Manual
Workshops (Excerpt)

Security and Administration Workshops

Copyright© Version 08/2020 bintec elmeg GmbH

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.

Copyright © bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH

bintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbHbintec elmeg GmbH reserves all rights to the data included – especially for duplication and disclosure.

Table of Contents

Chapter 1 Security - IPSec with certificates

1.1 Introduction

The following chapter describes how to configure an IPSec tunnel with dynamic IP addresses on both sides.

You use certificates instead of preshared keys for authentication. You also configure an entry for your DynDNS name in the gateway.

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

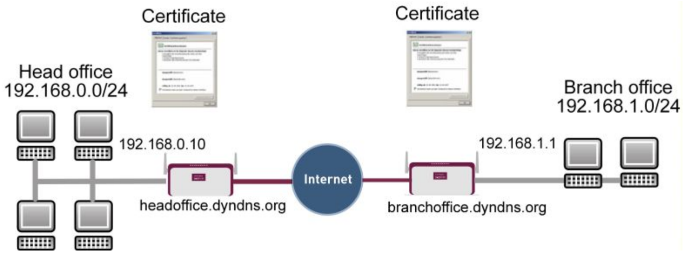


Fig. 1: Example scenario IPSec with certificates

Requirements

The following are required for the configuration:

- Basic configuration of the gateway, e.g. **bintec be.IP plus**
- A boot image version 10.1.1 must be used for the IPSec gateway
- Configuration requires working Internet access to the provider
- You must have registered a DynDNS name, e.g. *`headoffice.dyndns.org`* and *`branchoffice.dyndns.org`* for both gateways.
- You need a certification authority (CA) from which you can request certificates. Find out from your chosen certification authority what information is required to request certificates and the methods for sending the request.

1.2 Configuration

In our example, the configuration is described on the head office side.

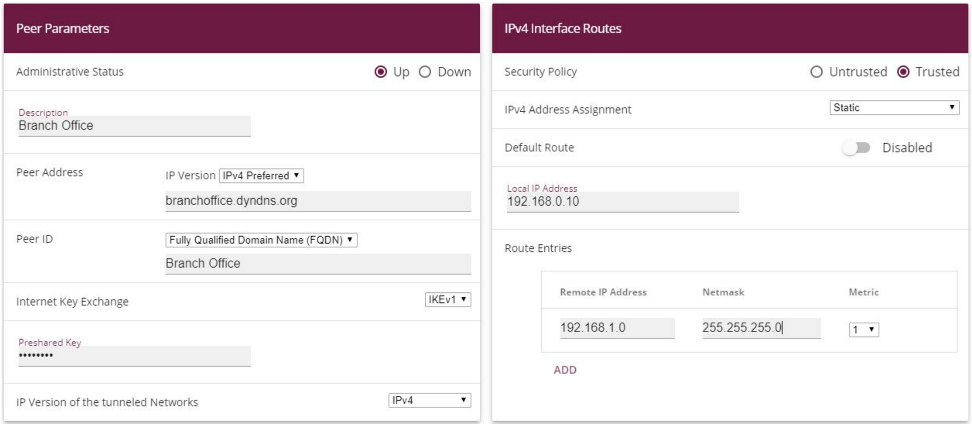
Note

Since the certificate implementation process is extremely complex, we first recommend configuring a functioning IPSec tunnel, e.g. with dynamic IP addresses, and then extending and changing this with certificates.

1.2.1 Creating an IPSec peer

The **IPSec Peers** submenu offers you the **New** option for adding connection partners for IPSec.

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



Peer Parameters

Administrative Status ● Up ○ Down

Description: Branch Office

Peer Address: IP Version: IPv4 Preferred, branchoffice.dyndns.org

Peer ID: Fully Qualified Domain Name (FQDN), Branch Office

Internet Key Exchange: IKEv1

Preshared Key: ••••••••

IP Version of the tunneled Networks: IPv4

IPv4 Interface Routes

Security Policy ○ Untrusted ● Trusted

IPv4 Address Assignment: Static

Default Route: Disabled

Local IP Address: 192.168.0.10

Route Entries

Remote IP Address	Netmask	Metric
192.168.1.0	255.255.255.0	1

ADD

Fig. 2: **VPN** -> **IPSec** ->**IPSec Peers**-> **New**

Proceed as follows to make the settings in the IPSec peer:

(1) Enter a **Description** for the connection, e.g. `Branch Office`.

(2) Enter the gateway IP address or DynDNS name of the connection partner, e.g. `branchoffice.dyndns.org` under **Peer Address**.

(3) Under **Peer ID** leave `Fully Qualified Domain Name (FQDN)` and enter `Branch Office`.

(4) Enter `bintec` as the shared password for the connection in **Preshared Key**.

(5) Deselect the **Default Route** option.

(6) Under **Local IP Address** enter `192.168.0.10`.

(7) Under **Route Entries** click **Add** to add a new entry.

(8) Under **Remote IP Address** enter the partner network to be reached, e.g. `192.168.1.0` and under **Netmask** enter `255.255.255.0`

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

Note

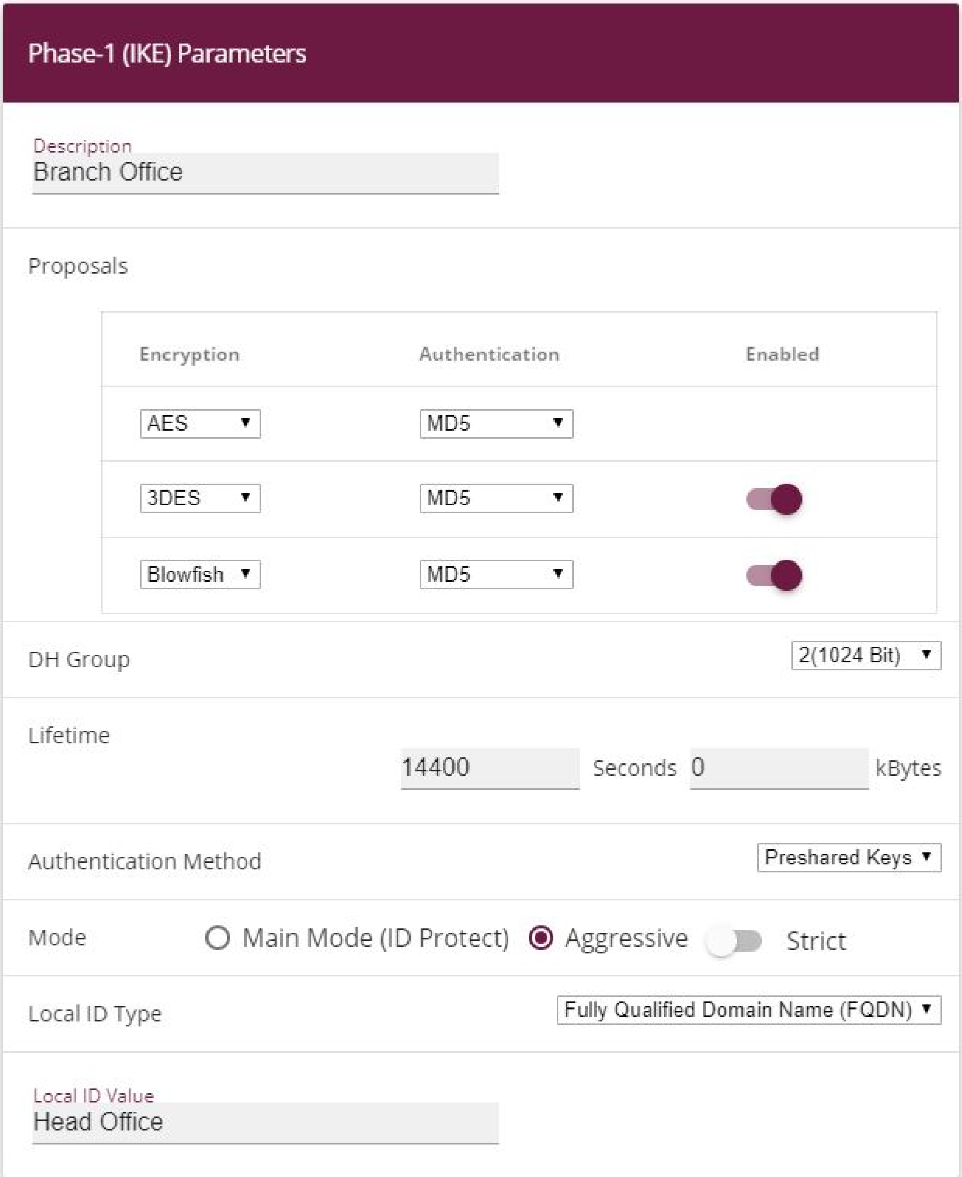
As you will use the certificates for your connection later, the complexity of the pre-shared keys is not important for this temporary connection.

Creating an IPSec peer automatically generates standard profiles for phase 1 and phase 2, which are changed in the following section to suit the requirements of this scenario.

1.2.2 Changing the Phase-1 Profiles

Go to the following menu to change the profile for phase-1:

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



Phase-1 (IKE) Parameters

Description
Branch Office

Proposals

Encryption	Authentication	Enabled
AES ▾	MD5 ▾	
3DES ▾	MD5 ▾	●
Blowfish ▾	MD5 ▾	●

DH Group 2(1024 Bit) ▾

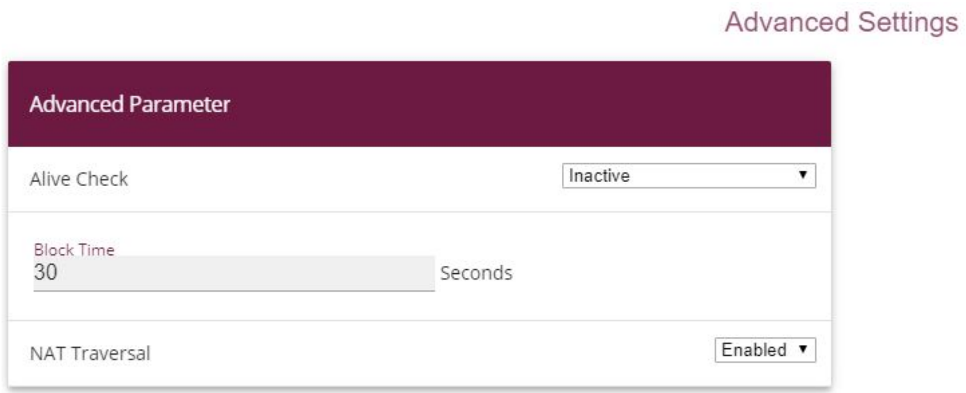
Lifetime 14400 Seconds 0 kBytes

Authentication Method Preshared Keys ▾

Mode ○ Main Mode (ID Protect) ● Aggressive ○ Strict

Local ID Type Fully Qualified Domain Name (FQDN) ▾

Local ID Value
Head Office



Advanced Settings

Advanced Parameter

Alive Check: Inactive

Block Time: 30 Seconds

NAT Traversal: Enabled

Fig. 4: **VPN** -> **IPSec** -> **Phase-1 Profiles**-> **<Multi-Proposal>** -> ✎

Configure the phase-1 profile with the following parameters:

(1) Under **Description** define a name for the profile, e.g. `Branch Office`.

(2) Under **Proposal Encryption** select `AES`, under **Authentication** select `MD5`.
Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.

(3) Set **Mode** to `Aggressive`, as you are using dynamic IP addresses.

(4) Under **Local ID Type** choose `Fully Qualified Domain Name (FQDN)`.

(5) Under **Local ID Value** enter the local ID of the gateway, e.g. `Head Office` (set under Peer ID for the Partner).

(6) Click **Advanced Settings**.

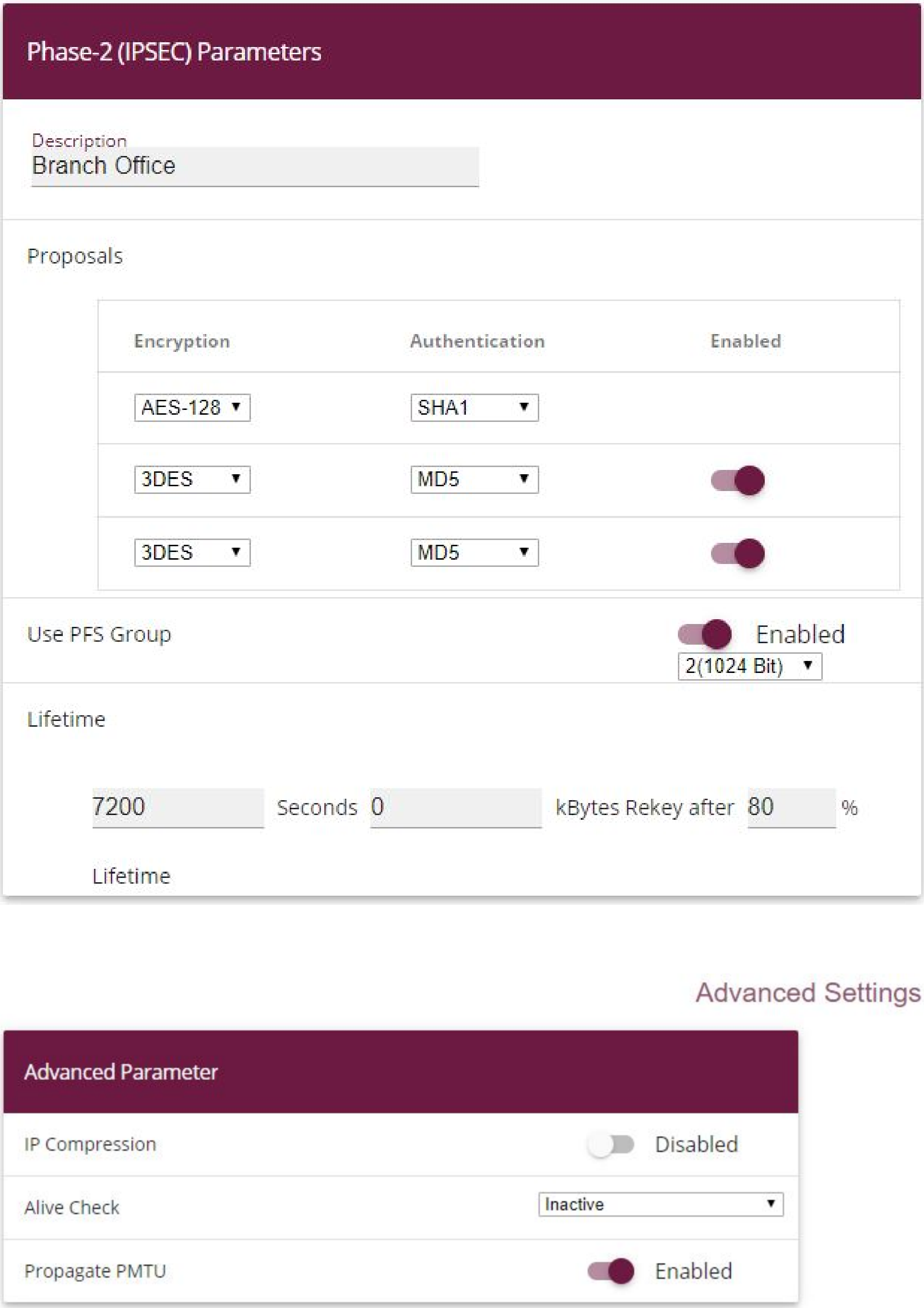
(7) Under **Alive check** select `Inactive`.

(8) Confirm with **OK**.

1.2.3 Changing the Phase-2 Profiles

Go to the following menu to change the profile for phase-2:

(1) Go to **VPN** -> **IPSec** -> **Phase-2 Profiles**-> **<Multi-Proposal>** -> ✎.



Phase-2 (IPSEC) Parameters

Description: Branch Office

Proposals

Encryption	Authentication	Enabled
AES-128	SHA1	
3DES	MD5	●
3DES	MD5	●

Use PFS Group: Enabled, 2(1024 Bit)

Lifetime

7200 Seconds 0 kBytes Rekey after 80 %

Lifetime

Advanced Settings

Advanced Parameter

IP Compression	Disabled
Alive Check	Inactive
Propagate PMTU	Enabled

Fig. 6: **VPN** -> **IPSec** -> **Phase-2 Profiles**-> **<Multi-Proposal>** -> ✎

Configure the phase-2 profile with the following parameters:

(1) Under **Description** define a name for the profile, e.g. *Branch Office*.

(2) Under **Proposal Encryption** select *AES-128*, under **Authentication** select *MD5*. Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.

(3) Click **Advanced Settings**.

(4) Set **Alive Check** to *Inactive*.

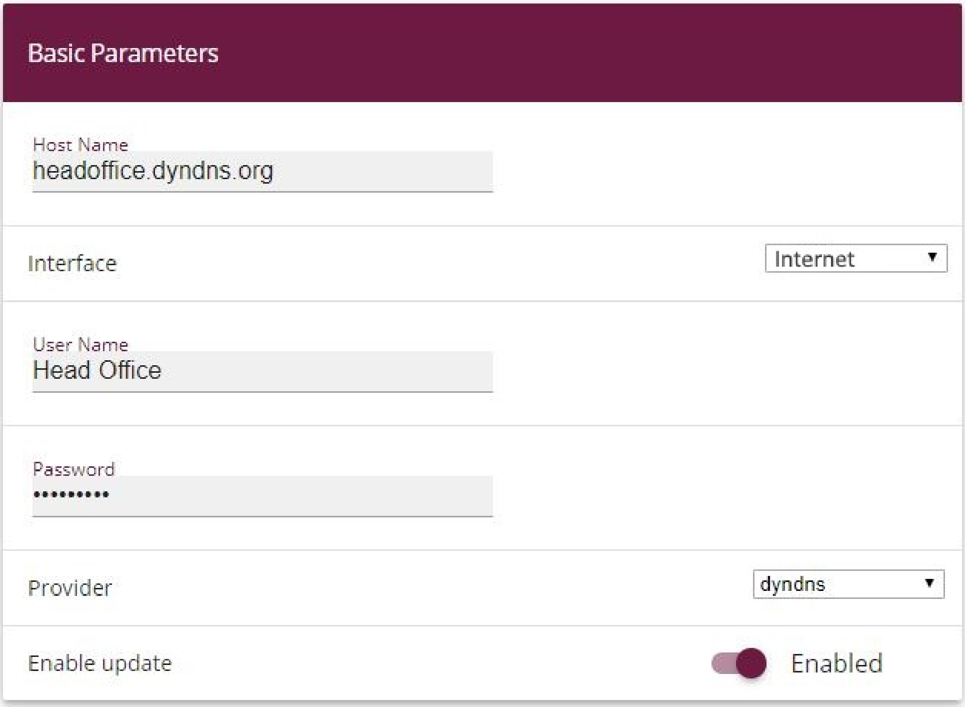
(5) Confirm with **OK**.

1.2.4 Configuring DynDNS

Create an entry in the gateway for your registered DynDNS name, e.g. *headoffice.dyndns.org*.

For this, go to the following menu:

(1) Go to **Local Services** -> **DynDNS Client** ->**DynDNS Update**-> **New**.



Basic Parameters

Host Name: headoffice.dyndns.org

Interface: Internet

User Name: Head Office

Password: •••••••••

Provider: dyndns

Enable update: Enabled

Fig. 7: **Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**

Proceed as follows:

(1) Under **Host Name** enter the complete host name you have registered, e. g. *headoffice.dyndns.org*.

(2) Select **Interface**, e.g. *Internet*.

(3) Under **User Name** enter *Head Office* for example.

(4) Under **Password** enter *password* for example.

(5) Leave **Provider** set to *dyndns*.

(6) Activate **Enable Update**.

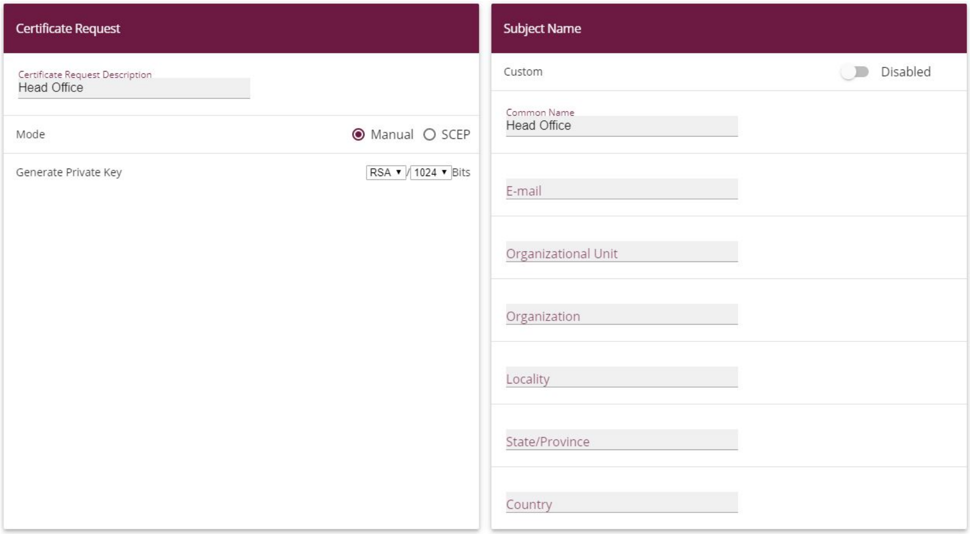
(7) Confirm with **OK**.

Once you have configured the IPSec tunnel and the DynDNS entry, you should carry out a connection test. If successful, now change the authentication parameters as follows: A certificate is requested and imported.

1.2.5 Requesting and importing certificates

Go to the following menu to configure a certificate request:

(1) Go to **System Management** -> **Certificates** -> **Certificate List** ->**Request**.



Certificate Request

Certificate Request Description: Head Office

Mode: ● Manual ○ SCEP

Generate Private Key: RSA / 1024 Bits

Subject Name

Custom: Disabled

Common Name: Head Office

E-mail

Organizational Unit

Organization

Locality

State/Province

Country

Fig. 8: **System Management** -> **Certificates** -> **Certificate List** -> **Request**

Note

Under Subject Name you can specify several identifiers for the head office according to the X.500 standard. For the sake of simplicity, we have only used one characteristic here.

Observe the requirements of your certification authority as necessary.

Proceed as follows:

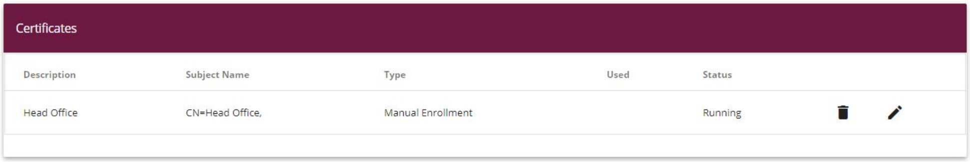
(1) Under **Certificate Request Description** enter `Head Office` for example.

(2) Leave **Mode** set to `Manual`.

(3) Under **Common Name** enter the ID of the head office, e.g. `Head Office` .

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

(1) Go to **System Management** -> **Certificates** -> **Certificate List**.



Certificates

Description	Subject Name	Type	Used	Status		
Head Office	CN=Head Office,	Manual Enrollment		Running	🗑	✎

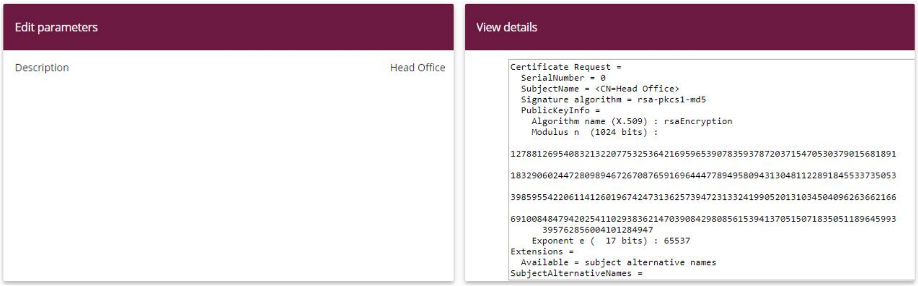
Fig. 9: **System Management** -> **Certificates** -> **Certificate List**

In the background the IPSec gateway generates the private and public keys.

Now proceed as follows:

(1) A dialogue box should now appear asking you to save the certificate requests to your computer with the name `Headoffice.req`. Alternatively, you can save the file by clicking the right green arrow ^ .

(2) Now you must request a certificate from your certification authority using the certificate request. Follow the instructions from your certification authority.
The request appears as follows:



Edit parameters

Description Head Office

View details

```
Certificate Request =
  SerialNumber = 0
  SubjectName = <CN=Head Office>
  Signature algorithm = rsa-pkcs1-md5
  PublicKeyInfo =
    Algorithm name (X.509) : rsaEncryption
    Modulus n  (1024 bits) :

1278812695408321322077532536421695965390783593787203715470530379015681891

1832906024472809894672670876591696444778949580943130481122891845533735053

3985955422061141260196742473136257394723133241990520131034504096263662166

6910084847942025411029383621470390842980856153941370515071835051189645993
      395762856004101284947
    Exponent e (  17 bits) : 65537
Extensions =
  Available = subject alternative names
SubjectAlternativeNames =
```

Fig. 10: **System Management** -> **Certificates** -> **Certificate List**

(3) You must now copy the certificate issued by the certification authority to your computer.

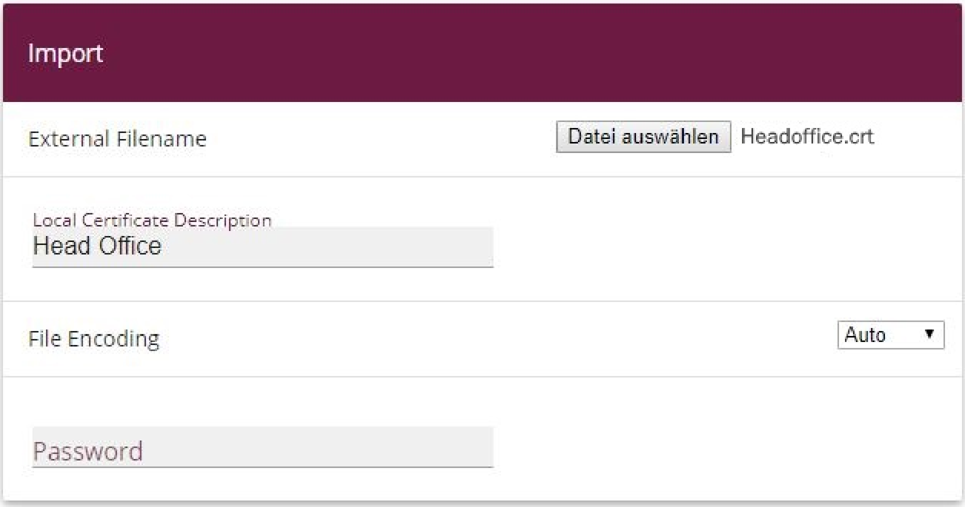
(4) Name the certificate *headoffice.crt*.

(5) You still need the certificate of the certification authority that issued the certificate. Copy this to your computer as well.

(6) Name the certificate from the certification authority *Ca.crt*.

Now go the following menu to import your own certificate and the certificate issued by the certification authority into the IPSec gateway:

(1) Go to **System Management** -> **Certificates** -> **Certificate List** -> **Import**.



