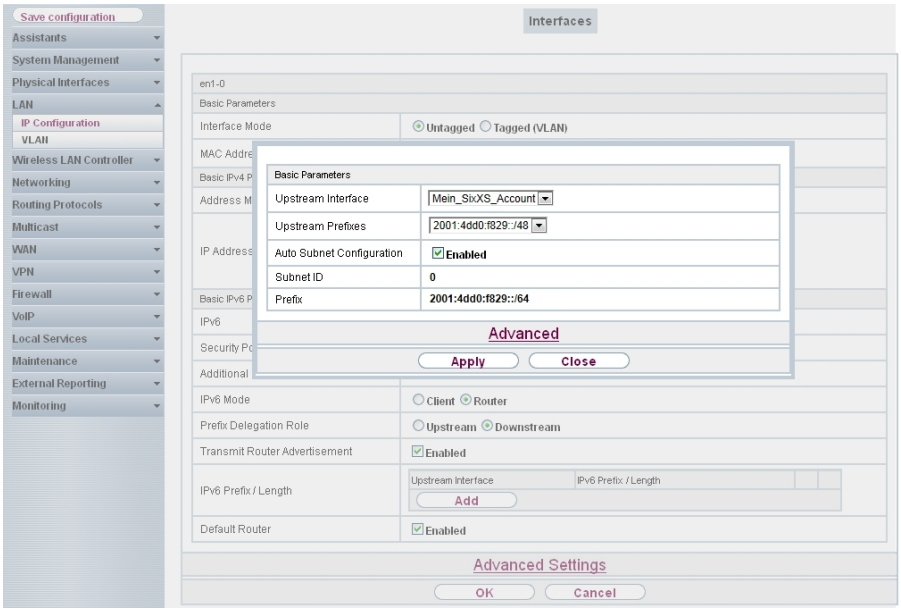


Fig. 65: **LAN** -> **IP Configuration** -> **Interfaces** -> **New** -> **Add**

(8) For **Upstream Interface**, select the interface that has already been configured, here `Mein_SixXS_Account`.

(9) For **Upstream Prefixes**, select the created prefix, e. g. `2001:4dd0:f829::/48` .

(10) Leave **Auto Subnet Configuration** set to `Enabled`.
The automatically created **Subnet-ID** `0` and the automatically created **Prefix** `2001:4dd0:f829::/64` for the subnet are displayed.

(11) Confirm with **Apply**.

(12) Leave the option **Default Router** `Enabled`.

(13) Confirm with **OK**.

8.3 Overview of Configuration Steps

Configure interface

Field	Menu	Value
Description	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New**	e. g. *Mein_SIXXS_Account*
Tunnel Mode	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New**	*SixXS*
Security Policy	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New**	*Untrusted*
Via Interface	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New**	e. g. *WAN_Interface*
User Name	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New**	e. g. *PCP4-SIXXS*
Password	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New**	is awarded by SixXS
Tunnel ID	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New**	is awarded by SixXS
Assigned IPv6 Prefix/ Length	**WAN ->IPv6 Tunnel -> IPv6 Tunnel -> New -> Add**	e. g. *2001:4dd0:f829::/48*

Configure LAN and the subnet generate

Field	Menu	Value
Based on Ethernet Interface	**LAN-> IP Configuration-> Interfaces -> New**	e. g. *en1-0*
IPv6	**LAN-> IP Configuration-> Interfaces -> New**	*Enabled*
Security Policy	**LAN-> IP Configuration-> Interfaces -> New**	*Trusted*
IPv6 Mode	**LAN-> IP Configuration-> Interfaces -> New**	*Router*
Prefix Delegation Role	**LAN-> IP Configuration-> Interfaces -> New**	*Downstream*
Transmit Router Advertisement	**LAN-> IP Configuration-> Interfaces -> New**	*Enabled*
Upstream Interface	**LAN-> IP Configuration-> Interfaces -> New -> Add**	*Mein_SixXS_Account*

Field	Menu	Value
Upstream Prefixes	**LAN**-> **IP Configuration**-> **Interfaces** -> **New** -> **Add**	*2001:4dd0:f829::/48*
Auto Subnet Configuration	**LAN**-> **IP Configuration**-> **Interfaces** -> **New** -> **Add**	*Enabled*
Default Router	**LAN**-> **IP Configuration**-> **Interfaces** -> **New**	*Enabled*

Chapter 9 IP - SixXS IP tunnel broker with prefix ::/48 and balancing using an IPSec tunnel

9.1 Introduction

This example describes the connection between the head office and a branch office.

The objective is to connect sites with IPv4 in the WAN and IPv4/IPv6 in the LAN with a ::/48 prefix from SixXS and a ::/64 prefix from the head office.

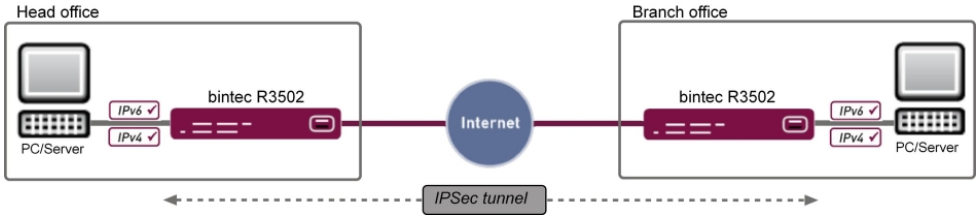


Fig. 66: Example scenario

Head Office

WAN	LAN
WAN interface: Internet Service Provider via DSL	LAN interface: en1-0
IP address: Dynamic IP address	IP address: 192.168.0.254/24
	DHCP range: 192.168.0.10 - 192.168.0.39

branch office

WAN	LAN
WAN interface: Internet Service Provider via DSL	LAN interface: en1-0
IP address: Dynamic IP address	IP address: 192.168.80.254/24
	DHCP range: 192.168.80.10 - 192.168.80.39

Graphical User Interface (GUI) is used for the configuration.

Requirements

The following are required for the configuration:

- A bintec gateway from the RS, Rxxx2 or RXL series, e. g. **bintec R3502** with system

software 8.2.1

- A functioning Internet connection
- Internet Protocol Version 6 (IPv6) enabled on the relevant computers (IPv6 is enabled by default on Windows 7)
- All the necessary interfaces with their basic configuration
- Access plus a network prefix for a tunnel broker, e. g. SixXS
- An existing IPSec tunnel between the two sites with a virtual interface

9.2 Configuration

Configuration at head office

(1) Go to **WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**.

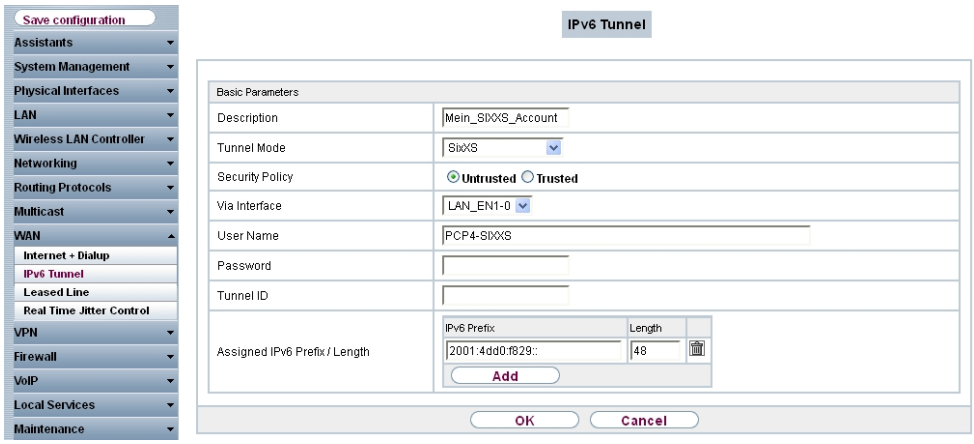


Fig. 67: **WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**

Proceed as follows to configure an interface for IPv6 with SixXS and enter the prefix:

(1) For **Description**, enter any description you want for the interface, e. g. `Mein_SIXXS_Account`.

(2) For **Tunnel Mode**, select `SixXS`. A SixXS tunnel (SixXS configuration profile for a 6in4 tunnel configuration) is used.

(3) For **Security Policy**, select `Untrusted`. IP packets are only allowed through if the connection has been initiated from "inside". Use this setting if you want to use IPv6 outside of your LAN.

(4) For **Via Interface** select the WAN-Interface, here `LAN_EN1-0` .

(5) For **Username**, enter the SixXS username which you have received from SixXS, e. g.

`PCP4-SIXXS`.

(6) For **Password**, enter the tunnel password that you configured through SixXS for your tunnel.

(7) Enter the **Tunnel ID** of your SixXS tunnel, which SixXS have given you.

(8) Click below to **Assigned IPv6 Prefix/Length** on **Add**.

(9) Specify the values for **IPv6 Prefix** and **Length** you have received from your service provider, e.g. `2001:4dd0:f829::` and `48`.

(10) Select **OK** to confirm your entries.

In the next step, the LAN interface is configured and the subnet automatically generated.

(1) Go to **LAN** -> **IP Configuration** -> **Interfaces** -> **New**.

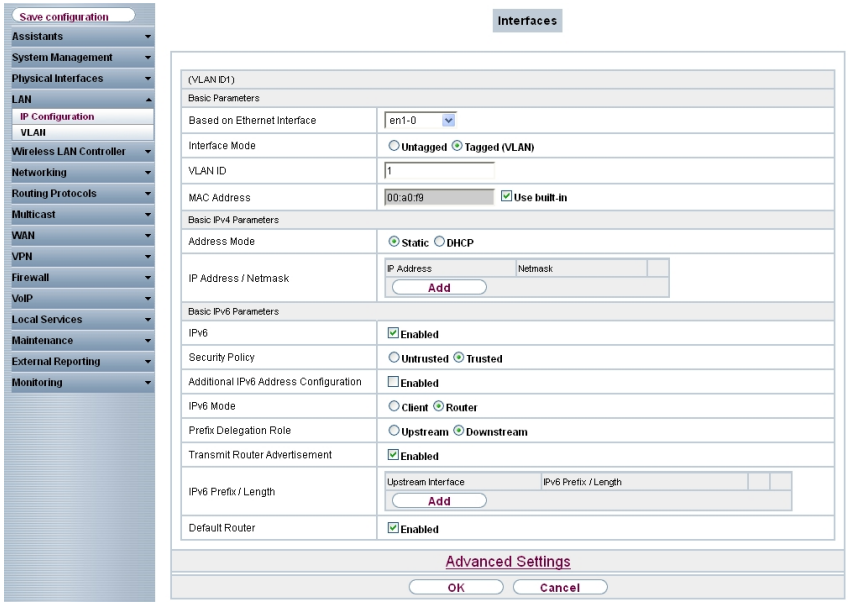


Fig. 68: **LAN** -> **IP Configuration** -> **Interfaces** -> **New**

(2) For **Based on Ethernet Interface**, select the interface, here e. g. `en1-0`.

(3) For **IPv6** select `Enabled`.

(4) For **Security Policy**, select `Trusted`. All IP packets are allowed through except for those which are explicitly prohibited.

(5) For **IPv6 Mode** leave the option `Router`.

(6) For **Prefix Delegation Role** leave the option `Downstream`.

(7) For **Transmit Router Advertisement**, select `Enabled`. Router advertisements are sent via the interface selected.

(8) In **IPv6 Prefix/Length** click **Add** in order to automatically create a subnet.

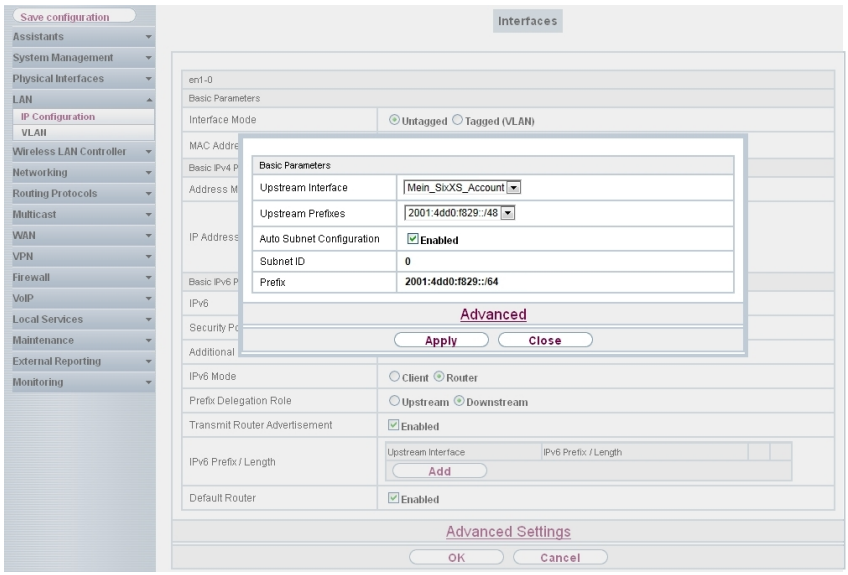


Fig. 69: **LAN** -> **IP Configuration** -> **Interfaces** -> **New** -> **Add**

(9) For **Upstream Interface**, select the interface that has already been configured, here `Mein_SixXS_Account` .

(10) For **Upstream Prefixes**, select the created prefix, e. g. `2001:4dd0:f829::/48` .

(11) Leave **Auto Subnet Configuration** set to `Enabled`.
The automatically created **Subnet ID** `0` and the automatically created **Prefix** `2001:4dd0:f829::/64` for the subnet are displayed.

(12) Confirm with **Apply**.

(13) Leave the option **Default Router** `Enabled`.

(14) Select **OK** to confirm your entries.

In the next step, the Tunnel interface is defined.

(1) Go to **WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** ->**New**.

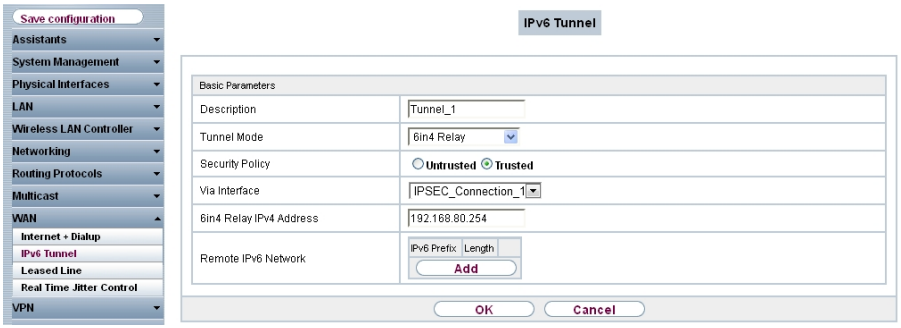


Fig. 70: **WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** ->**New**

Proceed as follows in order to create the tunnel interface and enter the prefix.

(1) For **Description**, enter any description you want for the interface, e. g. `Tunnel_1`.

(2) For **Tunnel Mode**, select `6in4 Relay`. A 6in4 tunnel configuration is used.

(3) For **Security Policy**, select `Trusted`. All IP packets are transmitted.

(4) For **Via Interface** select the WAN-Interface, here `IPSEC_Connection_1`.

(5) For **6in4Relay IPv4 Address** specify the IP address of the branch router, e.g. `192.168.80.254`.

(6) Select **OK** to confirm your entries.

In the last step, a static route is configured for the prefix in the branch office. This route is required in order for the central gateway to "know" through which interface the IPv6 packets of the branch office have to be routed.

(1) Go to **Networking** -> **Routes** -> **IPv6 Routes** -> **New**.

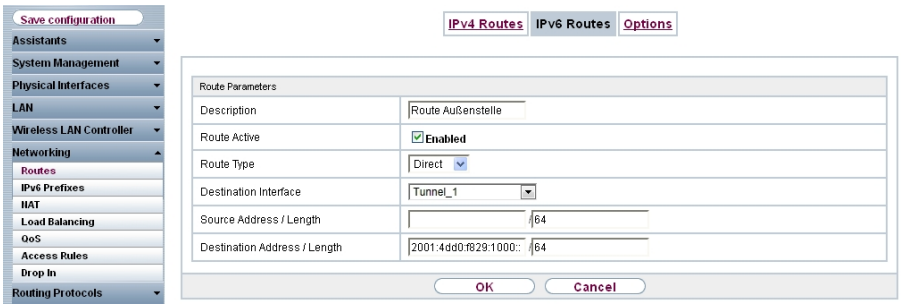


Fig. 71: **Networking** -> **Routes** -> **IPv6 Routes** -> **New**

Proceed as follows:

(1) Enter a **Description** e. g. `Route Außenstelle`.

(2) Leave the option **Route Active** `Enabled`.

(3) For **Route Type** select `Direct`.

(4) For **Destination Interface** select the tunnel interface, here `Tunnel_1`.

(5) For **Destination Address/Length** enter `2001:4dd0:f829:1000::/56`.
The value `:1000::` in the above address `::/48` further divides the prefix. In this way the central gateway "knows" that all requests from `2001:4dd9:f829:1000::/56` originate from the branch office.

(6) Confirm with **OK**.

Configuration at the branch office

First, the tunnel interface is defined.

(1) Go to **WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**.

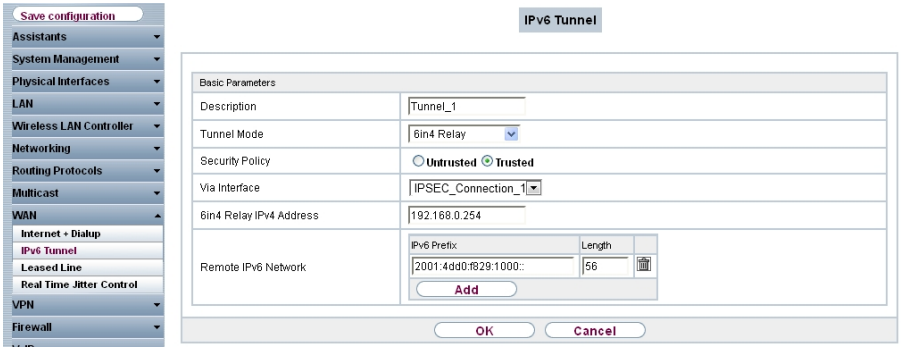


Fig. 72: **WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**

Proceed as follows to define the tunnel interface:

(1) For **Description**, enter any description that you want to use for the tunnel, e. g. `Tunnel1`.

(2) For **Tunnel Mode**, select `6in4 Relay`. A standard 6in4 tunnel interface is used.

(3) For **Security Policy**, select `Trusted`.

(4) For **Via interface**, select the name of the IPSec connection interface, here e. g. `IPSEC-Connection_1`.

(5) For **6to4 Relay Address**, enter the IP address of the router in the head office, e. g. `192.168.0.254`.

(6) In **Remote IPv6 Network** click **Add** and enter the prefix the branch office has received from the head office, e.g., `2001:4dd0:f829:1000::/56`.

(7) Select **OK** to confirm your entries.

In the next step, the LAN interface is configured.

(1) Go to **LAN** -> **IP Configuration** -> **Interfaces** -> **New**.

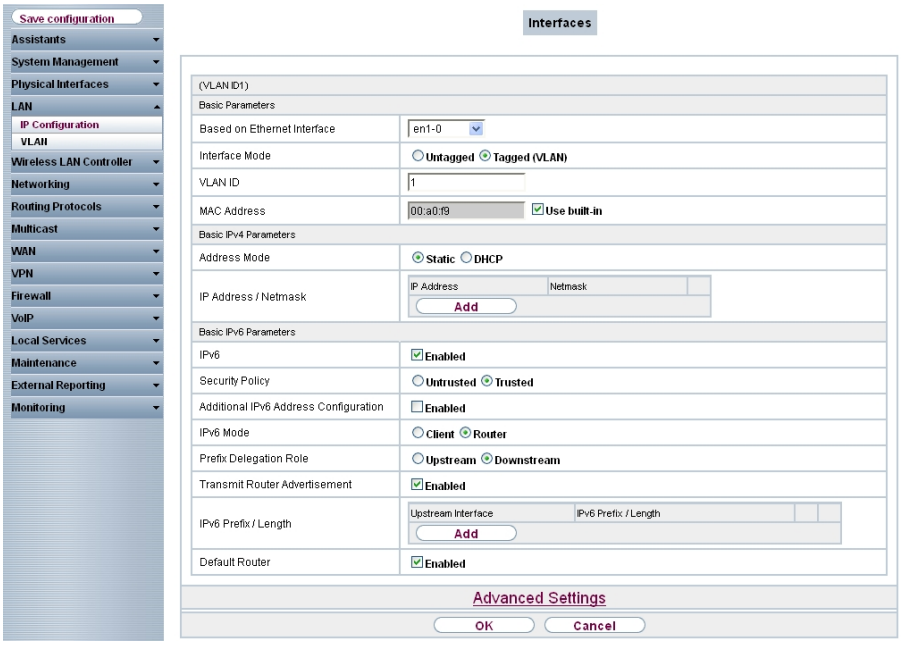


Fig. 73: **LAN** -> **IP Configuration** -> **Interfaces** -> **New**

Proceed as follows to configure the LAN interface:

(1) For **Based on Ethernet Interface**, select the interface, here e. g. `en1-0`.

(2) For **IPv6** select `Enabled`.

(3) For **Security Policy**, select `Trusted`. All IP packets are allowed through except for those which are explicitly prohibited.

(4) For **IPv6 Mode** leave the option `Router`.

(5) For **Prefix Delegation Role** leave the option `Downstream`.

(6) For **Transmit Router Advertisement**, select `Enabled`. Router advertisements are sent via the interface selected.

(7) For **IPv6 Prefix/Length** click on **Add.**

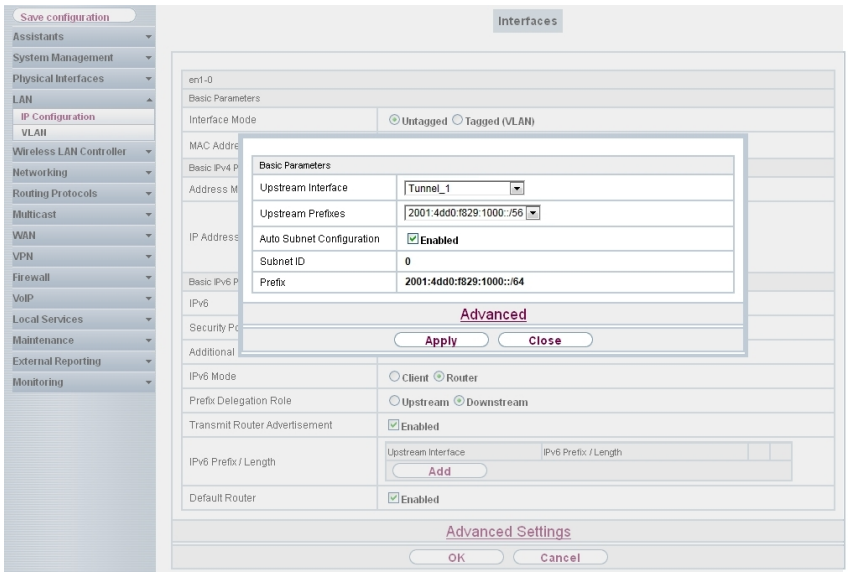


Fig. 74: **LAN** -> **IP Configuration** ->**Interfaces** -> **New** -> **Add**

(8) For **Upstream Interface**, select the 6in4 Relay tunnel that has already been configured, here `Tunnel_1` .

