



# **Manual Workshops (Excerpt)**

## **Security and Administration Workshops**

Copyright© Version 01/2020 bintec elmeg GmbH

## Legal Notice

### Warranty

This publication is subject to modifications.

bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH is not liable for the information in this manual. bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec 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 GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH bintec elmeg GmbH

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

## Table of Contents

Chapter 1	Security - IPSec VPN with callback . . . . .	1
1.1	Introduction . . . . .	1
1.2	Configuring the licence . . . . .	2
1.3	Configuration of ISDN interfaces . . . . .	3
1.4	Configuring internet access . . . . .	4
1.5	Configuring IPSec . . . . .	6
1.5.1	Configuring the IPSec peer and callback . . . . .	6
1.5.2	Changing the Phase-1 Profiles . . . . .	9
1.5.3	Changing the Phase-2 profile. . . . .	11
1.6	Result. . . . .	12
1.7	Checking the configuration. . . . .	12
1.7.1	Testing the connection and the ISDN callback . . . . .	12
1.8	Overview of configuration steps. . . . .	13
Chapter 2	Security - IPSec client authentication via XAuth on Microsoft RADIUS Server (IAS) . . . . .	17
2.1	Introduction . . . . .	17
2.2	Configuration . . . . .	17
2.2.1	Configuration of the VPN gateway . . . . .	18
2.2.2	Configuration of the Windows 2003 RADIUS Server . . . . .	25
2.2.3	Configuration of bintec secure IPSec clients . . . . .	31
2.3	Checking the connection. . . . .	35
2.4	Windows login per VPN (optional) . . . . .	38
2.5	Overview of configuration steps . . . . .	39

Chapter 3	Security - VPN IPSec authentication with KOBIL SecCOVID one-time password request . . . . .	43
3.1	Introduction . . . . .	43
3.2	Configuration . . . . .	44
3.2.1	Installation of the KOBIL SecCOVID server . . . . .	44
3.2.2	Configuration of the VPN gateway . . . . .	47
3.2.3	Configuration of bintec secure IPSec clients . . . . .	55
3.3	Overview of configuration steps. . . . .	61
Chapter 4	Security - Certificate-based VPN IPSec with optional KOBIL SecCOVID one-time password request . . . . .	64
4.1	Introduction . . . . .	64
4.2	Configuration . . . . .	64
4.2.1	Setting up the OpenSSL certification authority . . . . .	65
4.2.2	Generation of user certificates . . . . .	67
4.2.3	Configuration of the VPN gateway . . . . .	71
4.2.4	Configuration of bintec secure IPSec clients . . . . .	77
4.2.5	Setup of the VPN IPSec tunnel . . . . .	83
4.2.6	Additional securing of the VPN IPSec tunnel with a one-time password (optional) . . . . .	84
4.2.7	Adjusting the VPN gateway configuration for one-time password request . . . . .	88
4.2.8	Adjusting the bintec Secure IPSec configuration for one-time password request . . . . .	91
4.3	Overview of configuration steps. . . . .	93
Chapter 5	Security - VPN IPSec tunnel via HTTPS between the bintec Secure IPSec Client and a bintec router . . . . .	98
5.1	Introduction . . . . .	98
5.2	Configuration . . . . .	98

5.2.1	Configuration of the VPN gateway . . . . .	99
5.2.2	Configuration of the VPN IPSec tunnel . . . . .	99
5.2.3	Enable IPSec Pathfinder function . . . . .	100
5.2.4	Configuration of bintec Secure IPSec Client . . . . .	101
5.3	Overview of Configuration Steps . . . . .	107
<b>Chapter 6</b>	<b>Security - IPSec with certificates . . . . .</b>	<b>109</b>
6.1	Introduction . . . . .	109
6.2	Configuration. . . . .	109
6.2.1	Creating an IPSec peer . . . . .	110
6.2.2	Changing the Phase-1 Profiles . . . . .	111
6.2.3	Changing the Phase-2 Profiles . . . . .	113
6.2.4	Configuring DynDNS . . . . .	115
6.2.5	Requesting and importing certificates . . . . .	116
6.2.6	Changing the IPSec tunnel. . . . .	119
6.3	Result . . . . .	121
6.4	Checking the connection. . . . .	121
6.5	Overview of configuration steps. . . . .	122
<b>Chapter 7</b>	<b>Security - IPSec with dynamic IP addresses and DynDNS</b>	<b>126</b>
7.1	Introduction . . . . .	126
7.2	Configuration . . . . .	127
7.2.1	Configuration on the first router (Location A) . . . . .	127
7.2.2	Configuration on the second router (Location B) . . . . .	133
7.3	Checking the connection . . . . .	139
7.4	Overview of configuration steps . . . . .	140
<b>Chapter 8</b>	<b>Security - Bridging over an IPSec tunnel . . . . .</b>	<b>145</b>