Import

External Filename Datei auswählen Headoffice.crt

Local Certificate Description: Head Office

File Encoding: Auto ▼

Password

Fig. 11: **System Management** -> **Certificates** -> **Certificate List** -> **Import**

Proceed as follows to import your own certificate:

(1) Under **External Filename** select the file, e.g. *C:\Headoffice.crt* via the **browse**button.

(2) Under **Local Certificate Description** enter `Head Office` for example.

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

Proceed as follows to import the certificate issued by the certification authority:

(1) Under **External Filename** select the file, e.g. `C:\Ca.crt` via the **browse**button.

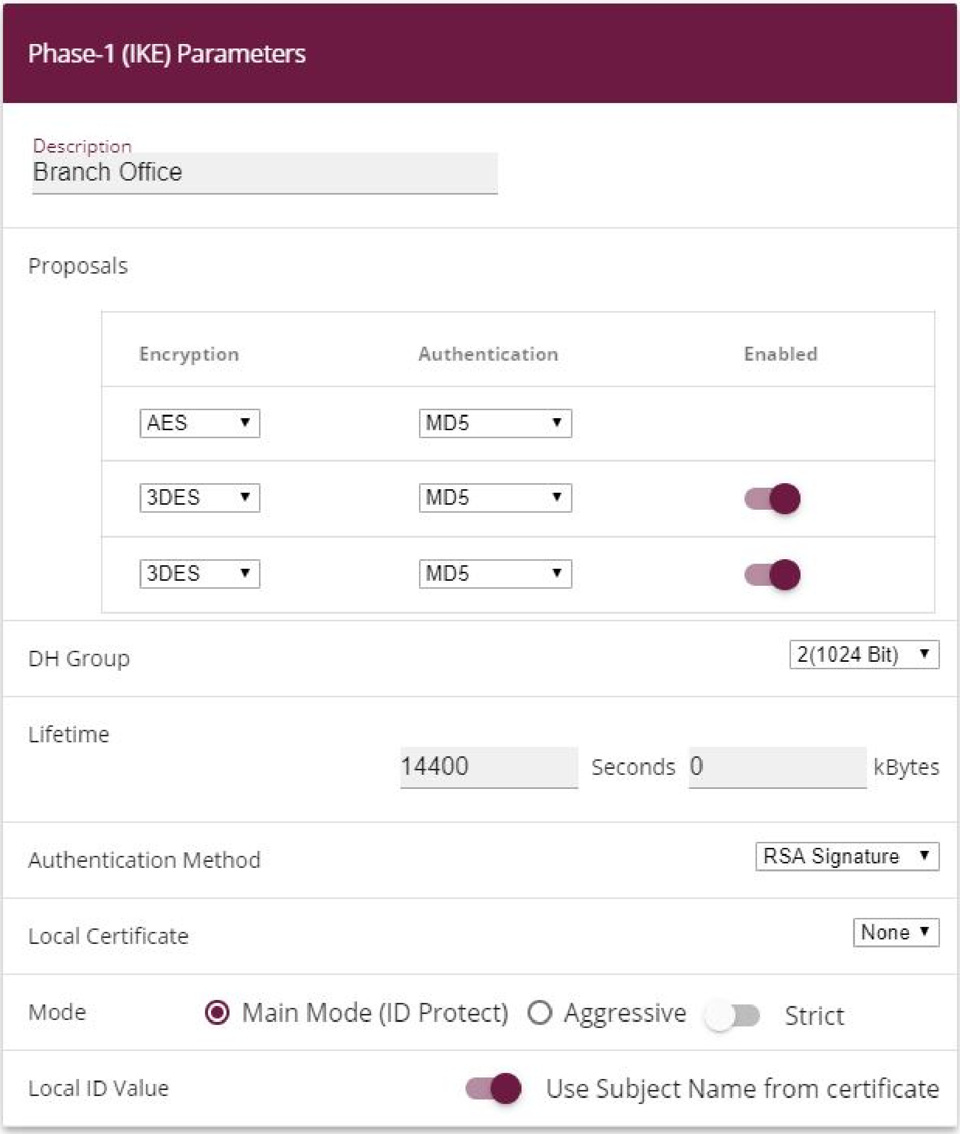
(2) Under **Local Certificate Description** enter `CA` for example.

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

1.2.6 Changing the IPSec tunnel

Before you can use the imported certificates you must make changes in the following menu:

(1) Go to **VPN** -> **IPSec** -> **Phase-1 Profiles**-> **<Branch Office>** -> ✎.



Phase-1 (IKE) Parameters

Description: Branch Office

Proposals

Encryption	Authentication	Enabled
AES ▼	MD5 ▼	
3DES ▼	MD5 ▼	●
3DES ▼	MD5 ▼	●

DH Group: 2(1024 Bit) ▼

Lifetime: 14400 Seconds 0 kBytes

Authentication Method: RSA Signature ▼

Local Certificate: None ▼

Mode: ● Main Mode (ID Protect) ○ Aggressive ○ Strict

Local ID Value: ● Use Subject Name from certificate

Fig. 12: **VPN** -> **IPSec** ->**Phase-1 Profiles** -> **<Branch Office>**-> ✎

Proceed as follows to change the entry:

(1) Set **Authentication Method** to `RSA Signature`.

(2) Set **Local Certificate** to your own certificate `Head Office`.

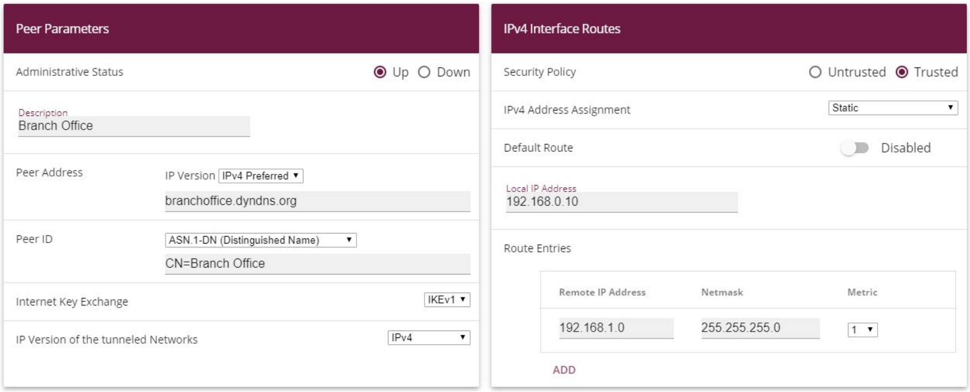
(3) Set **Mode** to `Main Mode (ID Protect)`.

(4) Under **Local ID Value** select `Use Subjectname from Certificate`.

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

Another menu requires changes to use certificates:

(1) Go to **VPN** -> **IPSec** -> **IPSec Peers**-> **<Branch Office>**-> ✎.



Peer Parameters

Administrative Status ● Up ○ Down

Description: Branch Office

Peer Address: IP Version IPv4 Preferred ▾ branchoffice.dyndns.org

Peer ID: ASN.1-DN (Distinguished Name) ▾ CN=Branch Office

Internet Key Exchange: IKEv1 ▾

IP Version of the tunneled Networks: IPv4 ▾

IPv4 Interface Routes

Security Policy ○ Untrusted ● Trusted

IPv4 Address Assignment: Static ▾

Default Route: Disabled

Local IP Address: 192.168.0.10

Route Entries

Remote IP Address	Netmask	Metric
192.168.1.0	255.255.255.0	1 ▾

ADD

Fig. 13: **VPN** -> **IPSec** ->**IPSec Peers**-> **<Branch Office>**-> ✎

Proceed as follows to change the entry:

(1) Under **Peer ID** enter the partner ID here (entered in the branch office under **Local ID**) *`ASN.1 Distinguished Name`*, for example, and enter *`CN=Branch Office`*.

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

1.3 Result

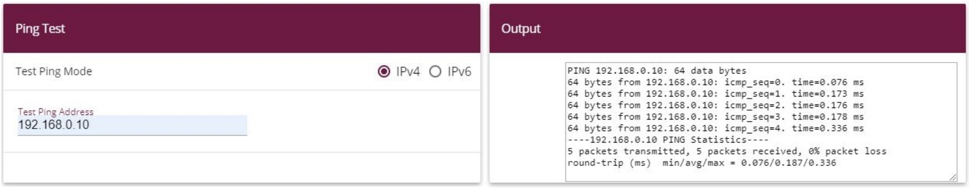
You have configured an IPSec tunnel with certificates between two gateways, using dynamic IP addresses in combination with DynDNS. As the instructions only show the example on the head office side, you must also configure the connection parameters on the branch office side.

1.4 Checking the connection

Go to the following menu to test the IPSec tunnel:

(1) Go to **Maintenance** -> **Diagnostics** ->**Ping Test**.

Once you have entered an IP address for the remote location under **Test Ping Address** and have pressed the **Go** button, you should see a similar message:



Ping Test

Test Ping Mode ● IPv4 ○ IPv6

Test Ping Address: 192.168.0.10

Output

```
PING 192.168.0.10: 64 data bytes
64 bytes from 192.168.0.10: icmp_seq=0. time=0.076 ms
64 bytes from 192.168.0.10: icmp_seq=1. time=0.173 ms
64 bytes from 192.168.0.10: icmp_seq=2. time=0.176 ms
64 bytes from 192.168.0.10: icmp_seq=3. time=0.178 ms
64 bytes from 192.168.0.10: icmp_seq=4. time=0.336 ms
----192.168.0.10 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0.076/0.187/0.336
```

Fig. 14: **Maintenance** -> **Diagnosis** ->**Ping Test**

Note

If the connection cannot be correctly established, this may be due to the local date or the local time settings of the gateway. Check the current date to ensure that the certificates are valid.

1.5 Overview of configuration steps

Creating an IPSec peer

Field	Menu	Value
Description	**VPN** -> **IPSec** ->**IPSec Peers**-> **New**	e.g. `Branch Office`
Peer Address	**VPN** -> **IPSec** ->**IPSec Peers**-> **New**	`branchoffice.dyndns.org`
Peer ID	**VPN** -> **IPSec** ->**IPSec Peers**-> **New**	`Fully Qualified Domain Name (FQDN)` and `Branch Office`
Preshared Key	**VPN** -> **IPSec** ->**IPSec Peers**-> **New**	e.g. `bintec`
Default Route	**VPN** -> **IPSec** ->**IPSec Peers**-> **New**	`Disabled`
Local IP Address	**VPN** -> **IPSec** ->**IPSec Peers**-> **New**	e.g. `192.168.0.10`
Route Entries	**VPN** -> **IPSec** ->**IPSec Peers**-> **New**	for **IP Address** `192.168.1.0` and for **Netmask** `255.255.255.0`

Changing the Phase-1 profile

Field	Menu	Value
Description	**VPN** -> **IPSec** -> **Phase-1**	e.g. `Branch Office`

Field	Menu	Value
	Profiles-> **<Multi-Proposal>** ->✎	
Proposals	**VPN** -> **IPSec** -> **Phase-1 Profiles** -> **<Multi-Proposal>** ->✎	*AES/MD5*
Mode	**VPN** -> **IPSec** -> **Phase-1 Profiles** -> **<Multi-Proposal>** ->✎	*Aggressive*
Local ID Type	**VPN** -> **IPSec** -> **Phase-1 Profiles** -> **<Multi-Proposal>** ->✎	*Fully Qualified Domain Name (FQDN)*
Local ID Value	**VPN** -> **IPSec** -> **Phase-1 Profiles** -> **<Multi-Proposal>** ->✎	*Head Office*
Alive Check	**VPN** -> **IPSec** -> **Phase-1 Profiles** -> **<Multi-Proposal>** ->✎-> **Advanced Settings**	*Inactive*

Changing the Phase-2 profile

Field	Menu	Value
Description	**VPN** -> **IPSec** -> **Phase-2 Profiles** -> **<Multi-Proposal>** ->✎	e.g. *Branch Office*
Proposal	**VPN** -> **IPSec** -> **Phase-2 Profiles** -> **<Multi-Proposal>** ->✎	*AES-128/MD5*
Alive Check	**VPN** -> **IPSec** -> **Phase-2 Profiles** -> **<Multi-Proposal>** ->✎-> **Advanced Settings**	*Inactive*

DynDNS

Field	Menu	Value
Hostname	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e. g. *headoffice.dyndns.org*
Interface	**Local Services** -> **DynDNS**	e.g. *Internet*

Field	Menu	Value
	Client -> **DynDNS Update** -> **New**	
User Name	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *Head Office*
Password	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *password*
Provider	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	*dyndns*
Enable update	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	Enabled

Requesting and importing certificates

Field	Menu	Value
Certificate Request Description	**System Management** -> **Certificates** -> **Request**	e.g. *Head Office*
Mode	**System Management**-> **Certificates** -> **Request**	*Manual*
Common Name	**System Management** -> **Certificates** -> **Request**	e.g. *Head Office*
External Filename	**System Management** -> **Certificates** -> **Import**	e.g. *C:\Headoffice.crt*
Local Certificate Description	**System Management** -> **Certificates** -> **Import**	e.g. *Head Office*
External Filename	**System Management** -> **Certificates** -> **Import**	e.g. *C:\Ca.crt*
Local Certificate Description	**System Management** -> **Certificates** -> **Import**	e.g. *CA*

Changing the IPSec tunnel

Field	Menu	Value
Authentication Method	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **<Branch Office>**->✎	*RSA Signature*
Local Certificate	**VPN** -> **IPSec** ->**Phase-1**	*Head Office*

Field	Menu	Value
	Profiles -> **<Branch Office>**->✎	
Mode	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **<Branch Office>**->✎	*Main Mode (ID Protect)*
Local ID Value	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **<Branch Office>**->✎	*Use Subjectname from Certificate*

Modifying IPSec Peers

Field	Menu	Value
Peer ID	**VPN** -> **IPSec** ->**IPSec Peers**-> **<Branch Office>**-> ✎	*ASN.1-DN (Distinguished Name)* and *CN=Branch Office*

Ping Test

Field	Menu	Value
Test Ping Address	**Maintenance** -> **Diagnosis** ->**Ping Test**	*192.168.0.10*

Chapter 2 Security - IPSec with dynamic IP addresses and DynDNS

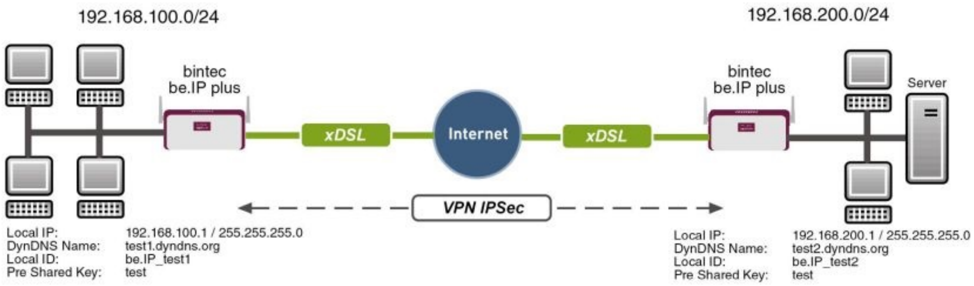
2.1 Introduction

This chapter describes IPSec configuration of bintec routers (here **bintec be.IP plus**), to provide a secure IPSec connection between two networks.

The use of dynamic IP addresses has the disadvantage that a host in the network can no longer be found once its IP address has changed. DynDNS ensures that your device can still be reached after a change to the IP address.

Preshared keys are used for authentication.

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



Local IP: 192.168.100.1 / 255.255.255.0
DynDNS Name: test1.dyndns.org
Local ID: be.IP_test1
Pre Shared Key: test

Local IP: 192.168.200.1 / 255.255.255.0
DynDNS Name: test2.dyndns.org
Local ID: be.IP_test2
Pre Shared Key: test

Fig. 15: Example scenario

Requirements

The following are required for the configuration:

- Two **bintec be.IP plus** from system software 10.1.1
- Both routers have an existing connection to the Internet provider
- In our example, both routers are connected to the Internet of via A-DLS flatrate
- Both routers are dynamically assigned an official IP address, and have configured a DynDNS account.

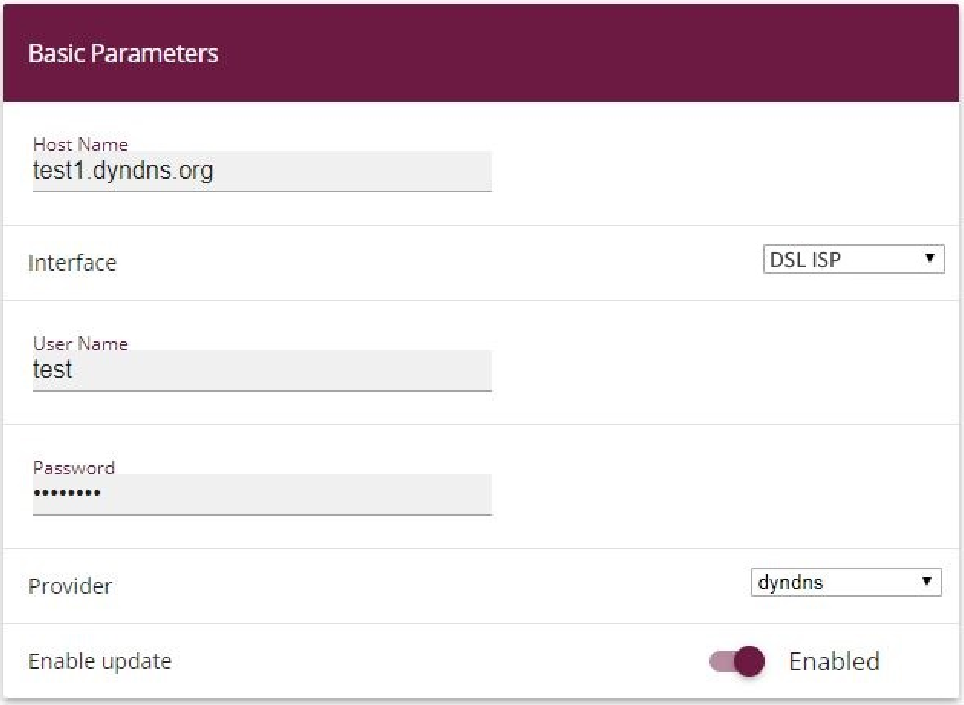
2.2 Configuration

2.2.1 Configuration on the first router (Location A)

Set up DynDNS account

A list of all configured DynDNS registrations is displayed in the DynDNS Update menu. Select the **New** button to perform additional DynDNS registrations.

(1) Go to **Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**.



Basic Parameters

Host Name
test1.dyndns.org

Interface: DSL ISP ▾

User Name
test

Password
••••••••

Provider: dyndns ▾

Enable update: Enabled

Fig. 16: **Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**

Proceed as follows:

(1) Under **Host Name** enter the complete host name as registered with the DynDNS provider, e.g. `test1.dyndns.org`.

(2) Select the WAN **Interface** whose IP address is to be propagated over the DynDNS service (e.g. `DSL ISP`, the interface of the Internet Service Provider).

(3) Enter the **User Name** as registered with the DynDNS provider.

(4) Enter the **Password** as registered with the DynDNS provider.

(5) Select the DynDNS **Provider** with which the above data is registered.

(6) Activate the function **Enable update**, the DynDNS entry configured here will be activated.

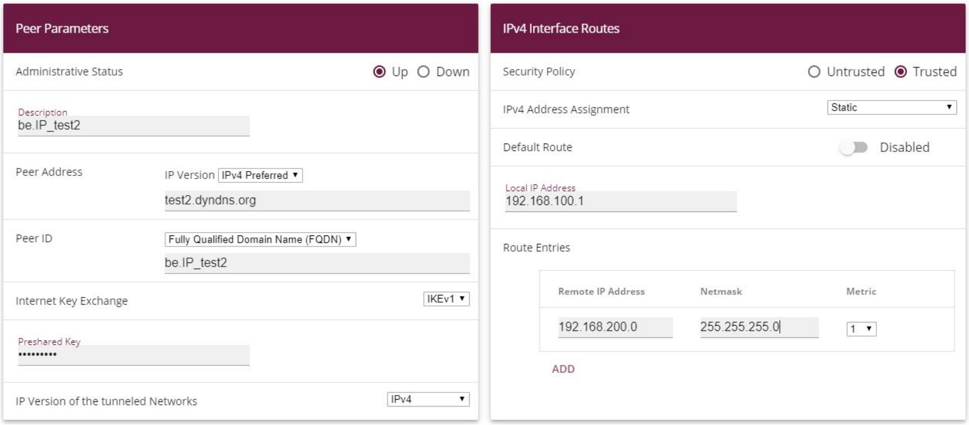
(7) Confirm with **OK**.

IPSec Peer Configuration

An endpoint of a communication is defined as peer in a computer network.

Select the **New** button to set up a new IPSec peer.

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



Peer Parameters

Administrative Status ● Up ○ Down

Description: be.IP_test2

Peer Address: IP Version IPv4 Preferred; test2.dyndns.org

Peer ID: Fully Qualified Domain Name (FQDN); be.IP_test2

Internet Key Exchange: IKEv1

Preshared Key: •••••••••

IP Version of the tunneled Networks: IPv4

IPv4 Interface Routes

Security Policy ○ Untrusted ● Trusted

IPv4 Address Assignment: Static

Default Route: Disabled

Local IP Address: 192.168.100.1

Route Entries

Remote IP Address	Netmask	Metric
192.168.200.0	255.255.255.0	1

Fig. 17: **VPN** -> **IPSec** -> **IPSec Peers** -> **New**

Proceed as follows to make the settings in the IPSec peer:

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

(2) Enter a **Description** of the peer that identifies it.

(3) Indicate the remote **Peer Address** (here, the DynDNS account of the bintec be.IP).

(4) The **Peer ID** must match the **Local ID value** of the remote terminal. Select `Full Qualified Domain Name (FQDN)` and enter an identification for the partner, e.g. `be.IP_test2`.

(5) Under **Preshared Key** enter the password for the encrypted connection.

(6) For **IPv4 Address Assignment**, select `Static`.

(7) Deselect the **Default Route** option.

(8) The **Local IP Address** is the IP address of the router LAN interface.

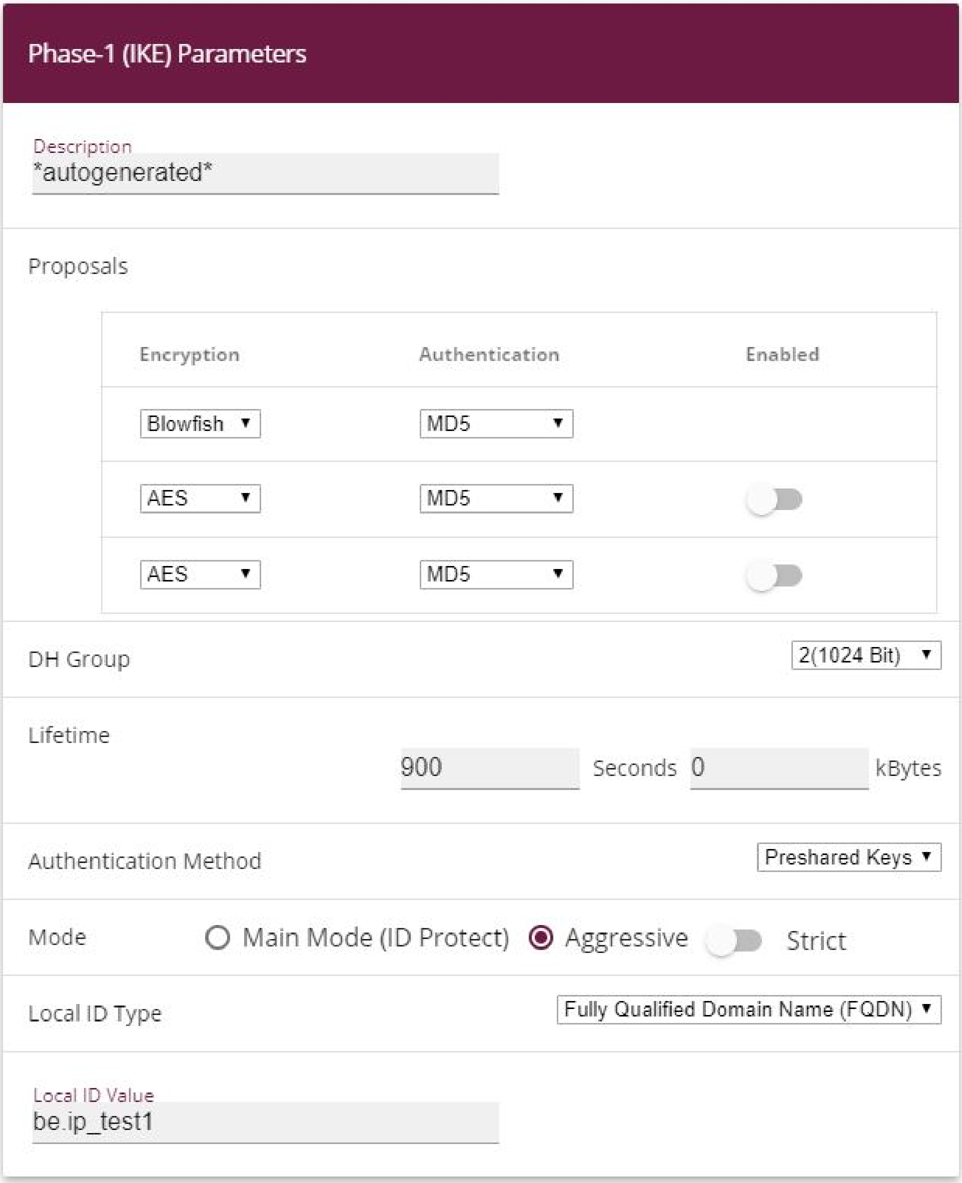
(9) Under **Remote IP Address** enter the partner network to be reached, e.g. *192.168.200.0* and under Netmask enter *255.255.255.0*.

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

Phase-1 Profiles

In the **Phase-1 Profiles** menu, you can define the Phase 1 (IKE) settings. Click on the ✎ icon to edit existing entries. Select the **New** button to create new profiles.

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



Phase-1 (IKE) Parameters

Description
autogenerated

Proposals

Encryption	Authentication	Enabled
Blowfish ▾	MD5 ▾	
AES ▾	MD5 ▾	○
AES ▾	MD5 ▾	○

DH Group 2(1024 Bit) ▾

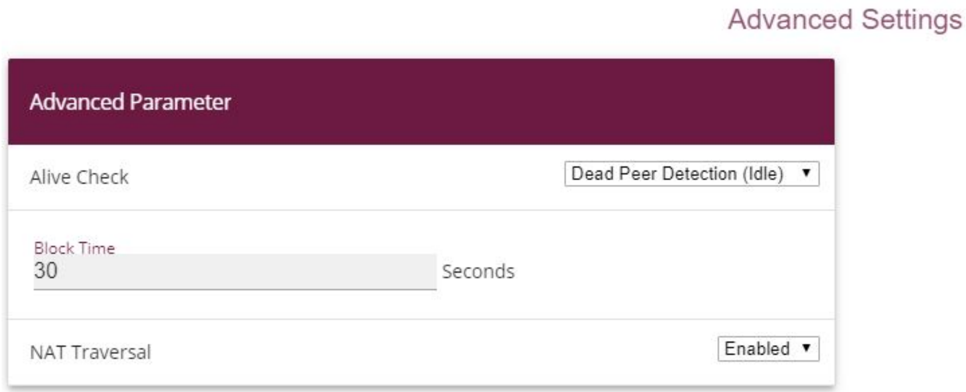
Lifetime 900 Seconds 0 kBytes

Authentication Method Preshared Keys ▾

Mode ○ Main Mode (ID Protect) ● Aggressive ○ Strict

Local ID Type Fully Qualified Domain Name (FQDN) ▾

Local ID Value
be.ip_test1



Advanced Settings

Advanced Parameter

Alive Check: Dead Peer Detection (Idle) ▾

Block Time: 30 Seconds

NAT Traversal: Enabled ▾

Fig. 19: **VPN** -> **IPSec** -> **Phase-1 Profiles** -> **New**

Proceed as follows:

(1) Enter a **Description** that uniquely defines the type of rule.