(9) For **Upstream Prefixes**, select the created prefix, e. g. `2001:4dd0:f829:1000::/56` .

(10) Leave **Auto Subnet Configuration** set to `Enabled`.
The automatically created **Subnet ID** `0` and the automatically created **Prefix** `2001:4dd0:f829::/64` for the subnet are displayed

(11) Confirm with **Apply**.

(12) Leave the option **Default Router** `Enabled`.

(13) Confirm with **OK**, to save your settings.

9.3 Overview of Configuration Steps

9.3.1 Configuration at head office

Configure interface

Field	Menu	Value
Description	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**	e. g. *Mein_SIXXS_Account*
Tunnel Mode	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**	*SixXS*
Security Policy	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**	*Untrusted*
Via Interface	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**	e. g. *LAN_EN1-0*
User Name	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**	e. g. *PCP4-SIXXS*
Password	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**	is awarded by SixXS
Tunnel ID	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New**	is awarded by SixXS
Assigned IPv6 Prefix/ Length	**WAN** ->**IPv6 Tunnel** ->**IPv6 Tunnel** -> **New** -> **Add**	e. g. *2001:4dd0:f829::/48*

Configure LAN and the subnet generate

Field	Menu	Value
Based on Ethernet Interface	**LAN**-> **IP Configuration**-> **Interfaces**-> **New**	e. g. *en1-0*
IPv6	**LAN**-> **IP Configuration**-> **Interfaces**-> **New**	*Enabled*
Security Policy	**LAN**-> **IP Configuration**-> **Interfaces**-> **New**	*Trusted*
IPv6 Mode	**LAN**-> **IP Configuration**-> **Interfaces**-> **New**	*Router*
Prefix Delegation Role	**LAN**-> **IP Configuration**-> **Interfaces**-> **New**	*Downstream*
Transmit Router Advertisement	**LAN**-> **IP Configuration**-> **Interfaces**-> **New**	*Enabled*
Upstream Interface	**LAN**-> **IP Configuration**-> **Interfaces**-> **New** -> **Add**	*Mein_SixXS_Account*

Field	Menu	Value
Upstream Prefixes	**LAN**-> **IP Configuration**-> **Interfaces**-> **New** -> **Add**	*2001:4dd0:f829::/48*
Auto Subnet Configuration	**LAN**-> **IP Configuration**-> **Interfaces**-> **New** -> **Add**	*Enabled*

Define tunnel interface

Field	Menu	Value
Description	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	e. g. *Tunnel_1*
Tunnel Mode	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	*6in4 Relay*
Security Policy	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	*Trusted*
Via Interface	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	e. g. *IPSEC_Connection_1*
6in4 Relay IPv4 Address	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	e. g. *192.168.80.254*

Assign address range

Field	Menu	Value
Description	**Networking**-> **Routes**-> **IPv6 Routes**-> **New**	*Route Außenstelle*
Route Active	**Networking**-> **Routes**-> **IPv6 Routes**-> **New**	*Enabled*
Route Type	**Networking**-> **Routes**-> **IPv6 Routes**-> **New**	*Direct*
Destination Interface	**Networking**-> **Routes**-> **IPv6 Routes**-> **New**	e. g. *Tunnel_1*
Destination Address/ Length	**Networking**-> **Routes**-> **IPv6 Routes**-> **New**	*2001:4dd0:f829:1000::/56*

9.3.2 Configuration at the branch office

Define tunnel interface

Field	Menu	Value
Description	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	e. g. *Tunnel_1*
Tunnel Mode	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	*6in4 Relay*
Security Policy	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	*Trusted*
Via interface	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	z. B. *IPSEC_Connection_1*
6in4 Relay IPv4 Address	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New**	e. g. *192.168.0.254*
Remote IPv6 Network	**WAN** -> **IPv6 Tunnel** -> **IPv6 Tunnel** -> **New** -> **Add**	*2001:4dd0:f829:1000::/56*

Configure LAN and the subnet generate

Field	Menu	Value
Based on Ethernet Interface	**LAN** -> **IP Configuration** ->**Interface**-> **New**	e. g. *en1-0*
IPv6	**LAN** -> **IP Configuration** ->**Interface**-> **New**	*Enabled*
Security Policy	**LAN** -> **IP Configuration** ->**Interface**-> **New**	*Trusted*
IPv6 Mode	**LAN** -> **IP Configuration** ->**Interface**-> **New**	*Router*
Prefix Delegation Role	**LAN** -> **IP Configuration** ->**Interface**-> **New**	*Downstream*
Transmit Router Advertisement	**LAN** -> **IP Configuration** ->**Interface**-> **New**	*Enabled*
Upstream Interface	**LAN** -> **IP Configuration** ->**Interface**-> **New** -> **Add**	e. g. *Tunnel_1*
Upstream Prefixes	**LAN** -> **IP Configuration** ->**Interface**-> **New** -> **Add**	*2001:4dd0:f829:1000::/56*
Auto Subnet Configuration	**LAN** -> **IP Configuration** ->**Interface**-> **New** -> **Add**	*Enabled*

Field	Menu	Value
Default Router	**LAN** -> **IP Configuration** ->**Interface**-> **New**	*Enabled*

Chapter 10 IP - Load balancing two Internet accesses used in parallel

10.1 Introduction

The following workshop shows the configuring of an Internet access gateway with two Internet accesses used in parallel. The first ADSL line is created with the ADSL modem integrated in the **bintec be.IP plus** used here. An external ADSL modem is connected to the **bintec be.IP plus** gateway's ETH5 port to create the second ADSL line. The data traffic is distributed half and half to the two ADSL lines based on IP sessions. We shall then take the example of encrypted HTTP connections (HTTPS) to describe how to effectively avoid any loss of connection that might occur when distributing to different Internet accesses.

The **GUI** (Graphical User Interface) is used for configuring.

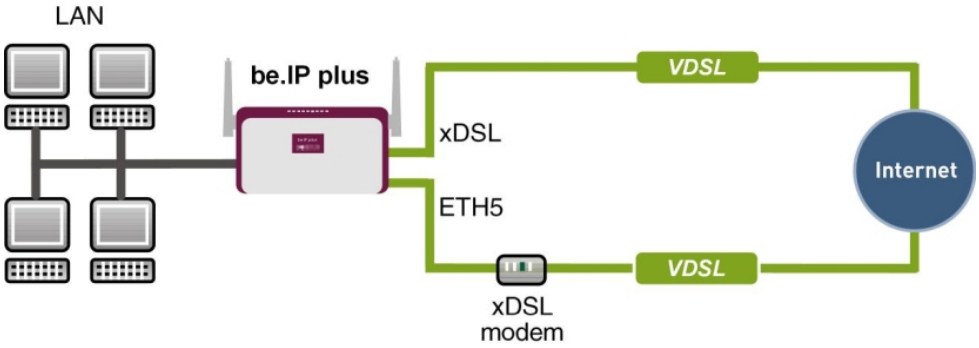


Fig. 75: Example scenario

Requirements

The following are required for the configuration:

- A bintec ADSL gateway e. g. **bintec be.IP plus** with system software 10.1.5 Patch 6
- Two independent ADSL Internet connections
- An external ADSL modem that is connected to the **bintec be.IP plus** gateway's ETH5 port.

10.2 Configuration

10.2.1 Configuring internet access

For configuration, open an Internet browser and start a web (HTTP) connection to the **bintec be.IP plus** gateway. The **GUI** comes with a wizard for configuring the two Internet accesses.

To do this, go to the following menu:

(1) Go to **Assistants** -> **Internet**-> **Internet Connections** -> **New**.

(2) For **Connection Type**, select `Internal ADSL Modem`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

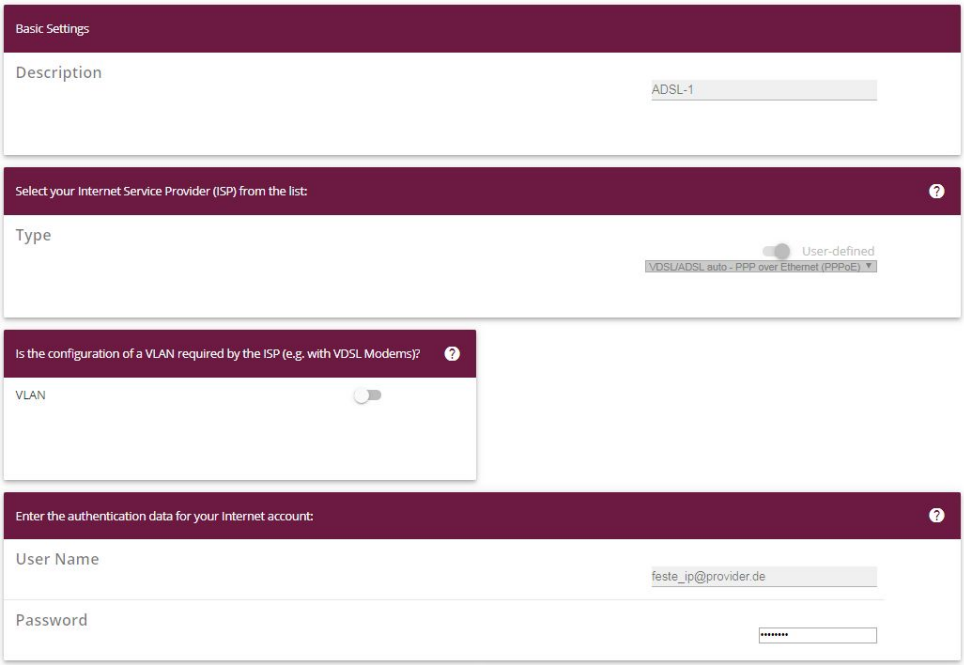


Fig. 76: **Assistants** -> **Internet**-> **Internet Connections** -> **New** -> **Next**

Proceed as follows to configure an Internet access:

(1) Under **Description** enter e.g. `ADSL-1` .

(2) For **Type**, select `User-defined via PPP over Ethernet (PPPoE)`.

(3) As the **User Name**, enter the name which your provider has given you, e. g. `feste-ip@provider.de`.

(4) Enter the **Password** that your provider has given you, e. g. `test12345`.

(5) Press **OK** to confirm your entries.

To set up the second ADSL connection, run the wizard again.

(1) Go to **Assistants** -> **Internet**-> **Internet Connections** -> **New**.

(2) For **Connection Type**, select *External xDSL Modem*.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

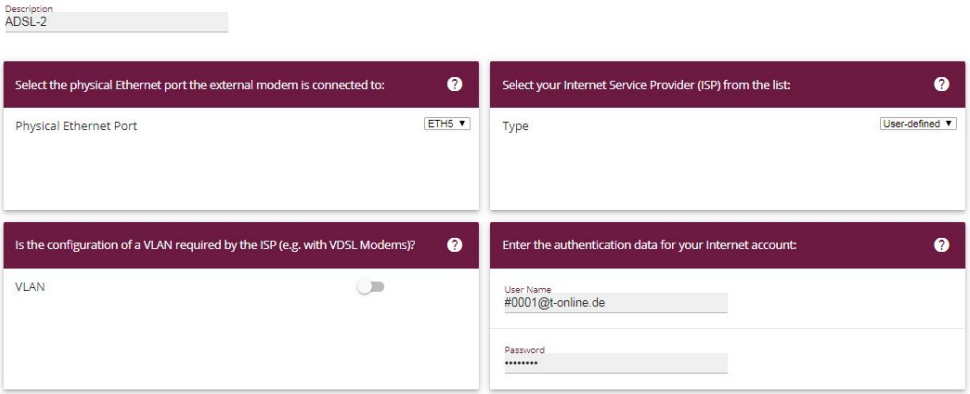


Fig. 77: **Assistants** -> **Internet**-> **Internet Connections** -> **New** -> **Next**

Note

The message you get when you create the second ADSL connection may be ignored. The IP load distribution avoids routing conflicts due to multiple standard routes!

Proceed as follows to configure the second Internet connection:

(1) Under **Description**, enter a name for the Internet connection, e. g. *ADSL-2*.

(2) Under **Physical Ethernet Port** select the physical Ethernet port to which the xDSL modem is connected, in this case *ETH5*.

(3) For **User Name**, enter the access data that your provider has sent you, e. g. *#0001@t-online.de*.

(4) Enter the **Password** that your provider has given you, e. g. *test12345*.

(5) In the **Always active** field, specify whether or not the Internet connection should always be on. Only activate this option if you have Internet access with a flatrate.

(6) Press **OK** to confirm your entries.

When the configuration is complete, the wizard for configuring Internet connections will show two entries.

(1) Go to **Assistants** -> **Internet**-> **Internet Connections**.

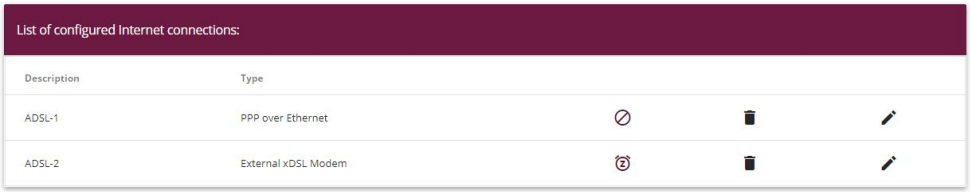


Fig. 78: **Assistants** -> **Internet** -> **Internet Connections**

10.2.2 Setting up the IP load distribution

A load balancing group needs to have been created before you can set up the IP load distribution.

(1) Go to **Network** -> **Load Balancing** -> **Load Balancing Groups** -> **New**.

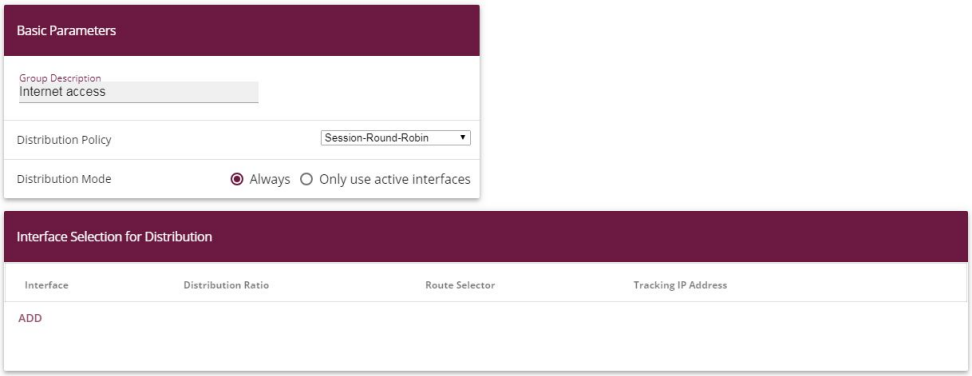


Fig. 79: **Network** ->**Load Balancing**->**Load Balancing Groups**->**New**

To create a load balancing group, proceed as follows:

(1) Under **Group Description**, enter a name for the load balancing group, e. g. `Internet access`.

(2) For **Distribution Policy**, select the method that will be used to distribute the data, here `Session-Round-Robin` (for load distribution based on IP sessions).

The two ADSL Internet accesses can then be added to this load balancing group.

To do this, click **Add**.

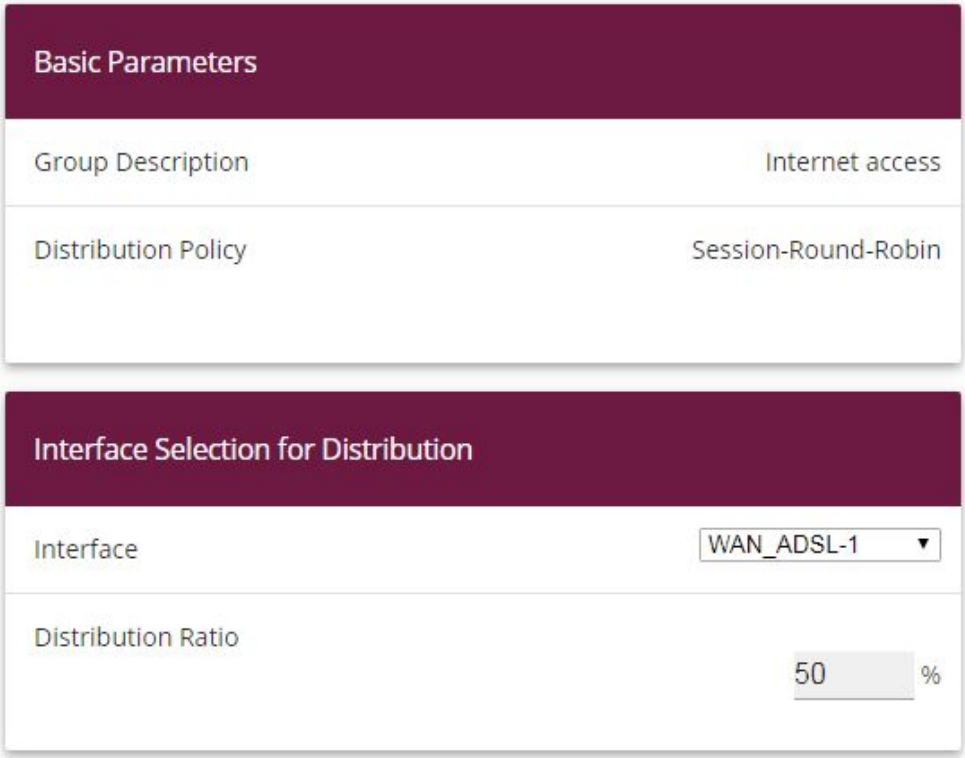


Fig. 80: **Network** -> **Load Balancing** ->**Load Balancing Groups** -> **New**-> **Add**

Proceed as follows:

(1) For **Interface**, select the first ADSL access `WAN_ADSL-1`.

(2) Enter `50` % for **Distribution Ratio**.

(3) Click **Apply**.

(4) Add the second ADSL line with **Add**.

(5) For **Interface**, select the second ADSL access `WAN_ADSL-2`.

(6) Enter `50` % for **Distribution Ratio**.

(7) Click **Apply**.

After this configuration step, the two Internet connections can be used with the IP load distribution.

(1) Go to **Network** -> **Load Balancing** -> **Load Balancing Groups**.

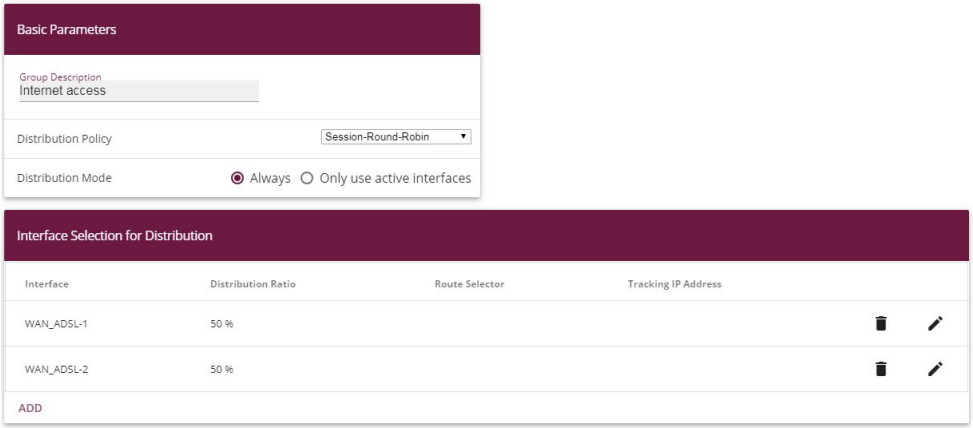


Fig. 81: **Network** -> **Load Balancing** -> **Load Balancing Groups**

10.2.3 Special load distribution handling for encrypted connections

With the configuration now complete, IP sessions are distributed half and half to the two ADSL lines. This behaviour can lead to problems and losses of connection with certain protocols (e. g. encrypted HTTPS connections). The reason for these connection problems lies in the different Internet IP address of the two ADSL connections. With parallel connections to the same server, the two ADSL lines would be used alternately. To get around this difficulty, IP sessions that are associated can temporarily be connected to one of the Internet connections. This type of critical connection is configured in the **Special Session Handling** menu.

(1) Go to **Network** -> **Load Balancing** -> **Special Session Handling** -> **New**.

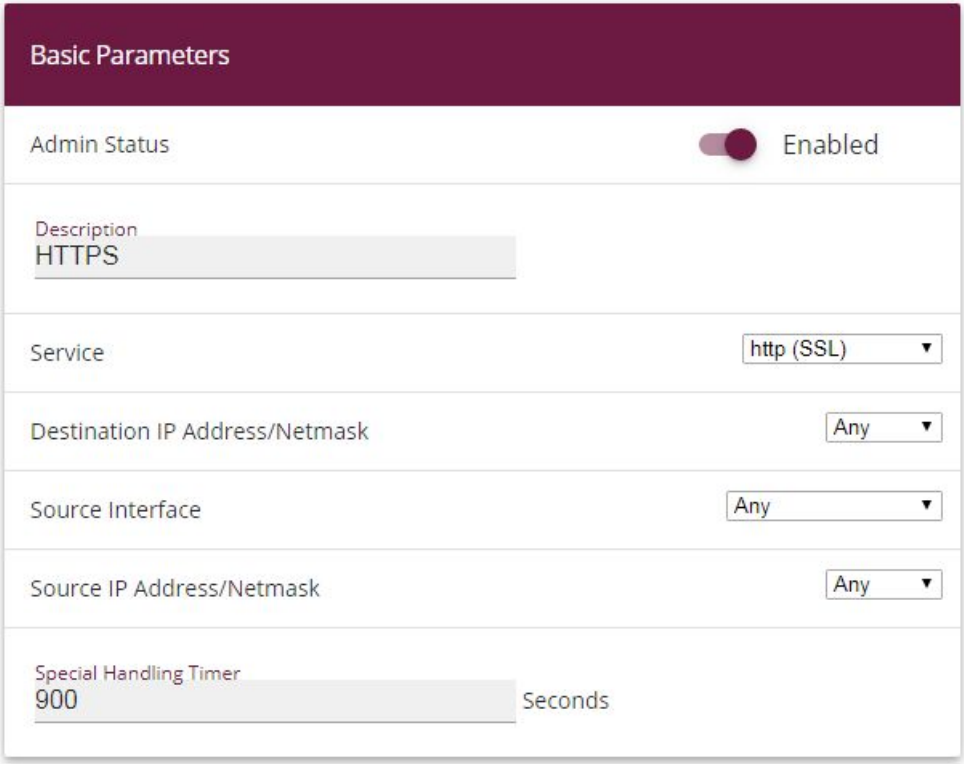


Fig. 82: **Network** -> **Load Balancing** -> **Special Session Handling** ->**New**

Proceed as follows:

(1) Under **Description**, enter a name for the entry, e. g. *HTTPS*.

(2) For **Service**, select *http (SSL)*.

(3) Set the **Special Handling Timer** to *900* seconds.