8.1	Introduction . . . . .	145
8.2	Configuration at location A (bintec be.IP plus-1) . . . . .	146
8.3	Configuration at location B (bintec be.IP plus-2) . . . . .	153
8.4	Overview of configuration steps. . . . .	160
<b>Chapter 9</b>	<b>Security - Stateful Inspection Firewall (SIF) . . . . .</b>	<b>165</b>
9.1	Introduction . . . . .	165
9.2	Firewall configuration . . . . .	166
9.2.1	Configuring aliases for IP addresses and network address . . . . .	166
9.2.2	Configuring service sets . . . . .	169
9.2.3	Configuring filter rules . . . . .	171
9.3	Result . . . . .	173
9.4	Checking the configuration. . . . .	174
9.5	Overview of configuration steps. . . . .	175
<b>Chapter 10</b>	<b>Security - VPN connection via a SMS PASSCODE server</b>	<b>178</b>
10.1	Introduction . . . . .	178
10.2	Configuration . . . . .	179
10.2.1	Information during installation and configuration of the SMS PASSCODE server . . . . .	179
10.2.2	Preparation for installing the SMS PASSCODE server . . . . .	179
10.2.3	Installation of SMS PASSCODE server . . . . .	179
10.2.4	Configuration of Web Administration Tool . . . . .	180
10.2.5	Configuration of RADIUS server to connect the VPN gateway . . . . .	182
10.2.6	Configuration of the VPN gateway . . . . .	183
10.2.7	Configuration of bintec Secure IPSec Client . . . . .	187
10.3	Testing of VPN connection/debug messages from the VPN gateway . . . . .	191
10.4	Overview of Configuration Steps . . . . .	193

# Chapter 1 Security - IPsec VPN with callback

## 1.1 Introduction

The configuration of an IPsec VPN with callback (IP address in the B/D-channel) with a **bintec RS232bw** is described in the following chapters.

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

The branch office of a company is to be connected to the head office over an IPsec tunnel. An xDSL connection is available for the Internet connection in both the branch office and head office. Both devices receive their IP address dynamically from the Internet Service Provider (ISP). To set up the IPsec tunnel in both directions, the IP address should be transferred to the partner over ISDN.

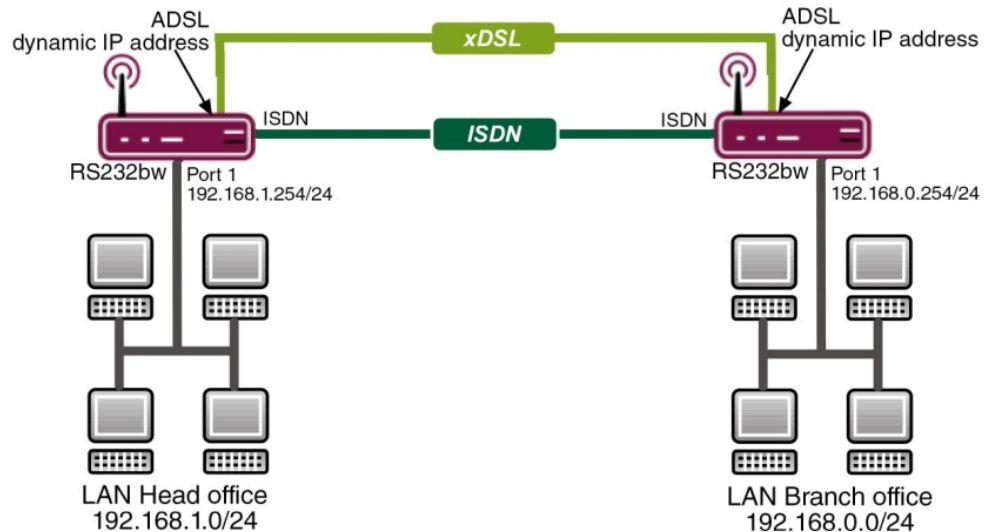


Fig. 1: Example scenario IPsec with callback

## Requirements

The following are required for the configuration:

- Two **bintec RS232bw** gateways.