(2) Under **Proposal Encryption** select *Blowfish*, under **Authentication** select *MD5* . Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.

(3) Under **DH Group** select *2 (1024 Bit)*.

(4) Create a **Lifetime** for phase 1 keys. For lifetime, enter *900* seconds. For lifetime as volume of processing data, enter *0* KByts.

(5) Select the **Authentication method** *Preshared Keys*.

(6) Set the **Mode** to *Aggressive* as you use dynamic IP addresses.

(7) Under **Local ID Type** choose *Fully Qualified Domain Name (FQDN)* .

(8) Under **Local ID Value** enter the local ID of the gateway, e.g. *be.IP_test1* (set under Peer ID for the Partner).

(9) Click **Advanced Settings**.

(10) Under **Alive Check** select *Dead Peer Detection (idle)*.

(11) Define under **Block Time** how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed.

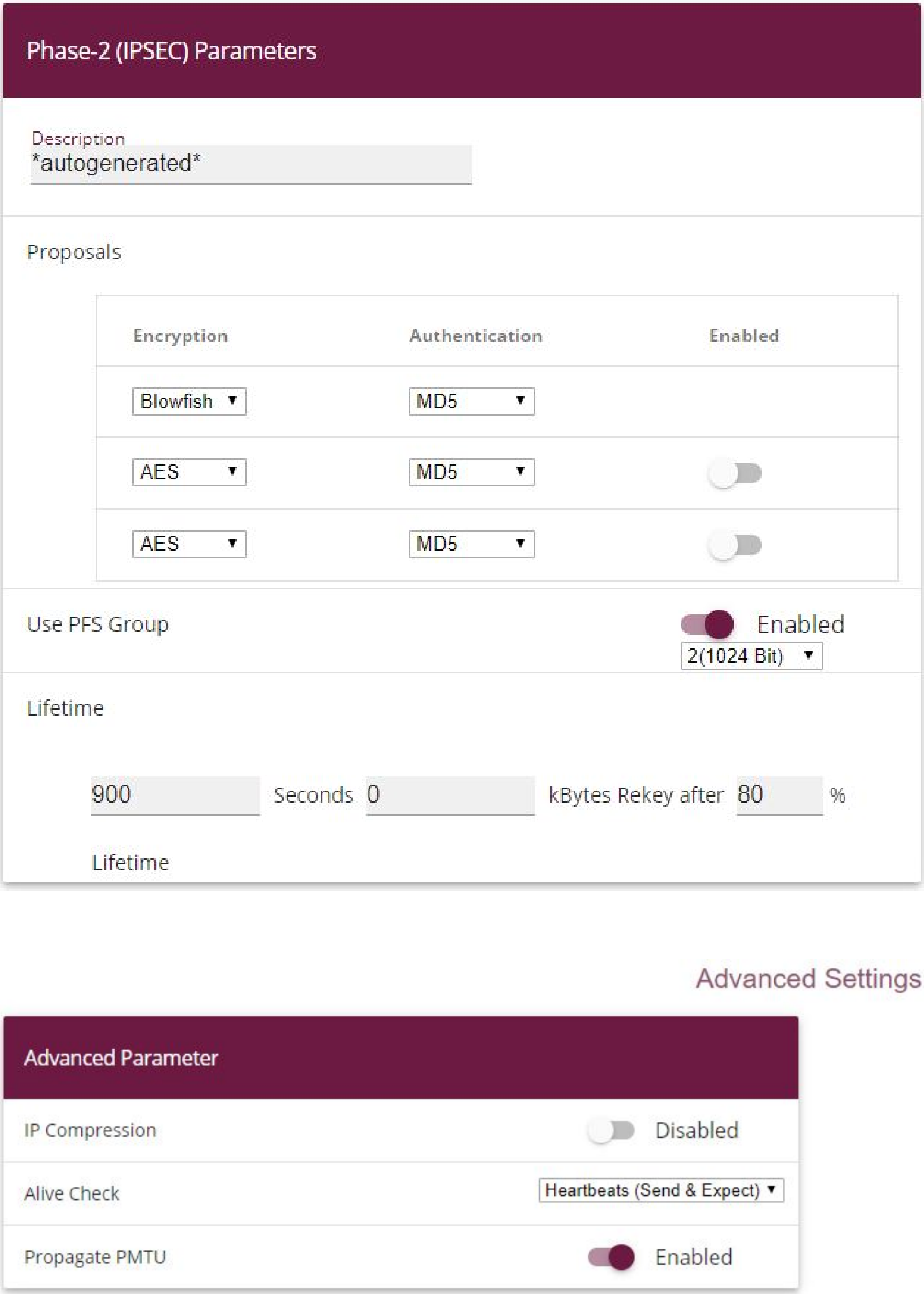
(12) Leave **NAT Traversal** on **Enabled**.

(13) Confirm with **OK**.

Phase-2 Profiles

You can define profiles for phase 2 of the tunnel setup just as for phase 1. Click on the ✎ icon to edit existing entries. Select the **New** button to create new profiles.

(1) Go to **VPN**-> **IPSec** -> **Phase-2 Profiles** -> **New**.



Phase-2 (IPSEC) Parameters

Description
autogenerated

Proposals

Encryption	Authentication	Enabled
Blowfish ▾	MD5 ▾	
AES ▾	MD5 ▾	○
AES ▾	MD5 ▾	○

Use PFS Group: ● Enabled, 2(1024 Bit) ▾

Lifetime

900 Seconds 0 kBytes Rekey after 80 %

Lifetime

Advanced Settings

Advanced Parameter

IP Compression: ○ Disabled

Alive Check: Heartbeats (Send & Expect) ▾

Propagate PMTU: ● Enabled

Fig. 21: **VPN** -> **IPSec** -> **Phase-2 Profiles** -> **New**

Proceed as follows:

(1) Enter a **Description** that uniquely identifies the profile.

(2) Under **Proposal Encryption** select *`Blowfish`* , under **Authentication** select *`MD5`* . Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.

(3) Activate the **Use PFS group** option and select *`2 (1024 bits)`*.

(4) Define how the **Lifetime** is defined that will expire before phase 2 SAs need to be renewed. For lifetime, enter *`900`* seconds. For lifetime as volume of processing data, enter *`0`* KByts.

(5) Click **Advanced Settings**.

(6) Set **Alive Check** to *`Heartbeats (send & expect)`*.

(7) Aktivate the option **Propagate PMTU**.

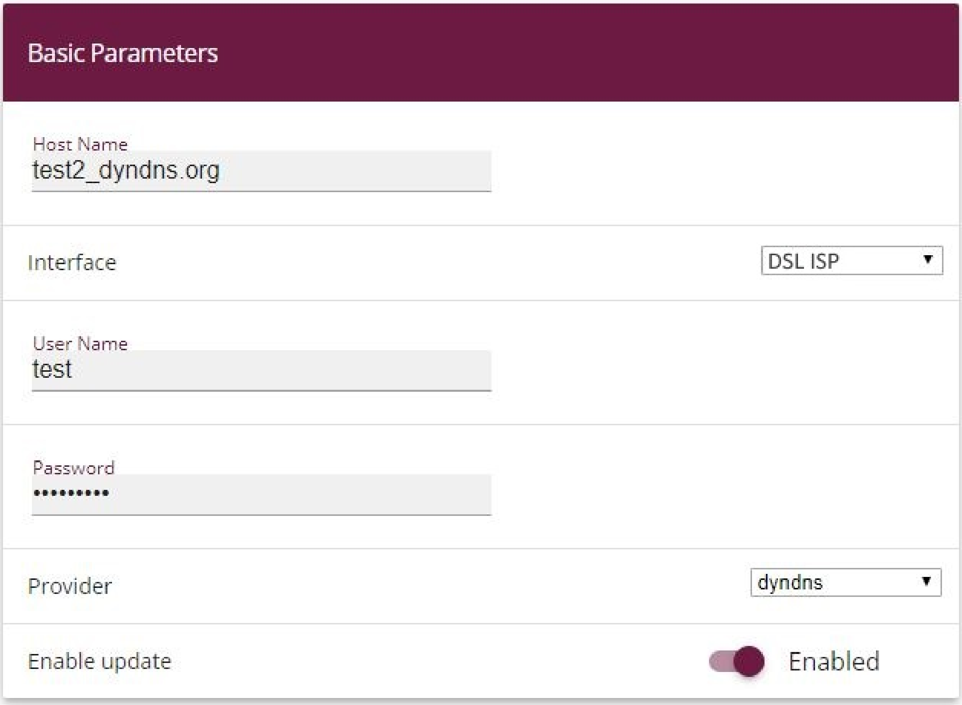
(8) Confirm with **OK**.

2.2.2 Configuration on the second router (Location B)

Set up DynDNS account

A list of all configured DynDNS registrations is displayed in the DynDNS Update menu. Select the **New** button to perform additional DynDNS registrations.

(1) Go to **Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**.



Basic Parameters

Host Name: test2_dyndns.org

Interface: DSL ISP

User Name: test

Password: ••••••••••

Provider: dyndns

Enable update: Enabled

Fig. 22: **Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**

Proceed as follows:

(1) Under **Host Name** enter the complete host name as registered with the DynDNS provider, e.g. `test2.dyndns.org`.

(2) Select the WAN **Interface** whose IP address is to be propagated over the DynDNS service (e.g. `DSL ISP`, the interface of the Internet Service Provider).

(3) Enter the **User Name** as registered with the DynDNS provider.

(4) Enter the **Password** as registered with the DynDNS provider.

(5) Select the DynDNS **Provider** with which the above data is registered.

(6) Activate the function **Enable update**, the DynDNS entry configured here will be activated.

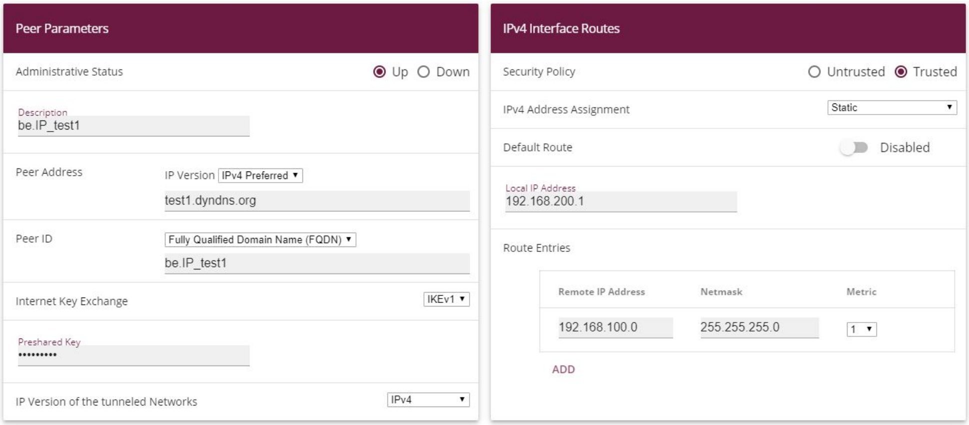
(7) Confirm with **OK**.

IPSec Peer Configuration

An endpoint of a communication is defined as peer in a computer network.

Select the **New** button to set up a new IPSec peer.

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



Peer Parameters

Administrative Status ● Up ○ Down

Description: be.IP_test1

Peer Address: IP Version IPv4 Preferred ▾ test1.dyndns.org

Peer ID: Fully Qualified Domain Name (FQDN) ▾ be.IP_test1

Internet Key Exchange: IKEv1 ▾

Preshared Key: •••••••••

IP Version of the tunneled Networks: IPv4 ▾

IPv4 Interface Routes

Security Policy ○ Untrusted ● Trusted

IPv4 Address Assignment: Static ▾

Default Route: Disabled

Local IP Address: 192.168.200.1

Route Entries

Remote IP Address	Netmask	Metric
192.168.100.0	255.255.255.0	1 ▾

Fig. 23: **VPN**-> **IPSec**-> **IPSec Peers**-> **New**

Proceed as follows to make the settings in the IPSec peer:

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

(2) Enter a **Description** of the peer that identifies it.

(3) Indicate the remote **Peer Address** (here, the DynDNS account of the bintec be.IP).

(4) The **Peer ID** must match the **local ID value** of the remote terminal. Select *Full Qualified Domain Name (FQDN)* and enter an identification for the partner, e.g. *be.IP_test1*.

(5) Under **Preshared Key** enter the password for the encrypted connection.

(6) For **IPv4 Address Assignment**, select *Static*.

(7) Deselect the **Default Route** option.

(8) The **Local IP Address** is the IP address of the router LAN interface.

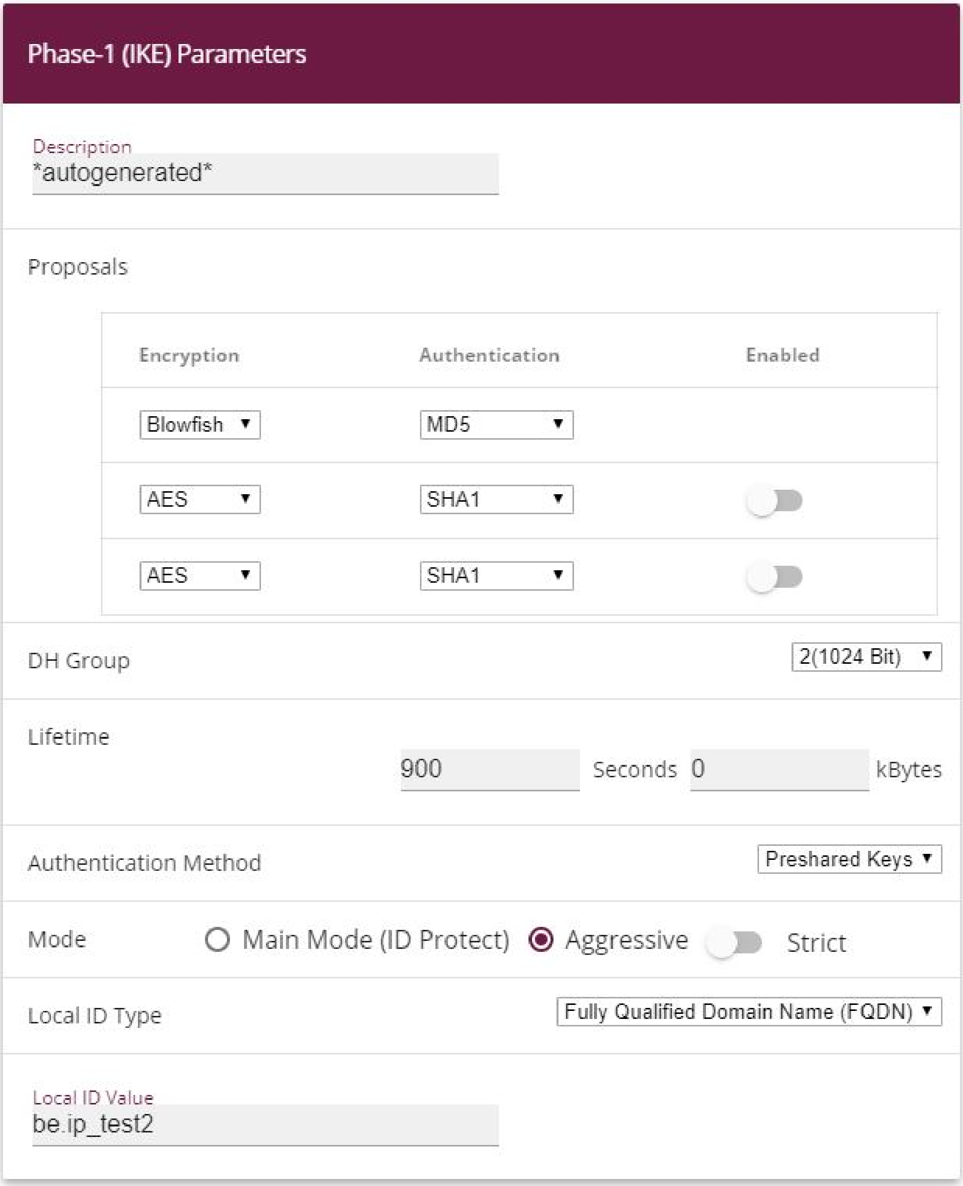
(9) Under **Remote IP Address** enter the partner network to be reached, e.g. *192.168.100.0* and under Netmask enter *255.255.255.0*.

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

Phase-1 Profiles

In the **Phase 1 Profiles** menu, you can define the Phase 1 (IKE) settings. Click on the ✎ icon to edit existing entries. Select the **New** button to create new profiles.

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



Phase-1 (IKE) Parameters

Description: *autogenerated*

Proposals

Encryption	Authentication	Enabled
Blowfish ▾	MD5 ▾	
AES ▾	SHA1 ▾	○
AES ▾	SHA1 ▾	○

DH Group: 2(1024 Bit) ▾

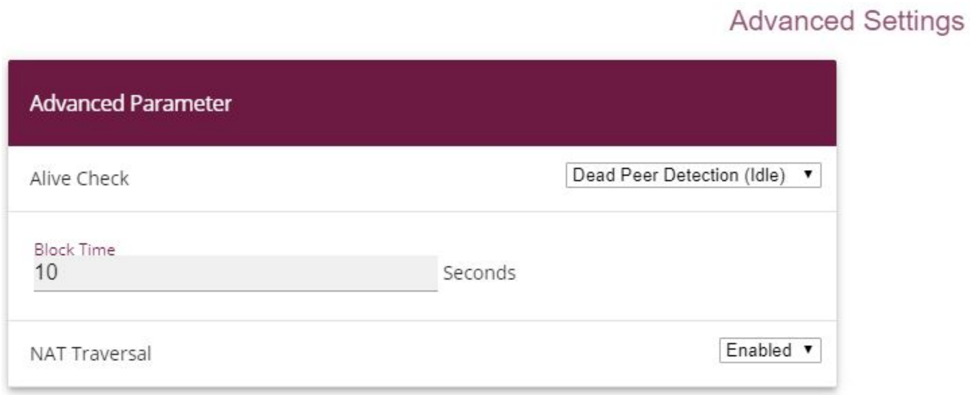
Lifetime: 900 Seconds 0 kBytes

Authentication Method: Preshared Keys ▾

Mode: ○ Main Mode (ID Protect) ● Aggressive ○ Strict

Local ID Type: Fully Qualified Domain Name (FQDN) ▾

Local ID Value: be.ip_test2



Advanced Settings

Advanced Parameter

Alive Check: Dead Peer Detection (Idle) ▼

Block Time: 10 Seconds

NAT Traversal: Enabled ▼

Fig. 25: **VPN** -> **IPSec** -> **Phase-1 Profiles** -> **New**

Proceed as follows:

(1) Enter a **Description** that uniquely defines the type of rule.

(2) Under **Proposal Encryption** select *Blowfish*, under **Authentication** select *MD5* . Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.

(3) Under **DH Group** select *2 (1024 Bit)*.

(4) Create a **Lifetime** for phase 1 keys. For lifetime, enter *900* seconds. For lifetime as volume of processing data, enter *0* KByts.

(5) Select the **Authentication method** *Preshared Keys*.

(6) Set the **Mode** to *Aggressive* as you use dynamic IP addresses.

(7) Under **Local ID Type** choose *Fully Qualified Domain Name (FQDN)* .

(8) Under **Local ID Value** enter the local ID of the gateway, e.g. *be.IP_test2* (set under Peer ID for the Partner).

(9) Click **Advanced Settings**.

(10) Under **Alive Check** select *Dead Peer Detection (idle)*.

(11) Define under **Block Time** how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed.

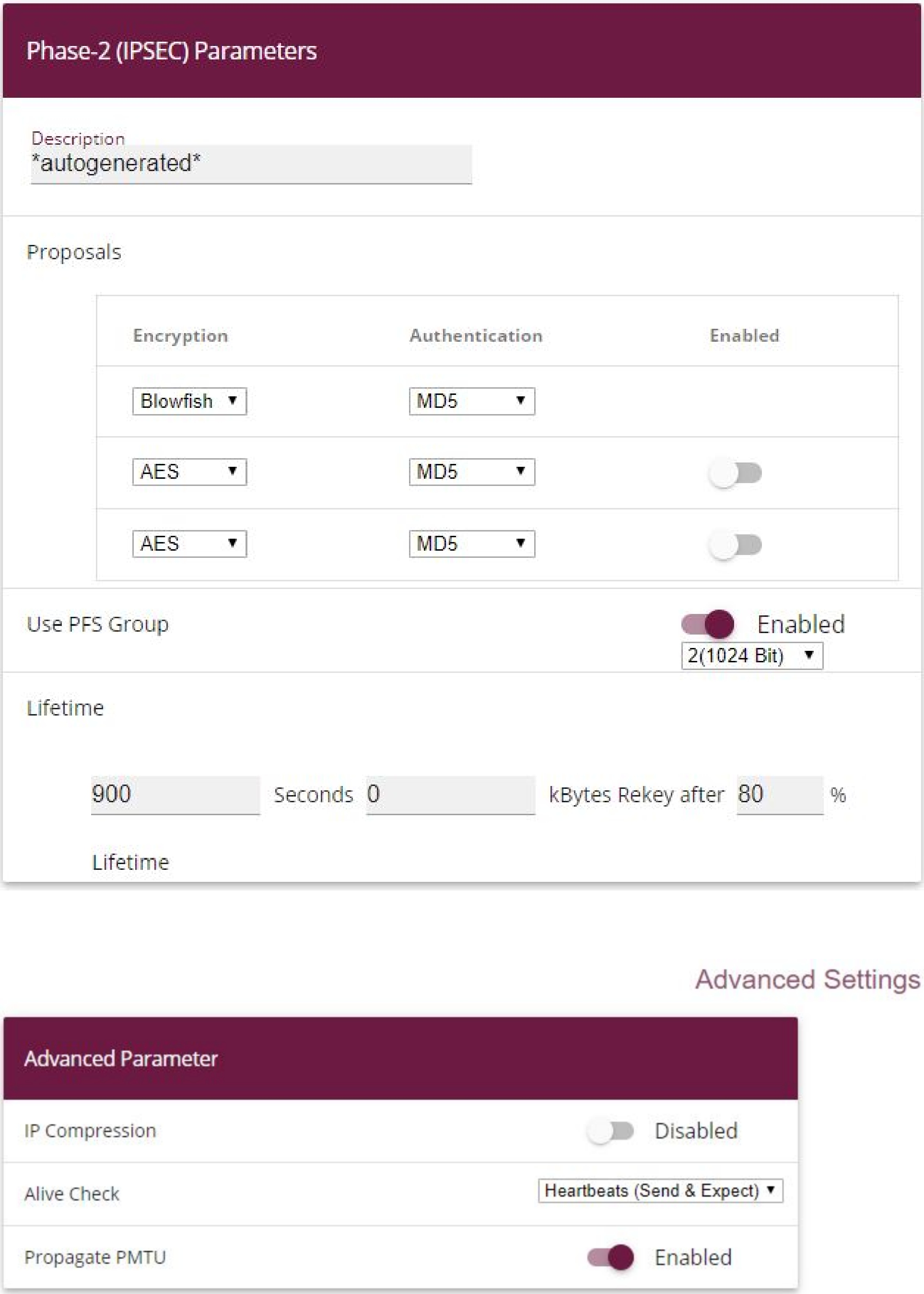
(12) Leave **NAT Traversal** on **Enabled**.

(13) Confirm with **OK**.

Phase-2 Profiles

You can define profiles for phase 2 of the tunnel setup just as for phase 1. Click on the ✎ icon to edit existing entries. Select the **New** button to create new profiles.

(1) Go to **VPN**-> **IPSec** -> **Phase-2 Profiles** -> **New**.



Phase-2 (IPSEC) Parameters

Description: *autogenerated*

Proposals

Encryption	Authentication	Enabled
Blowfish	MD5	
AES	MD5	○
AES	MD5	○

Use PFS Group: ● Enabled, 2(1024 Bit)

Lifetime

900 Seconds 0 kBytes Rekey after 80 %

Lifetime

Advanced Parameter

IP Compression: ○ Disabled

Alive Check: Heartbeats (Send & Expect)

Propagate PMTU: ● Enabled

Fig. 27: **VPN** -> **IPSec** -> **Phase-2 Profiles** -> **New**

Proceed as follows:

(1) Enter a **Description** that uniquely identifies the profile.

(2) Under **Proposal Encryption** select *Blowfish* , under **Authentication** select *MD5* . Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.

(3) Activate the **Use PFS group** option and select *2 (1024 bits)*.

(4) Define how the **Lifetime** is defined that will expire before phase 2 SAs need to be renewed. For lifetime, enter *900* seconds. For lifetime as volume of processing data, enter *0* KByts.

(5) Click **Advanced Settings**.

(6) Set **Alive Check** to *Heartbeats (send & expect)*.

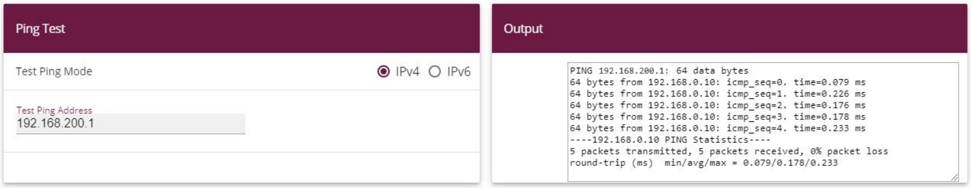
(7) Aktivate the option **Propagate PMTU**.

(8) Confirm with **OK**.

2.3 Checking the connection

With the **ping test** you can check the function of the VPN IPSec connection. You launch the ping test by entering the internal IP address of the remote gateway (here 192.168.200.1) and pressing the **Go**button. This initiates setup of the VPN IPSec tunnel. If the output field displays an answer in milliseconds, the ping test was successful.

(1) Go **Maintenance** -> **Diagnostics** -> **Ping Test**.