(4) Leave the remaining settings unchanged and confirm them with **OK**.

With this configuration, HTTPS connections that are sent from a single local host to the same HTTPS web server are connected to one of the two ADSL lines for a period of 900 seconds. This causes the address of the sender of the HTTPS data to remain the same, which prevents any loss of connection.

10.2.4 About configuring the DNS server

When creating the ADSL connections, besides the public IP address, the **bintec be.IP plus** also obtains the IP addresses of the DNS servers for resolving the name of the configured Internet provider. Particularly when using different Internet providers, the use of the DSN servers needs to be connection-specific. The following configuration was created automatically when the ADSL connections were created.

(1) Go to **Local Services** -> **DNS** ->**DNS Server**.

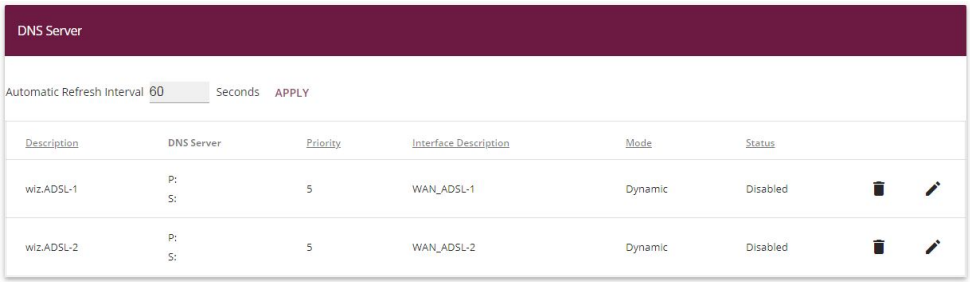


Fig. 83: **Local Services** -> **DNS** -> **DNS Server**

10.3 Overview of Configuration Steps

Set up first Internet connection

Field	Menu	Value
Connector Type	**Assistants -> Internet-> Internet Connections -> New**	*Internal ADSL Modem*
Description	**Assistants -> Internet ->Internet Connections -> New -> Next**	e. g. *ADSL-1*
User Name	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *feste_ip@provider.de*
Password	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *test12345*

Set up the second Internet connection

Field	Menu	Value
Connector Type	**Assistants -> Internet-> Internet Connections -> New**	*External xDSL Modem*
Description	**Assistants -> Internet-> Internet Con-**	e. g. *ADSL-2*

Field	Menu	Value
	nections -> New -> Next	
Physical Ethernet Port	**Assistants -> Internet-> Internet Connections -> New -> Next**	e.g. *ETH5*
User Name	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *#0001@t-online.de*
Password	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *test12345*

Create a load balancing group

Field	Menu	Value
Group Description	**Network -> Load Balancing ->Load Balancing Groups -> New**	e. g. *Internet Access.*
Distribution Policy	**Network -> Load Balancing ->Load Balancing Groups -> New**	*Session-Round-Robin*
Interface	**Network -> Load Balancing ->Load Balancing Groups -> New-> Add**	*WAN_ADSL-1*
Distribution Ratio	**Network -> Load Balancing ->Load Balancing Groups -> New-> Add**	*50* %
Interface	**Network -> Load Balancing ->Load Balancing Groups -> New-> Add**	*WAN_ADSL-2*
Distribution Ratio	**Network -> Load Balancing ->Load Balancing Groups -> New-> Add**	*50* %

Special Session Handling

Field	Menu	Value
Description	**Network -> Load Balancing-> Special Session Handling -> New**	e. g. *HTTPS*
Service	**Network -> Load Balancing-> Special Session Handling -> New**	*http (SSL)*
Special Handling Timer	**Network -> Load Balancing-> Special Session Handling -> New**	*900* seconds

Chapter 11 IP - Load distribution for two VPN IPSec tunnels via separate Internet accesses

11.1 Introduction

This workshop shows how to configure a VPN IPSec network in association with IP load distribution. Two independent Internet connections are used at the same time at the head office location, to improve reliability and achieve greater bandwidth. The gateway at the branch office location is connected to the Internet with an ADSL line and always initiates two VPN IPSec tunnels to the head office gateway in order that both of the ADSL lines can be used simultaneously. The head office gateway must be accessible from the Internet via two fixed WAN IP addresses or by using Dyndns (in the case of dynamic WAN IP addresses). Configuring the load distribution prevents routing conflicts in the Internet connections and the two VPN IPSec connections. The tunnel connections are mutually and periodically monitored by the two VPN gateways. If one tunnel falls over, all the data traffic is automatically diverted to the VPN tunnel which is still working.

The **GUI** (Graphical User Interface) is used for configuring.

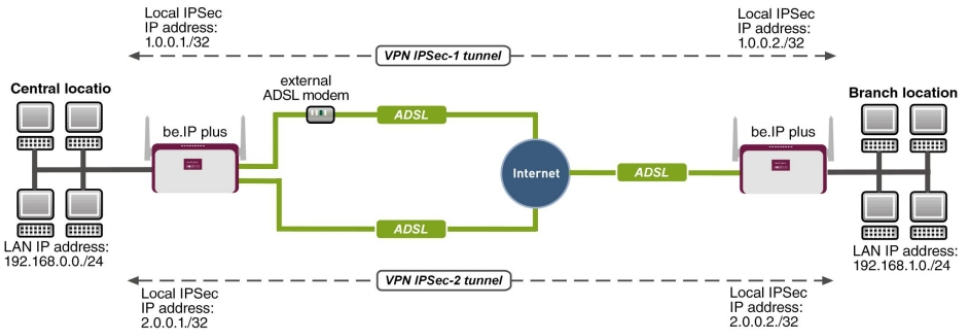


Fig. 84: Example scenario

Requirements

The following are required for the configuration:

Head office location

- A bintec VPN gateway e. g. **bintec be.IP plus** with system software 10.1.5 Patch 6
- Two independent ADSL Internet connections (with dynamic WAN IP addresses, you can

work with Dyndns)

- An external ADSL modem that is connected to the **bintec be.IP plus** gateway's ETH5 port.

Branch office location

- A bintec VPN gateway e. g. **bintec be.IP plus** with system software 10.1.5 Patch 6
- An ADSL Internet access

11.2 Configuration

11.2.1 Configure the gateway at head office

Setting up the Internet connections

Two ADSL Internet connections are used in parallel at the head office location, to improve reliability and achieve greater bandwidth. These Internet accesses are configured using the **Wizard**.

(1) Go to **Assistants** -> **Internet** -> **Internet Connections** -> **New**.

(2) For **Connection Type**, select `Internal ADSL Modem`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

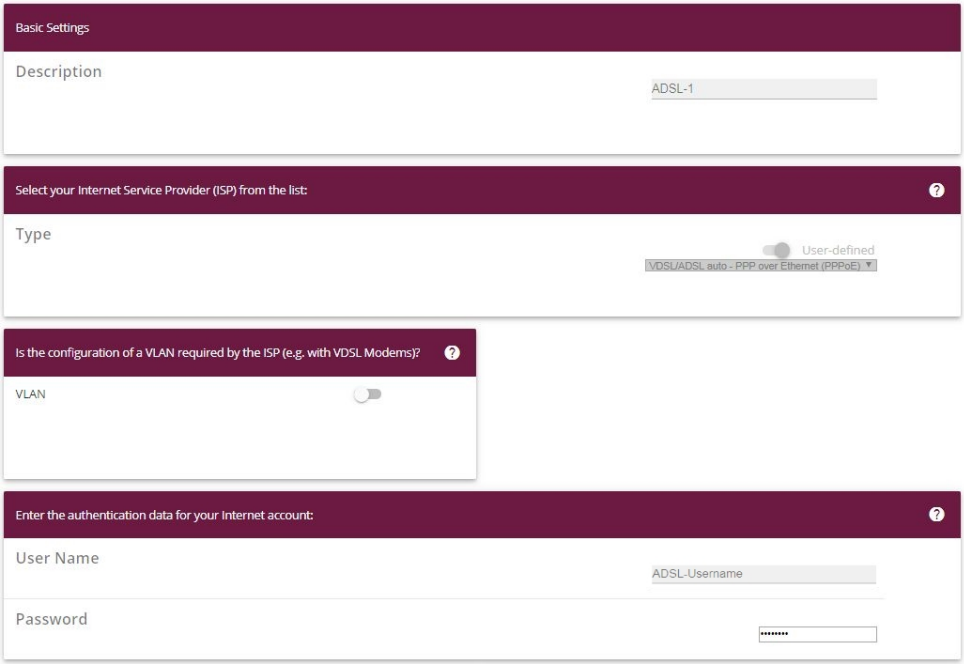


Fig. 85: **Assistants** -> **Internet** -> **Internet Connections** -> **New** -> **Next**

Proceed as follows to configure an Internet access:

(1) Under **Description** enter e.g. `ADSL-1` .

(2) For **Type**, select `User-defined via PPP over Ethernet (PPPoE)`.

(3) For **User Name**, enter the name that your provider has given you, e. g. `ADSL-Username`.

(4) Enter the **Password** that your provider has given you, e. g. `test12345`.

(5) In the **Always active** field, specify whether or not the Internet connection should always be on. Only activate this option if you have Internet access with a flatrate.

(6) Press **OK** to confirm your entries.

To set up the second ADSL connection, run the wizard again.

(1) Go to **Assistants** -> **Internet**-> **Internet Connections** -> **New**.

(2) For **Connection Type**, select `External xDSL Modem`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

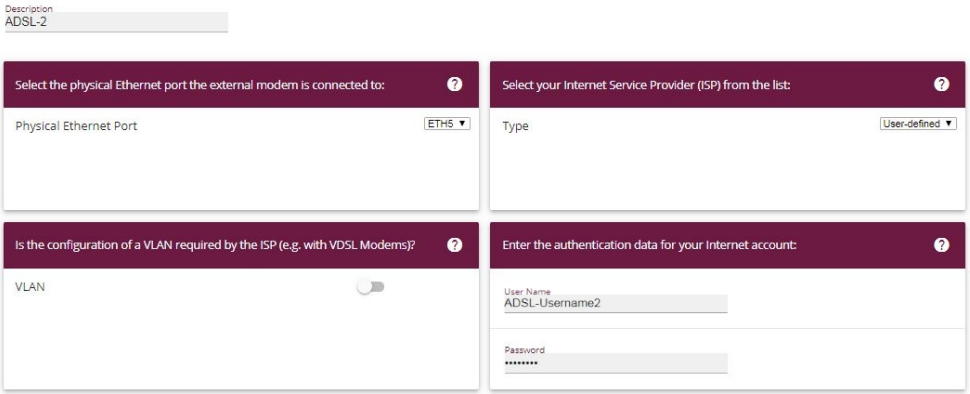


Fig. 86: **Assistants** -> **Internet** -> **Internet Connections** -> **New** -> **Next**

Note

The message you get when you create the second ADSL connection may be ignored. The IP load distribution avoids routing conflicts due to multiple standard routes!

Proceed as follows to configure the second Internet connection:

(1) Under **Description**, enter a name for the Internet connection, e. g. `ADSL-2`.

(2) Under **Physical Ethernet Port** select the physical Ethernet port to which the xDSL modem is connected, in this case `ETH5`.

(3) For **User Name**, enter the access data that your provider has given you, e. g. `ADSL-Username2`.

(4) Enter the **Password** that your provider has given you, e. g. `test12345`.

(5) Press **OK** to confirm your entries.

When the configuration is complete, the wizard for configuring Internet connections will show two entries.

(1) Go to **Assistants** -> **Internet**-> **Internet Connections**.

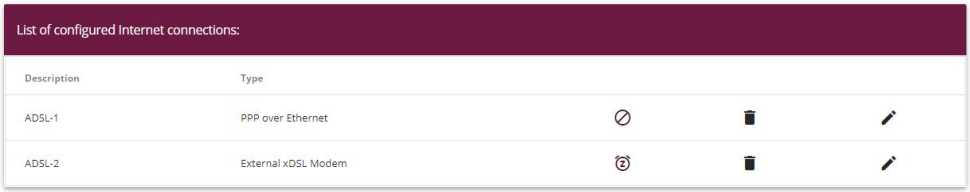


Fig. 87: **Assistants** -> **Internet** -> **Internet Connections**

Setting up the IP load distribution

A load balancing group needs to have been created before you can set up the IP load distribution.

(1) Go to **Network** -> **Load Balancing** -> **Load Balancing Groups** -> **New**.

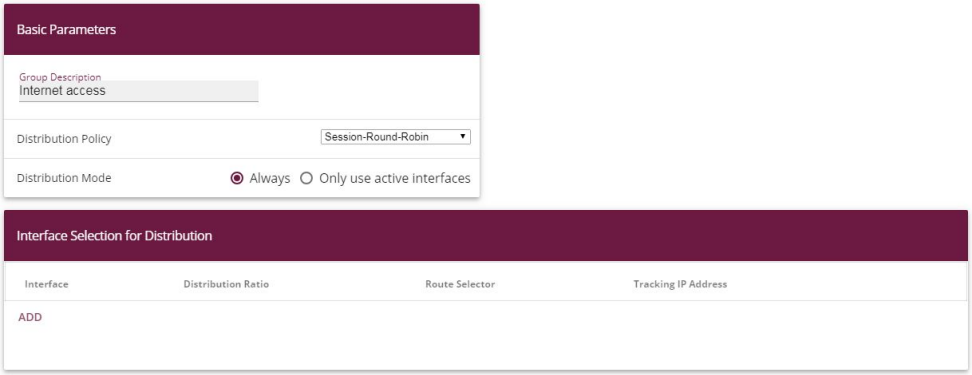


Fig. 88: **Network** ->**Load Balancing**->**Load Balancing Groups**->**New**

To create a load balancing group, proceed as follows:

(1) Under **Group Description**, enter a name for the load balancing group, e. g. `Internet access`.

(2) For **Distribution Policy**, select the method that will be used to distribute the data, here `Session-Round-Robin` (for load distribution based on IP sessions).

The two ADSL Internet accesses can then be added to this load balancing group.

To do this, click **Add**.

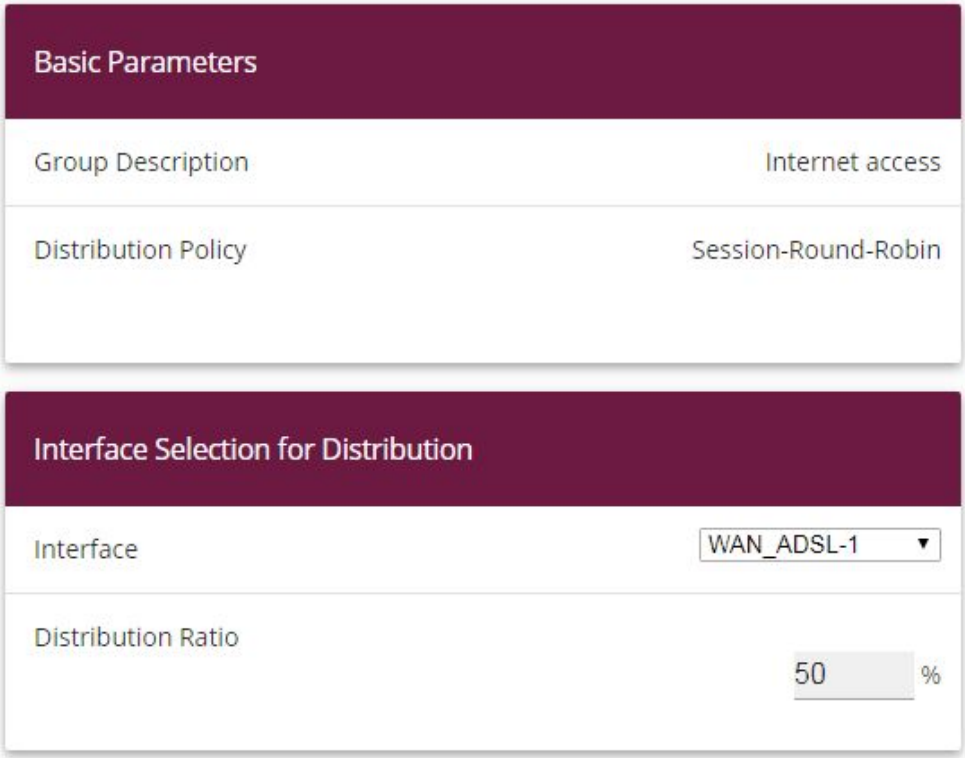


Fig. 89: **Network** ->**Load Balancing**->**Load Balancing Groups**->**Add**

Proceed as follows:

(1) For **Interface**, select the first ADSL access `WAN_ADSL-1`.

(2) Enter `50` % for **Distribution Ratio**.

(3) Click **Apply**.

(4) Add the second ADSL line with **Add**.

(5) For **Interface**, select the second ADSL access `WAN_ADSL-2`.

(6) Enter `50` % for **Distribution Ratio**.

(7) Click **Apply**.

Results:

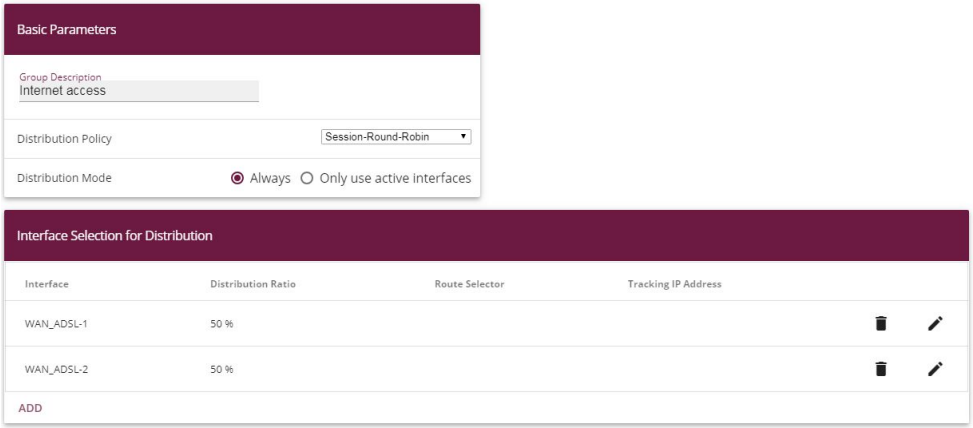


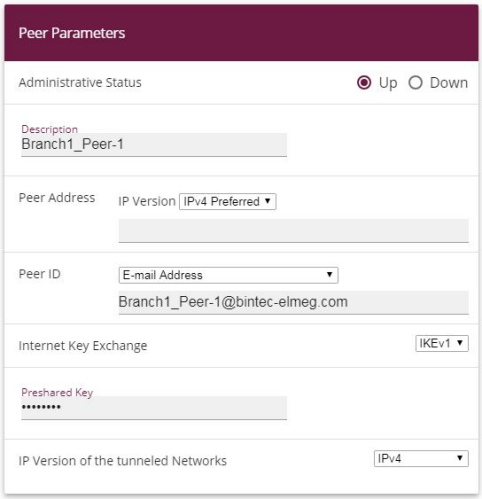
Fig. 90: **Network** -> **Load Balancing** -> **Load Balancing Groups**

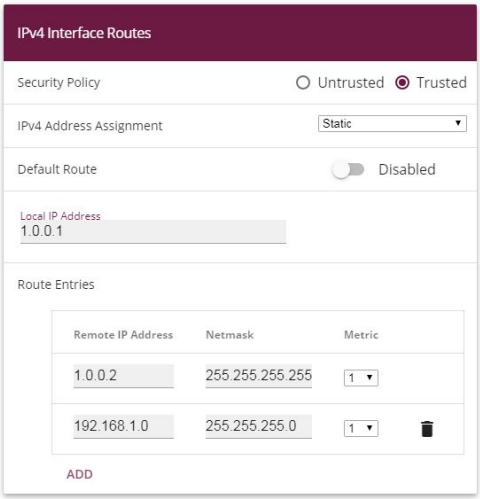
After this configuration step, the two Internet connections can be used with the IP load distribution. In this scenario, activating the IP load distribution means that no advanced routing entries are required to enable the VPN IPSec tunnel to be created.

Set up the VPN IPSec connections

In this scenario, the VPN IPSec connections are always set up from the branch office gateway to the head office gateway. The same IPSec Phase 1 and Phase 2 profile can be used for both tunnel connections. For this purpose, create two new VPN tunnels.

(1) Go to **VPN** -> **IPSec** -> **IPSec Peers** -> **New**.





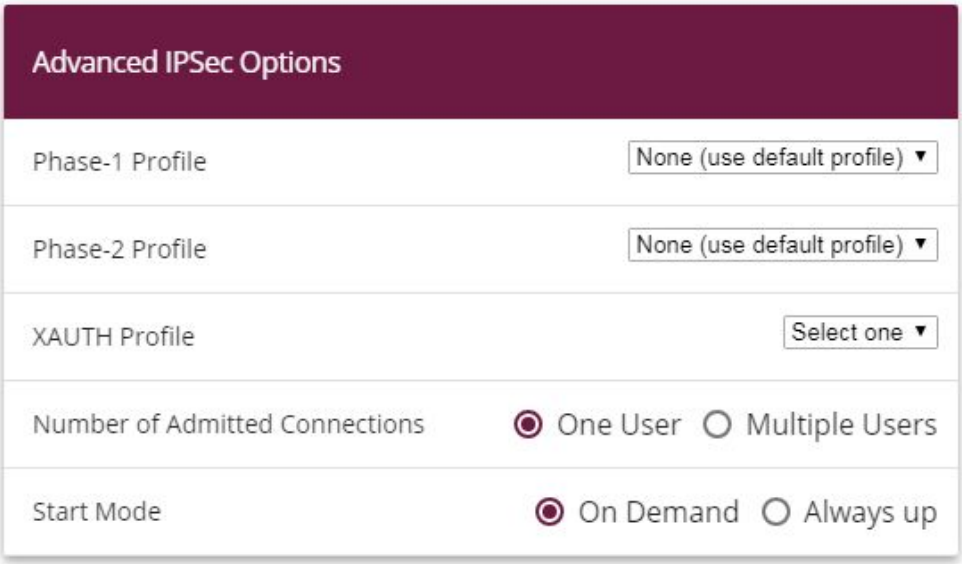


Fig. 92: **VPN**-> **IPSec**-> **IPSec Peers**-> **New**

To add a new connection, proceed as follows:

(1) Set the **Administrative Status** to `Up`. The peer is available for setting up a tunnel immediately after saving the configuration.

(2) For **Description**, enter a description of the peer which identifies it, e. g. `Branch1_Peer-1`.

(3) No address is entered for **Peer Address**, because the VPN tunnel is always set up from the branch office gateway to the head office gateway.

(4) For **Peer ID**, the ID type `E-mail Address` and the ID value `Branch1_Peer-1@bintec-elmeg.com` is used for the first VPN tunnel for connecting the branch office. The **peer ID** must be unique and match the remote terminal's local ID value.

(5) Select the version of the Internet Key Exchange protocol for **IKE (Internet Key Exchange)**. In this scenario, `IKEv1` must be used.

(6) For **Preshared Key**, enter the password for the encrypted connection (e. g. `test12345`.