- Boot image from version 7.10.1
- An xDSL internet access at head office and at the branch
- An ISDN connection at head office and at the branch
- The LAN must be connected to one of the ports **1** to **4** on the gateway

## 1.2 Configuring the licence

You require an additional licence to transmit the IP address in the B/D-channel. You can request these free of charge from [www.bintec-elmeg.com](http://www.bintec-elmeg.com) (under **Services** -> **Online Services**).

Once you have received the licence data, proceed as follows:

- (1) Go to **System Administration** -> **Global Settings** -> **System Licences**.

Fig. 2: **System Management** -> **Global Settings** -> **System Licences** -> **New**

### Relevant fields in the System Licences menu

Field	Meaning
Licence Serial Number	This is the serial number of the licence.
Licence Key	This is the licence key.

To enter the new licence, proceed as follows:

- (1) Click **New** to add a licence.
- (2) Under **Licence Serial Number** enter the serial number of your licence.
- (3) Enter your licence key under **Licence Key**.
- (4) Confirm with **OK**.

Check whether the licence has been enabled correctly as follows:



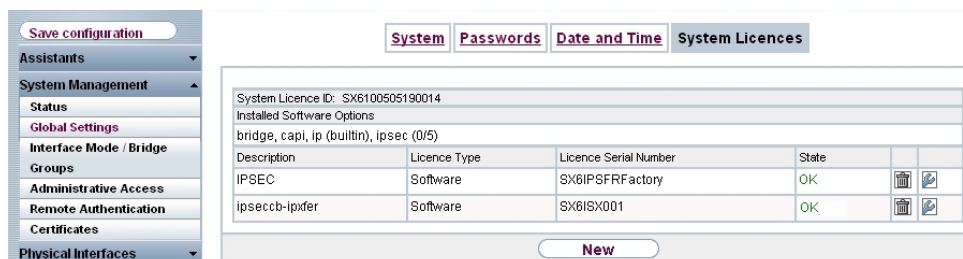


Fig. 3: System Management -> Global Settings -> System Licences

## 1.3 Configuration of ISDN interfaces

You must configure one of your Multiple Subscriber Numbers (MSN) so that IPsec callback is used for incoming calls.

Go to the following menu to configure an MSN for IPsec callback at head office:

- (1) Go to **Physical Interfaces -> ISDN Ports -> MSN Configuration -> New**.

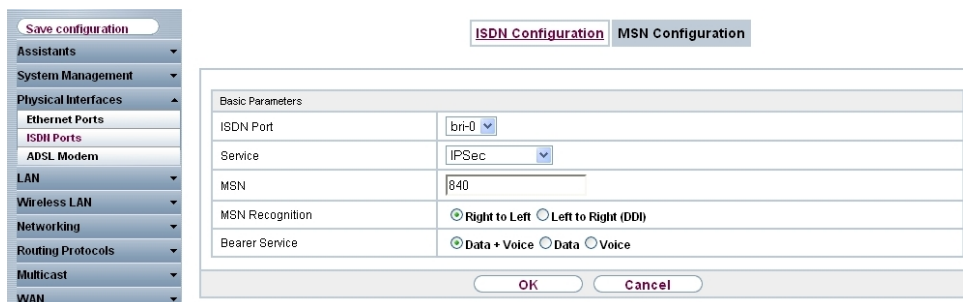


Fig. 4: Physical Interfaces -> ISDN Ports -> MSN Configuration -> New

### Relevant fields in the MSN Configuration menu

Field	Meaning
ISDN Port	Enter the port to which the ISDN connection is connected.
Service	Defines the service used to respond to the MSN.
MSN	This is the subscriber number of the service.
MSN Recognition	Defines the type of incoming number check.
Bearer Service	Defines whether to respond to a voice or data call or both.