Ping Test

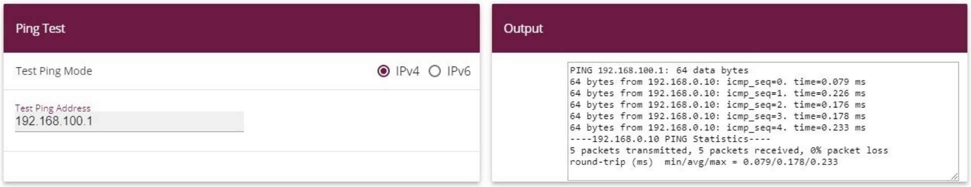
Test Ping Mode ● IPv4 ○ IPv6

Test Ping Address 192.168.200.1

Output

```
PING 192.168.200.1:  64 data bytes
64 bytes from 192.168.0.10: icmp_seq=0. time=0.079 ms
64 bytes from 192.168.0.10: icmp_seq=1. time=0.226 ms
64 bytes from 192.168.0.10: icmp_seq=2. time=0.176 ms
64 bytes from 192.168.0.10: icmp_seq=3. time=0.178 ms
64 bytes from 192.168.0.10: icmp_seq=4. time=0.233 ms
----192.168.0.10 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0.079/0.178/0.233
```

Fig. 28: **Maintenance->Diagnosis->Ping Test**



Ping Test

Test Ping Mode ● IPv4 ○ IPv6

Test Ping Address 192.168.100.1

Output

```
PING 192.168.100.1:  64 data bytes
64 bytes from 192.168.0.10: icmp_seq=0. time=0.079 ms
64 bytes from 192.168.0.10: icmp_seq=1. time=0.226 ms
64 bytes from 192.168.0.10: icmp_seq=2. time=0.176 ms
64 bytes from 192.168.0.10: icmp_seq=3. time=0.178 ms
64 bytes from 192.168.0.10: icmp_seq=4. time=0.233 ms
----192.168.0.10 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0.079/0.178/0.233
```

Fig. 29: **Maintenance->Diagnosis->Ping Test**

2.4 Overview of configuration steps

Set up DynDNS account on the first router (Location A)

Field	Menu	Value
Host Name	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *test1.dyndns.org*
Interface	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	*DSL ISP*
User Name	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *test*
Password	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *test*
Provider	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	*dyndns*
Enable update	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	Disabled

IPSec configuration - IPSec peers

Field	Menu	Value
Administrative Status	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	Active
Description	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	e.g. *be.IP_test2*
Peer Address	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	e.g. *test2.dyndns.org*
Peer ID	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	*Fully Qualified Domain Name (FQDN)* / *be.IP_test2*
Preshared Key	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	e.g. *test*
IP Address Assignment	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	Static
Default Route	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	Disabled
Local IP Address	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	*192.168.100.1*
Route Entries	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	*192.168.200.0* / *255.255.255.0*

IPSec configuration - Phase 1

Field	Menu	Value
Description	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	e.g. **autogenerated**
Proposals	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*Blowfish, MD5*
DH Group	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*2 (1024 Bit)*
Lifetime	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*900* seconds, *0* kBytes
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**	*Fully Qualified Domain Name (FQDN)*
Local ID Value	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*be.IP_test1*
Alive Check	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New** -> **Advanced Settings**	*Dead Peer Detection (idle)*
Block Time	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New** -> **Advanced Settings**	*10* seconds
NAT Traversal	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New** -> **Advanced Settings**	Enabled

IPSec configuration - Phase 2

Field	Menu	Value
Description	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	e.g. **autogenerated**
Proposals	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	*Blowfish, MD5*
Use PFS Group	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	*2 (1024 Bit)*
Lifetime	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	*900* seconds, *0* kBytes
IP Compression	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New** -> **Advanced Settings**	*Disabled*
Alive Check	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New** -> **Advanced Settings**	*Heartbeats (send & expect)*

Field	Menu	Value
Propagate PMTU	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New** -> **Advanced Settings**	Enabled

Set up DynDNS account on the second router (Location B)

Field	Menu	Value
Host Name	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *test2.dyndns.org*
Interface	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	*DSL ISP*
User Name	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *test*
Password	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	e.g. *test*
Provider	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	*dyndns*
Enable update	**Local Services** -> **DynDNS Client** -> **DynDNS Update** -> **New**	Enabled

IPSec configuration - IPSec peers

Field	Menu	Value
Administrative Status	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	Active
Description	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	e.g. *be.IP_test1*
Peer Address	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	e.g. *test1.dyndns.org*
Peer ID	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	*Fully Qualified Domain Name (FQDN)*/ *be.IP_test1*
Preshared Key	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	e.g. *test*
IP Address Assignment	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	Static
Default Route	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	Disabled
Local IP Address	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	*192.168.200.1*
Route Entries	**VPN** -> **IPSec** ->**IPSec Peers** -> **New**	*192.168.100.0*/ *255.255.255.0*

IPSec configuration - Phase 1

Field	Menu	Value
Description	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	e.g. **autogenerated**
Proposals	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*Blowfish, MD5*
DH Group	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*2 (1024 Bit)*
Lifetime	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*900* seconds, *0* kBytes
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**	*Fully Qualified Domain Name (FQDN)*
Local ID Value	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New**	*be.IP_test2*
Alive Check	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New** -> **Advanced Settings**	*Dead Peer Detection (idle)*
Block Time	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New** -> **Advanced Settings**	*10* seconds
NAT Traversal	**VPN** -> **IPSec** ->**Phase-1 Profiles** -> **New** -> **Advanced Settings**	Enabled

IPSec configuration - Phase 2

Field	Menu	Value
Description	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	e.g. **autogenerated**
Proposals	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	*Blowfish, MD5*
Use PFS Group	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	*2 (1024 Bit)*
Lifetime	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New**	*900* seconds, *0* kBytes
IP Compression	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New** -> **Advanced Settings**	*Disabled*
Alive Check	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New** -> **Advanced Settings**	*Heartbeats (send & expect)*

Field	Menu	Value
Propagate PMTU	**VPN** -> **IPSec** ->**Phase-2 Profiles** -> **New** -> **Advanced Settings**	Enabled

Chapter 3 Security - Bridging over an IPSec tunnel

3.1 Introduction

This solution shows an option for connecting two locations over IPSec with overlapping or identical IP network ranges (e.g. Location A: 192.168.1.0/24 and Location B: 192.168.1.0/24).

In this case IPSec does not function, as IPSec requires different IP networks between the locations being networked to function as a Layer3 (IP Layer) protocol. This workshop shows how the security of IPSec can continue to be used for location networking in such a case.

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

To solve this problem, L2TP (Layer2 Tunnelling Protocol) can be used as a transport protocol. L2TP offers the option to create bridge connections over routed IP connections. In our example, this means that the locations are connected over IPSec and that the actual traffic tunnelled in L2TP is routed via the IPSec tunnel.

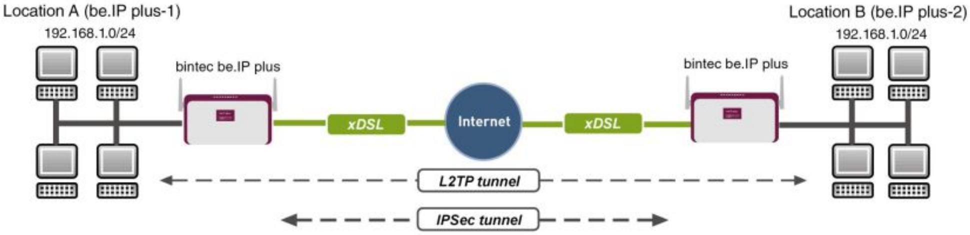


Fig. 30: Example scenario

The user data is routed via the L2TP tunnel and the L2TP packets are sent over the IPSec tunnel.

Requirements

The following are required for the configuration:

(1) Two bintec ADSL gateways, e.g. **bintec be.IP plus**

(2) A boot image of version 7.9.1 or later.

(3) Both gateways require an independent connection to the Internet.

Notes on test setup

bintec be.IP plus Location A

System name	be.IP_plus-1
LAN IP address	192.168.1.253
LAN IP subnet mask	255.255.255.0
Public Internet IP address	10.1.1.1 (a host name can also be used here)
Local IP address of the IPSec interface	1.1.1.1 (any private IP address)
Local IP address of the L2TP interface	1.1.1.3

bintec be.IP plus Location B

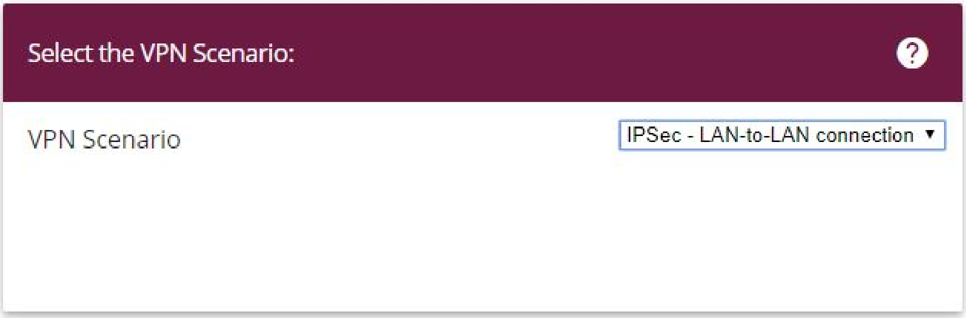
System name	be.IP_plus-2
LAN IP address	192.168.1.254
LAN IP subnet mask	255.255.255.0
Public Internet IP address	10.1.1.4 (a host name can also be used here)
Local IP address of the IPSec interface	1.1.1.2 (any private IP address)
Local IP address of the L2TP interface	1.1.1.4

3.2 Configuration at location A (bintec be.IP plus-1)

Configuring the IPSec tunnel with the VPN assistants

Add a new connection to the VPN assistants. For this, go to the following menu:

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



Select the VPN Scenario:

VPN Scenario: IPSec - LAN-to-LAN connection

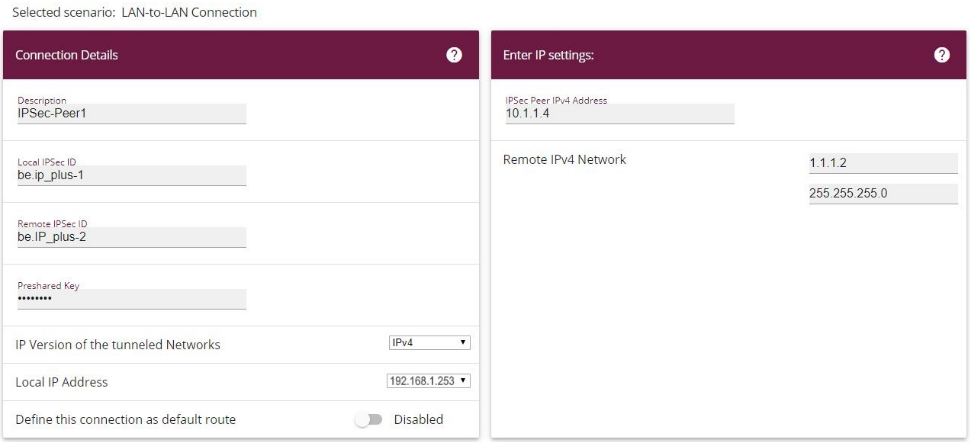
Fig. 31: **Assistants** -> **VPN** -> **VPN Connections** -> **New**

Proceed as follows:

(1) Under **VPN scenario** select *IPSec LAN-to-LAN connection*.

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

Enter the data required for the VPN connection.



Selected scenario: LAN-to-LAN Connection

Connection Details

Description: IPSec-Peer1

Local IPSec ID: be.ip_plus-1

Remote IPSec ID: be.IP_plus-2

Preshared Key: ••••••••

IP Version of the tunneled Networks: IPv4

Local IP Address: 192.168.1.253

Define this connection as default route: Disabled

Enter IP settings:

IPSec Peer IPv4 Address: 10.1.1.4

Remote IPv4 Network: 1.1.1.2 / 255.255.255.0

Fig. 32: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

Proceed as follows to configure a new VPN connection:

(1) For example, under **Description** enter `IPSec-Peer1`.

(2) Enter the ID of your own IPSec gateway under **Local IPSec ID**, e.g. `be.IP_plus-1`.

(3) For example, under **Remote IPSec ID** enter `be.IP_plus-2`.

(4) Under **Preshared Key** enter, for example, `secret` for authentication. The preshared key must be identical on both sides.

(5) Select the **Local IP Address** of the gateway, for example `192.168.1.253`.

(6) Leave **Define this connection as default route** set to disabled.

(7) Under **IPSec Peer Address** enter the IP address or host name of the remote IPSec partner, e. g. `10.1.1.4`.

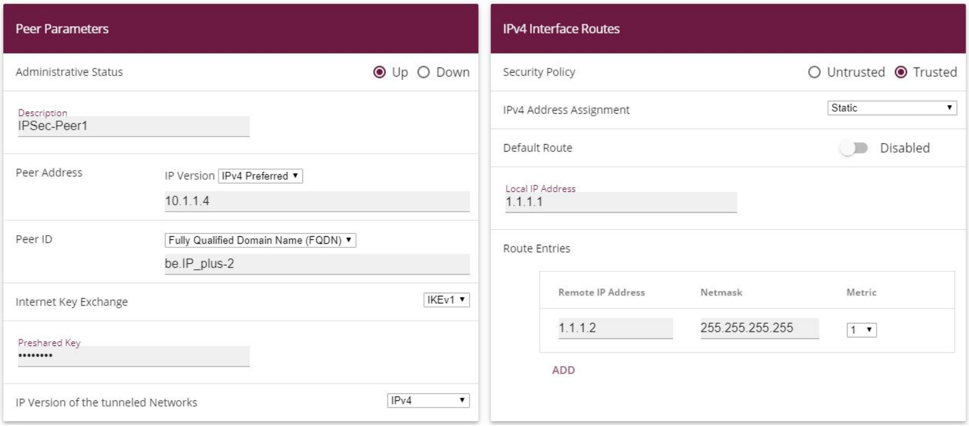
(8) Enter the destination address used for the connection under **IP Address of Remote Network** e.g. `1.1.1.2`.

(9) Under **Subnet Mask** enter the host mask, e.g. `255.255.255.255`.

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

To change the local IP address, select the following menu options:

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



Peer Parameters

Administrative Status ● Up ○ Down

Description: IPSec-Peer1

Peer Address: IP Version IPv4 Preferred ▾ 10.1.1.4

Peer ID: Fully Qualified Domain Name (FQDN) ▾ be.IP_plus-2

Internet Key Exchange: IKEv1 ▾

Preshared Key: ••••••••

IP Version of the tunneled Networks: IPv4 ▾

IPv4 Interface Routes

Security Policy ○ Untrusted ● Trusted

IPv4 Address Assignment: Static ▾

Default Route: Disabled

Local IP Address: 1.1.1.1

Route Entries

Remote IP Address	Netmask	Metric
1.1.1.2	255.255.255.255	1 ▾

ADD

Fig. 33: **VPN** -> **IPSec** -> **IPSec Peers** -> ✎

Proceed as follows:

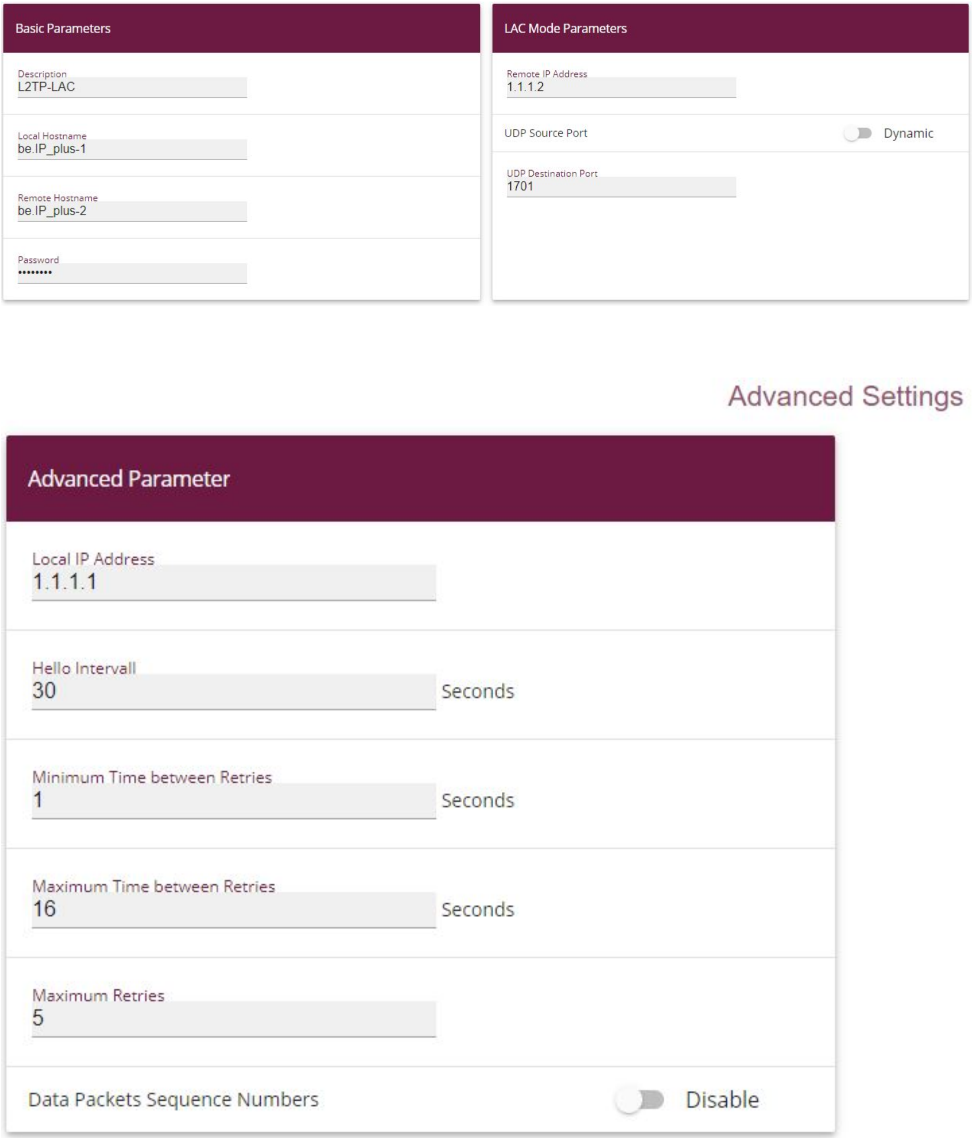
(1) Under **Local IP Address** enter, for example `1.1.1.1`.

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

Configuring the L2TP connection

To create a tunnel profile, go to the following menu:

(1) Go to **VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**.



Basic Parameters

Description: L2TP-LAC

Local Hostname: be.IP_plus-1

Remote Hostname: be.IP_plus-2

Password: ••••••••

LAC Mode Parameters

Remote IP Address: 1.1.1.2

UDP Source Port: Dynamic

UDP Destination Port: 1701

Advanced Settings

Advanced Parameter

Local IP Address: 1.1.1.1

Hello Intervall: 30 Seconds

Minimum Time between Retries: 1 Seconds

Maximum Time between Retries: 16 Seconds

Maximum Retries: 5

Data Packets Sequence Numbers: Disable

Fig. 35: **VPN**->**L2TP**->**Tunnel Profiles**->**New**

(1) For example, under **Description** enter `L2TP-LAC`.

(2) Enter the ID of your own IPSec gateway under **Local Hostname**, e.g. `be.IP_plus-1`.

(3) For example, under **Remote Hostname** enter `be.IP_plus-2`.

(4) Enter the **Password**, e.g. `secret` for authentication.

(5) Enter the destination address used for the connection under **Remote IP Address** e.g.

`1.1.1.2`.

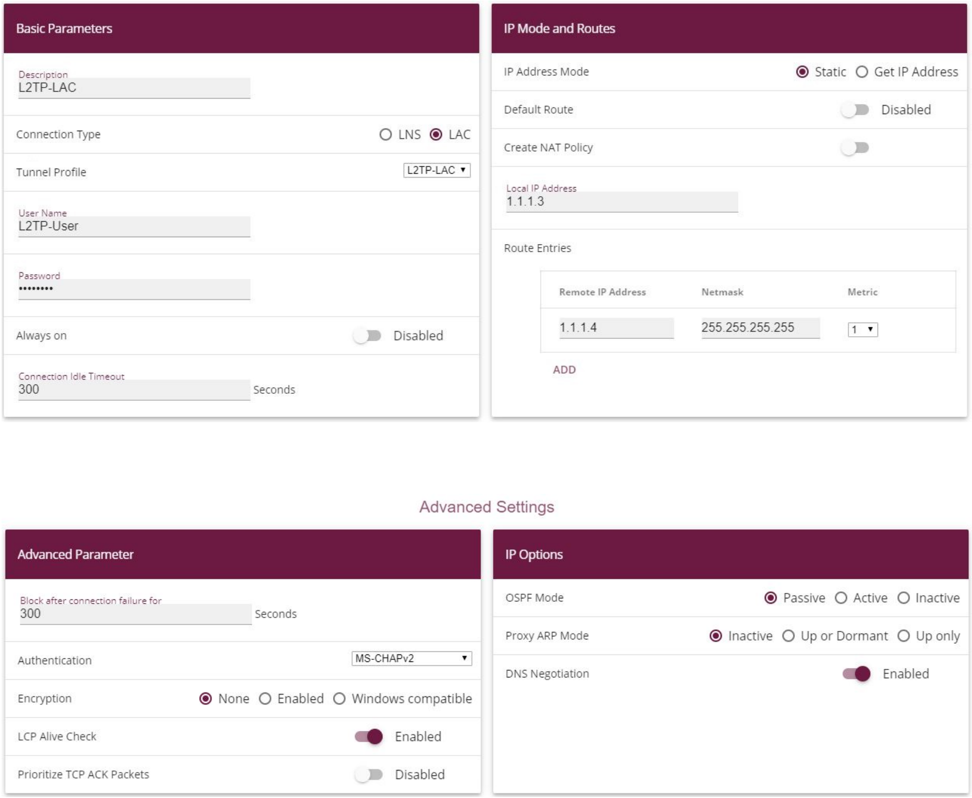
(6) Click **Advanced Settings**.

(7) Enter the **Local IP Address**, e.g. `1.1.1.1`.

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

A user must be configured in the next step. For this, go to the following menu:

(1) Go to **VPN** -> **L2TP** -> **User** -> **New**.



Basic Parameters

Description: L2TP-LAC

Connection Type: ○ LNS ● LAC

Tunnel Profile: L2TP-LAC ▾

User Name: L2TP-User

Password: ••••••••

Always on: Disabled

Connection Idle Timeout: 300 Seconds

IP Mode and Routes

IP Address Mode: ● Static ○ Get IP Address

Default Route: Disabled

Create NAT Policy

Local IP Address: 1.1.1.3

Route Entries

Remote IP Address	Netmask	Metric
1.1.1.4	255.255.255.255	1 ▾

ADD

Advanced Settings

Advanced Parameter

Block after connection failure for: 300 Seconds

Authentication: MS-CHAPv2 ▾

Encryption: ● None ○ Enabled ○ Windows compatible

LCP Alive Check: Enabled

Prioritize TCP ACK Packets: Disabled

IP Options

OSPF Mode: ● Passive ○ Active ○ Inactive

Proxy ARP Mode: ● Inactive ○ Up or Dormant ○ Up only

DNS Negotiation: Enabled

Fig. 37: **VPN**->**L2TP**->**Users**->**New**

To create a new user, proceed as follows.

(1) For example, under **Description** enter `L2TP-LAC`.

(2) Select the **Connection Type** `LAC`.

(3) For example, under **Tunnel Profile** select `L2TP-LAC`.

(4) Under **User Name** enter `L2TP-User` for example.

(5) Enter the **password**, e.g. `secret`.

(6) Enter the **Local IP Address**, e.g. `1.1.1.3`. To avoid conflicts with other interfaces or

existing routes, the local IP address must be unique.

(7) Under **Route Entries** enter the remote IP address, e.g. *1.1.1.4* and the netmask e.g. *255.255.255.255*.

(8) Click **Advanced Settings**.

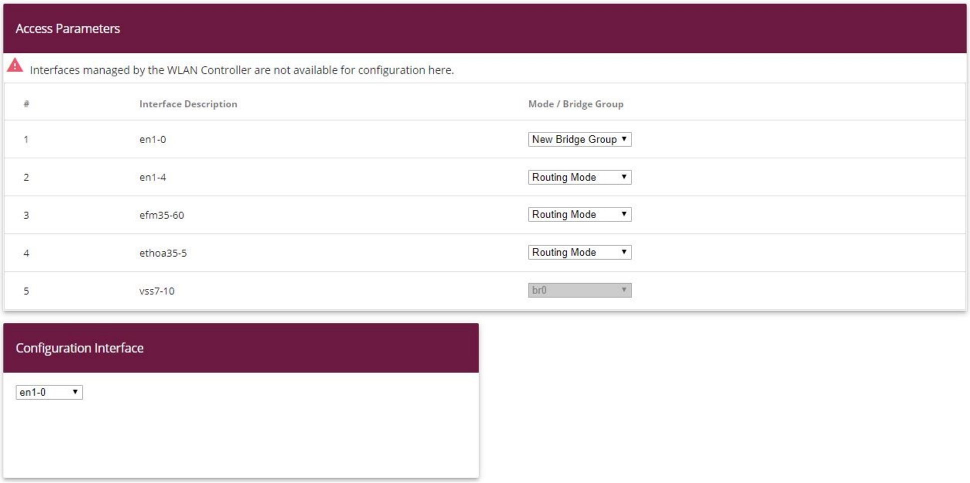
(9) Under **Encryption** click *None*. As a secure IPSec connection already exists, additional encryption is not required.

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

Configuring the bridge group

To enable bridging between the LAN interface and the L2TP interface, both interfaces must be assigned to a bridge group. For this, go to the following menu:

(1) Go to **System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**.



Access Parameters

Interfaces managed by the WLAN Controller are not available for configuration here.

#	Interface Description	Mode / Bridge Group
1	en1-0	New Bridge Group ▾
2	en1-4	Routing Mode ▾
3	efm35-60	Routing Mode ▾
4	ethoa35-5	Routing Mode ▾
5	vss7-10	br0 ▾

Configuration Interface

en1-0 ▾

Fig. 38: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**

Proceed as follows:

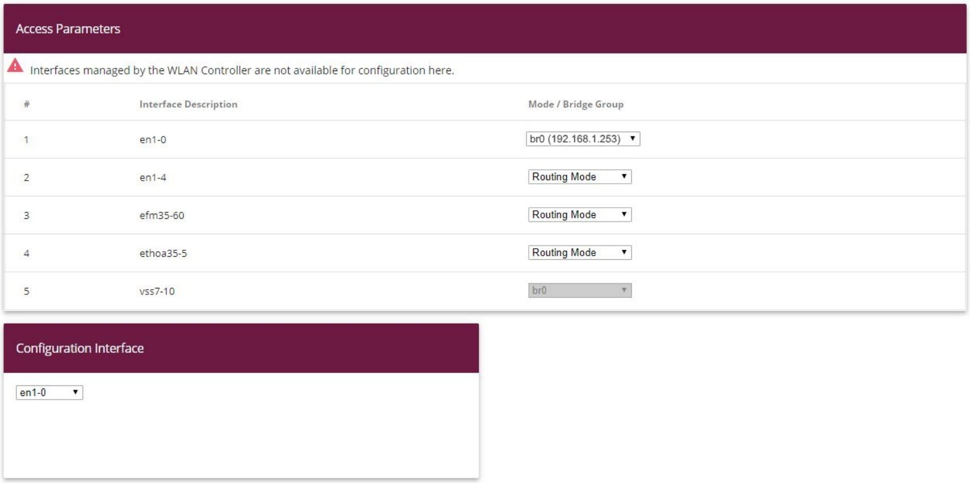
(1) Under **Mode / Bridge Group** select *New Bridge Group*. In our example, the interface *en1-0* is used as the LAN interface.

(2) Under **Configuration Interface** select *en1-0*.

(3) Confirm with **OK**. After clicking **OK**, a new bridge group is created automatically.

If no bridge group exists, the new interface uses the alias *br0* (otherwise *br1*, *br2*, etc.).

The configuration looks like this:



Access Parameters

Interfaces managed by the WLAN Controller are not available for configuration here.