(7) For **IPv4 Address Assignment**, select the configuration mode `Static`.

(8) In this scenario, the **Default route** option is not set.

(9) The **Local IP Address** is the IP address that is linked to the tunnel interface. Here, an address from a network that has not been previously used is used, e. g. `1.0.0.1`. This unique IP address enables ping requests for monitoring the VPN tunnel to be sent systematically via the VPN tunnel interface.

(10) The IP address / netmask of the destination network is defined as the **route entry**. If additional destination networks are to be routed over the tunnel, these can be added with the **Add** button.

Two routing entries are required in our example.

Enter an address from the range of the **local IP Address** of the tunnel interface which is being used to monitor the tunnel, e. g. `1.0.0.2`. This address must match the **local IP Address** of the VPN tunnel interface at the branch office gateway for the branch office **network**, in this example `192.168.1.0/24` another routing entry is required.

(11) As the **Phase-1 Profile**, the `None (use default profile)`, which has been generated automatically, is used.

(12) As the **Phase-2 Profile**, the `None (use default profile)`, which has been generated automatically, is used.

(13) Leave the remaining settings unchanged and confirm them with **OK**.

After configuring the first VPN IPSec connection to connect the branch office, the second VPN IPSec tunnel can now be created.

(1) Go to **VPN** -> **IPSec** -> **IPSec Peers** -> **New**.

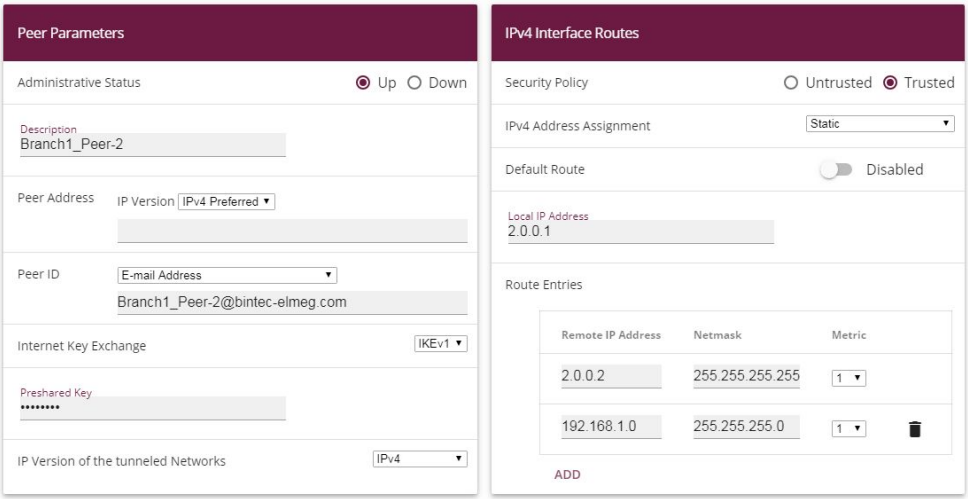


Fig. 93: **VPN**-> **IPSec**-> **IPSec Peers**-> **New**

To add a new connection, proceed as follows:

(1) Set the **Administrative Status** to `Up`. The peer is available for setting up a tunnel immediately after saving the configuration.

(2) For **Description**, enter a description of the peer which identifies it, e. g. `Branch1_Peer-2`.

(3) No address is entered for **Peer Address**, because the VPN tunnel is always set up from the branch office gateway to the head office gateway.

(4) For **Peer ID**, the ID type *E-mail Address* and the ID value *Branch1_Peer-2@bintec-elmeg.com* is used for the first VPN tunnel for connecting the branch office. The **Peer ID** must be unique and match the remote terminal's local ID value.

(5) Select the version of the Internet Key Exchange protocol for **IKE (Internet Key Exchange)**. In this scenario, *IKEv1* must be used.

(6) For **Preshared Key**, enter the password for the encrypted connection (e. g. *test12345*.

(7) For **IPv4 Address Assignment**, select the configuration mode *Static*.

(8) In this scenario, the **Default route** option is not set.

(9) The **Local IP Address** is the IP address that is linked to the tunnel interface. Here, an address from a network that has not been previously used is used, e. g. *2.0.0.1*. This unique IP address enables ping requests for monitoring the VPN tunnel to be sent systematically via the VPN tunnel interface.

(10) The IP address / netmask of the destination network is defined as the **route entry**. If additional destination networks are to be routed over the tunnel, these can be added with the **Add** button.

Two routing entries are required in our example.

Enter an address from the range of the **local IP address** of the tunnel interface which is being used to monitor the tunnel, e. g. *2.0.0.2*. This address must match the **local IP address** of the VPN tunnel interface at the branch office gateway for the branch office **network**, in this example *192.168.1.0/24* another routing entry is required.

(11) As the **Phase-1 Profile**, the *None (use default profile)*, which has been generated automatically, is used.

(12) As the **Phase-2 Profile**, the *None (use default profile)*, which has been generated automatically, is used.

(13) Leave the remaining settings unchanged and confirm them with **OK**.

When the first VPN IPSec connection was created, an IPSec **phase 1 profile** was created which both the VPN IPSec tunnels point to. To be able to use this **phase 1 profile** for the IPSec authentication, the local IPsec ID needs to be changed.

(1) Go to **VPN** -> **IPSec** -> **Phase 1 Profiles** -> **<Multi-Proposal>** ✎

Phase-1 (IKE) Parameters

Description
Multi-Proposal

Proposals

Encryption	Authentication	Enabled
AES	SHA2 256	
AES	MD5	●
3DES	MD5	●

DH Group: 2(1024 Bit)

Lifetime: 14400 Seconds 0 kBytes

Authentication Method: Preshared Keys

Mode

○ Main Mode (ID Protect) ◉ Aggressive

Strict

Local ID Type: E-mail Address

Local ID Value
central@bintec-elmeg.com

Fig. 94: **VPN** -> **IPSec** -> **Phase 1 Profiles** -> **<Multi-Proposal>**

Proceed as follows:

(1) For the **Local ID Type**, select the type of the local ID, here `E-mail Address`.

(2) For the **Local ID Value**, enter a value that can be used to identify the head office gateway, here e. g. `central@bintec-elmeg.com`.

(3) Leave the remaining settings unchanged and confirm them with **OK**.

Monitor the VPN IPSec connections

Ping requests are periodically sent to the branch office gateway via both tunnels in order to monitor the VPN IPSec tunnel connections. If this ping request fails to be answered three times, the head office gateway permits no new connections via the tunnel concerned. As soon as the branch office gateway answers the ping request three times once more, new IP connections are permitted. While one VPN tunnel is down, all the data is routed via the remaining VPN tunnel.

When the IPSec peers were being created, unique IP addresses (1.0.0.2 and 2.0.0.2 in this example) were issued for the VPN IPSec tunnel's ping monitoring. These addresses are used to periodically check that the branch office gateway can be accessed.

In the **Hosts** menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.

(1) Go to **Local Services**->**Surveillance**->**Hosts**->**New**.

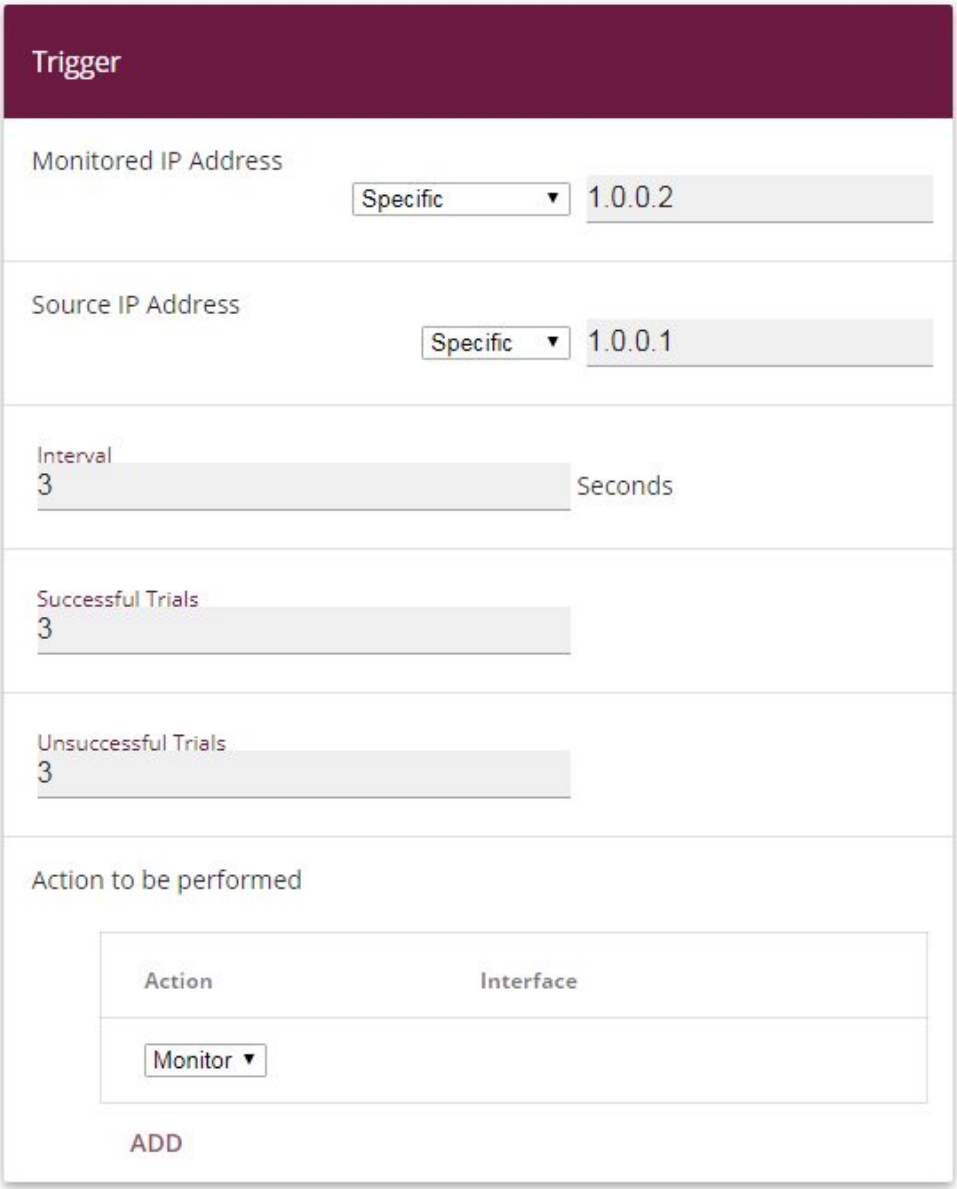


Fig. 95: **Local Services**->**Surveillance**->**Hosts**->**New**

Proceed as follows:

(1) The host surveillance can be linked to groups using the **group ID**. In this scenario, each instance of host surveillance must use a unique group ID.

(2) For **Monitored IP Address**, enter the IP address of the host that is to be monitored. For the monitoring of the first VPN IPSec tunnel, in our example the monitoring of the

branch office gateway is done with the address `1.0.0.2`.

(3) By setting the **Source IP Address** for host surveillance, you ensure that the ping packet with the **local IP address** of the VPN tunnel interface has been sent so that the branch office gateway can, in turn, reply via this same route. Select `Specific` and enter the local IP address of the first VPN IPSec interface, e. g. `1.0.0.1`.

(4) For **Interval**, enter the time interval (in seconds) which is to be used for checking that the host is available, here e. g. `3` seconds.

(5) For **Successful Trials**, enter the number of pings that must remain unanswered for the host to be regarded as unavailable. Here, e. g., after `3` failed attempts.

(6) For **Unsuccessful Trials**, enter the number of pings that must be answered for the host to be regarded as available once more. In our example, a host is regarded as available again after `3` successful ping requests/replies. This function is aimed at preventing frequent jitters in the connections.

(7) Under **Actions to be performed**, select the `Monitor` option, because the status of interfaces is not to be changed.

(8) Confirm with **OK**.

To monitor the second VPN IPSec tunnel, after saving a second entry for host surveillance must be created. Create the second host surveillance entry in the same way as the first entry except for the IP addresses. In the second entry for host surveillance, the **local IP addresses** of the second VPN IPSec interface are used. In our example, the address `2.0.0.2` is used as the **Monitored IP Mddress**, and `2.0.0.1` is used for the **Source IP Address**.

When the configuration is complete, the list of monitored hosts shows two entries that monitor the availability of the branch office gateway's IP addresses.

Results:

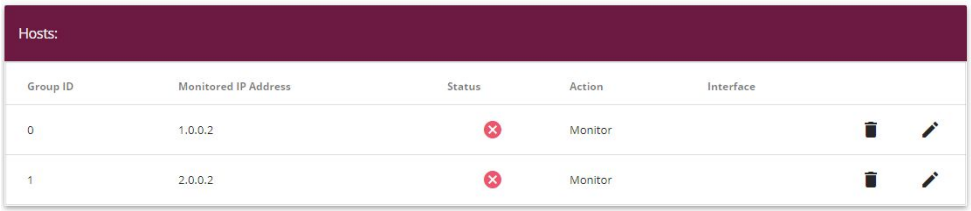


Fig. 96: **Local Services** -> **Surveillance** -> **Hosts**

Configure the IP load distribution for the VPN IPSec connections

Another load balancing group is created to distribute the IP sessions to the two VPN IPSec connections.

(1) Go to **Network** -> **Load Balancing** -> **Load Balancing Groups** -> **New**.

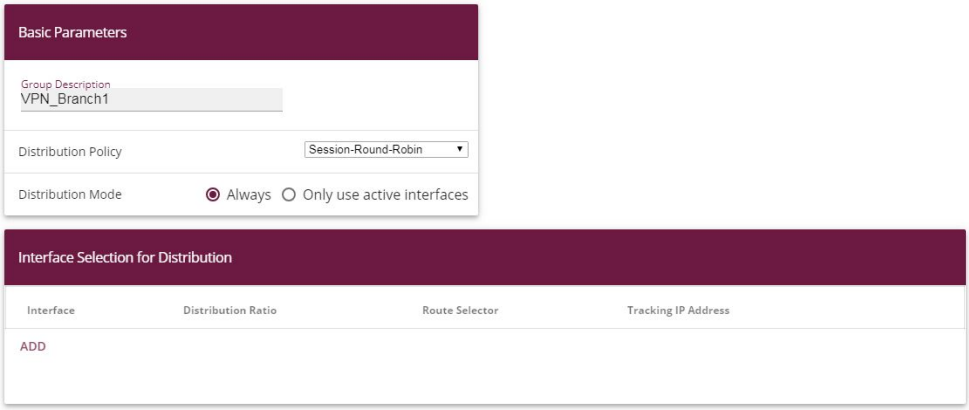


Fig. 97: **Network** ->**Load Balancing**->**Load Balancing Groups**->**New**

To create a load balancing group, proceed as follows:

(1) Under **Group description**, enter a name for the load balancing group, e. g. `VPN_Branch1`.

(2) For **Distribution policy**, select the method that will be used to distribute the data, here `Session-Round-Robin` (for load distribution based on IP sessions).

The two IPSec interfaces can then be added to this load balancing group.

To do this, click **Add**.

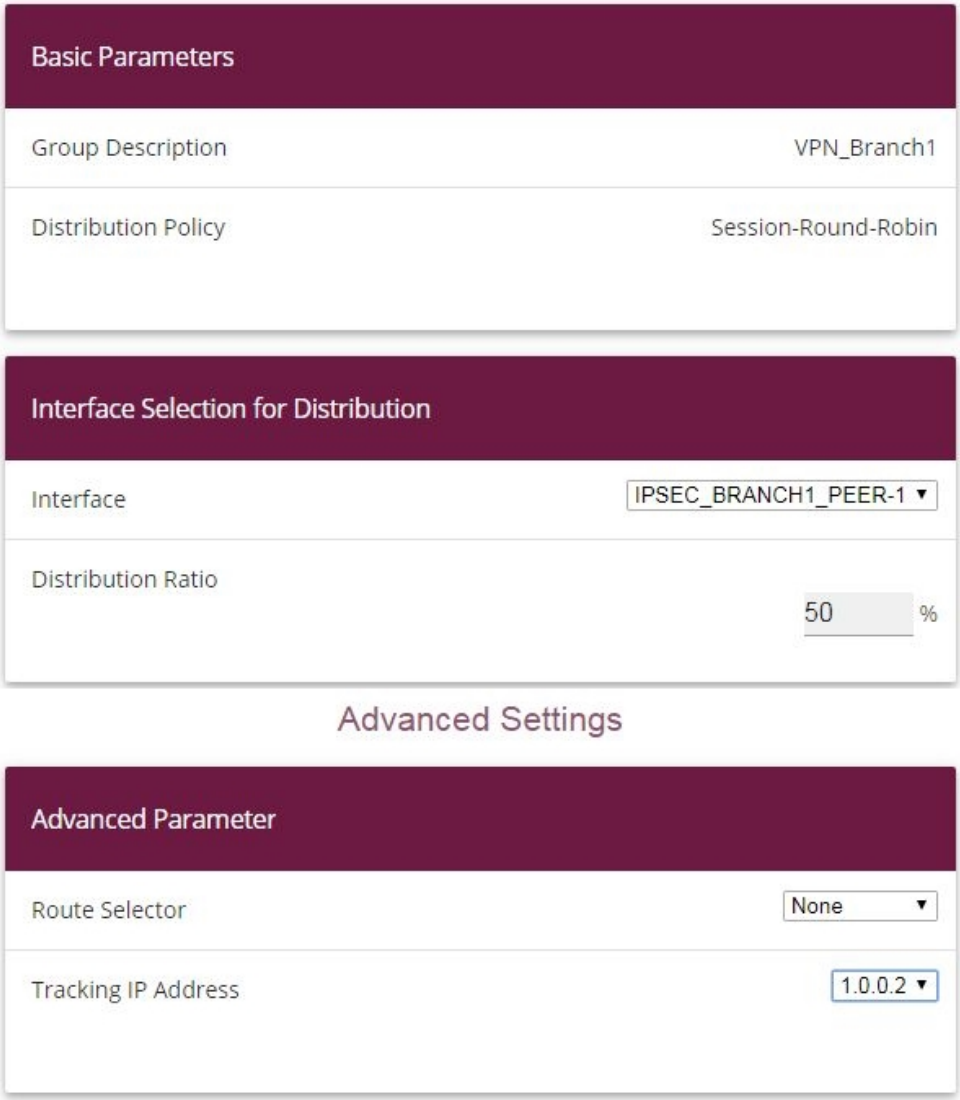


Fig. 98: **Network** ->**Load Balancing**->**Load Balancing Groups**->**Add**

Proceed as follows:

(1) For **Interface**, select the first VPN IPSec interface for connecting the branch office, here `IPSEC_BRANCH1_PEER-1` .

(2) Enter `50` % for **Distribution Ratio**. This option specifies the ratio in which new IP sessions are distributed to the interfaces in the IP load balancing group.

(3) In this example, the **Route selector** is left at `None`, since no interfaces have been assigned more than once in different load balancing groups.

(4) The **Tracing IP Address** option is used to select the IP address from the configured host monitoring, e. g. `1.0.0.2`. When the host surveillance detects that the connection has been broken, no more IP sessions are set up via this VPN IPSec tunnel.

(5) Click **Apply**.

(6) Add the second VPN IPSec interface with **Add**.

(7) For **Interface**, select `IPSEC_BRANCH1_PEER-2`.

(8) Enter `50` % for **Distribution Ratio**.

(9) Select the **Tracing IP Address**, e. g. `2.0.0.2`.

(10) Click **Apply**.

Results:

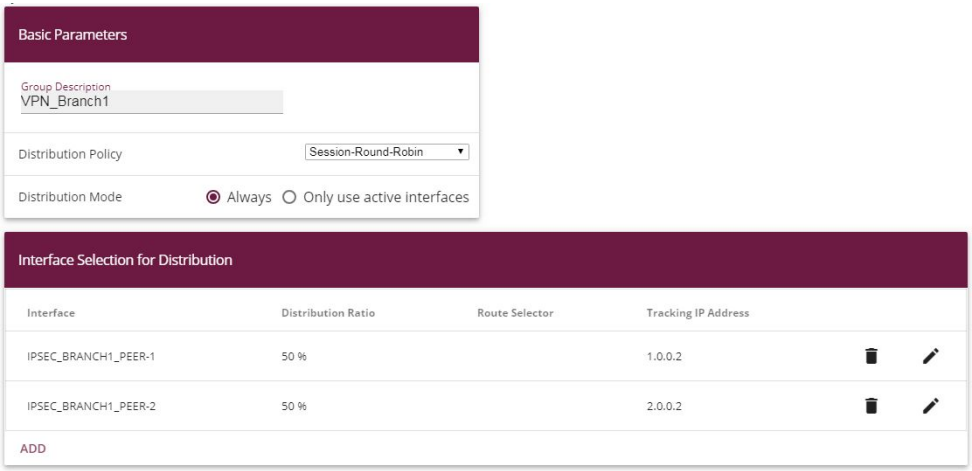


Fig. 99: **Network** -> **Load Balancing** -> **Load Balancing Groups**

11.2.2 Configure the gateway at the branch office

Setting up the Internet connection

The **Wizard** can be used to set up the branch office gateway's Internet access.

(1) Go to **Assistants** -> **Internet**-> **Internet Connections** -> **New**.

(2) For **Connection Type**, select `Internal ADSL Modem`.

(3) Click on **Next** to configure a new Internet connection.

(4) Enter the required data for the connection.

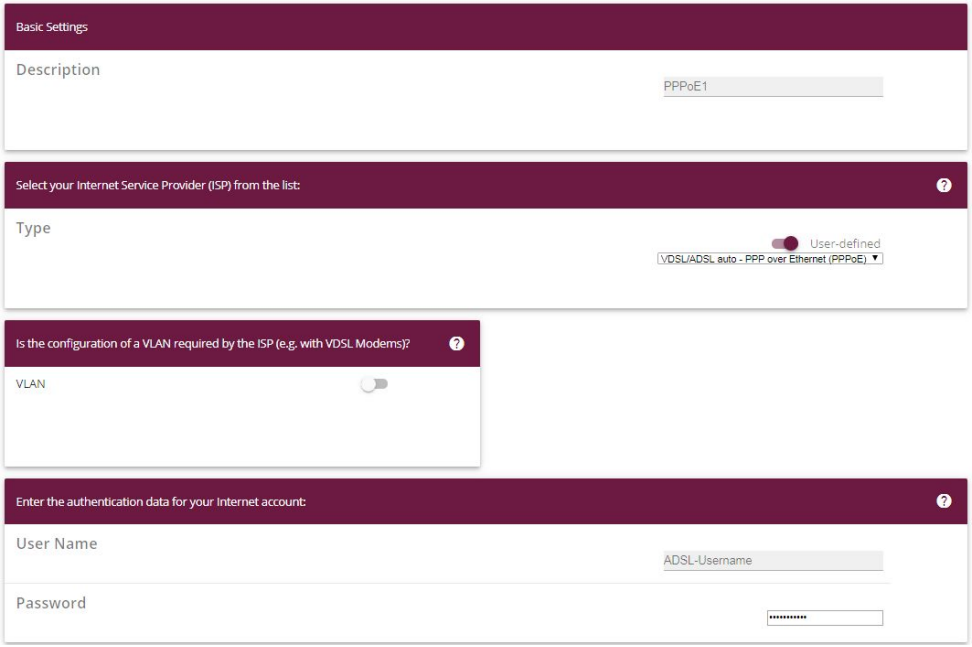


Fig. 100: **Assistants** -> **Internet**-> **Internet Connections** -> **New** -> **Next**

Proceed as follows to configure an Internet access:

(1) Under **Description** enter e.g. `PPPoE1` .

(2) For **Type**, select `User-defined via PPP over Ethernet (PPPoE)`.

(3) For **User Name**, enter the name that your provider has given you, e. g. `ADSL-Username`.

(4) Enter the **Password** that your provider has given you, e. g. `test12345`.

(5) Enable the **Always active** option.

(6) Press **OK** to confirm your entries.

Set up the VPN IPSec connections

The two IPSec peers at the branch office gateway need to be using different local IPSec IDs. Before configuring the actual IPSec peers, create the two phase 1 profiles.

(1) Go to **VPN** -> **IPSec** -> **Phase 1 Profiles** -> **New**

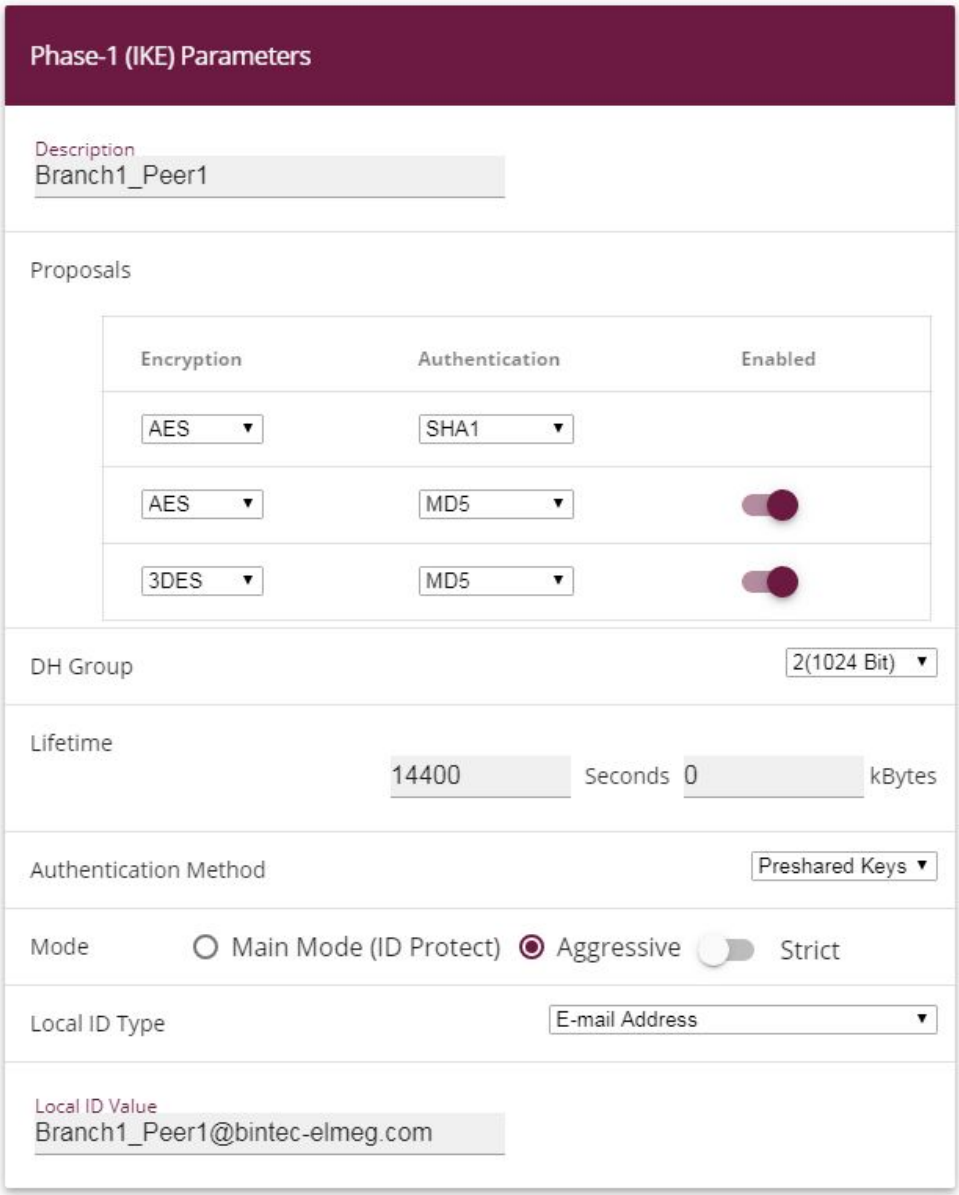


Fig. 101: **VPN** -> **IPSec** -> **Phase 1 Profiles** -> **New**

Proceed as follows.

(1) For **Description**, give the phase 1 profile a unique name, e. g. `Branch1_Peer1`.

(2) For **Proposals**, a combination of encryption and authentication algorithm is selected, e. g. `AES` / `SHA1`. This setting must match that of the head office gateway.

(3) Select the **DH Group**, (Diffie-Hellmann group) which is to be used in key calculation for creating the IPSec phase 1. This setting must match that of the head office gateway, e.g. DH Group `2 (1024 Bit)`.

(4) The **Lifetime** specifies the validity of the calculated key. The default value of `14400` seconds can be adopted here. This setting must match that of the head office gateway.

(5) In our example, the VPN IPSec tunnels are authenticated using the `Preshared Keys` **Authentication Method**. A shared password is issued for this purpose when the IPSec peer is being configured.

(6) Because, in this example, Internet accesses with dynamic addresses and preshared keys are used for the IPSec authentication, the **Mode** must be set to `Aggressive`. This setting must match that of the head office gateway.

(7) The **Local ID Type** specifies the type of the local ID value. In our example, a local ID of type `E-mail address` is used.

(8) The **Local ID Value** must be unique and match the peer ID option at the head office gateway. In this example, `Branch1_Peer1@bintec-elmeg.com` is used for the phase 1 profile of the first IPSec connection.

(9) Press **OK** to confirm your entries.

The second IPSec **phase 1 profile** can be created in the same way except for the description and the local ID value.

You configure the second IPsec **Phase 1 Profile** in the same way as you configured the first profile.

(1) Go to **VPN** -> **IPSec** -> **Phase 1 Profiles** -> **New**

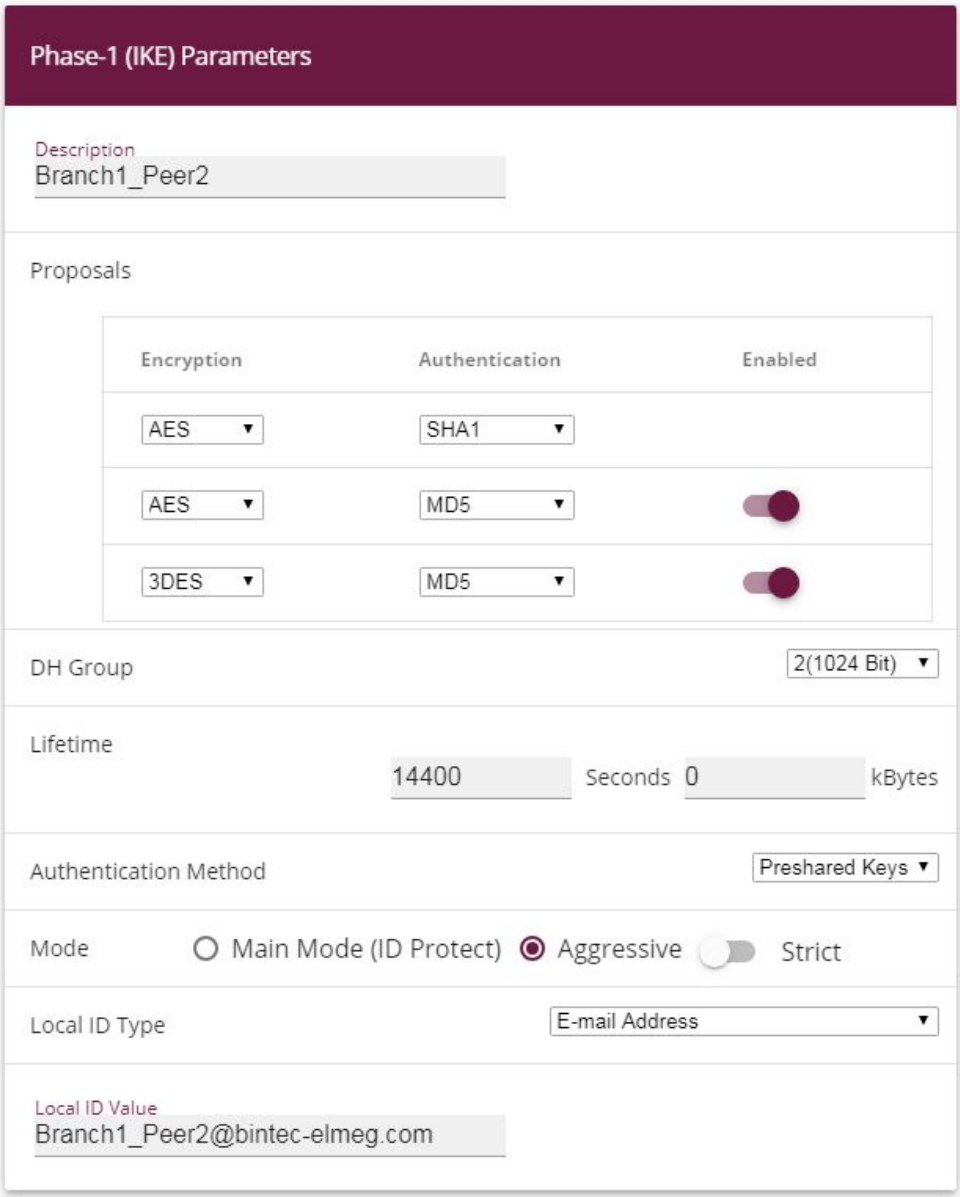


Fig. 102: **VPN** -> **IPSec** -> **Phase 1 Profiles** -> **New**

Proceed as follows.

(1) For **Description**, give the phase 1 profile a unique name, e. g. `Branch1_Peer2`.

(2) For **Proposals**, a combination of encryption and authentication algorithm is selected, e. g. `AES` / `SHA1`. This setting must match that of the head office gateway.

(3) Select the **DH Group**, (Diffie-Hellmann group) which is to be used in key calculation for creating the IPSec phase 1. This setting must match that of the head office gateway, e.g. DH Group `2 (1024 Bit)`.

(4) The **Lifetime** specifies the validity of the calculated key. The default value of `14400` seconds can be adopted here. This setting must match that of the head office gateway.

(5) In our example, the VPN IPSec tunnels are authenticated using the `Preshared Keys` **Authentication Method**. A shared password is issued for this purpose when the IPSec peer is being configured.

(6) Because, in this example, Internet accesses with dynamic addresses and preshared keys are used for the IPSec authentication, the **Mode** must be set to `Aggressive`. This setting must match that of the head office gateway.

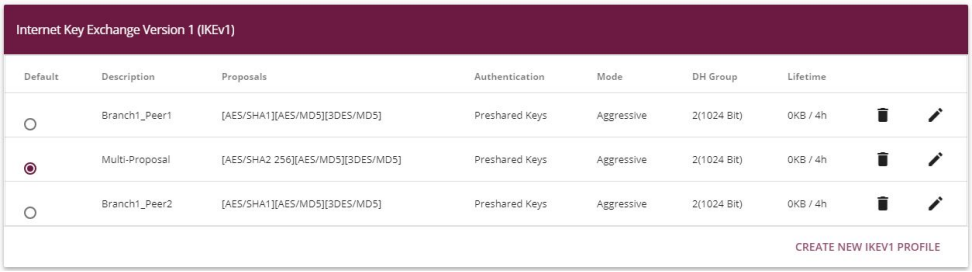
(7) The **Local ID Type** specifies the type of the local ID value. In our example, a local ID of type `E-mail address` is used.

(8) The **Local ID Value** must be unique and match the peer ID option at the head office gateway. In this example, `Branch1_Peer2@bintec-elmeg.com` is used for the phase 1 profile of the first IPSec connection.

(9) Press **OK** to confirm your entries.

Two entries for the IPSec connections that are to be configured then display in the overview of the IPSec **phase 1 profile**.

(1) Go to **VPN** -> **IPSec** -> **Phase 1 Profiles**.



Default	Description	Proposals	Authentication	Mode	DH Group	Lifetime
○	Branch1_Peer1	[AES/SHA1][AES/MD5][3DES/MD5]	Preshared Keys	Aggressive	2(1024 Bit)	0KB / 4h
◉	Multi-Proposal	[AES/SHA2 256][AES/MD5][3DES/MD5]	Preshared Keys	Aggressive	2(1024 Bit)	0KB / 4h
○	Branch1_Peer2	[AES/SHA1][AES/MD5][3DES/MD5]	Preshared Keys	Aggressive	2(1024 Bit)	0KB / 4h

Fig. 103: **VPN** -> **IPSec** -> **Phase-1 Profiles**

Two IPSec connections are now added to connect the head office.

(1) Go to **VPN** -> **IPSec** -> **IPSec Peers** -> **New**.

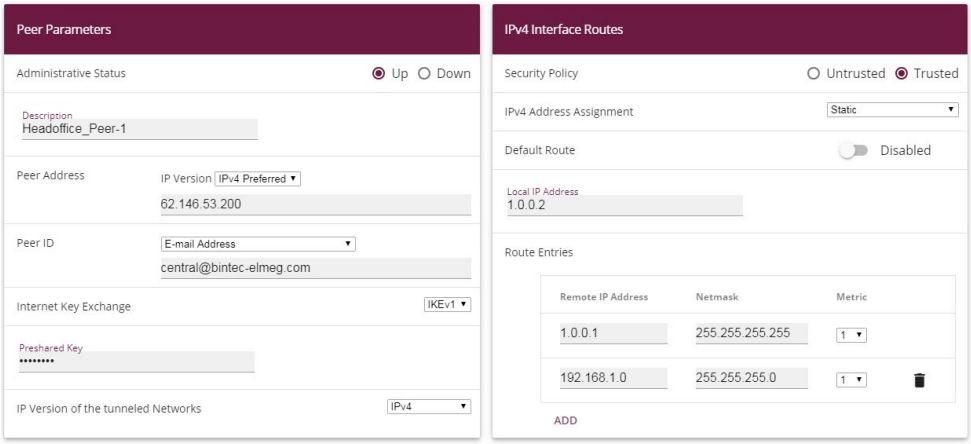


Fig. 104: **VPN**-> **IPSec**-> **IPSec Peers**-> **New**

To add a new connection, proceed as follows:

(1) Set the **Administrative Status** to `Up`. The peer is available for setting up a tunnel immediately after saving the configuration.

(2) For **Description**, enter a description of the peer which identifies it, e. g. `Headoffice_Peer-1`.

(3) For **Peer Address**, enter the static IP address or the host name used to access the first Internet access of the head office gateway. In our example, this is the static IP address `62.146.53.200`.

(4) The **Peer ID** must match the local ID value of the head office gateway. In this example, the type `E-mail address` and the ID value `central@bintec-elmeg.com` are used.

(5) Select the version of the Internet Key Exchange protocol for **IKE (Internet Key Exchange)**. In this scenario, `IKEv1` must be used.

(6) For **Preshared Key**, enter the password for the encrypted connection (e. g. `test12345`.

(7) For **IPv4 Address Assignment**, select the configuration mode `Static`.

(8) Select whether the route to this IPSec peer is to be defined as the default route. In this scenario, the **Default route** option is not set.

(9) The **Local IP Address** is the IP address that is linked to the tunnel interface, here e. g. `1.0.0.2`. An address from a previously unused network is used here. The VPN IPsec tunnel is monitored with this address.

(10) The IP address / netmask of the destination network is defined as the **route entry**. If additional destination networks are to be routed over the tunnel, these can be added with the **Add** button.

Two routing entries are required in our example.

Enter the IP address that is used as the local IP address of the tunnel interface at the head office gateway, e. g. `1.0.0.1`. A routing entry also needs to be created for the head office network, `192.168.0.0/24` in this example.

(11) As the **Phase-1 Profile**, you must select the IPSec phase 1 profile that was created previously for the first VPN IPSec tunnel, e. g. `Branch1_Peer1` .

(12) As the **Phase-2 Profile**, the default phase 2 profile that was automatically generated, here the `*Multi-Proposal`, is used.

(13) The **XAUTH profile** is not used in this scenario.

(14) **Number of Admitted Connections** can be left at the default value `One user`.

(15) As the VPN IPSec connections are always created from the branch office gateway to the head office gateway, the **Start Mode** here must be set to `Always up`.

(16) Leave the remaining settings unchanged and confirm them with **OK**.

After configuring the first VPN IPSec connection to connect the head office, the second VPN IPSec tunnel can now be created.

(1) Go to **VPN** -> **IPSec** -> **IPSec Peers** -> **New**.

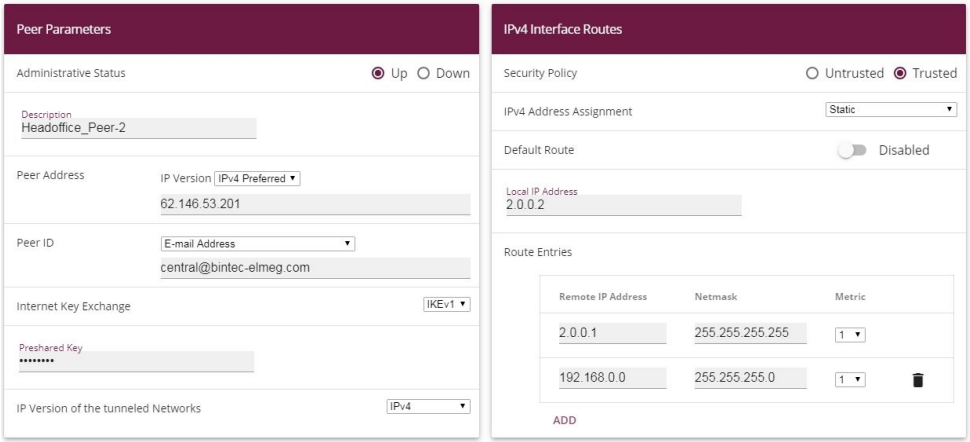


Fig. 105: **VPN**-> **IPSec**-> **IPSec Peers**-> **New**

To add a new connection, proceed as follows:

(1) Set the **Administrative Status** to `Up`. The peer is available for setting up a tunnel immediately after saving the configuration.

(2) For **Description**, enter a description of the peer which identifies it, e. g. `Headoffice_Peer-2`.

(3) For **Peer Address**, enter the static IP address or the host name used to access the first Internet access of the head office gateway. In our example, this is the static IP address `62.146.53.201`.

(4) The **Peer ID** must be unique and match the remote terminal's local ID value. In our example, the type *E-mail address* and the ID value *central@bintec-elmeg.com* are used.

(5) Select the version of the Internet Key Exchange protocol for **IKE (Internet Key Exchange)**. In this scenario, *IKEv1* must be used.

(6) For **Preshared Key**, enter the password for the encrypted connection (e. g. *test12345*.

(7) For **IPv4 Address Assignment**, select the configuration mode *Static*.

(8) In this scenario, the **Default route** option is not set.

(9) The **Local IP Address** is the IP address that is linked to the tunnel interface, here e. g. *2.0.0.2*. An address from a previously unused network is used here. The VPN IPsec tunnel is monitored with this address.

(10) The target IP address / netmask of the destination network is defined as the **route entry**. If additional destination networks are to be routed over the tunnel, these can be added with the **Add** button.

Two routing entries are required in our example.

Enter the IP address that is used as the local IP address of the tunnel interface at the head office gateway, e. g. *2.0.0.1*. For the head office **Network**, in this example *192.168.1.0/24*, another routing entry is also required.

(11) As the **Phase-1 Profile**, you must select the IPSec phase 1 profile that was created previously for the first VPN IPSec tunnel, e. g. *Branch1_Peer2*.

(12) As the **Phase-2 Profile**, the default phase 2 profile that was automatically generated, here the **Multi-Proposal*, is used.

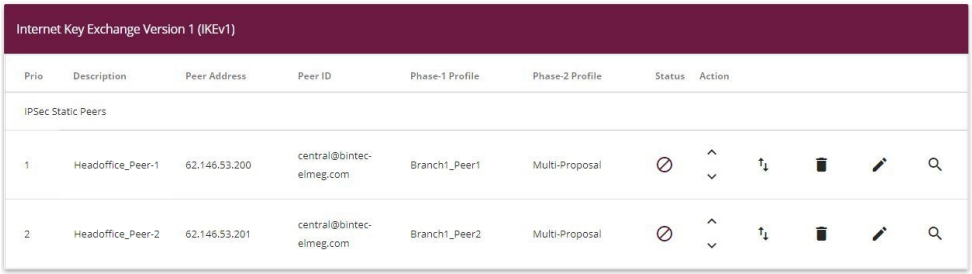
(13) The **XAUTH profile** is not used in this scenario.

(14) **Number of Admitted Connections** can be left at the default value *One user*.

(15) As the VPN IPSec connections are always created from the branch office gateway to the head office gateway, the **Start Mode** here must be set to *Always up*.

(16) Leave the remaining settings unchanged and confirm them with **OK**.

Results:



Internet Key Exchange Version 1 (IKEv1)

Prio	Description	Peer Address	Peer ID	Phase-1 Profile	Phase-2 Profile	Status	Action
IPSec Static Peers							
1	Headoffice_Peer-1	62.146.53.200	central@bintec-elmeg.com	Branch1_Peer1	Multi-Proposal		
2	Headoffice_Peer-2	62.146.53.201	central@bintec-elmeg.com	Branch1_Peer2	Multi-Proposal		

Fig. 106: **VPN**->**IPSec**->**IPSec Peers**

Monitor the VPN IPSec connections

Ping requests are periodically sent to the head office gateway via both tunnels in order to monitor the VPN IPSec tunnel connections. If this ping request fails to be answered three times, the branch office gateway permits no new connections via the tunnel concerned. As soon as the head office gateway answers the ping request three times once more, new IP connections are permitted. While one VPN tunnel is down, all the data is routed via the remaining VPN tunnel.

When the IPSec peers were being created, unique IP addresses (1.0.0.1 and 2.0.0.1 in this example) were issued for the VPN IPSec tunnel's ping monitoring. These addresses are used to periodically check that the branch office gateway can be accessed.

In the **Hosts** menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.

(1) Go to **Local Services**->**Surveillance**->**Hosts**->**New**.