#	Interface Description	Mode / Bridge Group
1	en1-0	br0 (192.168.1.253) ▾
2	en1-4	Routing Mode ▾
3	efm35-60	Routing Mode ▾
4	ethoa35-5	Routing Mode ▾
5	vss7-10	br0 ▾

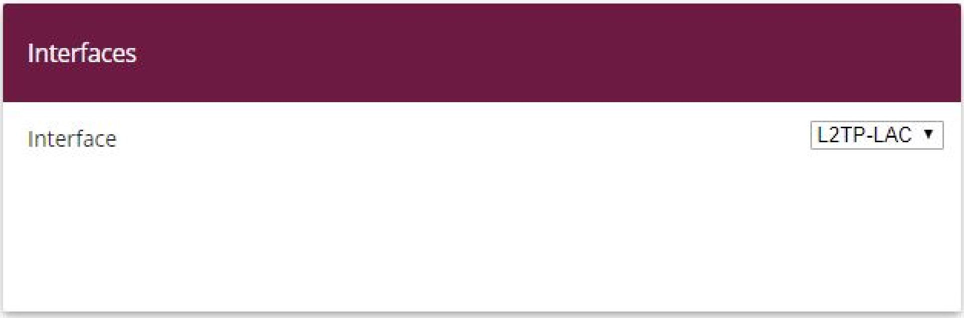
Configuration Interface

en1-0 ▾

Fig. 39: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**

Now is assigned to the newly created bridge Grupppe the L2TP interface. For this, go to the following menu:

(1) Go to **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces** -> **Add**.



Interfaces

Interface L2TP-LAC ▾

Fig. 40: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces** -> **Add**

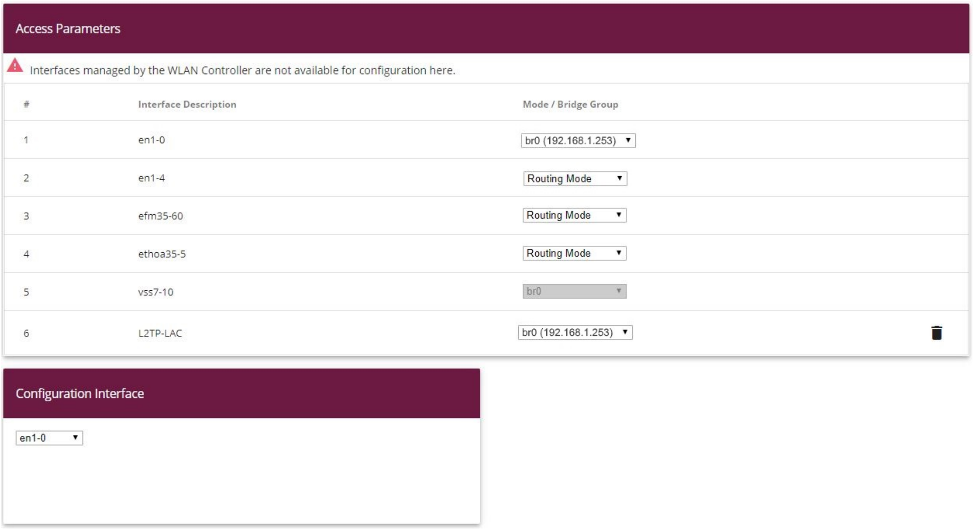
Proceed as follows:

(1) Under **Mode / Bridge Group** select the WAN-Partner *L2TP-LAC*.

(2) Confirm with **OK**.

To enable bridging between the LAN interface and the L2TP interface, both interfaces must be assigned to a bridge group. For this, go to the following menu:

(1) Go to **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**.



Access Parameters

Interfaces managed by the WLAN Controller are not available for configuration here.

#	Interface Description	Mode / Bridge Group
1	en1-0	br0 (192.168.1.253)
2	en1-4	Routing Mode
3	efm35-60	Routing Mode
4	ethoa35-5	Routing Mode
5	vss7-10	br0
6	L2TP-LAC	br0 (192.168.1.253)

Configuration Interface

en1-0

Fig. 41: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**

Proceed as follows:

(1) Under **Mode / Bridge Group** select *br0 (192.168.1.253)*.

(2) Confirm with **OK**. After clicking **OK**, a new bridge group is created automatically.

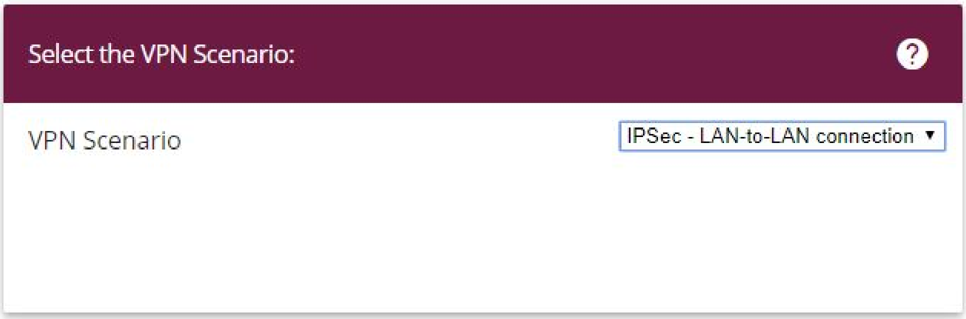
This concludes the configuration of the **bintec be.IP plus** gateway as location A.

3.3 Configuration at location B (bintec be.IP plus-2)

Configuring the IPSec tunnel with the VPN assistants

Add a new connection to the VPN assistants. For this, go to the following menu:

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



Select the VPN Scenario:

VPN Scenario: IPSec - LAN-to-LAN connection ▾

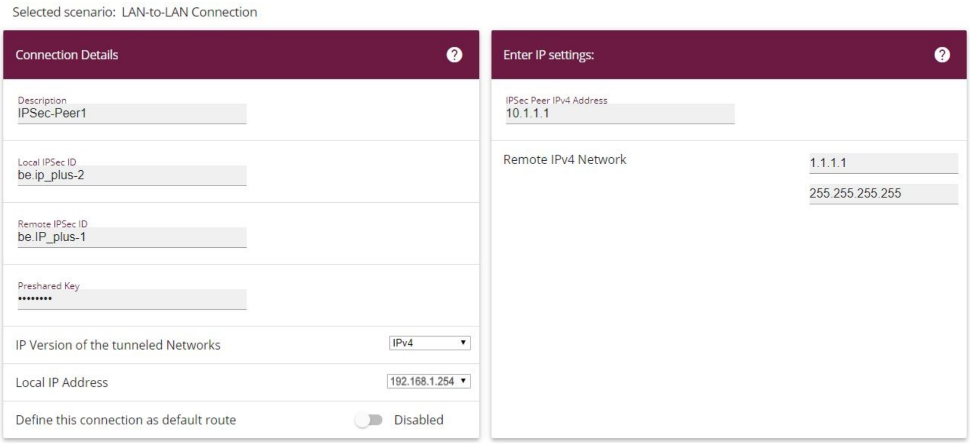
Fig. 42: **Assistants** -> **VPN** -> **VPN Connections** -> **New**

Proceed as follows:

(1) Under **VPN scenario** select `IPSec LAN-to-LAN connection`.

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

Enter the data required for the VPN connection.



Selected scenario: LAN-to-LAN Connection

Connection Details

Description: IPSec-Peer1

Local IPSec ID: be.ip_plus-2

Remote IPSec ID: be.IP_plus-1

Preshared Key: ••••••••

IP Version of the tunneled Networks: IPv4 ▾

Local IP Address: 192.168.1.254 ▾

Define this connection as default route: Disabled

Enter IP settings:

IPSec Peer IPv4 Address: 10.1.1.1

Remote IPv4 Network: 1.1.1.1 / 255.255.255.255

Fig. 43: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

Proceed as follows to configure a new VPN connection:

(1) For example, under **Description** enter `IPSec Peer1`.

(2) Enter the ID of your own IPSec gateway under **Local IPSec ID**, e.g. `be.IP_plus-2`.

(3) For example, under **Remote IPSec ID** enter `be.IP_plus-1`.

(4) Under **Preshared Key** enter, for example, `secret` for authentication. The preshared key must be identical on both sides.

(5) Select the **Local IP Address** of the gateway, for example `192.168.1.254`.

(6) Leave **Define this connection as default route** set to disabled.

(7) Under **IPSec Peer Address** enter the IP address or host name of the remote IPSec partner, e. g. `10.1.1.1`.

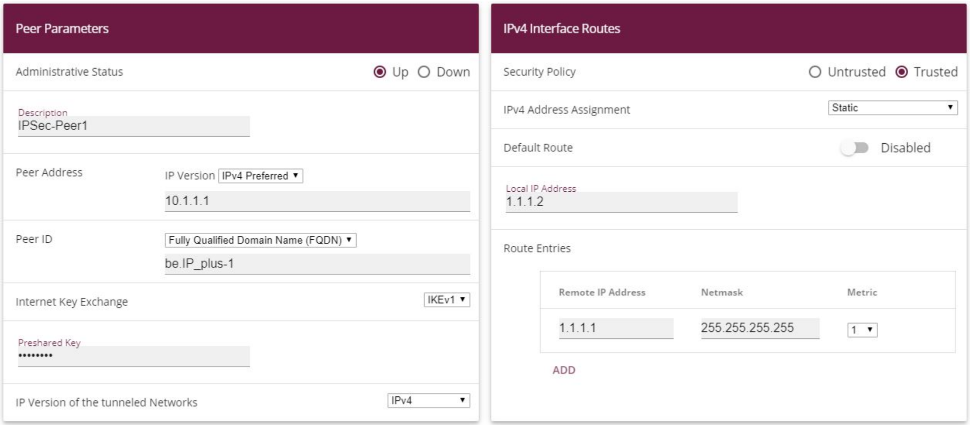
(8) Enter the destination address used for the connection under **IP Address of Remote Network** e.g. `1.1.1.1`.

(9) Under **Subnet Mask** enter the host mask, e.g. `255.255.255.255`.

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

To change the local IP address, select the following menu options:

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



Peer Parameters

Administrative Status ● Up ○ Down

Description: IPSec-Peer1

Peer Address: IP Version IPv4 Preferred ▾ 10.1.1.1

Peer ID: Fully Qualified Domain Name (FQDN) ▾ be.IP_plus-1

Internet Key Exchange: IKEv1 ▾

Preshared Key: ••••••••

IP Version of the tunneled Networks: IPv4 ▾

IPv4 Interface Routes

Security Policy ○ Untrusted ● Trusted

IPv4 Address Assignment: Static ▾

Default Route: Disabled

Local IP Address: 1.1.1.2

Route Entries

Remote IP Address	Netmask	Metric
1.1.1.1	255.255.255.255	1 ▾

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

Proceed as follows:

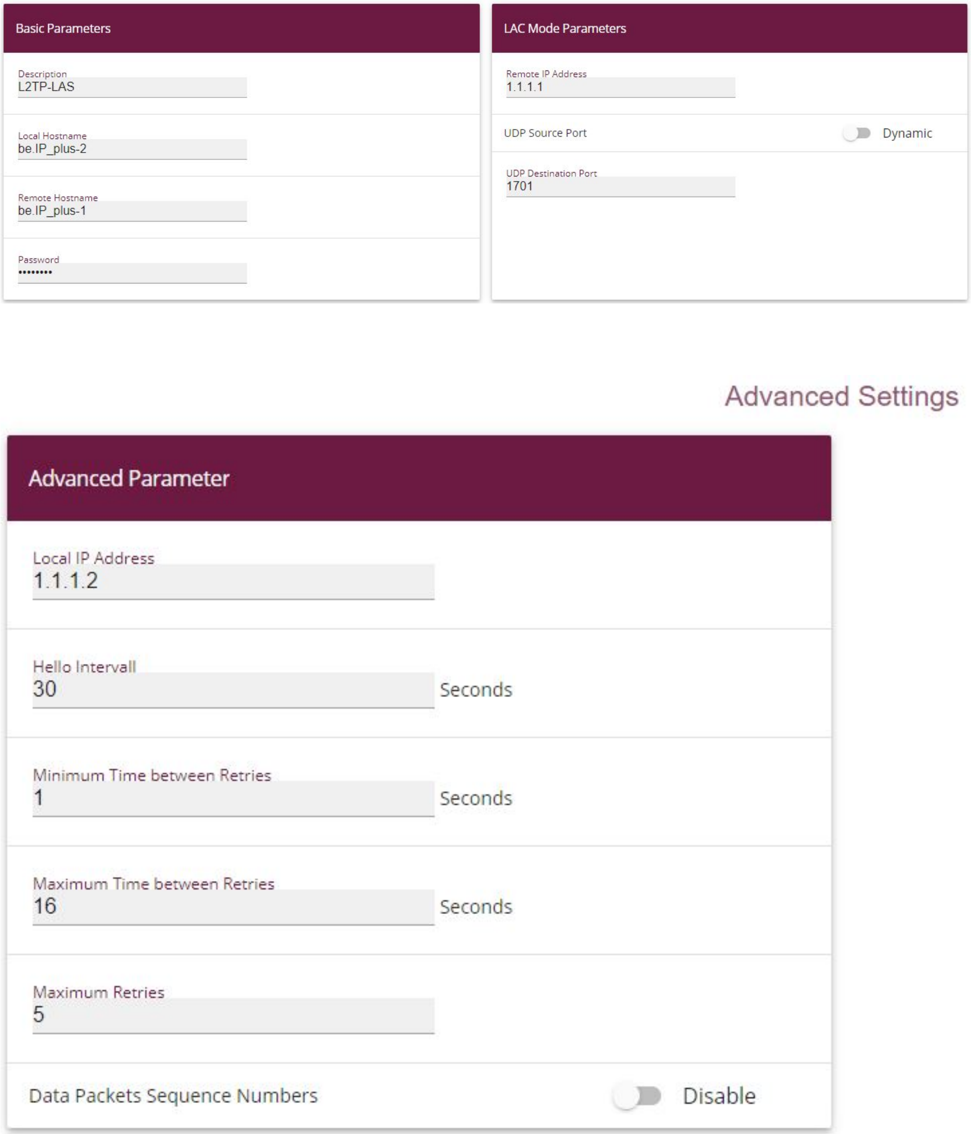
(1) Under **Local IP Address** enter, for example `1.1.1.2`.

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

Configuring the L2TP connection

To create a tunnel profile, go to the following menu:

(1) Go to **VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**.



Basic Parameters

Description
L2TP-LAS

Local Hostname
be.IP_plus-2

Remote Hostname
be.IP_plus-1

Password
••••••••

LAC Mode Parameters

Remote IP Address
1.1.1.1

UDP Source Port ○ Dynamic

UDP Destination Port
1701

Advanced Settings

Advanced Parameter

Local IP Address
1.1.1.2

Hello Intervall
30 Seconds

Minimum Time between Retries
1 Seconds

Maximum Time between Retries
16 Seconds

Maximum Retries
5

Data Packets Sequence Numbers ○ Disable

Fig. 46: **VPN**->**L2TP**->**Tunnel Profiles**->**New**

(1) For example, under **Description** enter *L2TP-LAS*.

(2) Enter the ID of your own IPSec gateway under **Local Hostname**, e.g. *be.IP_plus-2*.

(3) For example, under **Remote Hostname** enter *be.IP_plus-1*.

(4) Enter the **password**, e.g. *secret* for authentication.

(5) Enter the destination address used for the connection under **Remote IP Address** e.g. *1.1.1.1*.

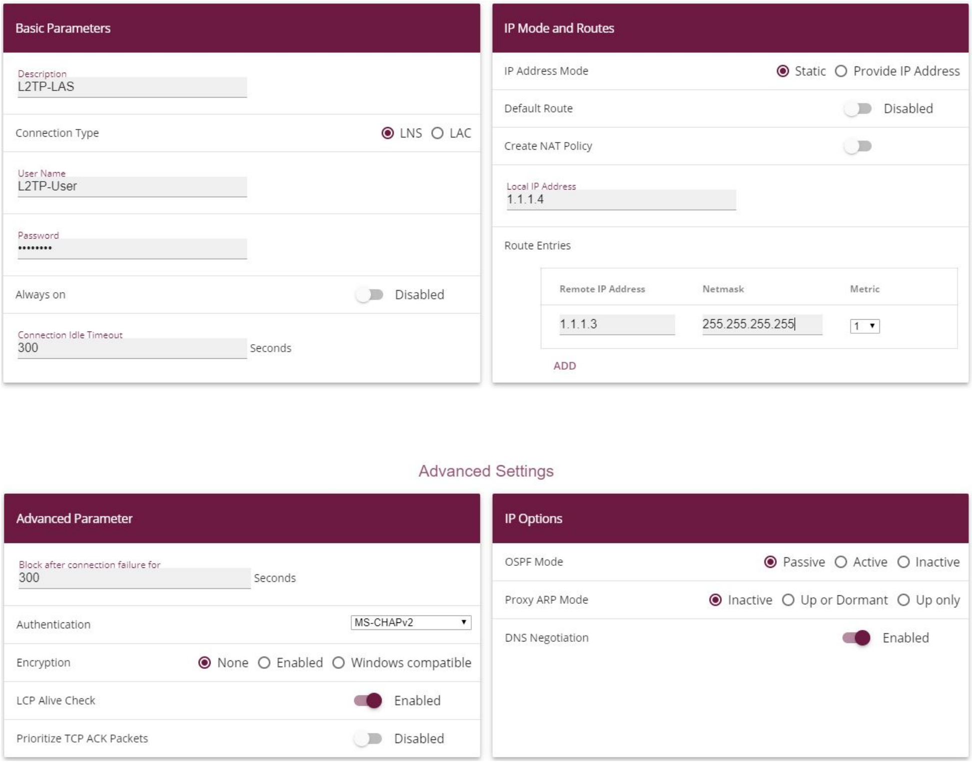
(6) Click **Advanced Settings**.

(7) Enter the **Local IP Address**, e.g. `1.1.1.2`.

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

A user must be configured in the next step. For this, go to the following menu:

(1) Go to **VPN** -> **L2TP** -> **User** -> **New**.



Basic Parameters

Description: L2TP-LAS

Connection Type: ● LNS ○ LAC

User Name: L2TP-User

Password: ••••••••

Always on: Disabled

Connection Idle Timeout: 300 Seconds

IP Mode and Routes

IP Address Mode: ● Static ○ Provide IP Address

Default Route: Disabled

Create NAT Policy

Local IP Address: 1.1.1.4

Route Entries

Remote IP Address	Netmask	Metric
1.1.1.3	255.255.255.255	1

ADD

Advanced Settings

Advanced Parameter

Block after connection failure for: 300 Seconds

Authentication: MS-CHAPv2

Encryption: ● None ○ Enabled ○ Windows compatible

LCP Alive Check: Enabled

Prioritize TCP ACK Packets: Disabled

IP Options

OSPF Mode: ● Passive ○ Active ○ Inactive

Proxy ARP Mode: ● Inactive ○ Up or Dormant ○ Up only

DNS Negotiation: Enabled

Fig. 48: **VPN**->**L2TP**->**Users**->**New**

To create a new user, proceed as follows.

(1) For example, under **Description** enter `L2TP-LAS`.

(2) Select the **Connection Type** `LNS`.

(3) Under **User Name** enter `L2TP-User` for example.

(4) Enter the **password**, e.g. `secret`.

(5) Enter the **Local IP Address**, e.g. `1.1.1.4`. To avoid conflicts with other interfaces or existing routes, the local IP address must be unique.

(6) Under **Route Entries** enter the remote IP address, e.g. `1.1.1.3` and the netmask e.g. `255.255.255.255`.

(7) Click **Advanced Settings**.

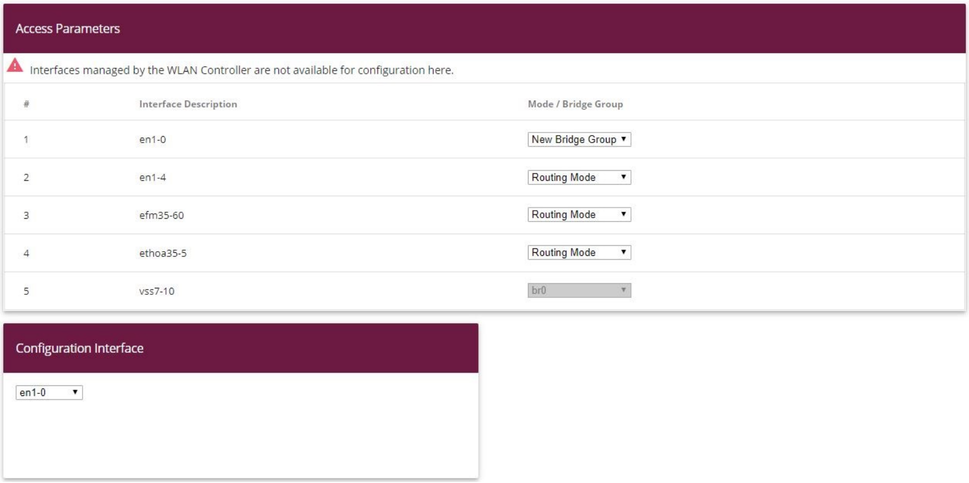
(8) Under **Encryption** click *None*. As a secure IPSec connection already exists, additional encryption is not required.

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

Configuring the bridge group

To enable bridging between the LAN interface and the L2TP interface, both interfaces must be assigned to a bridge group. For this, go to the following menu:

(1) Go to **System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**.



Access Parameters

⚠ Interfaces managed by the WLAN Controller are not available for configuration here.

#	Interface Description	Mode / Bridge Group
1	en1-0	New Bridge Group ▾
2	en1-4	Routing Mode ▾
3	efm35-60	Routing Mode ▾
4	ethoa35-5	Routing Mode ▾
5	vss7-10	br0 ▾

Configuration Interface

en1-0 ▾

Fig. 49: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**

Proceed as follows:

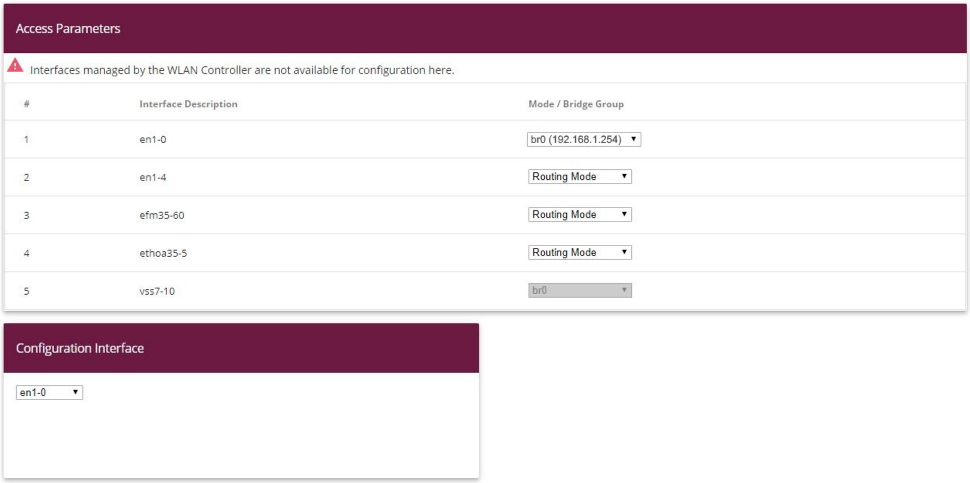
(1) Under **Mode / Bridge Group** select *New Bridge Group*. In our example, the interface *en1-0* is used as the LAN interface.

(2) Under **Configuration Interface** select *en1-0*.

(3) Confirm with **OK**. After clicking **OK**, a new bridge group is created automatically.

If no bridge group exists, the new interface uses the alias *br0* (otherwise *br1*, *br2*, etc.).

The configuration looks like this:



Access Parameters

Interfaces managed by the WLAN Controller are not available for configuration here.

#	Interface Description	Mode / Bridge Group
1	en1-0	br0 (192.168.1.254) ▾
2	en1-4	Routing Mode ▾
3	efm35-60	Routing Mode ▾
4	ethoa35-5	Routing Mode ▾
5	vss7-10	br0 ▾

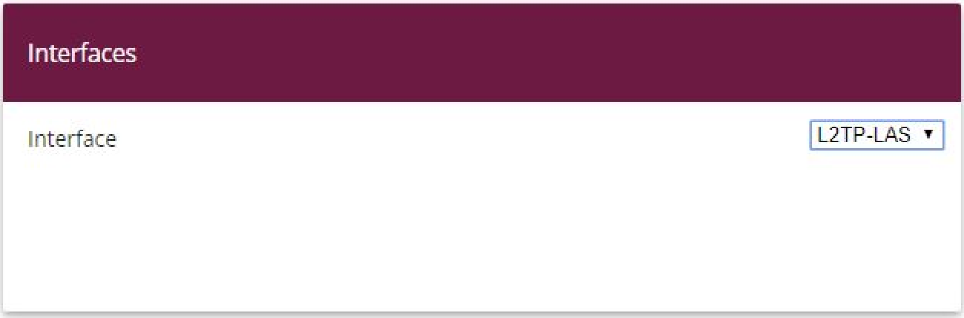
Configuration Interface

en1-0 ▾

Fig. 50: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**

Now is assigned to the newly created bridge Grupppe the L2TP interface. For this, go to the following menu:

(1) Go to **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces** -> **Add**.



Interfaces

Interface L2TP-LAS ▾

Fig. 51: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces** -> **Add**

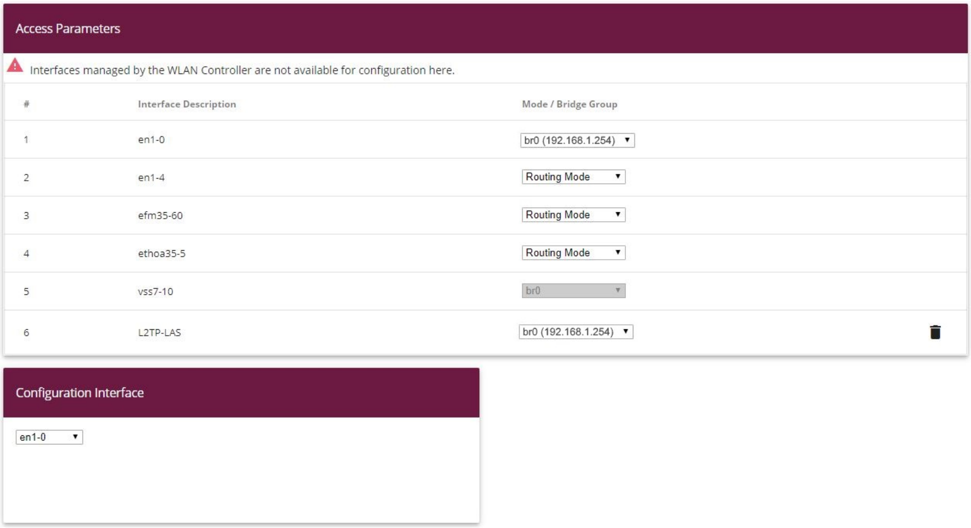
Proceed as follows:

(1) Under **Mode / Bridge Group** select the WAN-Partner *L2TP-LAS*.

(2) Confirm with **OK**.

To enable bridging between the LAN interface and the L2TP interface, both interfaces must be assigned to a bridge group. For this, go to the following menu:

(1) Go to **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**.