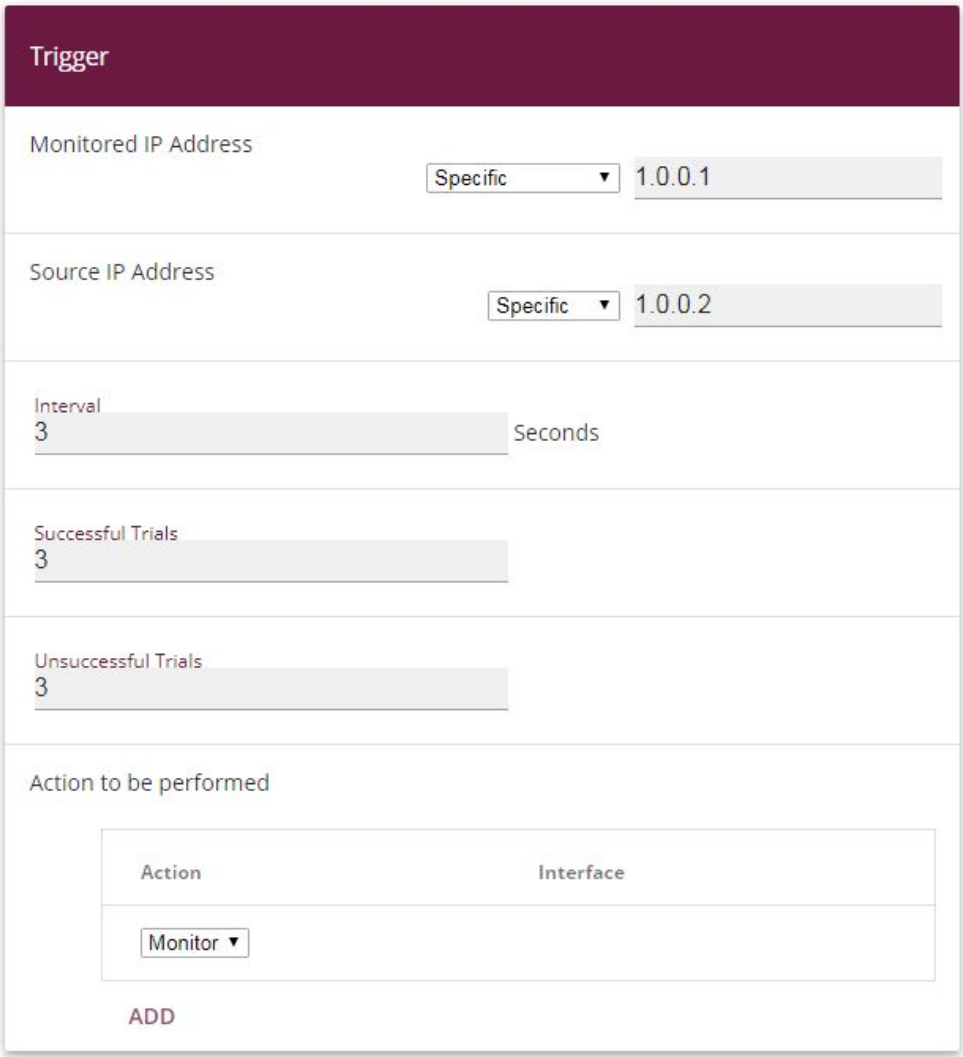


Fig. 107: **Local Services**->**Surveillance**->**Hosts**->**New**

Proceed as follows:

(1) The host surveillance can be linked to groups using the **group ID**. In this scenario, each instance of host surveillance must use a unique group ID.

(2) For **Monitored IP Address**, enter the IP address of the host that is to be monitored. For the monitoring of the first VPN IPSec tunnel, in our example the monitoring of the branch office gateway is done with the address `1.0.0.1`.

(3) By setting the **Source IP Address** for host surveillance, you ensure that the ping packet with the **local IP address** of the VPN tunnel interface has been sent so that the branch office gateway can, in turn, reply via this same route. Select `Specific`

and enter the local IP address of the first VPN IPSec interface, e. g. `1.0.0.2`.

(4) For **Interval**, enter the time interval (in seconds) which is to be used for checking that the host is available, here e. g. `3` seconds.

(5) For **Successful Trials**, enter the number of pings that must remain unanswered for the host to be regarded as unavailable. Here, e. g., after `3` failed attempts.

(6) For **Unsuccessful Trials**, enter the number of pings that must be answered for the host to be regarded as available once more. In our example, a host is regarded as available again after `3` successful ping requests/replies. This function is aimed at preventing frequent jitters in the connections.

(7) Under **Actions to be performed**, select the `Monitor` option, because the status of interfaces is not to be changed.

(8) Confirm with **OK**.

To monitor the second VPN IPSec tunnel, after saving a second entry for host surveillance must be created. Create the second host surveillance entry in the same way as the first entry except for the IP addresses. In the second entry for host surveillance, the **local IP addresses** of the second VPN IPSec interface are used. In our example, the address `2.0.0.1` is used as the **Monitored IP address**, and `2.0.0.2` is used for the **Source IP address**.

When the configuration is complete, the list of monitored hosts shows two entries that monitor the availability of the branch office gateway's IP addresses.

Results:

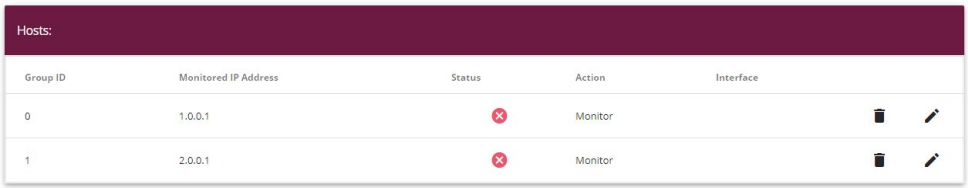


Fig. 108: **Local Services** -> **Surveillance** -> **Hosts**

Configure the IP load distribution for the VPN IPSec connections

A load balancing group is created to distribute the IP sessions to the two VPN IPSec connections.

(1) Go to **Network** -> **Load Balancing** -> **Load Balancing Groups** -> **New**.

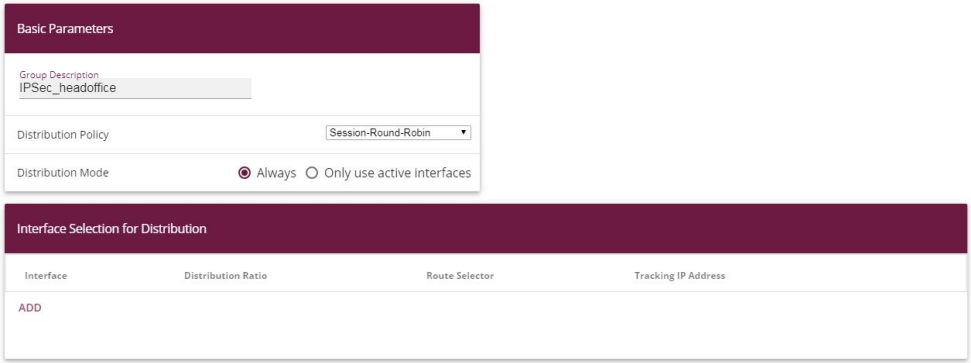


Fig. 109: **Network ->Load Balancing->Load Balancing Groups->New**

To create a load balancing group, proceed as follows:

(1) Under **Group Description**, enter a name for the load balancing group, e. g. `IPSec_headoffice`.

(2) For **Distribution Policy**, select the method that will be used to distribute the data, here `Session-Round-Robin` (for load distribution based on IP sessions).

The two ADSL Internet accesses can then be added to this load balancing group.

To do this, click **Add**.

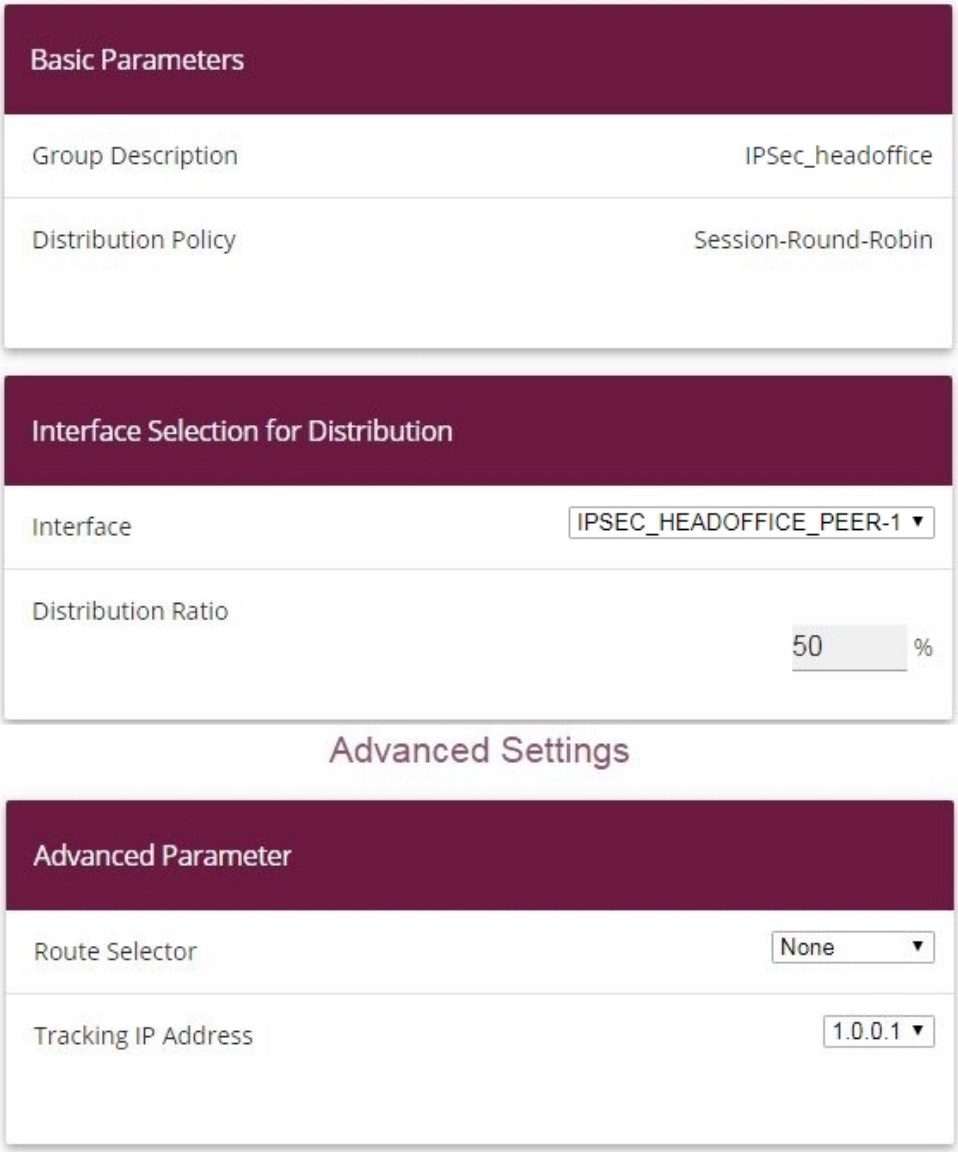


Fig. 110: **Network ->Load Balancing->Load Balancing Groups->Add**

Proceed as follows:

(1) For **Interface**, select the first VPN IPSec interface for connecting the head office, here `IPSEC_HEADOFFICE_PEER-1`.

(2) Enter `50` % for **Distribution Ratio**. This option specifies the ratio in which new IP sessions are distributed to the interfaces in the IP load balancing group.

(3) In this example, the **Route selector** is left at `None`, since no interfaces have been as-

signed more than once in different load balancing groups.

(4) The **Tracing IP Address** option is used to select an IP address from the configured host monitoring, e. g. `1.0.0.1`. When the host surveillance detects that the connection has been broken, no more IP sessions are set up via this VPN IPSec tunnel.

(5) Click **Apply**.

(6) Add the second VPN IPSec interface with **Add**.

(7) For **Interface**, select `IPSEC_HEADOFFICE_PEER-2`.

(8) Enter `50` % for **Distribution Ratio**.

(9) Select the **Tracing IP Address**, e. g. `2.0.0.1`.

(10) Click **Apply**.

Results:

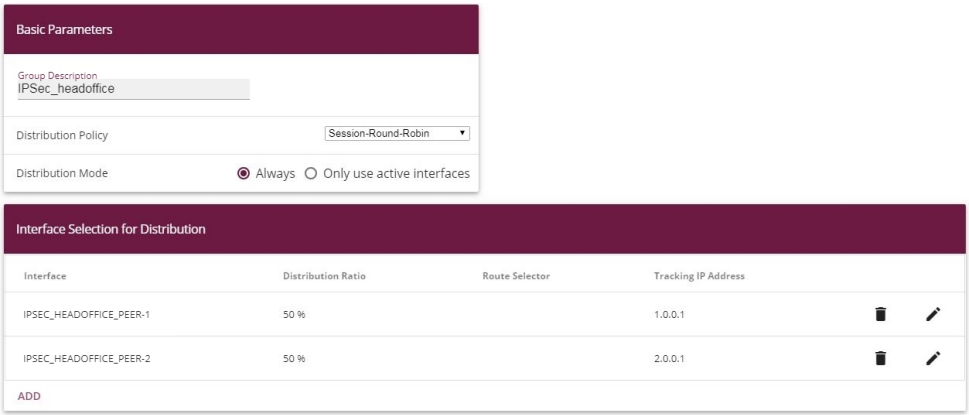


Fig. 111: **Network** -> **Load Balancing** -> **Load Balancing Groups**

11.3 Overview of Configuration Steps

Configure the Internet connections (head office)

Field	Menu	Value
Connector Type	**Assistants -> Internet-> Internet Connections -> New**	*Internal ADSL Modem*
Description	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *ADSL-1*
Type	**Assistants -> Internet-> Internet Connections -> New -> Next**	*User-defined via PPP over Ethernet (PPPoE)*
User Name	**Assistants -> Internet-> Internet Connections -> New -> Next**	e.g. *ADSL-Username*
Password	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *test12345*
Always Active	**Assistants -> Internet-> Internet Connections -> New -> Next**	*Enabled*
Connector Type	**Assistants -> Internet-> Internet Connections -> New**	*External ADSL modem*
Description	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *ADSL-2*
Physical Ethernet Port	**Assistants -> Internet-> Internet Connections -> New -> Next**	*ETH5*
User Name	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *ADSL-Username2*
Password	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *test12345*
Always Active	**Assistants -> Internet-> Internet Connections -> New -> Next**	*Enabled*

Create a load balancing group

Field	Menu	Value
Group Description	**Network ->Load Balancing ->Load Balancing Groups ->New**	e. g. *Internet Access.*
Distribution Policy	**Network ->Load Balancing ->Load Balancing Groups ->New**	*Session-Round-Robin*
Interface	**Network ->Load Balancing ->Load Bal-**	*WAN_ADSL-1*

Field	Menu	Value
	ancing Groups-> Add	
Distribution Ratio	**Network ->Load Balancing ->Load Balancing Groups-> Add**	*50* %
Interface	**Network ->Load Balancing ->Load Balancing Groups-> Add**	*WAN_ADSL-2*
Distribution Ratio	**Network ->Load Balancing-> Load Balancing Groups-> Add**	*50* %

Set up the VPN IPSec connections

Field	Menu	Value
Administrative Status	**VPN-> IPSec-> IPSec Peers-> New**	*Up*
Description	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *Branch1_Peer-1*
Peer ID	**VPN-> IPSec-> IPSec Peers-> New**	*E-mail address* and e. g. *Branch1_Peer-1@bintec-elmeg.com*
IKE (Internet Key Exchange)	**VPN-> IPSec-> IPSec Peers-> New**	*IKEv1*
Preshared Key	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *test12345*
IPv4 Address Assignment	**VPN-> IPSec-> IPSec Peers-> New**	*Static*
Local IP Address	**VPN-> IPSec-> IPSec Peers-> New**	*1.0.0.1*
Route Entries	**VPN-> IPSec-> IPSec Peers-> New**	*1.0.0.2/255.255.255.255* and *192.168.1.0/255.255.255.0*
Phase-1 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	None (use Default Profile)
Phase-2 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	None (use Default Profile)
Administrative Status	**VPN-> IPSec-> IPSec Peers-> New**	*Active*
Description	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *Branch1_Peer-2*
Peer ID	**VPN-> IPSec-> IPSec Peers-> New**	*E-mail address* and e. g. *Branch1_Peer-2@bin*

Field	Menu	Value
		tec-elmeg.com
IKE (Internet Key Exchange)	**VPN-> IPSec-> IPSec Peers-> New**	*IKEv1*
Preshared Key	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *test12345*
IPv4 Address Assignment	**VPN-> IPSec-> IPSec Peers-> New**	*Static*
Local IP Address	**VPN-> IPSec-> IPSec Peers-> New**	*2.0.0.1*
Route Entries	**VPN-> IPSec-> IPSec Peers-> New**	*2.0.0.2* / *255.255.255.255* and *192.168.1.0* / *255.255.255.0*
Phase-1 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	*None (use Default Profile)*
Phase-2 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	*None (use Default Profile)*
Local ID Type	**VPN -> IPSec -> Phase-1 Profiles -> <Multi-Proposal>**	*E-mail Address*
Local ID Value	**VPN -> IPSec -> Phase-1 Profiles -> <Multi-Proposal>**	e. g. *central@bintec-elmeg.com*

Set up monitoring tasks

Field	Menu	Value
Monitored IP Address	**Local Services-> Surveillance ->Hosts-> New**	e. g. *1.0.0.2*
Source IP Address	**Local Services ->Surveillance ->Hosts-> New**	*Specific* / e. g. *1.0.0.1*
Interval	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3* seconds
Successful Trials	**Local Services ->Surveillance ->Hosts-> New**	e. g. *3*
Unsuccessful Trials	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3*
Action to be performed	**Local Services ->Surveillance ->Hosts-> New**	*Monitor*
Monitored IP Address	**Local Services-> Surveillance ->Hosts-> New**	e. g. *2.0.0.2*

Field	Menu	Value
Source IP Address	**Local Services ->Surveillance ->Hosts-> New**	*Specific* / e. g. *2.0.0.1*
Interval	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3* seconds
Successful Trials	**Local Services ->Surveillance ->Hosts-> New**	e. g. *3*
Unsuccessful Trials	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3*
Action to be performed	**Local Services ->Surveillance ->Hosts-> New**	*Monitor*

Configure the IP load distribution

Field	Menu	Value
Group Description	**Network ->Load Balancing ->Load Balancing Groups ->New**	e. g. *VPN_Branch1*
Distribution Policy	**Network ->Load Balancing ->Load Balancing Groups ->New**	*Session-Round-Robin*
Interface	**Network ->Load Balancing ->Load Balancing Groups ->Add**	*IPSEC_BRANCH1_PEER-1*
Distribution Ratio	**Network ->Load Balancing ->Load Balancing Groups-> Add**	*50* %
Route Selector	**Network -> Load Balancing -> Load Balancing Groups -> Add -> Advanced Settings**	*open*
Tracing IP Address	**Network ->Load Balancing ->Load Balancing Groups-> Add**	e. g. *1.0.0.2*
Interface	**Network ->Load Balancing ->Load Balancing Groups-> Add**	*IPSEC_BRANCH1_PEER-2*
Distribution Ratio	**Network ->Load Balancing ->Load Balancing Groups-> Add**	*50* %
Route Selector	**Network -> Load Balancing -> Load Balancing Groups -> Add -> Advanced Settings**	*open*
Tracing IP Address	**Network ->Load Balancing ->Load Balancing Groups ->Add**	e. g. *2.0.0.2*

Configure the Internet connections (branch)

Field	Menu	Value
Connector Type	**Assistants -> Internet-> Internet Connections -> New**	*Internal ADSL Modem*
Description	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *PPPoE1*
Type	**Assistants -> Internet-> Internet Connections -> New -> Next**	*User-defined via PPP over Ethernet (PPPoE)*
User Name	**Assistants -> Internet-> Internet Connections -> New -> Next**	e.g. *ADSL-Username*
Password	**Assistants -> Internet-> Internet Connections -> New -> Next**	e. g. *test12345*
Always Active	**Assistants -> Internet-> Internet Connections -> New -> Next**	*Enabled*

Set up the VPN IPSec connections

Field	Menu	Value
Description	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *Branch1_Peer1*
Proposals	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *AES / SHA1*
DH Group	**VPN -> IPSec -> Phase-1 Profiles -> New**	e.g. *2(1024 Bit)*
Lifetime	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *14400*
Authentication Method	**VPN -> IPSec -> Phase-1 Profiles -> New**	*Preshared keys*
Mode	**VPN -> IPSec -> Phase-1 Profiles -> New**	*Aggressive*
Local ID Type	**VPN -> IPSec -> Phase-1 Profiles -> New**	*E-mail Address*
Local ID Value	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *Branch1_Peer1@bintec-elmeg.com*
Description	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *Branch1_Peer2*
Proposals	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *AES / SHA1*

Field	Menu	Value
DH Group	**VPN -> IPSec -> Phase-1 Profiles -> New**	e.g. *2(1024 Bit)*
Lifetime	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *14400*
Authentication Method	**VPN -> IPSec -> Phase-1 Profiles -> New**	*Preshared keys*
Mode	**VPN -> IPSec -> Phase-1 Profiles -> New**	*Aggressive*
Local ID Type	**VPN -> IPSec -> Phase-1 Profiles -> New**	*E-mail Address*
Local ID Value	**VPN -> IPSec -> Phase-1 Profiles -> New**	e. g. *Branch1_Peer2@bintec-elmeg.com*

Add IPSec connections

Field	Menu	Value
Administrative Status	**VPN-> IPSec-> IPSec Peers-> New**	*Up*
Description	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *Headoffice_Peer-1*
Peer Address	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *62.146.53.200*
Peer ID	**VPN-> IPSec-> IPSec Peers-> New**	*E-mail address* and e. g. *central@bintec-elmeg.com*
IKE (Internet Key Exchange)	**VPN-> IPSec-> IPSec Peers-> New**	*IKEv1*
Preshared Key	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *test12345*
IPv4 Address Assignment	**VPN-> IPSec-> IPSec Peers-> New**	*Static*
Local IP Address	**VPN-> IPSec-> IPSec Peers-> New**	*1.0.0.2*
Route Entries	**VPN-> IPSec-> IPSec Peers-> New**	*1.0.0.1/255.255.255.255* and *192.168.0.0/255.255.255.0*
Phase-1 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	Branch1_Peer1

Field	Menu	Value
Phase-2 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	* Multi-Proposal
Number of Admitted Connections	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	One User
Start Mode	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	Always up
Administrative Status	**VPN-> IPSec-> IPSec Peers-> New**	*Active*
Description	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *Headoffice_Peer-2*
Peer Address	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *62.146.53.201*
Peer ID	**VPN-> IPSec-> IPSec Peers-> New**	*E-mail address* and e. g. *central@bintec-elmeg.com*
IKE (Internet Key Exchange)	**VPN-> IPSec-> IPSec Peers-> New**	*IKEv1*
Preshared Key	**VPN-> IPSec-> IPSec Peers-> New**	e. g. *test12345*
IPv4 Address Assignment	**VPN-> IPSec-> IPSec Peers-> New**	*Static*
Local IP Address	**VPN-> IPSec-> IPSec Peers-> New**	*2.0.0.2*
Route Entries	**VPN-> IPSec-> IPSec Peers-> New**	*2.0.0.1* / *255.255.255.255* and *192.168.0.0* / *255.255.255.0*
Phase-1 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	Branch1_Peer2
Phase-2 Profile	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	* Multi-Proposal
Number of Admitted Connections	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	One User
Start Mode	**VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings**	Always up

Set up monitoring tasks

Field	Menu	Value
Monitored IP Ad-	**Local Services-> Surveillance ->Hosts-**	e. g. *1.0.0.1*

Field	Menu	Value
dress	**> New**	
Source IP Address	**Local Services ->Surveillance ->Hosts-> New**	*Specific* / e. g. *1.0.0.2*
Interval	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3* seconds
Successful Trials	**Local Services ->Surveillance ->Hosts-> New**	e. g. *3*
Unsuccessful Trials	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3*
Action to be performed	**Local Services ->Surveillance ->Hosts-> New**	*Monitor*
Monitored IP Address	**Local Services-> Surveillance ->Hosts-> New**	e. g. *2.0.0.1*
Source IP Address	**Local Services ->Surveillance ->Hosts-> New**	*Specific* / e. g. *2.0.0.2*
Interval	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3* seconds
Successful Trials	**Local Services ->Surveillance ->Hosts-> New**	e. g. *3*
Unsuccessful Trials	**Local Services-> Surveillance ->Hosts-> New**	e. g. *3*
Action to be performed	**Local Services ->Surveillance ->Hosts-> New**	*Monitor*

Configure the IP load distribution

Field	Menu	Value
Group Description	**Network ->Load Balancing-> Load Balancing Groups ->New**	e. g. *IPSec_headoffice*
Distribution Policy	**Network ->Load Balancing ->Load Balancing Groups ->New**	*Session-Round-Robin*
Interface	**Network ->Load Balancing-> Load Balancing Groups ->Add**	*IPSEC_HEADOFFICE_PEER-1*
Distribution Ratio	**Network ->Load Balancing ->Load Balancing Groups-> Add**	*50* %
Route Selector	**Network -> Load Balancing ->Load Balancing Groups -> Add -> Advanced Settings**	*open*

Field	Menu	Value
Tracing IP Address	**Network ->Load Balancing ->Load Balancing Groups ->Add**	e. g. *1.0.0.1*
Interface	**Network ->Load Balancing ->Load Balancing Groups ->Add**	*IPSEC_HEADOFFICE_PEER-2*
Distribution Ratio	**Network ->Load Balancing ->Load Balancing Groups-> Add**	*50* %
Route Selector	**Network -> Load Balancing ->Load Balancing Groups -> Add -> Advanced Settings**	*open*
Tracing IP Address	**Network ->Load Balancing ->Load Balancing Groups-> Add**	e. g. *2.0.0.1*

Chapter 12 IP - Using Drop-in to connect a branch office to head office with a VPN tunnel

12.1 Introduction

In this example, we shall describe how the Drop-in group functionality can be used to connect a branch office to the head office by a VPN tunnel.

Using a Drop-in group is an option if the current Internet access at the branch does not allow a VPN tunnel to be set up and it cannot be replaced. The advantage of the Drop-in group is that there is no need to change the network structure and the configuration of the individual routers in the branch.

A **bintec** router is put between the provider gateway and the current network in the branch. This establishes the tunnel to the head office and routes all the packets for the head office through it, while all the rest are routed as normal to the provider gateway.

The **GUI** (Graphical User Interface) is used for configuring.

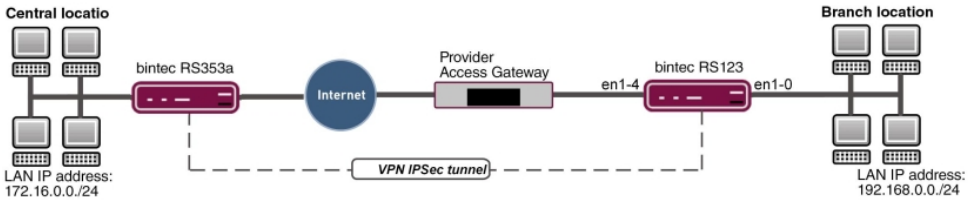


Fig. 112: Example scenario

Requirements

- A **bintec RS123** router
- Firmware version at least 10.2.5
- Branch office has a dynamic Internet access
- Head office has a VPN-capable gateway that can be accessed via a static IP address, e. g. **bintec RS353a**

12.2 Configuration

Open a web browser and create an http connection to the device. In our example, the local network in the branch is identical to the device's preset default network.

Configure the Drop-in group.

Firstly, a new **Drop-in group** is created for the local extension network.

(1) Go to **Network** -> **Drop In** -> **Drop In Groups** -> **New**.

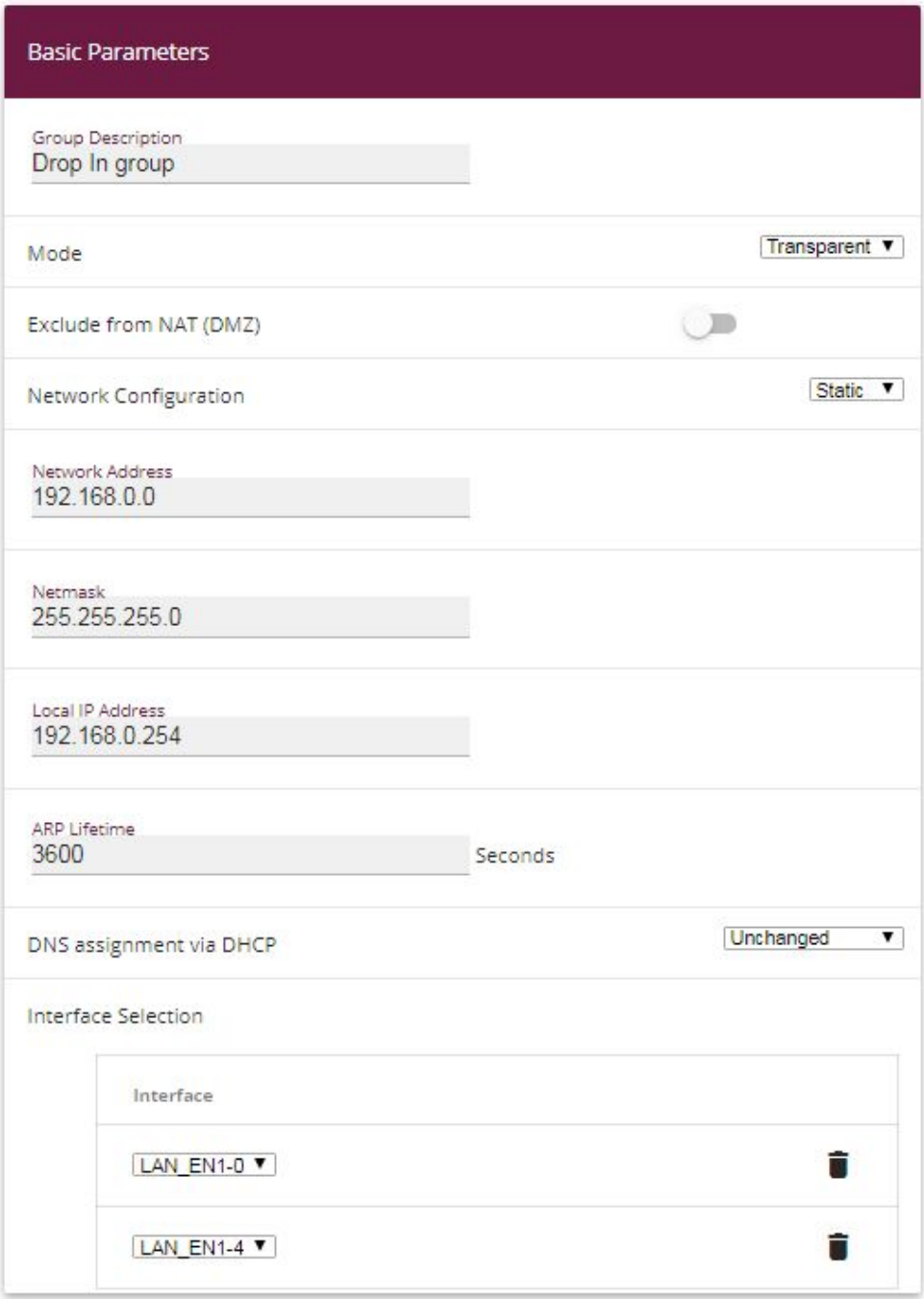


Fig. 113: **Network** -> **Drop In** -> **Drop In Groups** -> **New**

Proceed as follows:

(1) Under **Group Description** enter a unique description for the drop-in group, e. g. `Drop In group`.

(2) Under **Mode**, select `Transparent`. ARP packets and IP packets belonging to the drop-in network are routed transparently (unchanged).

(3) Under **Network Configuration**, select how an IP address is assigned to the network components, in this case `Static`.

(4) Enter the **Network Address** of the drop-in network, in this case e. g. `192.168.0.0`.

(5) Enter the relevant **Netmask**, e. g. in this case `255.255.255.0`.

(6) Enter the drop-in group's **Local IP Address**, e. g. `192.168.0.254`.

(7) For **Interface Selection**, select all the ports that are to be included in the drop-in group (in the network), e. g. `LAN_EN1-0` and `LAN_EN1-4`.

(8) Confirm with **OK**.

Set up the default route

In the next step, you set up a default route to the provider gateway. In doing this, you need to select the interface for the drop-in group to which the gateway is later connected.

(1) Go to **Network** -> **Routes** ->**IPv4 Route Configuration** ->**New**.

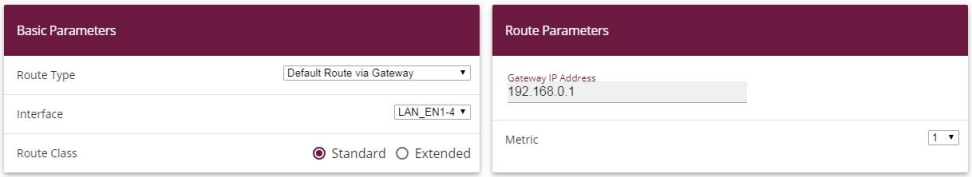


Fig. 114: **Network** -> **Routes** -> **IPv4 Route Configuration**-> **New**

Proceed as follows:

(1) Select `Default Route via Gateway` as the **Route Type**.

(2) Select the **Interface** that is to be used for this route, in this case `LAN_EN1-4`.

(3) For **Gateway IP Address**, enter the IP address of the provider gateway, in this case e. g. `192.168.0.1`.

(4) Confirm with **OK**.

Set up the VPN tunnel endpoint in the branch

The **GUI** has a **wizard** to help you to configure an endpoint for the VPN (IPSec) connection in the branch.

To do this, you need to know the static address under which the remote terminal at head office can be accessed. The **wizard** automatically creates a route for the head office network that is to be accessed via the tunnel. To do this, go to the following menu:

(1) Go to **Assistants** -> **VPN** -> **VPN Connections** -> **New**.

(2) For **VPN Scenario** select `IPSec-LAN-LAN Connection`.

(3) Click on **Next** to configure a new VPN connection.

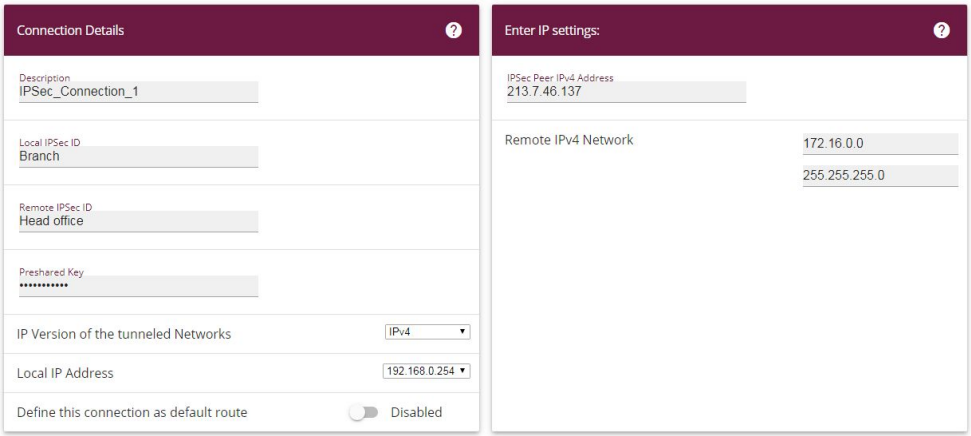


Fig. 115: **Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**

Proceed as follows:

(1) Under **Description**, enter a name for the connection, e. g. `IPSec_Connection_1`.

(2) For **Local IPSec ID** enter the ID of your own IPSec gateway, e. g. `Branch`.

(3) For **Remote IPSec ID** enter the ID of the remote IPSec gateway, e. g. `Head office`.

(4) Enter a **Preshared Key** for the authentication. The preshared key must be configured identically on both sides.

(5) Select the **Local IP Address** `192.168.0.254`.

(6) For **IPSec Peer IPv4 Address**, enter the IP address of the remote IPSec partner, in this case e. g. `213.7.46.137`.

(7) Enter the IP address of the **Remote IPv4 Network**, in this case e. g. `172.16.0.0`.

(8) Enter the relevant **Netmask** of the destination network, e. g. in this case `255.255.255.0`.

(9) Press **OK** to confirm your entries.

Set up the VPN tunnel endpoint at head office

Configure the relevant remote terminal of the VPN tunnel at head office.

(1) Go to **Assistants** -> **VPN** -> **VPN Connections** -> **New**.

(2) For **VPN Scenario** select `IPSec-LAN-LAN Connection`.

(3) Click on **Next** to configure a new VPN connection.

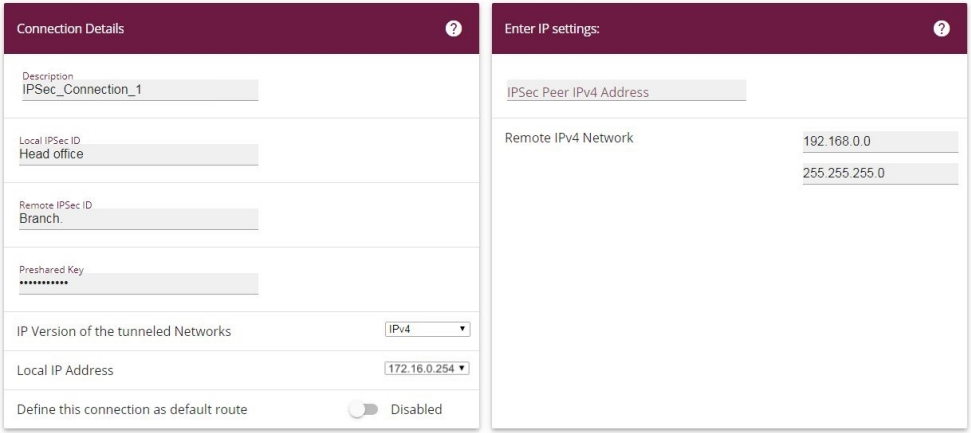


Fig. 116: **Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**

Proceed as follows:

(1) Under **Description**, enter a name for the connection, e. g. `IPSec_Connection_1`.

(2) For **Local IPSec ID** enter the ID of your own IPSec gateway, e. g. `Head office`.

(3) For **Remote IPSec ID** enter the ID of the remote IPSec gateway, e. g. `Branch`.

(4) Enter a **Preshared Key** for the authentication. The preshared key must be configured identically on both sides.

(5) Enter the required **Local IP Address** of the gateway, e.g. `172.16.0.254`.

(6) As the drop-in router at the branch is not to be accessed from outside, the tunnel always needs to be initiated by the branch. So the field **IPSec Peer Address** at head office remains empty.

(7) Enter the IP address of the **Remote IPv4 Network**, in this case e. g. `192.168.0.0`.

(8) Enter the relevant **Netmask** of the destination network, e. g. in this case `255.255.255.0`.

(9) Press **OK** to confirm your entries.

This completes the configuration. Save the configuration with **Save configuration** and confirm the selection with **OK**.

12.3 Overview of Configuration Steps

Configure a drop-in group

Field	Menu	Value
Group Description	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *Drop-in group*.
Mode	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	*Transparent*
Network Configuration	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	*Static*
Network Address	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *192.168.0.0*
Netmask	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *255.255.255.0*
Local IP Address	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *192.168.0.254*
Interface Selection	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *LAN_EN1-0*, *LAN_EN1-4*

Set up the default route

Field	Menu	Value
Route Type	**Network** -> **Routes** -> **IPv4 Route Configuration** -> **New**	*Default Route*
Interface	**Network** -> **Routes** -> **IPv4 Route Configuration** -> **New**	*LAN_EN1-4*
Gateway IP Address	**Network** -> **Routes** -> **IPv4 Route Configuration** -> **New**	e. g. *192.168.0.1*

Set up a VPN connection (branch)

Field	Menu	Value
VPN Scenario	**Assistants** -> **VPN** -> **VPN Connections** -> **New**	*IPSec - LAN-to-LAN connection*
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *IPSec_Connection_1*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	*Branch*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connec-**	*Head office*

Field	Menu	Value
	tions -> **New** -> **Next**	
Preshared key	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	Enter password
Local IP Address	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *192.168.0.254*
IPSec Peer IPv4 Address	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *213.7.46.137*
Remote IPv4 Network	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *172.16.0.0*
Netmask	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *255.255.255.0*

Set up a VPN connection (head office)

Field	Menu	Value
VPN Scenario	**Assistants** -> **VPN** -> **VPN Connections** -> **New**	*IPSec - LAN-to-LAN connection*
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *IPSec_Connection_1*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	*Head office*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	*Branch*
Preshared key	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	Enter password
Local IP Address	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *172.16.0.254*
Remote IPv4 Network	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *192.168.0.0*
Netmask	**Assistants** -> **VPN** -> **VPN Connections** -> **New** -> **Next**	e. g. *255.255.255.0*

Chapter 13 IP - Set up a DMZ with the drop-in group's functionality

13.1 Introduction

We shall now describe how to set up a DMZ (Demilitarized Zone) with the functionality of the drop-in group.

The solution can be useful if, for example, one has access to a small IP network with public addresses. In such cases, the connection to the Internet is achieved via a gateway managed by the provider, without any administrative access.

A **bintec** router with the drop-in functionality is placed between the provider gateway and the hosts in the DMZ. The drop-in group now establishes the connection between the gateway and the DMZ, without the shared IP network being separated in the process. A private LAN network is also connected via the gateway.

The traffic between the gateway's interfaces and, therefore, between the provider gateway, the DMZ and the LAN can then be controlled using firewall rules. An address from the public IP network is required for the gateway.

The **GUI** (Graphical User Interface) is used for configuring.

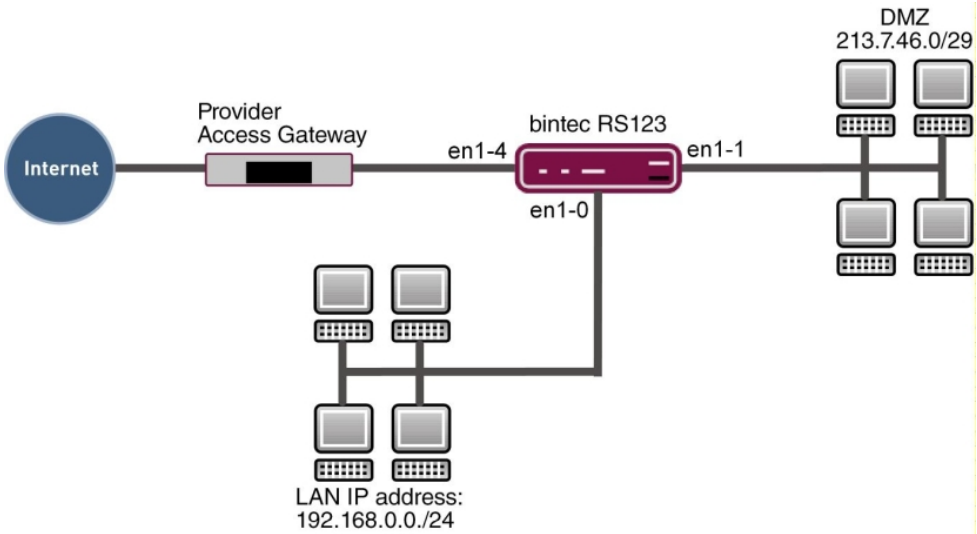


Fig. 117: Example scenario

Requirements

- A **bintec** router, e.g. **bintec RS123**
- Firmware version at least 10.2.5
- The configuration requires a working Internet access with public addresses. For example, **Company Connect** with 8 IP addresses.

13.2 Configuration

In our example, the IP network set up in advance on the gateway is used for the private LAN. Open a web browser and create an http connection to the device.

13.2.1 Configuration of the port

Firstly, you require an additional Ethernet interface. An Ethernet interface is a physical interface for connection to the local network or external networks.

Assign a new Ethernet interface to a switch port.

(1) Go to **Physical Interfaces** ->**Ethernet Ports** -> **Port Configuration**.

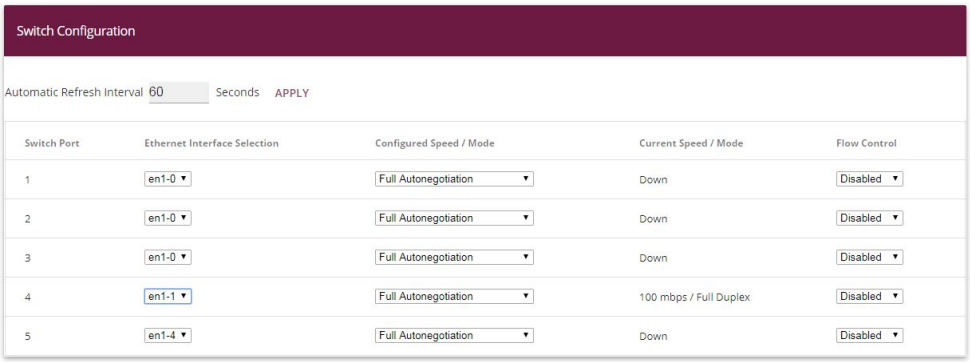


Fig. 118: **Physical Interfaces** -> **Ethernet Ports** -> **Port Configuration**

Proceed as follows to assign the port to the interface:

(1) Under **Ethernet Interface Selection**, select `en1-1` in the dropdown menu for **Switch Port 4**.

(2) Confirm with **OK**.

13.2.2 Configure the Drop-in group

In the next step, a drop-in group is created.

(1) Go to **Network** -> **Drop In** -> **Drop In Groups** -> **New**.