Access Parameters

⚠ Interfaces managed by the WLAN Controller are not available for configuration here.

#	Interface Description	Mode / Bridge Group
1	en1-0	br0 (192.168.1.254)
2	en1-4	Routing Mode
3	efm35-60	Routing Mode
4	ethoa35-5	Routing Mode
5	vss7-10	br0
6	L2TP-LAS	br0 (192.168.1.254)

Configuration Interface

en1-0

Fig. 52: **System Management** -> **Interface Mode / Bridge Groups** ->**Interfaces**

Proceed as follows:

(1) Under **Mode / Bridge Group** select `br0 (192.168.1.254)`.

(2) Confirm with **OK**. After clicking **OK**, a new bridge group is created automatically.

This concludes the configuration of the **bintec be.IP plus** gateway as location B.

3.4 Overview of configuration steps

Configuring location A

Field	Menu	Value
VPN Scenario	**Assistants** -> **VPN** -> **VPN Connections** -> **New**	*IPSec - LAN-to-LAN connection*

Configuring VPN assistants

Field	Menu	Value
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *IPSec-Peer1*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *be.IP_plus-1*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *be.IP_plus-2*
Preshared Key	**Assistants** -> **VPN** -> **VPN Connec-**	e.g. *secret*

Field	Menu	Value
	tions -> Next	
Local IP Address	**Assistants -> VPN -> VPN Connections -> Next**	e.g. *192.168.1.253*
IPSec Peer Address	**Assistants -> VPN -> VPN Connections -> Next**	e.g. *10.1.1.4*
IP Address of Remote Network	**Assistants -> VPN -> VPN Connections -> Next**	e.g. *1.1.1.2*
Subnet Mask	**Assistants -> VPN -> VPN Connections -> Next**	e.g. *255.255.255.255*

Changing the local IP address

Field	Menu	Value
Local IP Address	**VPN -> IPSec -> IPSec Peers ->** ✎	e.g. *1.1.1.1*

Configuring tunnel profiles

Field	Menu	Value
Description	**VPN -> L2TP -> Tunnel Profiles -> New**	e.g. *L2TP-LAC*
Local Hostname	**VPN -> L2TP -> Tunnel Profiles -> New**	e.g. *be.IP_plus-1*
Remote Hostname	**VPN -> L2TP -> Tunnel Profiles -> New**	e.g. *be.IP_plus-2*
Password	**VPN -> L2TP -> Tunnel Profiles -> New**	e.g. *secret*
Remote IP Address	**VPN -> L2TP -> Tunnel Profiles -> New**	e.g. *1.1.1.2*
Local IP Address	**VPN -> L2TP -> Tunnel Profiles -> New**	e.g. *1.1.1.1*

Configuring new users

Field	Menu	Value
Description	**VPN -> L2TP -> Users -> New**	e.g. *L2TP-LAC*
Connector Type	**VPN -> L2TP -> Users -> New**	*LAC*
Tunnel Profile	**VPN -> L2TP -> Users -> New**	*L2TP-LAC*
User Name	**VPN -> L2TP -> Users -> New**	e.g. *L2TP-User*
Password	**VPN -> L2TP -> Users -> New**	e.g. *secret*
Local IP Address	**VPN -> L2TP -> Users -> New**	e.g. *1.1.1.3*

Field	Menu	Value
Remote IP Address	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *1.1.1.4*
Subnet Mask	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *255.255.255.255*
Encryption	**VPN** -> **L2TP** -> **Users** -> **New**	*None*

Configuring bridge groups

Field	Menu	Value
Mode / Bridge Group	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**	*New Bridge Group*
Configuration Interface	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**	*en1-0*

Assigning a L2TP interface

Field	Menu	Value
Interface	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces** -> **Add**	*L2TP-LAC*
Mode / Bridge Group	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**	*br0(192.168.1.253)*

Configuring location B

Field	Menu	Value
VPN Scenario	**Assistants** -> **VPN**-> **VPN Connections** -> **New**	*IPSec - LAN-to-LAN connection*

Configuring VPN assistants

Field	Menu	Value
Description	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *IPSec-Peer1*
Local IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *be.IP_plus-2*
Remote IPSec ID	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *be.IP_plus-1*
Preshared Key	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *secret*
Local IP Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *192.168.1.254*
IPSec Peer Address	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *10.1.1.1*

Field	Menu	Value
IP Address of Remote Network	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *1.1.1.1*
Subnet Mask	**Assistants** -> **VPN** -> **VPN Connections** -> **Next**	e.g. *255.255.255.255*

Changing the local IP address

Field	Menu	Value
Local IP Address	**VPN** -> **IPSec** -> **IPSec Peers** -> ✎	e.g. *1.1.1.2*

Configuring tunnel profiles

Field	Menu	Value
Description	**VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**	e.g. *L2TP-LAS*
Local Hostname	**VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**	e.g. *be.IP_plus-2*
Remote Hostname	**VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**	e.g. *be.IP_plus-1*
Password	**VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**	e.g. *secret*
Remote IP Address	**VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**	e.g. *1.1.1.1*
Local IP Address	**VPN** -> **L2TP** -> **Tunnel Profiles** -> **New**	e.g. *1.1.1.2*

Configuring new users

Field	Menu	Value
Description	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *L2TP-LAS*
Connector Type	**VPN** -> **L2TP** -> **Users** -> **New**	*LNS*
User Name	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *L2TP-User*
Password	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *secret*
Local IP Address	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *1.1.1.4*
Remote IP Address	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *1.1.1.3*
Subnet Mask	**VPN** -> **L2TP** -> **Users** -> **New**	e.g. *255.255.255.255*
Encryption	**VPN** -> **L2TP** -> **Users** -> **New**	*None*

Configuring bridge groups

Field	Menu	Value
Mode / Bridge Group	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**	*New Bridge Group*
Configuration Interface	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**	*en1-0*

Assigning a L2TP interface

Field	Menu	Value
Interface	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces** -> **Add**	*L2TP-LAS*
Mode / Bridge Group	**System Management** -> **Interface Mode / Bridge Groups** -> **Interfaces**	*br0(192.168.1.254)*

Chapter 4 Security - Stateful Inspection Firewall (SIF)

4.1 Introduction

The configuration of the SIF (Stateful Inspection Firewall) with a **bintec be.IP** is described in the following chapters.

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

Only certain Internet services are to be available for the staff of a company (HTTP, HTTPS, FTP, DNS). The gateway should operate as a DNS proxy, which means that the clients use the gateway as a DNS server. Only the system administrator and the director should be able to established an HTTP and a Telnet connection to the gateway. In addition, the director must be able to use all services in the Internet. All other data traffic will be blocked.

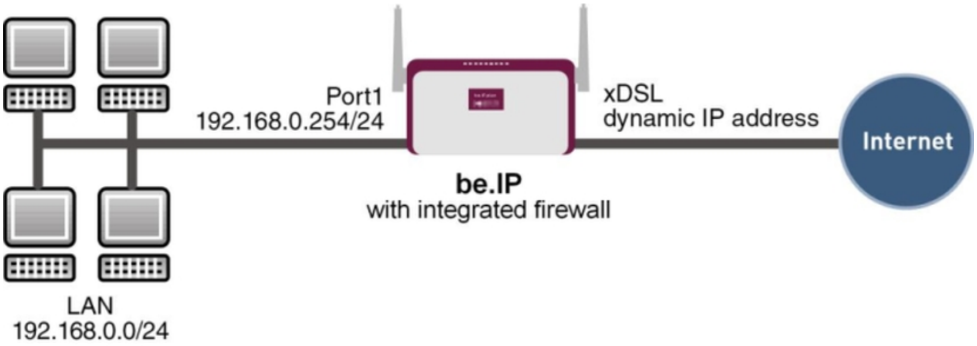


Fig. 53: Example scenario SIF

Requirements

The following are required for the configuration:

- A **bintec be.IP** gateway.
- Boot image from version 10.1.1
- Internet connection
- Your LAN must be connected to one of ports **1** to **4** on the gateway.

4.2 Firewall configuration

⚠ **Important**

An incorrect configuration of the firewall can significantly disrupt the functionality of the gateway or drop the connections.

The usual principle for firewalls also applies: Everything that is not explicitly allowed is prohibited.

This means accurate planning of the filter rules and filter rule chain is necessary to ensure correct operation.

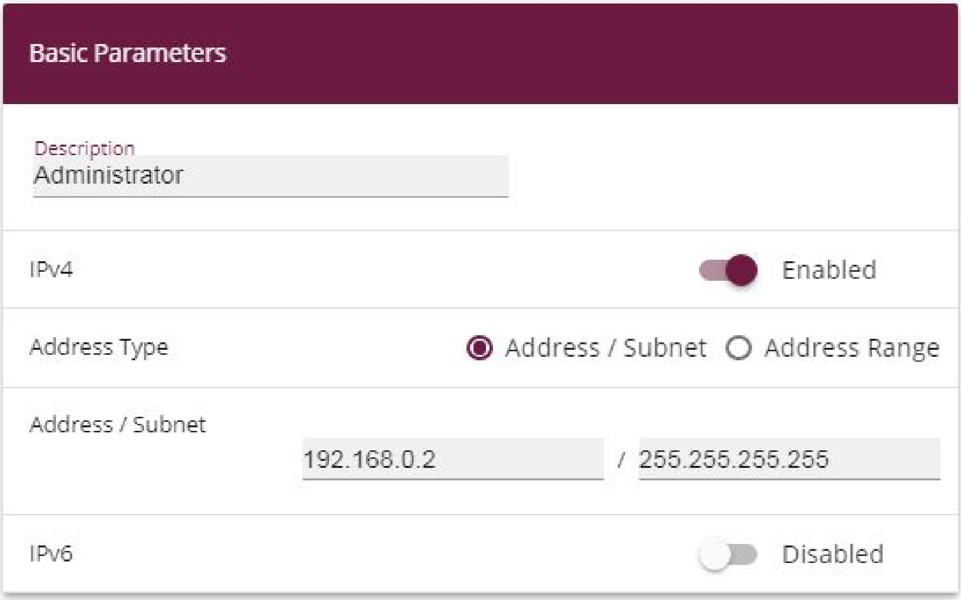
4.2.1 Configuring aliases for IP addresses and network address

Address alias

You must create aliases for your users and your network so that you can identify users and the network when configuring the filter rules.

Go to the following menu to create aliases:

(1) Go to **Firewall** -> **Addresses** -> **Address List** -> **New**.



Basic Parameters

Description
Administrator

IPv4 Enabled

Address Type ● Address / Subnet ○ Address Range

Address / Subnet 192.168.0.2 / 255.255.255.255

IPv6 Disabled

Fig. 54: **Firewall** -> **Addresses** -> **Address List**-> **New**

Proceed as follows to set up an alias for the administrator:

(1) Enter the name of the alias under **Description**, e.g. `Administrator`.

(2) Under **Address Type** select `Address / Subnet`

(3) Under **Address / Subnet** enter the IP address and corresponding subnet mask,e.g. `192.168.0.2` and `255.255.255.255`.

(4) Confirm with **OK**.

Proceed in the same way as for configuring the aliases for the director (`Director`) for your gateway (`be.IP`) and for the network (`Network Internal`).

Proceed as follows to set up an alias for the director:

(1) Enter the name of the alias under **Description**, e.g. `Director`.

(2) Under **Address Type** select `Address / Subnet`

(3) Under **Address / Subnet** enter the IP address and corresponding subnet mask,e.g. `192.168.0.3` and `255.255.255.255`.

(4) Confirm with **OK**.

Proceed as follows to set up an alias for your gateway:

(1) Enter the name of the alias under **Description**, e.g. `be.IP`.

(2) Under **Address Type** select `Address / Subnet`

(3) Under **Address / Subnet** enter the IP address and corresponding subnet mask,e.g.

192.168.0.254 and *255.255.255.255*.

(4) Confirm with **OK**.

Proceed as follows to set up an alias for the internal network:

(1) Enter the name of the alias under **Description**, e.g. *Network Internal*.

(2) Under **Address Type**select *Address / Subnet*

(3) Under **Address / Subnet** enter the IP address and corresponding subnet mask,e.g. *192.168.0.0* and *255.255.255.0*.

(4) Confirm with **OK**.

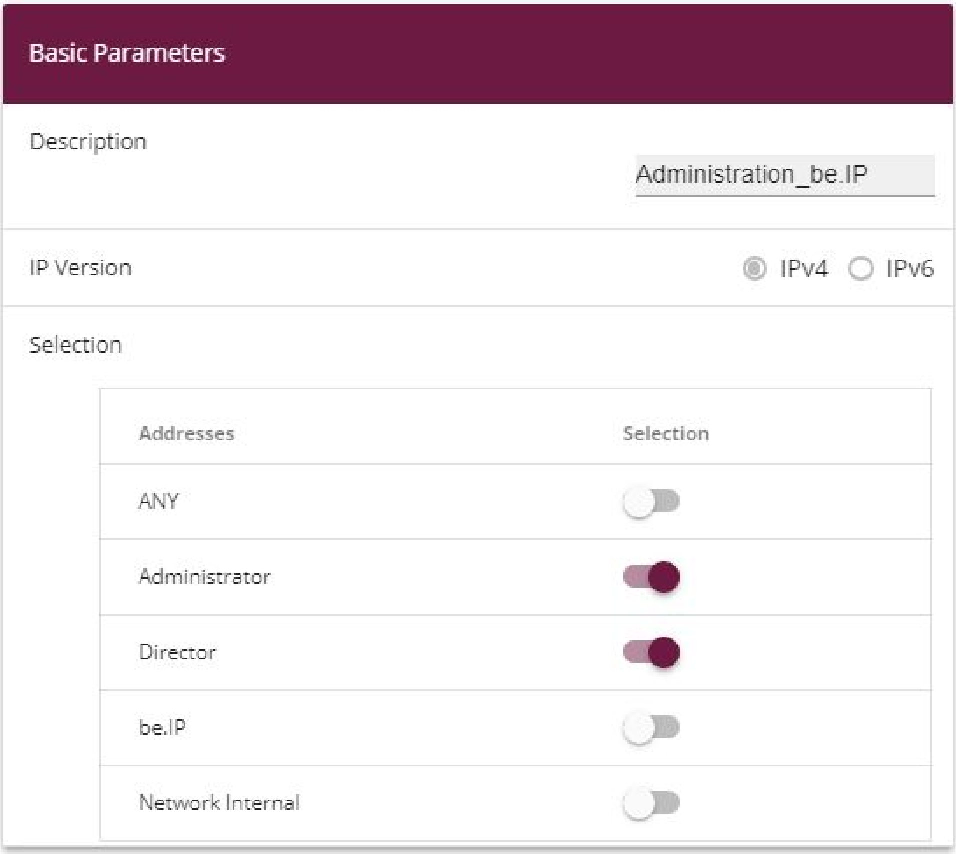
Address groups

You can group together several aliases into groups to make it easier to configure the filter rules.

Since the administrator and the director can access the gateway over HTTP and Telnet, these are grouped together.

Go to the following menu to create a group:

(1) Go to **Firewall** -> **Addresses** -> **Groups**-> **New**.



Basic Parameters

Description: Administration_be.IP

IP Version: ● IPv4 ○ IPv6

Selection

Addresses	Selection
ANY	○
Administrator	●
Director	●
be.IP	○
Network Internal	○

Fig. 55: **Firewall** -> **Addresses** ->**Groups** -> **New**

Proceed as follows to create a group:

(1) Enter the name of the group under **Description**, e.g. *`Administration_be.IP`*.

(2) Select the **Addresses** to be included in the group, in this example *`Administrator`* and *`Director`*.

(3) Confirm with **OK**.

4.2.2 Configuring service sets

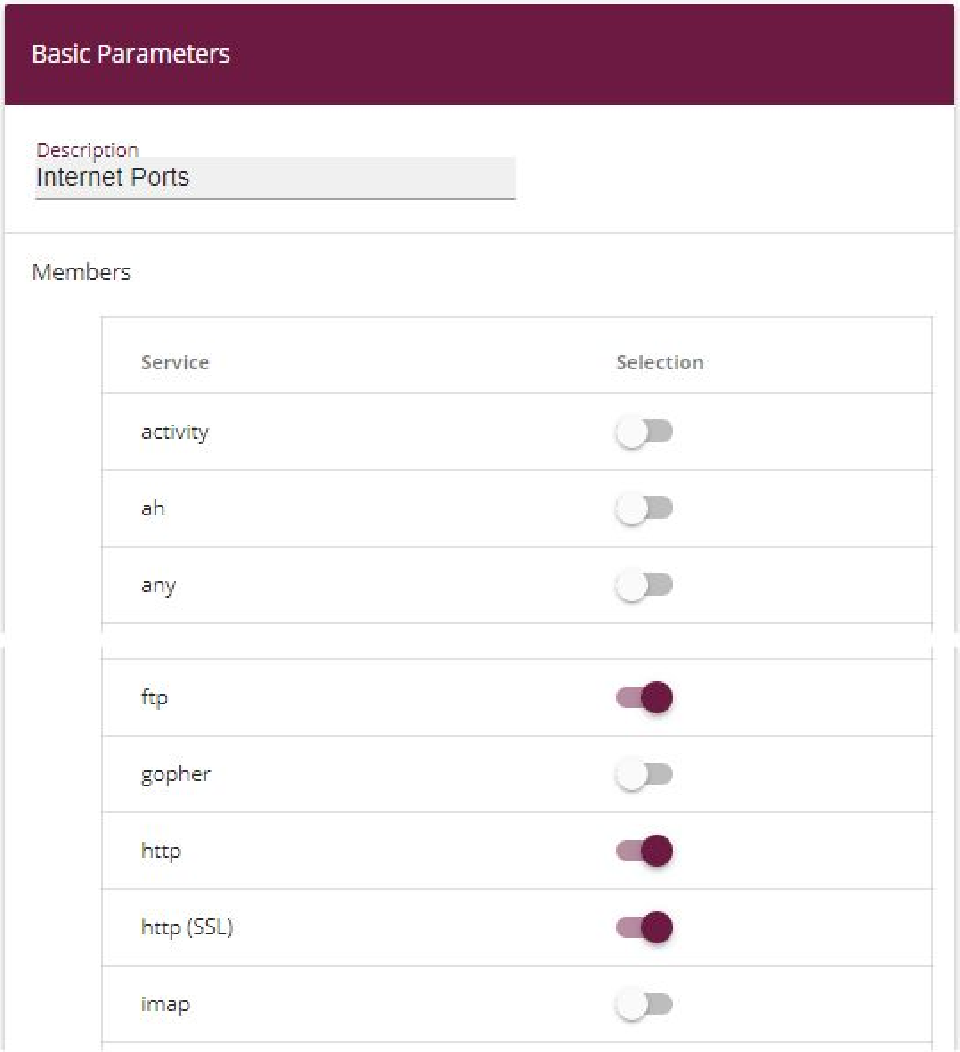
You must create aliases for the required services in the **Firewall**-> **Services** menu so that you can identify specific services when configuring the filter rules. A large number of frequently used services that are pre-configured already exists. If you require a service that is not included in this list, you must create a new service.

You can group together several services into groups to make it easier to configure the filter rules.

Since the users in this network can use HTTP, HTTPS and FTP services, you can group these together.

Go to the following menu to create a group:

(1) Go to **Firewall** -> **Services** -> **Groups**-> **New**.



Basic Parameters

Description
Internet Ports

Members

Service	Selection
activity	○
ah	○
any	○
ftp	●
gopher	○
http	●
http (SSL)	●
imap	○

Fig. 56: **Firewall** -> **Services** ->**Groups**-> **New**

Proceed as follows to create a group:

(1) Enter the name of the group under **Description**, e.g. `Internet Ports`.

(2) Select the services to be included in the group, in this example `ftp`, `http` and `http (SSL)`.

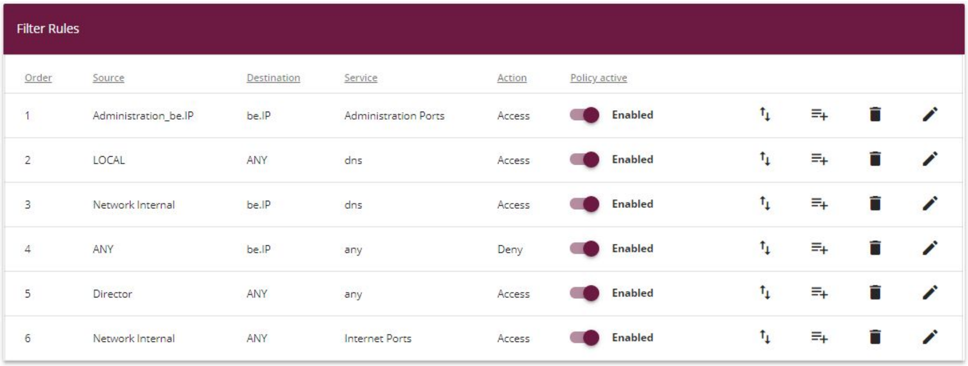
(3) Confirm with **OK**.

Group together HTTP and Telnet in the `Administration Ports` group for the administration of the gateway.

4.2.3 Configuring filter rules

Once you have completed the configuration of the alias names for IP addresses and services, you can define the filter rules in the **Firewall** -> **Policies** menu.

A complete filter rule chain looks like this:



Filter Rules

Order	Source	Destination	Service	Action	Policy active
1	Administration_be.IP	be.IP	Administration Ports	Access	Enabled
2	LOCAL	ANY	dns	Access	Enabled
3	Network Internal	be.IP	dns	Access	Enabled
4	ANY	be.IP	any	Deny	Enabled
5	Director	ANY	any	Access	Enabled
6	Network Internal	ANY	Internet Ports	Access	Enabled

Fig. 57: **Firewall** -> **Policies** ->**Filter Rules**

Relevant fields in the Filter Rules menu

Field	Meaning
Source Location	Source address for which this rule applies.
Destination	Destination address for which this rule applies.
Service	Service for which this rule applies.
Action	Determines whether data traffic is allowed or rejected.

⚠ **Important**

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 Internet and/or the gateway.

First configure a rule that allows the administrator and director to access the gateway over HTTP and Telnet. You must define this rule first otherwise communication with the **GUI** will be impossible.

Go to the following menu to create a new rule:

(1) Go to **Firewall** -> **Policies** -> **Filter Rules**.

(2) Click **New** to create a new rule.

(3) Under **Source** select the group *Administration_be.IP*.

(4) Under **Destination**, select *be.IP*.

(5) Select the **Service** *Administration Ports*.

(6) Under **Action** select *Access*.

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

Next configure a rule that allow the gateway to forward DNS queries to the Internet.

Go to the following menu to create a new rule:

(1) Go to **Firewall** -> **Policies** -> **Filter Rules**.

(2) Click **New** to create a new rule.

(3) Under **Source** select *LOCAL*.

(4) Set **Destination** to *ANY*.

(5) Select the **Service** *dns*.

(6) Under **Action** select *Access*.

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

Configure a rule that allows the entire network to forward DNS queries to the gateway.

Go to the following menu to create a new rule:

(1) Go to **Firewall** -> **Policies** -> **Filter Rules** .

(2) Click **New** to create a new rule.

(3) Under **Source** select *Network_Internal*.

(4) Under **Destination**, select *be.IP*.

(5) Select the **Service** *dns*.

(6) Under **Action** select *Access*.

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

Now configure a rule that rejects all other queries to the gateway.

Go to the following menu to create a new rule:

(1) Go to **Firewall** -> **Policies** -> **Filter Rules**.

(2) Click **New** to create a new rule.

(3) Set **Source** to *ANY*.

(4) Under **Destination**, select *be.IP*.

(5) Select the **Service** *any*.

(6) Under **Action** select *Deny*.

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

Now configure a rule that allows the director access to all internet services.

(1) Go to **Firewall** -> **Policies** -> **Filter Rules**.

(2) Click **New** to create a new rule.

(3) Set **Source** to *Director*.

(4) Set **Destination** to *ANY*.

(5) Select the **Service** *any*.

(6) Under **Action** select *Access*.

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

Finally configure a rule that allows the internal network to use the HTTP, HTTPS and FTP services.

(1) Go to **Firewall** -> **Policies** -> **Filter Rules**.

(2) Click **New** to create a new rule.

(3) Under **Source** select *Network_Internal*.

(4) Set **Destination** to *ANY*.

(5) Select the **Service** *Internet Ports*.

(6) Under **Action** select *Access*.

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

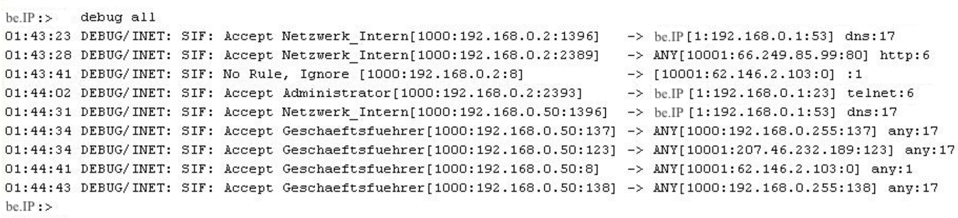
Click **Save Configuration** and confirm with **OK** to save the configuration permanently.

4.3 Result

You have now configured the firewall so that the gateway can forward DNS queries to the Internet and the internal network can access HTTP, HTTPS and FTP services. The administrator also has access to the gateway and the director can use all internet services. All other data traffic is prevented by the gateway.

4.4 Checking the configuration

If you enter `debug all` on the shell for the gateway you can track how the gateway allows or denies data traffic according to the filter rules.



```
be.IP:>   debug all
01:43:23 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.2:1396]    -> be.IP[1:192.168.0.1:53] dns:17
01:43:28 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.2:2389]    -> ANY[10001:66.249.85.99:80] http:6
01:43:41 DEBUG/INET: SIF: No Rule, Ignore [1000:192.168.0.2:8]             -> [10001:62.146.2.103:0] :1
01:44:02 DEBUG/INET: SIF: Accept Administrator[1000:192.168.0.2:2393]      -> be.IP [1:192.168.0.1:23] telnet:6
01:44:31 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.50:1396]   -> be.IP [1:192.168.0.1:53] dns:17
01:44:34 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:137] -> ANY[1000:192.168.0.255:137] any:17
01:44:34 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:123] -> ANY[10001:207.46.232.189:123] any:17
01:44:41 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:8]   -> ANY[10001:62.146.2.103:0] any:1
01:44:43 DEBUG/INET: SIF: Accept Geschaeftsfuehrer[1000:192.168.0.50:138] -> ANY[1000:192.168.0.255:138] any:17
be.IP:>
```

This debug extract shows that a ping attempt from 192.168.0.2 to the address 62.146.2.103 was rejected. DNS queries or a Telnet connection, for example, from the director were allowed.