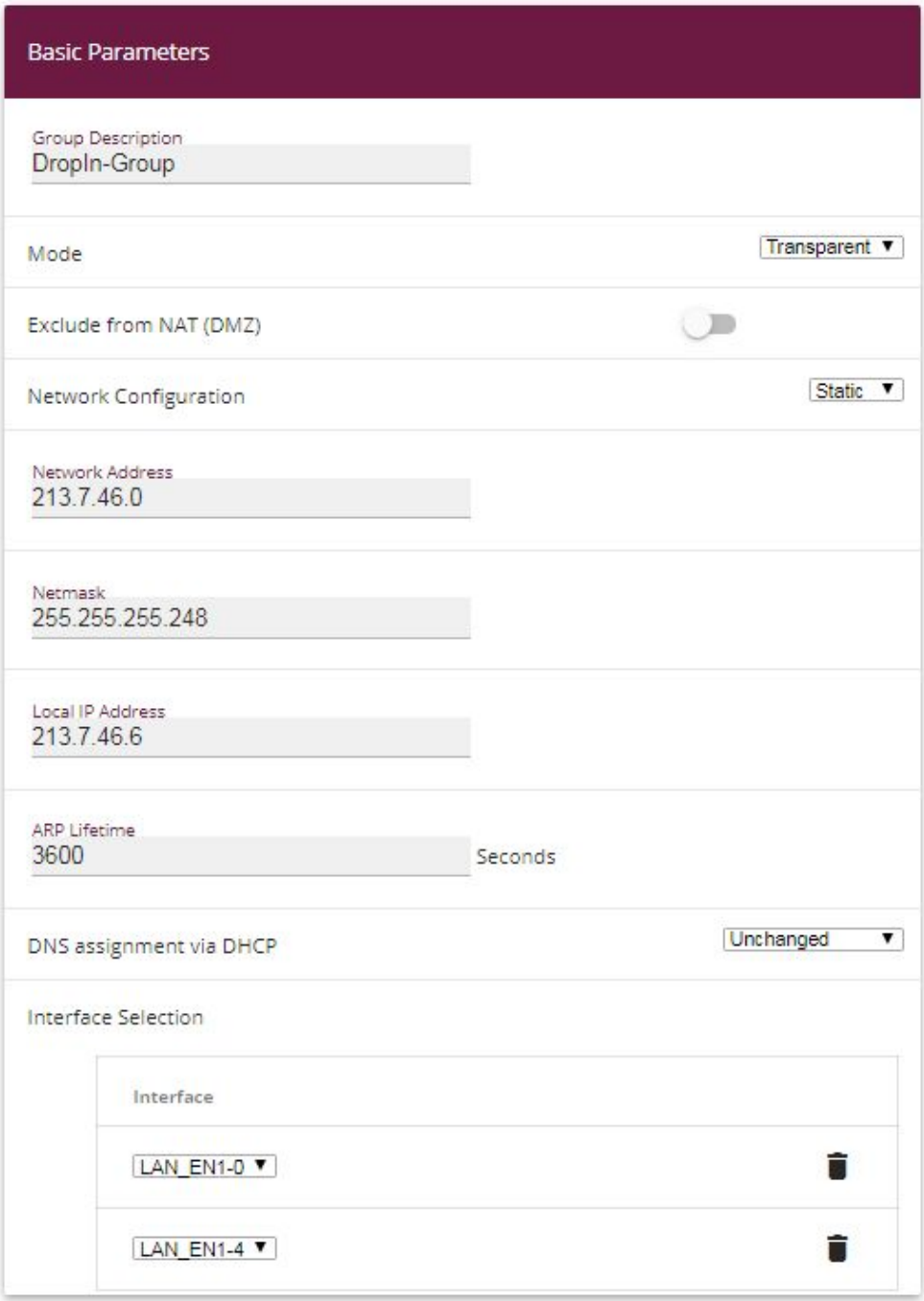


Fig. 119: **Network** -> **Drop In** -> **Drop In Groups** -> **New**

Proceed as follows:

(1) Under **Group Description** enter a unique description for the drop-in group, e. g. *DropIn-Group*.

(2) Under **Mode**, select *Transparent*. ARP packets and IP packets belonging to the drop-in network are routed transparently (unchanged).

(3) Under **Network Configuration**, select how an IP address is assigned to the network components, in this case *Static*.

(4) Enter the **Network Address** of the drop-in network, in this case e. g. *213.7.46.0*.

(5) Enter the relevant **Netmask**, e. g. in this case *255.255.255.248*.

(6) Enter the drop-in group's **Local IP Address**, e. g. *213.7.46.6*.

(7) For **Interface Selection**, select all the ports that are to be included in the drop-in group (in the network), in this case e. g. *LAN_EN1-1* and *LAN_EN1-4*.

(8) Confirm with **OK**.

13.2.3 Set up the default route

Next, a default route will be set up on the gateway. In doing this, you need to select the interface for the drop-in group to which the gateway is later connected.

(1) Go to **Network** -> **Routes** ->**IPv4 Route Configuration** -> **New**.

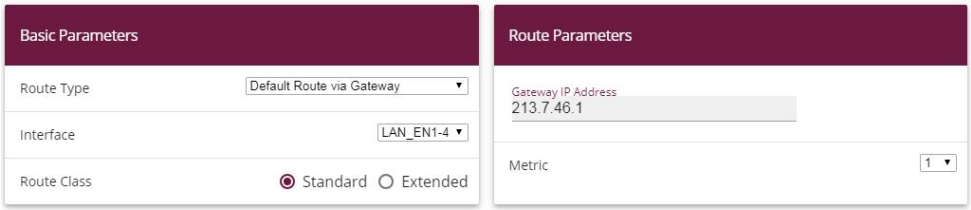


Fig. 120: **Network** -> **Routes** -> **IPv4 Route Configuration** -> **New**

Proceed as follows:

(1) Select *Default Route via Gateway* as the **Route type**.

(2) Select the **Interface** that is to be used for this route, in this case *LAN_EN1-4*.

(3) For **Gateway IP Address**, enter the IP address of the provider gateway, in this case e. g. *213.7.46.1*.

(4) Confirm with **OK**.

13.2.4 Activating Network Address Translation (NAT)

NAT is enabled on the drop-in group interface that is connected to the gateway. Only the traffic from the private LAN will go through the NAT because of the option **Remove from NAT (DMZ)** which was set in the drop-in group configuration.

A list of all IP interfaces is displayed in the NAT interface menu.

Go to the following menu to enable NAT for your interface:

(1) Go to **Network** -> **NAT** ->**NAT Interfaces**.

Fig. 121: **Network** -> **NAT** ->**NAT Interfaces**

Proceed as follows:

(1) Select **NAT active** for the `LAN_EN1-4` interface. This is how the NAT feature is enabled for the interface.

(2) Also select **Silent Deny**. When this function is enabled, attempts to access the LAN from outside are immediately rejected.

(3) Confirm with **OK**.

13.2.5 Firewall configuration

The firewall is now enabled in order to control the traffic between the individual zones (LAN, DMZ and Internet).

When this is done, connections going from the LAN to anywhere, plus connections going from the DMZ to the Internet are generally permitted. By default, other traffic is blocked.

A filter rule is created for each of the services on the servers in the DMZ which are to be accessible from the Internet. In our example, these are a web server and additionally an email server for receiving emails and also provides the option to get emails with pop3 or imap from outside via an encrypted connection.

The firewall's basic setting is to block traffic to all the interfaces. So everything that is not explicitly permitted is prohibited.

In the default setting, the firewall becomes active when the first rule is configured. So it is important that the first rule also permits access to the router itself to configure it.

Configure the alias names for the server's IP addresses

To be able to identify the servers when configuring the filter rules, alias names are created for the web and E-mail servers' IP addresses.

Go to the following menu to create aliases:

(1) Go to **Firewall** -> **Addresses** -> **Address List**-> **New**.

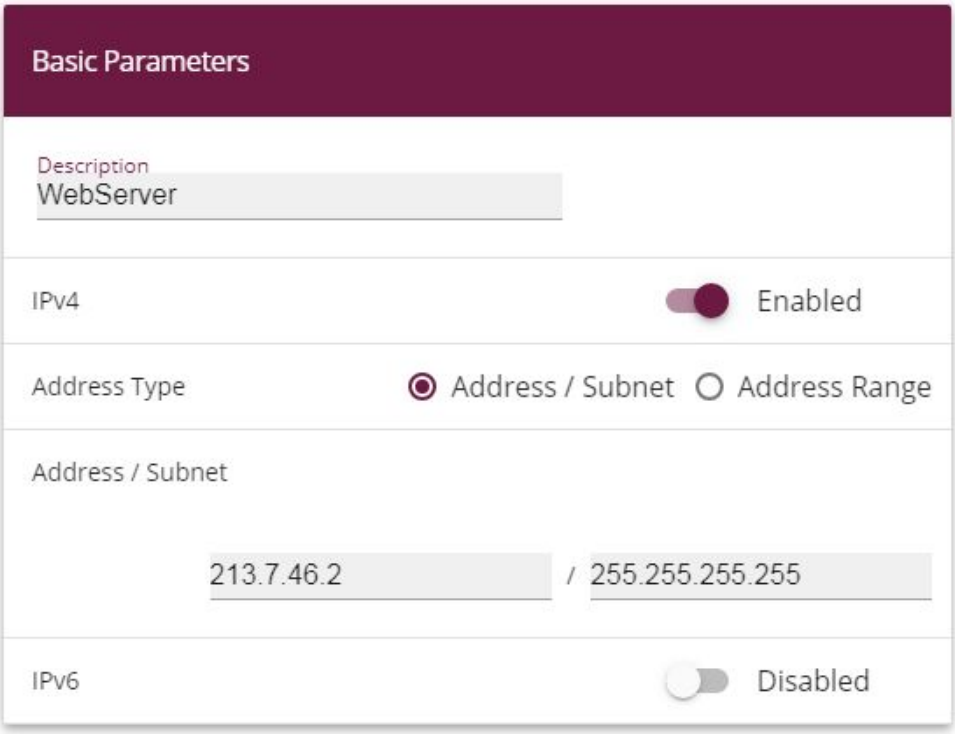


Fig. 122: **Firewall** -> **Addresses** -> **Address List**-> **New**

Proceed as follows:

(1) Enter the name of the alias under **Description**, e. g. `WebServer`.

(2) Under **Address Type** select `Address / Subnet`

(3) Under **Address / Subnet** enter the IP address and corresponding subnet mask, in this case e. g. `213.7.46.2` and `255.255.255.255`.

(4) Confirm with **OK**.

Proceed in the same way to configure the alias name for the E-mail server.

(1) Go to **Firewall** -> **Addresses** -> **Address List**-> **New**.

(2) Enter the name of the alias under **Description**, e. g. *EMailServer*.

(3) Under **Address Type** select *Address / Subnet*

(4) Under **Address / Subnet** enter the IP address and corresponding subnet mask, in this case e. g. *213.7.46.3* and *255.255.255.255*.

(5) Confirm with **OK**.

Configuring service sets

Each of the servers is to provide various services. You can group together several services into groups to make it easier to configure the filter rules.

Go to the following menu to create a group:

(1) Go to **Firewall** -> **Services** -> **Groups**-> **New**.

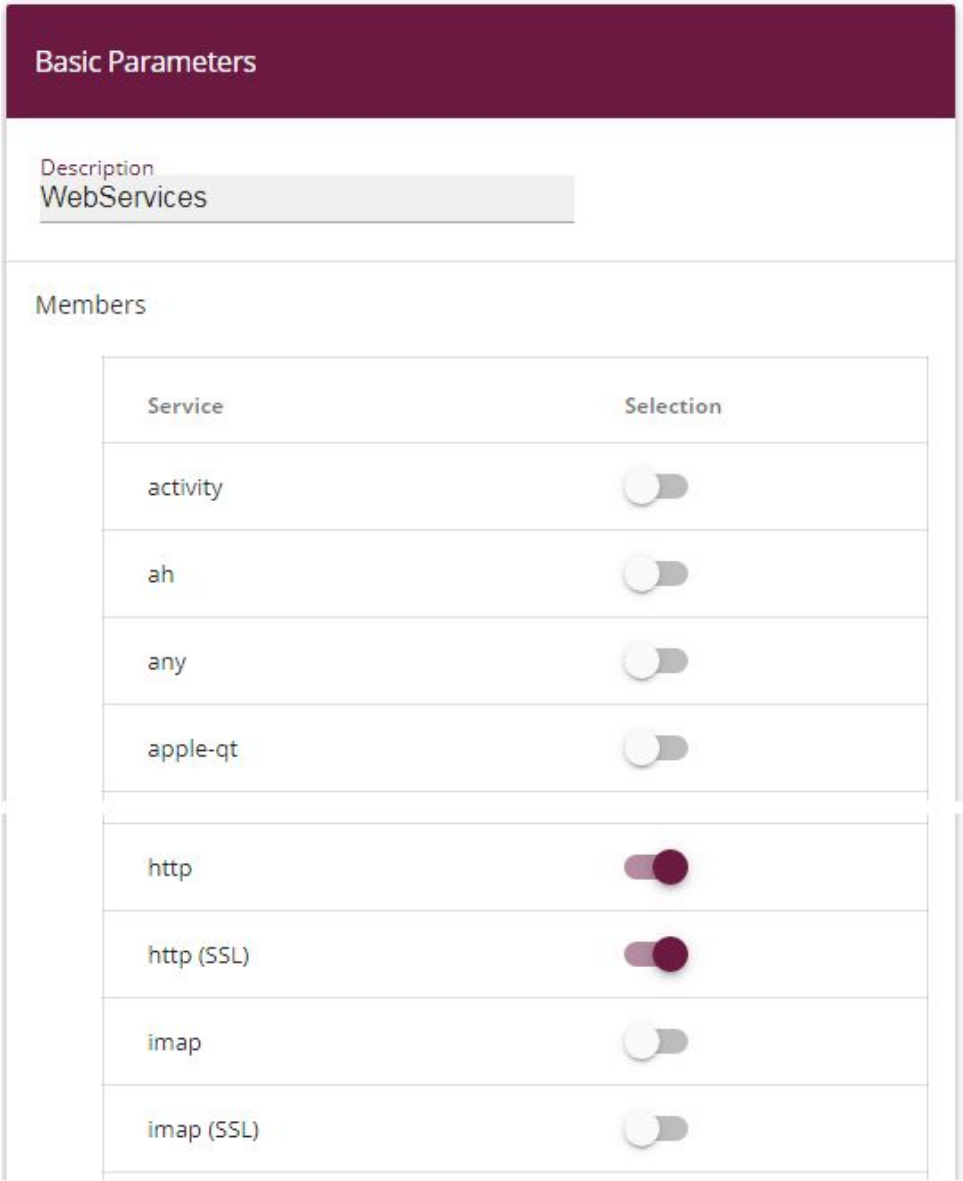


Fig. 123: **Firewall** -> **Services** ->**Groups**-> **New**

Proceed as follows to create a group:

(1) Enter a name for the group under **Description**, e. g. `WebServices`.

(2) Select the services to be included in the group, in this example `http` and `http (SSL)`.

(3) Confirm with **OK**.

Proceed in the same way to configure the service group for the E-mail server.

(1) Go to **Firewall** -> **Services** -> **Groups**-> **New**.

(2) Enter the name of the group under **Description**, e. g. *EmailServices*.

(3) Select the services to be included in the group, in this example *smtp*, *pop3 (SSL)* snd *imap (SSL)*.

(4) Confirm with **OK**.

Configure policies

Note

The correct configuration of the filter rules and the right arrangement in the filter rule chain are decisive factors for the operation of the firewall. An incorrect configuration may possibly prevent further communication with the router!

Once you have completed the configuration of the alias names for IP addresses and services, you can define the filter rules.

Proceed as follows to configure the first rule:

(1) Go to **Firewall** -> **Policies** -> **IPv4 Filter Rules** ->**New**.

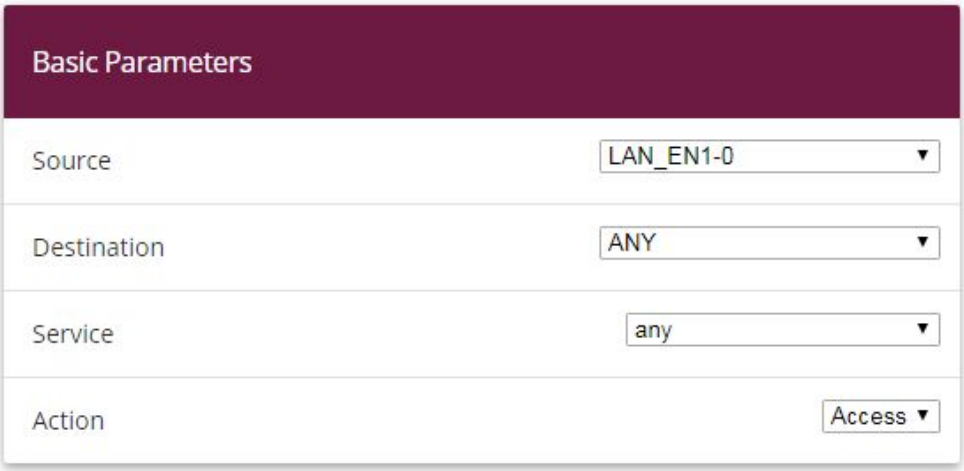


Fig. 124: **Firewall**->**Policies**->**IPv4 Filter Rules**->**New**

Proceed as follows:

(1) Select the packet's **Source**, in this case *LAN_EN1-0*.

(2) Set the **Destination** to *ANY*. Neither the destination interface or the destination ad-

dress will be checked.

(3) For **Service**, select *any*.

(4) Select the **Action** that is to be applied, in this case *Access*. The packets are forwarded on the basis of the entries.

(5) Confirm with **OK**.
With these settings, outgoing connections are allowed from the LAN to the DMZ and to the Internet, including the LAN-side access to the router.

Configure the second filter rule in the same way as you configured the first rule.

(1) Go to **Firewall** -> **Policies** -> **Filter Rules** ->**New**.

(2) Select the packet's **Source**, in this case *LAN_EN1-1*.

(3) As the **Destination**, select *LAN_EN1-4*. Source and destination interface will be checked.

(4) For **Service**, select *any*.

(5) Select the **Action** that is to be applied, in this case *Access*. The packets are forwarded on the basis of the entries.

(6) Confirm with **OK**.
With these settings, outgoing connections are allowed from the DMZ to the Internet.

Now rules can be create for accessing the web server from the Internet.

(1) Go to **Firewall** -> **Policies** -> **Filter Rules** ->**New**.

(2) Select the packet's **Source**, in this case *LAN_EN1-4*.

(3) Set the **Destination** to *WebServer*.

(4) For **Service**, select *WebServices*.

(5) Select the **Action** that is to be applied, in this case *Access*. The packets are forwarded on the basis of the entries.

(6) Confirm with **OK**.

Finally, the rules are created for accessing the E-mail server from the Internet.

(1) Go to **Firewall** -> **Policies** -> **Filter Rules** ->**New**.

(2) Select the packet's **Source**, in this case *LAN_EN1-4*.

(3) Set the **Destination** to *EmailServer*.

(4) For **Services**, select *EmailServices*.

(5) Select the **Action** that is to be applied, in this case *Access*. The packets are forwarded on the basis of the entries.

(6) Confirm with **OK**.

The list of the filter rules that have been configured should now look like this:

Go to **Firewall** -> **Policies** -> **Filter Rules**.

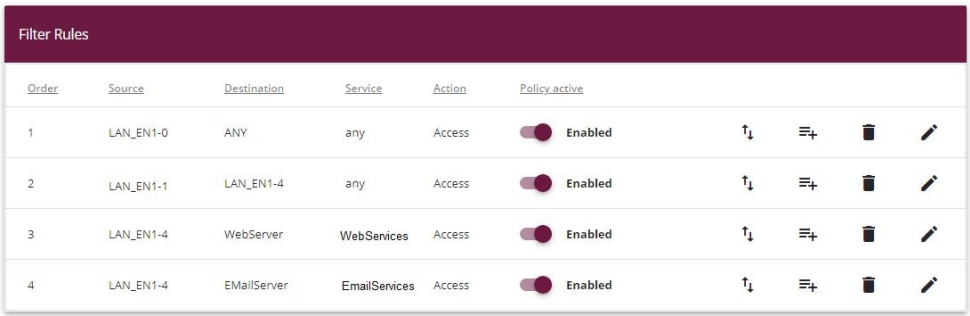


Fig. 125: **Firewall** -> **Policies** -> **Filter Rules**

This completes the configuration. Save the configuration with **Save configuration** and confirm the selection with **OK**.

13.3 Overview of Configuration Steps

Assign interface

Field	Menu	Value
Switch Port 4	**Physical Interfaces** ->**Ethernet Ports** ->**Port Configuration**	*en1-1*

Configure a drop-in group

Field	Menu	Value
Group Description	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *DropIn-Group*.
Mode	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	*Transparent*
Network Configuration	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	*Static*
Network Address	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *213.7.46.0*
Netmask	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *255.255.255.248*
Local IP Address	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e.g. *213.7.46.6*
Interface Selection	**Network** -> **Drop In** -> **Drop In Groups** -> **New**	e. g. *LAN_EN1-4*, *LAN_EN1-1*

Set up the default route

Field	Menu	Value
Route Type	**Network -> Routes -> IPv4 Route Configuration-> New**	*Default Route via Gateway*
Interface	**Network -> Routes -> IPv4 Route Configuration-> New**	*LAN_EN1-4*
Gateway IP Address	**Network -> Routes -> IPv4 Route Configuration-> New**	e. g. *213.7.46.1*

Enable NAT

Field	Menu	Value
NAT active	**Network -> NAT ->NAT Interfaces**	*Enabled* for **LAN_EN1-4**
Silent Deny	**Network -> NAT ->NAT Interfaces**	*Enabled* for **LAN_EN1-4**

Configure the alias names

Field	Menu	Value
Description	**Firewall ->Addresses -> Address List ->New**	*WebServer*
Address Type	**Firewall ->Addresses -> Address List ->New**	*Address / Subnet*
Address / Subnet	**Firewall-> Addresses -> Address List-> New**	e. g. *213.7.46.2/ 255.255.255.255*
Description	**Firewall ->Addresses -> Address List ->New**	*EMailServer*
Address Type	**Firewall A->ddresses -> Address List ->New**	*Address / Subnet*
Address / Subnet	**Firewall ->Addresses -> Address List ->New**	e. g. *213.7.46.3/ 255.255.255.255*

Configuring service sets

Field	Menu	Value
Description	**Firewall -> Services -> Groups -> New**	e. g. *WebServices*.
Members	**Firewall -> Services -> Groups -> New**	*http*, *http (SSL)*
Description	**Firewall -> Services -> Groups -> New**	e. g. *EmailServices*.

Field	Menu	Value
Members	**Firewall** -> **Services** -> **Groups** -> **New**	*smtp*, *pop3 (SSL)*, *imap (SSL)*

Configure policies

Field	Menu	Value
Source	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*LAN_EN1-0*
Destination	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*ANY*
Service	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*any*
Action	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*Access*
Source	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*LAN_EN1-1*
Destination	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*LAN_EN1-4*
Service	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*any*
Action	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*Access*
Source	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*LAN_EN1-4*
Destination	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*WebServer*
Service	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*WebServices*
Action	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*Access*
Source	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*LAN_EN1-4*
Destination	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*EMailServer*
Service	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*EmailServices*
Action	**Firewall** ->**Policies** ->**Filter Rules** ->**New**	*Access*