4.5 Overview of configuration steps

Aliases for IP addresses and network address

Field	Menu	Value
Description	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *Administrator*
Address Type	**Firewall** -> **Addresses** -> **Address List** -> **New**	*Address / Subnet*
Address / Subnet	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *192.168.0.2* with *255.255.255.255*
Description	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *Director*
Address Type	**Firewall** -> **Addresses** -> **Address List** -> **New**	*Address / Subnet*
Address / Subnet	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *192.168.0.3* with *255.255.255.255*
Description	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *be.IP*
Address Type	**Firewall** -> **Addresses** -> **Address List** -> **New**	*Address / Subnet*
Address / Subnet	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *192.168.0.254* with *255.255.255.255*
Description	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *Network Internal*
Address Type	**Firewall** -> **Addresses** -> **Address List** -> **New**	*Address / Subnet*
Address / Subnet	**Firewall** -> **Addresses** -> **Address List** -> **New**	e.g. *192.168.0.0* with *255.255.255.0*

Address groups

Field	Menu	Value
Description	**Firewall** -> **Addresses** ->**Groups** -> **New**	e.g. *Administration_be.IP*
Selection	**Firewall** -> **Addresses** ->**Groups** -> **New**	e.g. *Administrator* and *Director*

Service Sets

Field	Menu	Value
Description	**Firewall** -> **Services** ->**Groups** -> **New**	e.g. *Internet Ports*
Members	**Firewall** -> **Services** ->**Groups** -> **New**	e.g. *http*, *http (SSL)* and *ftp*
Description	**Firewall** -> **Services** ->**Groups** -> **New**	e.g. *Administration Ports*
Members	**Firewall** -> **Services** ->**Groups** -> **New**	e.g. *http* and *telnet*

Filter Rules

Field	Menu	Value
Source Location	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Administration_be.IP*
Destination	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*be.IP*
Service	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Administration Ports*
Action	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Access*
Source Location	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*LOCAL*
Destination	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*ANY*
Service	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*dns*
Action	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Access*
Source Location	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Network_Internal*
Destination	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*be.IP*
Service	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*dns*
Action	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Access*
Source Location	**Firewall** -> **Policies** -> **Filter**	*ANY*

Field	Menu	Value
	Rules -> **New**	
Destination	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*be.IP*
Service	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*any*
Action	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Deny*
Source Location	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Director*
Destination	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*ANY*
Service	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*any*
Action	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Access*
Source Location	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Network_Internal*
Destination	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*ANY*
Service	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Internet Ports*
Action	**Firewall** -> **Policies** -> **Filter Rules** -> **New**	*Access*

Chapter 5 Security - VPN connection via a SMS PASSCODE server

5.1 Introduction

This workshop describes the VPN IPSec Client connection of the **bintec Secure IPSec Cliens** to a bintec VPN gateway using an additional one-time password authentication. This is notified to the user when the connection is being set up in the form of a SMS (IPSec one-time password). The users and their mobile telephone numbers are managed in Active Directory on Windows Server 2008, and a bintec VPN gateway (e.g. **bintec be.IP**) is used for VPN IPSec authentication purposes. The one-time password software of **SMS PASSCODE** accesses the Active Directory in order to send the one-time passwords by SMS and authenticates the user by using the RADIUS server (NPS) integrated in Windows Server 2008.

The **GUI** (Graphical User Interface) is used here for configuring the bintec VPN gateway.

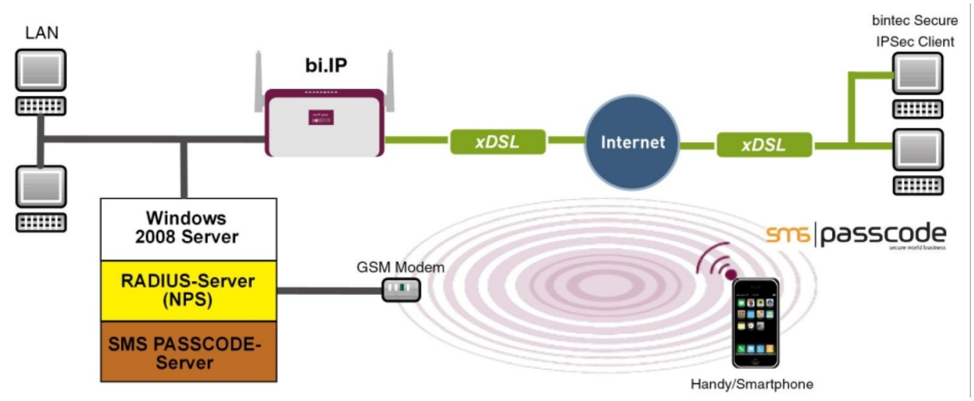


Fig. 58: Example scenario

Requirements

- A bintec VPN gateway (e.g. **bintec be.IP** Version 10.1.1) which is accessible on the Internet via its IP address or via DNS
- A Windows Server (e.g. Windows Server 2008 R2) with installed Active Directory role and available Network Policy Server (NPS/RADIUS server)
- One-time password software of **SMS PASSCODE** Version 6 with compatible GSM mo-

dem/SIM card (for more information see *http://www.smspasscode.com*)

- At least one **bintec Secure IPSec Client**

5.2 Configuration

5.2.1 Information during installation and configuration of the SMS PASSCODE server

This section of the workshop provides some information regarding the installation and configuration of the **SMS PASSCODE** server. The **SMS PASSCODE** Administration Manual should be consulted first of all. The individual installation steps and configuration of the RADIUS server are both explained in great detail in this document (see *http://www.smspasscode.com*).

5.2.2 Preparation for installing the SMS PASSCODE server

A RADIUS server (Windows Server 2003/2008 component) must be installed prior to installing the **SMS PASSCODE** server. For Windows Server 2008, as used in this example, the RADIUS server is installed by adding the NPS role or the **Network Policy Server (Windows Server 2008 (R2))**.

Prior to installing the **SMS PASSCODE** software, a GSM modem must be connected to the Windows Server in order to send SMS messages. **SMS PASSCODE** supports GSM modems by Cinterion (previously Siemens), such as the MC35i, MC52i, MC55i, TC65 or MC75 models.

A SIM card is required for the GSM modem in order to send SMS messages.

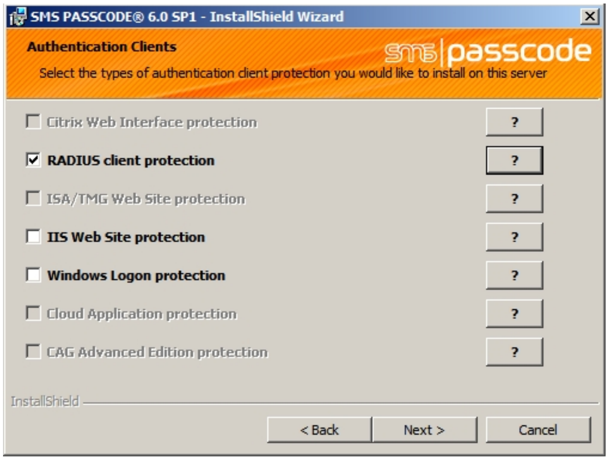
5.2.3 Installation of SMS PASSCODE server

When you actually install the **SMS PASSCODE** server software, the **Simple Installation** chapter in the **SMS PASSCODE** Administration Manual should be used as reference. Simple installation involves all components being installed on a single server.

The serial COM interface of the GSM modem must be selected in the Installation Wizard. The SIM card PIN can also be entered in this dialog box.

The authentication types must be selected in a subsequent step of the Installation Wizard.

In order to be able to connect the bintec VPN gateway at a later point, `RADIUS client protection` must be selected in this scenario.



Authentication Clients

Select the types of authentication client protection you would like to install on this server

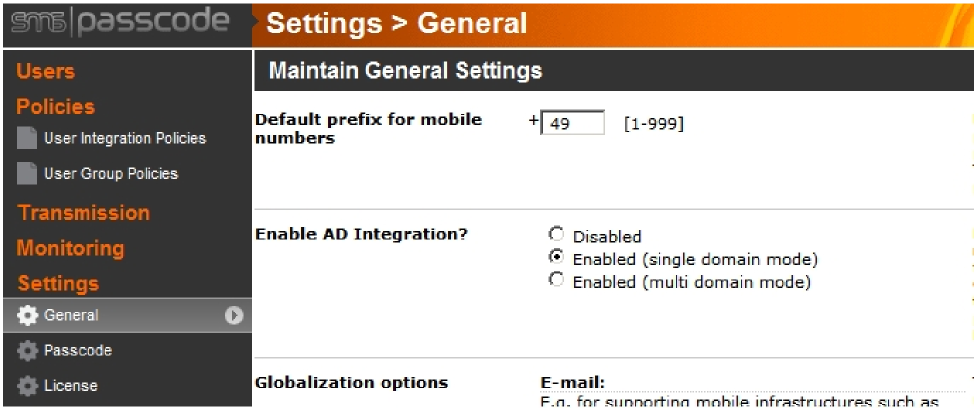
- ☐ Citrix Web Interface protection ?
- ☑ RADIUS client protection ?
- ☐ ISA/TMG Web Site protection ?
- ☐ IIS Web Site protection ?
- ☐ Windows Logon protection ?
- ☐ Cloud Application protection ?
- ☐ CAG Advanced Edition protection ?

Fig. 59: **SMS PASSCODE**

5.2.4 Configuration of Web Administration Tool

Configuration using the Web Administration Tool may commence following the successful installation of the **SMS PASSCODE** server. **SMS PASSCODE** offers separate user administration or access to the Microsoft Windows Server **Active Directory**. In this scenario, the users should use the **Active Directory** which is added to a separate user group for this purpose, e.g. **SMS Passcode Users**. Please note that a mobile telephone number must be stored for each user.

`AD Integration` is enabled in the **Settings** -> **General** menu in order for the **SMS PASSCODE** server to access the **SMS Passcode Users** user group of the **Active Directory**.



Settings > General

Maintain General Settings

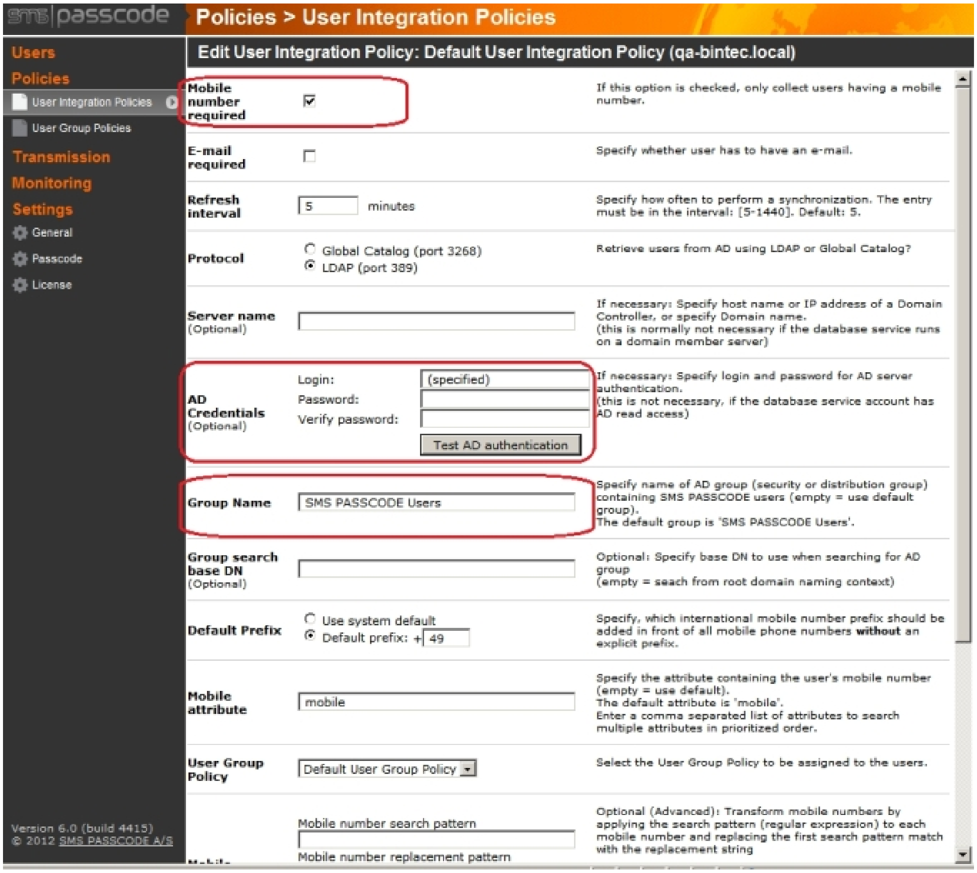
Default prefix for mobile numbers +49 [1-999]

Enable AD Integration?
○ Disabled
● Enabled (single domain mode)
○ Enabled (multi domain mode)

Globalization options **E-mail:**
E.g. for supporting mobile infrastructures such as

Fig. 60: **Settings** -> **General**

Other settings can then be made in the **Policies** -> **User Integration Policies** menu in order to access the **Active Directory** users.



Policies > User Integration Policies

Edit User Integration Policy: Default User Integration Policy (qa-bintec.local)

Mobile number required	☑	If this option is checked, only collect users having a mobile number.
E-mail required	□	Specify whether user has to have an e-mail.
Refresh interval	5 minutes	Specify how often to perform a synchronization. The entry must be in the interval: [5-1440]. Default: 5.
Protocol	○ Global Catalog (port 3268) ● LDAP (port 389)	Retrieve users from AD using LDAP or Global Catalog?
Server name (Optional)		If necessary: Specify host name or IP address of a Domain Controller, or specify Domain name. (this is normally not necessary if the database service runs on a domain member server)
AD Credentials (Optional)	Login: (specified) Password: Verify password: Test AD authentication	If necessary: Specify login and password for AD server authentication. (this is not necessary, if the database service account has AD read access)
Group Name	SMS PASSCODE Users	Specify name of AD group (security or distribution group) containing SMS PASSCODE users (empty = use default group). The default group is 'SMS PASSCODE Users'.
Group search base DN (Optional)		Optional: Specify base DN to use when searching for AD group (empty = seach from root domain naming context)
Default Prefix	○ Use system default ● Default prefix: + 49	Specify, which international mobile number prefix should be added in front of all mobile phone numbers **without** an explicit prefix.
Mobile attribute	mobile	Specify the attribute containing the user's mobile number (empty = use default). The default attribute is 'mobile'. Enter a comma separated list of attributes to search multiple attributes in prioritized order.
User Group Policy	Default User Group Policy	Select the User Group Policy to be assigned to the users.
	Mobile number search pattern Mobile number replacement pattern	Optional (Advanced): Transform mobile numbers by applying the search pattern (regular expression) to each mobile number and replacing the first search pattern match with the replacement string

Fig. 61: **Policies** -> **User Integration Policies**

(1) Enable the `Mobile number required` option.

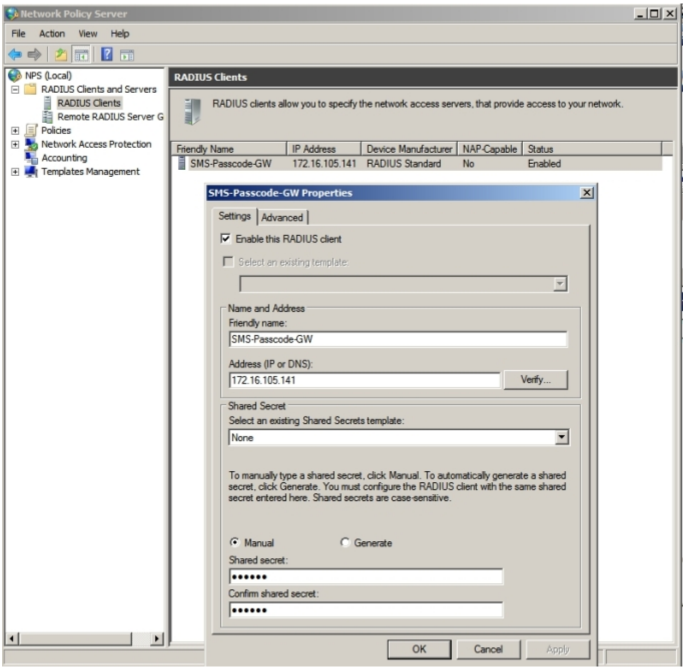
(2) Define the **Access Data** for the **Active Directory** and the **User Group** of **SMS PASSCODE** users.

A more precise description of the **Active Directory** integration of the **SMS PASSCODE** server can be found in the **SMS PASSCODE** Administration Manual.

5.2.5 Configuration of RADIUS server to connect the VPN gateway

The bintec VPN gateway is connected by using the RADIUS server which is already installed (NPS server role in Windows Server 2008). A RADIUS client (= bintec VPN gateway) is connected to the RADIUS server by using the Microsoft Management Console:

- **Internet Authentication Service (IAS)** must be used for Windows Server 2003.
- The Microsoft Management Console is used for **Network Policy Server (NPS)** when using Windows Server 2008.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
SMS-Passcode-GW	172.16.105.141	RADIUS Standard	No	Enabled

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: SMS-Passcode-GW

Address (IP or DNS): 172.16.105.141

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••

Confirm shared secret: ••••••

Fig. 62: **Network Policy Server (NPS)**

(1) Activate the `Enable this RADIUS client` option.

(2) Enter a description of the bintec VPN gateway under **Friendly name**, e.g. *`SMS Passcode-GW`*.

(3) Enter the **IP Address** or **Host Name** of the bintec VPN gateway, e.g. *`172.16.105.141`*.

(4) Enter a **Password** for the RADIUS communication with the VPN gateway, e.g. *`supersecret`*.

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

5.2.6 Configuration of the VPN gateway

In this scenario as regards the VPN configuration on the bintec gateway, an IPSec peer configuration entry is created which allows the simultaneous connection of multiple clients (IPSec Multi-User). Following the IPSec pre-shared key authentication, the one-time authentication between the bintec VPN client and the **SMS PASSCODE** server is completed via the RADIUS server.

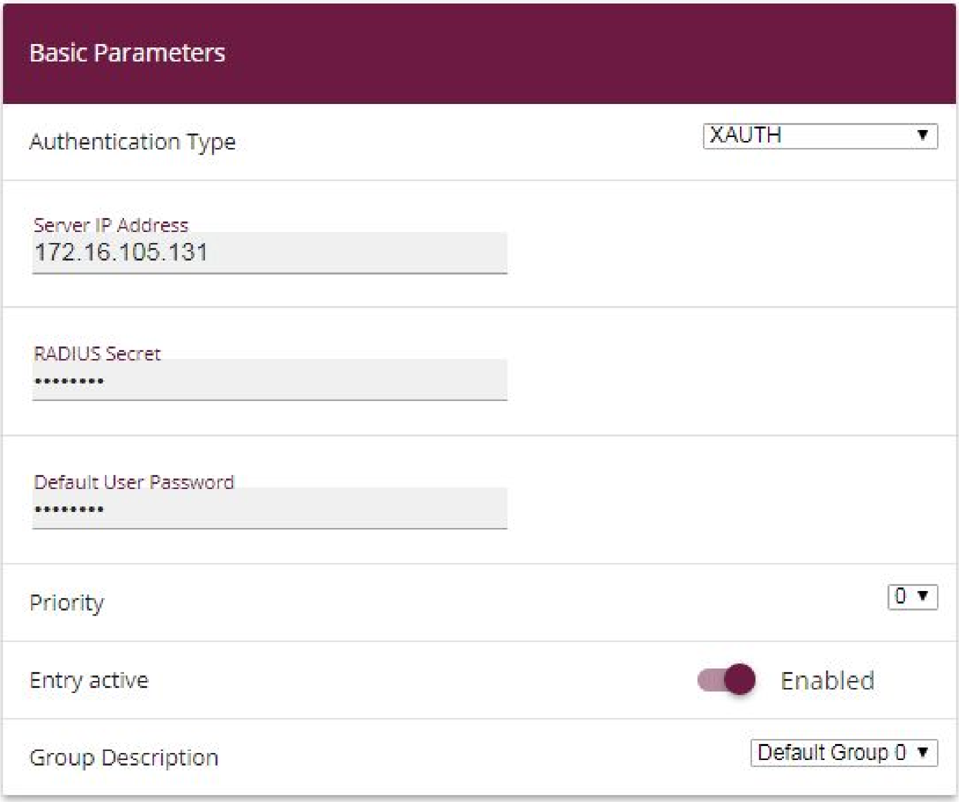
Note

Instead of the **Multi-User IPSec configuation**, there is also the option to create a separate IPSec peer configuration entry for each VPN client.

The priority of the Multi-User IPSec peer must always be lower than other IPSec peer configuration entries.

In order to connect the RADUIS server to the bintec VPN gateway, go to the following menu:

(1) Go to **System Management** -> **Remote Authentication** -> **RADIUS** ->**New**.



Basic Parameters

Authentication Type: XAUTH

Server IP Address: 172.16.105.131

RADIUS Secret: ••••••••

Default User Password: ••••••••

Priority: 0

Entry active: Enabled

Group Description: Default Group 0

Fig. 63: **System Management**->**Remote Authentication**->**RADIUS**->**New**

Proceed as follows:

(1) Select **Authentication Type** `XAUTH` in order to enable authentication via the Windows Server.

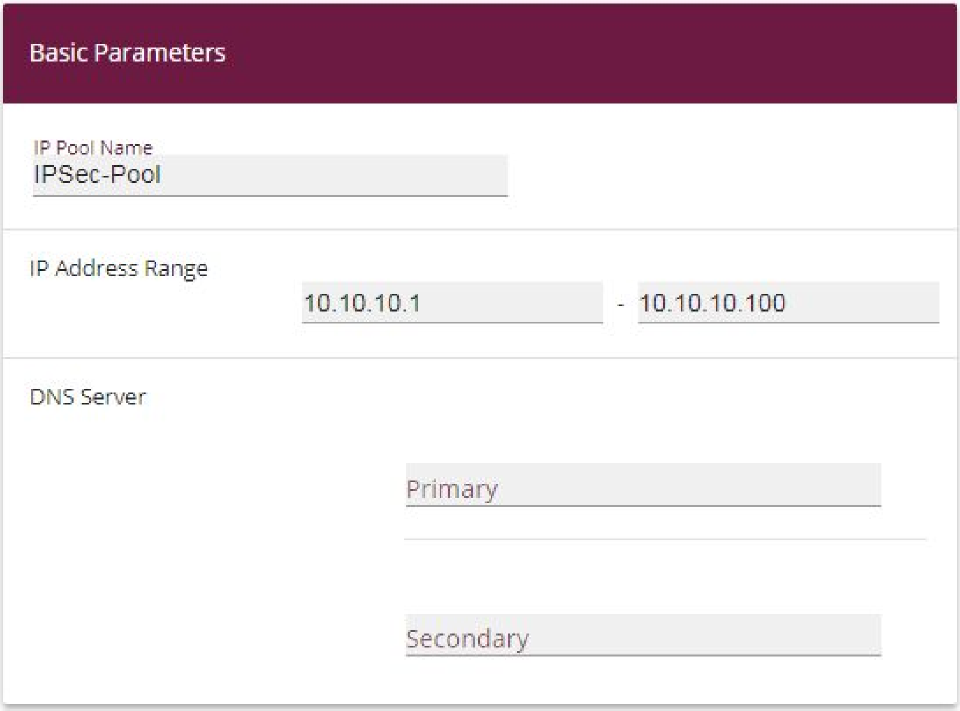
(2) Enter the**Server IP Address**, e.g. `172.16.105.131`, to communicate with the Microsoft RADIUS server.

(3) Enter the shared password used for communication between the RADIUS server and your device, e.g. `supersecret`.

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

An address pool must be created in order to assign an IP pool to the VPN profile of the Multi-User IPSec peer.

(1) Go to **VPN** -> **IPSec** -> **IP Pools** -> **Add** .



Basic Parameters

IP Pool Name
IPSec-Pool

IP Address Range
10.10.10.1 - 10.10.10.100

DNS Server

Fig. 64: **VPN** -> **IPSec** -> **IP Pools** -> **Add**

Proceed as follows:

(1) Enter the name of the IP pool for **IP Pool Name**, e.g. `IPSec-Pool`.

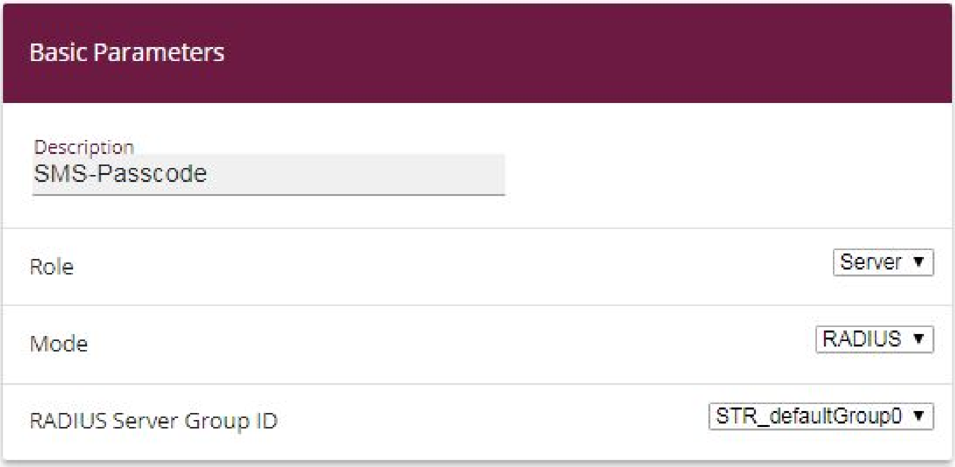
(2) For **IP Pool Range**, enter the first IP address of the address pool in the first field, e.g. `10.10.10.1`.

(3) Enter the last IP address of the address pool in the second field, e.g. `10.10.10.100`.

(4) Click **Add**.

A profile must then be created in order to be able to refer to the RADIUS server.

Go to **VPN** -> **IPSec** -> **XAUTH Profiles** -> **New**.



Basic Parameters

Description
SMS-Passcode

Role: Server ▾

Mode: RADIUS ▾

RADIUS Server Group ID: STR_defaultGroup0 ▾

Fig. 65: **VPN** -> **IPSec** -> **XAUTH Profiles** -> **New**

Proceed as follows in order to set up a profile:

(1) Enter a **Description** for this XAuth profile, e.g. *SMS Passcode*.

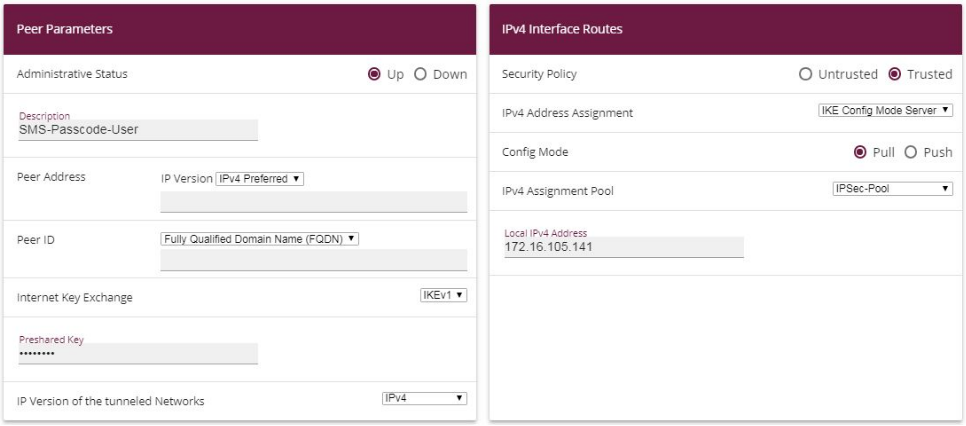
(2) Select the **Role** of the gateway for the XAuth authentication; in this instance, *Server*.

(3) Under **Mode** select *RADIUS* . Authentication is carried out via the RADIUS server.

(4) Confirm with **OK**.

Now the actual **IPSec Peer** is created.

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



Peer Parameters

Administrative Status: ● Up ○ Down

Description
SMS-Passcode-User

Peer Address: IP Version IPv4 Preferred ▾

Peer ID: Fully Qualified Domain Name (FQDN) ▾

Internet Key Exchange: IKEv1 ▾

Preshared Key
••••••••

IP Version of the tunneled Networks: IPv4 ▾

IPv4 Interface Routes

Security Policy: ○ Untrusted ● Trusted

IPv4 Address Assignment: IKE Config Mode Server ▾

Config Mode: ● Pull ○ Push

IPv4 Assignment Pool: IPSec-Pool ▾

Local IPv4 Address
172.16.105.141

Fig. 66: **VPN** -> **IPSec** -> **IPSec Peers** -> **New**

Proceed as follows:

(1) Enter a **Description** of the peer which identifies it, e.g. *SMS Passcode User*.

(2) In this scenario, no IPSec peer ID is saved in order to enable the Multi-User IPSec connections.

(3) Under **Preshared Key** enter the password agreed with the peer, e.g. *supersecret*.

(4) For **IP Address Assignment**, select the configuration mode of the interface; in this instance, *Server In IKE Configuration Mode*.

(5) Select a configured **IP Assignment Pool**, e.g. *IPSec Pool*.

(6) Enter the LAN IP address of the VPN gateway under **Local IP Address**, e.g. *172.16.105.141*.

(7) Click **Advanced Settings**.

(8) If selecting *None (Use Standard Profile)*, the profile indicated as standard in **Phase 1 Profile**/**Phase 2 Profile** is used.

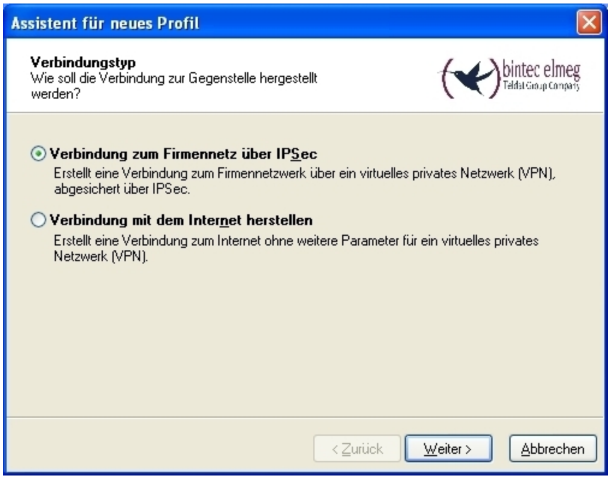
(9) Select the **XAUTH Profile** that has already been configured, e.g. *SMS Passcode*.

(10) For **Number of Admitted Connections**, set it to *Multiple Users* in order to enable IPSec Multi-User mode.

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

5.2.7 Configuration of bintec Secure IPSec Client

The **bintec Secure IPSec Clients** is called up via **Start** -> **Program** -> **bintec Secure IPSec Client** -> **Secure Client Monitor**. The **bintec Secure IPSec Clients** is configured using the Wizard. The **New Profile Wizard** starts automatically upon first launch of the **bintec Secure IPSec Clients**. Select **Company Network Connection over IPSec**.



Assistent für neues Profil

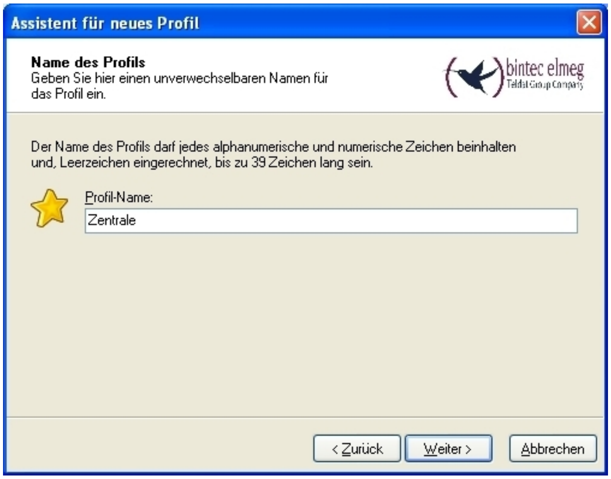
Verbindungstyp
Wie soll die Verbindung zur Gegenstelle hergestellt werden?

● Verbindung zum Firmennetz über IPSec
Erstellt eine Verbindung zum Firmennetzwerk über ein virtuelles privates Netzwerk (VPN), abgesichert über IPSec.

○ Verbindung mit dem Internet herstellen
Erstellt eine Verbindung zum Internet ohne weitere Parameter für ein virtuelles privates Netzwerk (VPN).

Fig. 67: Connection Type

Enter a name for the profile, e.g. `Head Office`.



Assistent für neues Profil

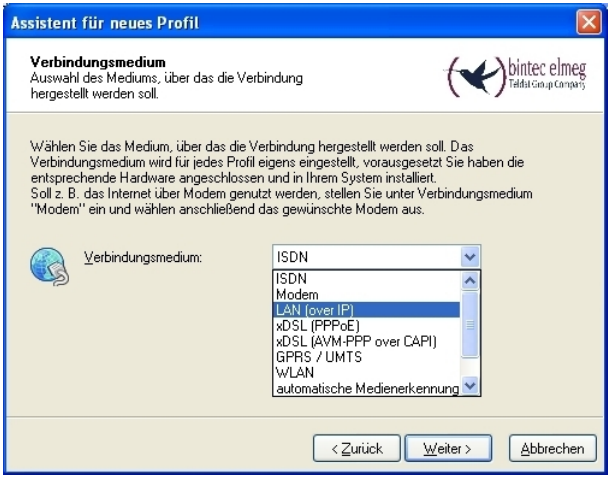
Name des Profils
Geben Sie hier einen unverwechselbaren Namen für das Profil ein.

Der Name des Profils darf jedes alphanumerische und numerische Zeichen beinhalten und, Leerzeichen eingerechnet, bis zu 39 Zeichen lang sein.

Profil-Name: Zentrale

Fig. 68: Profile Name

In the next step of the Wizard, you must select a **Connection Medium** over which to set up a connection to the Internet. In our example, the *LAN (over IP)* selection is used as the VPN client establishes no direct Internet access but uses an Internet access router.



Assistent für neues Profil

Verbindungsmedium
Auswahl des Mediums, über das die Verbindung hergestellt werden soll.

Wählen Sie das Medium, über das die Verbindung hergestellt werden soll. Das Verbindungsmedium wird für jedes Profil eigens eingestellt, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem System installiert.
Soll z. B. das Internet über Modem genutzt werden, stellen Sie unter Verbindungsmedium "Modem" ein und wählen anschließend das gewünschte Modem aus.

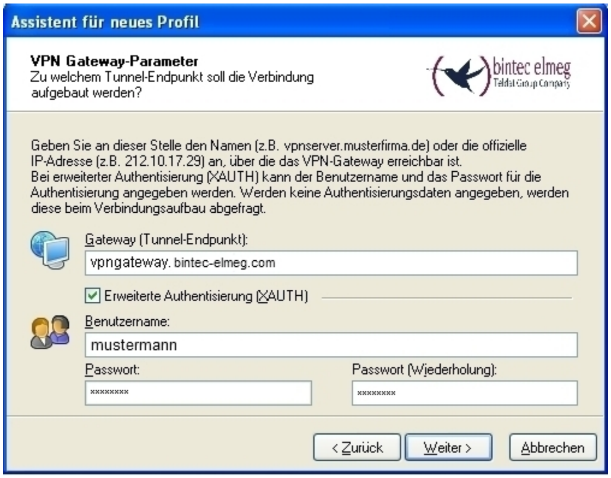
Verbindungsmedium: ISDN

Fig. 69: Connection Medium

Under the option **Gateway (Tunnel Endpoint)** the address at which the VPN gateway is accessible over the Internet is saved. Enable the option *Advanced Authentication (XAUTH)*.

Note

The Windows Active Directory logon data of the respective user can be stored for XAUTH **User Name** and **Password**.



Assistent für neues Profil

VPN Gateway-Parameter
Zu welchem Tunnel-Endpunkt soll die Verbindung aufgebaut werden?

Geben Sie an dieser Stelle den Namen (z.B. vpnserver.musterfirma.de) oder die offizielle IP-Adresse (z.B. 212.10.17.29) an, über die das VPN-Gateway erreichbar ist.
Bei erweiterter Authentisierung (XAUTH) kann der Benutzername und das Passwort für die Authentisierung angegeben werden. Werden keine Authentisierungsdaten angegeben, werden diese beim Verbindungsaufbau abgefragt.

Gateway (Tunnel-Endpunkt): vpngateway. bintec-elmeg.com

☑ Erweiterte Authentisierung (XAUTH)

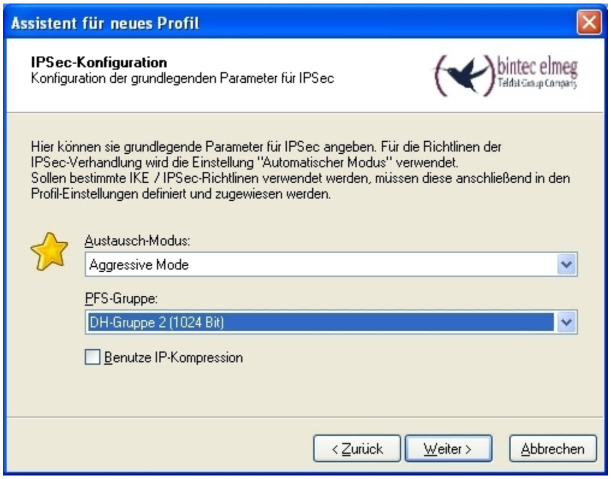
Benutzername: mustermann

Passwort: ********

Passwort (Wiederholung): ********

Fig. 70: VPN gateway parameters

Next, `Aggressive Mode` is used as **Exchange Mode** because the **bintec be.IP** router and the **bintec Secure IPSec Client** are assigned dynamic IP addresses by the provider. Set **PFS Group** to `DH Group 2 (1024 Bit)`, for example. The option `Use IP Compression` is not employed in this configuration.



Assistent für neues Profil

IPSec-Konfiguration
Konfiguration der grundlegenden Parameter für IPSec

Hier können sie grundlegende Parameter für IPSec angeben. Für die Richtlinen der IPSec-Verhandlung wird die Einstellung "Automatischer Modus" verwendet.
Sollen bestimmte IKE / IPSec-Richtlinen verwendet werden, müssen diese anschließend in den Profil-Einstellungen definiert und zugewiesen werden.

Austausch-Modus: Aggressive Mode

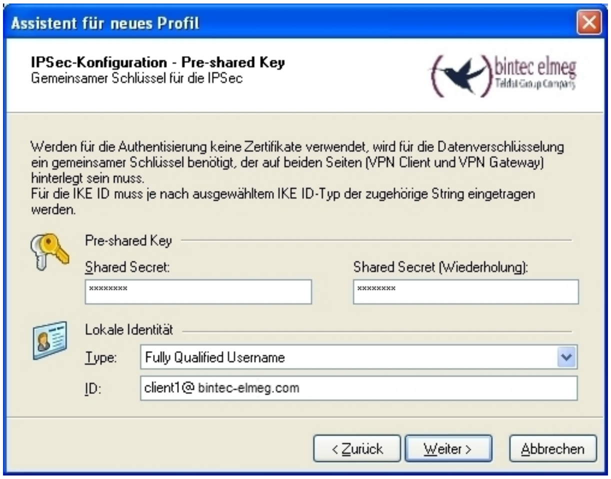
PFS-Gruppe: DH-Gruppe 2 (1024 Bit)

☐ Benutze IP-Kompression

Fig. 71: IPSec Configuration

In the next step of the Wizard, the **Preshared Key** saved in the VPN gateway and the IPSec **ID** of the VPN client are saved.

The selection in the **Type** field must be such that it is suitable for the actual IPSec ID (e.g. `Fully Qualified Username` when using an ID in the form of an e-mail address).



Assistent für neues Profil

IPSec-Konfiguration - Pre-shared Key
Gemeinsamer Schlüssel für die IPSec

Werden für die Authentisierung keine Zertifikate verwendet, wird für die Datenverschlüsselung ein gemeinsamer Schlüssel benötigt, der auf beiden Seiten (VPN Client und VPN Gateway) hinterlegt sein muss.
Für die IKE ID muss je nach ausgewähltem IKE ID-Typ der zugehörige String eingetragen werden.

Pre-shared Key

Shared Secret: ********

Shared Secret (Wiederholung): ********

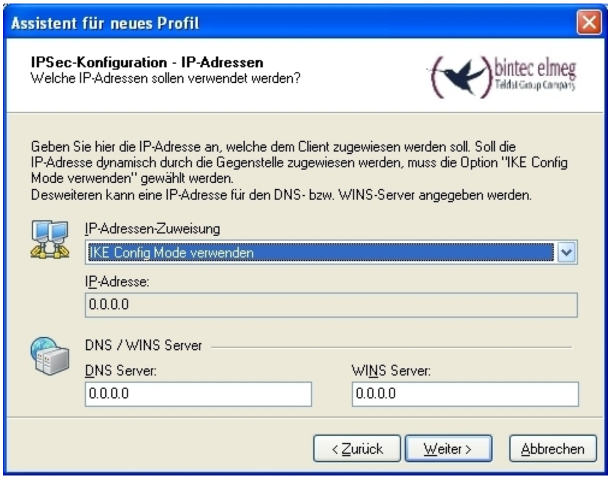
Lokale Identität

Type: Fully Qualified Username

ID: client1@ bintec-elmeg.com

Fig. 72: Preshared Key

In this example, a dynamic VPN IP address is assigned to the VPN IPSec client. For this, the option `Use IKE Config Mode` must be selected.



Assistent für neues Profil

IPSec-Konfiguration - IP-Adressen
Welche IP-Adressen sollen verwendet werden?

Geben Sie hier die IP-Adresse an, welche dem Client zugewiesen werden soll. Soll die IP-Adresse dynamisch durch die Gegenstelle zugewiesen werden, muss die Option "IKE Config Mode verwenden" gewählt werden.
Desweiteren kann eine IP-Adresse für den DNS- bzw. WINS-Server angegeben werden.

IP-Adressen-Zuweisung: IKE Config Mode verwenden

IP-Adresse: 0.0.0.0

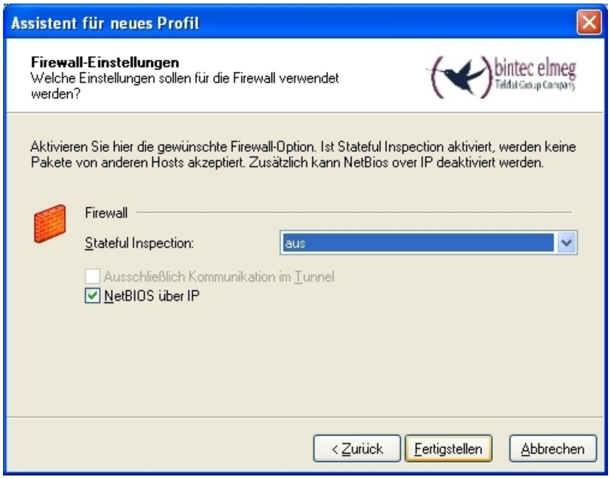
DNS / WINS Server

DNS Server: 0.0.0.0

WINS Server: 0.0.0.0

Fig. 73: IKE Config Mode

In the final step, the **Firewall** of the **bintec Secure IPSec Clients** is configured. If the client is directly connected to the Internet, the firewall should be enabled.



Assistent für neues Profil

Firewall-Einstellungen
Welche Einstellungen sollen für die Firewall verwendet werden?

Aktivieren Sie hier die gewünschte Firewall-Option. Ist Stateful Inspection aktiviert, werden keine Pakete von anderen Hosts akzeptiert. Zusätzlich kann NetBios over IP deaktiviert werden.

Firewall

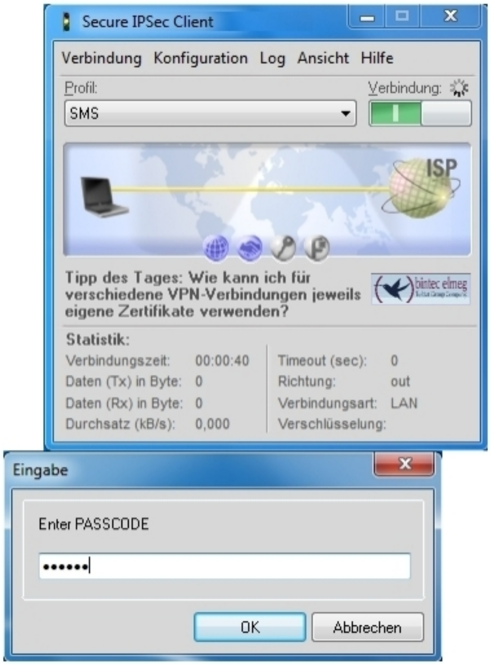
Stateful Inspection: aus

□ Ausschließlich Kommunikation im Tunnel
☑ NetBIOS über IP

Fig. 74: Firewall

5.3 Testing of VPN connection/debug messages from the VPN gateway

When establishing a connection, the **bintec Secure IPSec Clients** is authenticated using the Preshared Key. A dual user/password request is then made which is authenticated via the Windows and **SMS PASSCODE** servers. First of all, the login takes place here using the respective Windows Active Directory user and password details, whereby the **SMS PASSCODE** server can be assigned to a user and his/her mobile number. A one-time password is then sent via SMS. After entering the password received via SMS, the VPN tunnel is then fully established.



Profil: SMS

Verbindung:

Tipp des Tages: Wie kann ich für verschiedene VPN-Verbindungen jeweils eigene Zertifikate verwenden?

Statistik:

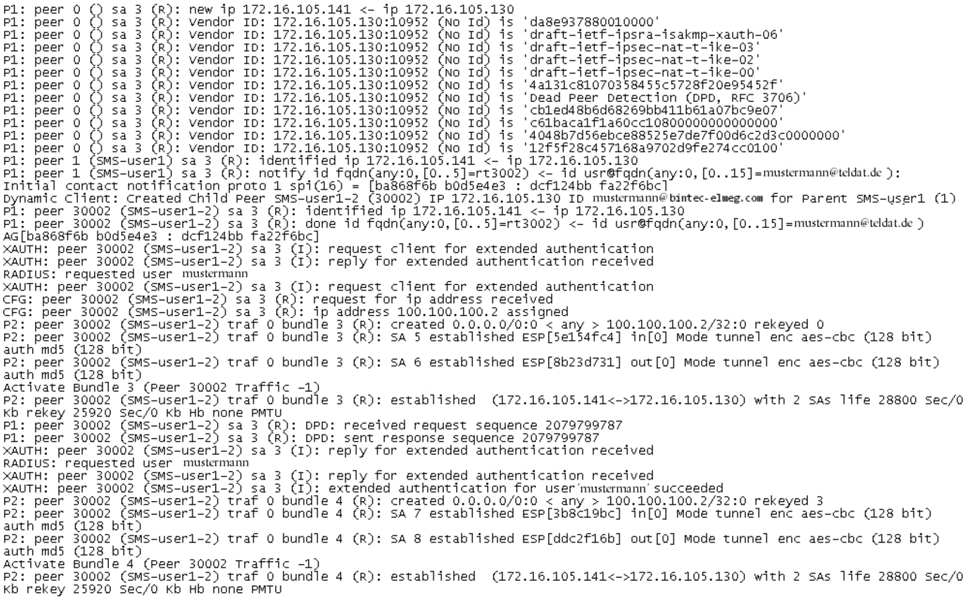
Verbindungszeit:	00:00:40	Timeout (sec):	0
Daten (Tx) in Byte:	0	Richtung:	out
Daten (Rx) in Byte:	0	Verbindungsart:	LAN
Durchsatz (kB/s):	0,000	Verschlüsselung:	

Enter PASSCODE

••••••

Fig. 75: Secure IP Sec Client

Debug messages from the VPN gateway when establishing a connection



```
P1: peer 0 () sa 3 (R): new ip 172.16.105.141 <- ip 172.16.105.130
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'da8e937880010000'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsra-isakmp-xauth-06'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsec-nat-t-ike-03'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsec-nat-t-ike-02'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'draft-ietf-ipsec-nat-t-ike-00'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is '4a131c81070358455c5728f20e95452f'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'Dead Peer Detection (DPD, RFC 3706)'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'cb1ed48b6d68269bb411b61a07bc9e07'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is 'c61baca1f1a60cc10800000000000000'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is '4048b7d56ebce88525e7de7f00d6c2d3c0000000'
P1: peer 0 () sa 3 (R): Vendor ID: 172.16.105.130:10952 (No Id) is '12f5f28c457168a9702d9fe274cc0100'
P1: peer 1 (SMS-user1) sa 3 (R): identified ip 172.16.105.141 <- ip 172.16.105.130
P1: peer 1 (SMS-user1) sa 3 (R): notify id fqdn(any:0,[0..5]=rt3002) <- id usr@fqdn(any:0,[0..15]=mustermann@teldat.de ):
Initial contact notification proto 1 spi(16) = [ba868f6b b0d5e4e3 : dcf124bb fa22f6bc]
Dynamic Client: Created Child Peer SMS-user1-2 (30002) IP 172.16.105.130 ID mustermann@bintec-elmeg.com for Parent SMS-user1 (1)
P1: peer 30002 (SMS-user1-2) sa 3 (R): identified ip 172.16.105.141 <- ip 172.16.105.130
P1: peer 30002 (SMS-user1-2) sa 3 (R): done id fqdn(any:0,[0..5]=rt3002) <- id usr@fqdn(any:0,[0..15]=mustermann@teldat.de )
AG[ba868f6b b0d5e4e3 : dcf124bb fa22f6bc]
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): request client for extended authentication
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): reply for extended authentication received
RADIUS: requested user mustermann
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): request client for extended authentication
CFG: peer 30002 (SMS-user1-2) sa 3 (R): request for ip address received
CFG: peer 30002 (SMS-user1-2) sa 3 (R): ip address 100.100.100.2 assigned
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): created 0.0.0.0/0:0 < any > 100.100.100.2/32:0 rekeyed 0
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): SA 5 established ESP[5e154fc4] in[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): SA 6 established ESP[8b23d731] out[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
Activate Bundle 3 (Peer 30002 Traffic -1)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 3 (R): established  (172.16.105.141<->172.16.105.130) with 2 SAs life 28800 Sec/0
Kb rekey 25920 Sec/0 Kb Hb none PMTU
P1: peer 30002 (SMS-user1-2) sa 3 (R): DPD: received request sequence 2079799787
P1: peer 30002 (SMS-user1-2) sa 3 (R): DPD: sent response sequence 2079799787
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): reply for extended authentication received
RADIUS: requested user mustermann
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): reply for extended authentication received
XAUTH: peer 30002 (SMS-user1-2) sa 3 (I): extended authentication for user'mustermann' succeeded
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): created 0.0.0.0/0:0 < any > 100.100.100.2/32:0 rekeyed 3
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): SA 7 established ESP[3b8c19bc] in[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): SA 8 established ESP[ddc2f16b] out[0] Mode tunnel enc aes-cbc (128 bit)
auth md5 (128 bit)
Activate Bundle 4 (Peer 30002 Traffic -1)
P2: peer 30002 (SMS-user1-2) traf 0 bundle 4 (R): established  (172.16.105.141<->172.16.105.130) with 2 SAs life 28800 Sec/0
Kb rekey 25920 Sec/0 Kb Hb none PMTU
```

5.4 Overview of Configuration Steps

Installation of SMS PASSCODE server

Field	Menu	Value
RADIUS client protection	**SMS PASSCODE -> Install Shield Wizard**	*Enabled*

Configuration of Web Administration Tool

Field	Menu	Value
Enable AD Integration	**Settings -> General**	*Enabled (single domain mode)*
Mobile number required	**Policies -> User Integration Policies**	*Enabled*
AD Credentials	**Policies -> User Integration Policies**	Login/Password
Group Name	**Policies -> User Integration Policies**	e.g. *SMS PASSCODE Users*

Configuration of RADIUS server

Field	Menu	Value
Enable this RADIUS client	**Network Policy Server -> RADIUS Clients**	*Enabled*
Friendy name	**Network Policy Server -> RADIUS Clients**	e.g. *SMA Passcode GW*
Address (IP or DNS)	**Network Policy Server -> RADIUS Clients**	e.g. *172.16.105.141*
Shared secret	**Network Policy Server -> RADIUS Clients**	e. g. *supersecret*

Configuration of the VPN gateway

Field	Menu	Value
Authentication Type	**System Management -> Remote Authentication -> RADIUS -> New**	*XAUTH*
Server IP Address	**System Management -> Remote Authentication -> RADIUS -> New**	e.g. *172.16.105.131*
RADIUS Password	**System Management -> Remote Authentication -> RADIUS -> New**	e. g. *supersecret*

Create IP Address Pool

Field	Menu	Value
IP Pool Name	**VPN -> IPSec -> IP Pools -> Add**	e.g. *IPSec Pool*

Field	Menu	Value
IP Pool Range	**VPN** -> **IPSec** -> **IP Pools** -> **Add**	e.g. *10.10.10.1* - *10.10.10.100*

Create XAUTH Profile

Field	Menu	Value
Description	**VPN** -> **IPSec** -> **XAUTH Profiles** -> **New**	e.g. *SMS Passcode*
Role	**VPN** -> **IPSec** -> **XAUTH Profiles** -> **New**	*Server*
Mode	**VPN** -> **IPSec** -> **XAUTH Profiles** -> **New**	*RADIUS*

Configure IPSec Peers

Field	Menu	Value
Description	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	e.g. *SMS Passcode Users*
Preshared Key	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	e. g. *supersecret*
IP Address Assignment	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	*Server In IKE Configuration Mode*
IP Assignment Pool	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	*IPSec Pool*
Local IP Address	**VPN** -> **IPSec** -> **IPSec Peers** -> **New**	e.g. *172.16.105.141*
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)*
XAUTH Profile	**VPN** -> **IPSec** -> **IPSec Peers** -> **New** -> **Advanced Settings**	*SMS Passcode*
Number of Admitted Connections	**VPN** -> **IPSec** -> **IPSec Peers** -> **New** -> **Advanced Settings**	*Several users*

Configuration of bintec Secure IPSec Client

Field	Menu	Value
Connection Type	**Wizard for new profile**	*Connection to company network via IPSec*
Profile Name	**Wizard for new profile**	*Head Office*
Connection Medium	**Wizard for new profile**	*LAN (over IP)*

Field	Menu	Value
Gateway (Tunnel Endpoint)	**Wizard for new profile**	e.g. *vpngateway.bintec-elmeg.com*
Advanced authentication (XAUTH)	**Wizard for new profile**	Enabled
Login name	**Wizard for new profile**	e.g. *mustermann*
Password	**Wizard for new profile**	e. g. *supersecret*
Exchange Mode	**Wizard for new profile**	Aggressive Mode
PFS Group	**Wizard for new profile**	DH Group 2 (1024 Bit)
Shared secret	**Wizard for new profile**	e.g. *bintec elmeg*
Shared Secret (Retry)	**Wizard for new profile**	e.g. *bintec elmeg*
Type	**Wizard for new profile**	e.g. *Fully Qualified Username*
ID	**Wizard for new profile**	e.g. *client1@bintec-elmeg.com*
IP address assignment	**Wizard for new profile**	*Use IKE Config Mode*
Stateful Inspection	**Wizard for new profile**	*off*
NetBIOS over IP	**Wizard for new profile**	Enabled