Proceed as follows:

- (1) Set **ISDN Port** to *bri-0*.

- (2) Select the **Service** *IPSec*.
- (3) Under **MSN** enter the MSN to which the gateway should respond with an IPSec call-back, in this example *840*.
- (4) Leave **MSN Recognition** set to *Right to Left*.
- (5) Leave the **Bearer Service** set to *Data + Voice*.
- (6) Confirm with **OK**.

Configure an MSN to the gateway in the branch in the same way.



#### Note

If your gateway is connected to a point-to-point ISDN connection, it may be necessary to set **MSN Recognition** to *Left to Right (DDI)*.

## 1.4 Configuring internet access

An entry is created for both Internet connections over xDSL on each gateway. The subsequent configuration refers to the entry for the internet connection at head office.

Go to the following menu to set up an internet access over xDSL at head office:

- (1) Go to **WAN -> Internet + Dialup -> PPPoE-> New**.

The screenshot shows the configuration page for a new PPPoE connection. The left sidebar contains a navigation menu with categories like Assistants, System Management, Physical Interfaces, LAN, Wireless LAN, Networking, Routing Protocols, Multicast, WAN, Internet + Dialup, ATM, Real Time Jitter Control, VPN, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The main content area has tabs for PPPoE, PPTP, PPPoA, ISDN, and IP Pools. The 'Basic Parameters' section includes: Description (T-Online), PPPoE Mode (Standard selected), PPPoE Ethernet Interface (ethoa50-0), User Name (t-online.de), Password (masked), VLAN (Disabled), Always on (Disabled), and Connection Idle Timeout (120 Seconds). The 'Advanced Settings' section includes: Block after connection failure for (60 Seconds), Maximum Number of Dialup Retries (5), Authentication (PAP), DNS Negotiation (Enabled), Prioritize TCP ACK Packets (Disabled), LCP Alive Check (Disabled), and MTU (Automatic). Buttons for 'OK' and 'Cancel' are at the bottom.

Fig. 5: WAN -> Internet + Dialup ->PPPoE -> New

### Relevant fields in the PPPoE menu

Field	Meaning
Description	Define a name for the xDSL Internet connection.
PPPoE ethernet interface	Specify the interface for your gateway over which the xDSL connection is to be established.
User Name	Enter the user name you received from the provider.
Password	Enter the password you received from the provider.
Always on (flat-rate mode)	This indicates that the gateway does not automatically clear the connection.
Connection Idle Timeout	Define the time in seconds after which the gateway clears the connection in the absence of data traffic.
IP address mode	Defines the mode following which the gateway receives the IP address.
Default Route	For this connection, a standard route is automatically created.
Create NAT entry	NAT is enabled for this connection.

Proceed as follows:

- (1) Under **Description** enter the name for the connection, e.g. *T-Online*.
- (2) For **PPPoE Ethernet Interface**, select *ethoa50-0*.
- (3) Under **User Name** enter your user name defined in the access data for your provider.
- (4) Under **Password** enter the password for your Internet access.
- (5) Leave the default setting *Not activated* for **Always on (flat-rate mode)** if you do not have a DSL connection with flatrate. If you have an Internet access without flatrate enter the time in seconds after which the gateway should clear the Internet connection when there is no further data exchange under **Connection Idle Timeout**, for example *120*.  
If you have an Internet access with flatrate, select **Always on (Flatrate Mode)**. If selected the gateway will never clear the Internet connection automatically.
- (6) Leave **IP Address Mode** set to *Get IP Address*.
- (7) Keep **Default Route** selected.
- (8) Select **Create NAT Policy**.
- (9) Leave the remaining settings unchanged and confirm them with **OK**.

Configure an MSN to the internet connection in the branch in the same way.

## 1.5 Configuring IPSec

The following chapter describes how to configure an IPSec peer with callback and how to change the standard profile for Phase-1 and Phase-2.

### 1.5.1 Configuring the IPSec peer and callback

An IPSec peer always refers to a remote terminal, in this example the branch office.

To create an IPSec peer, proceed as follows:

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

Save configuration

- Assistants
- System Management
- Physical Interfaces
- LAN
- Wireless LAN
- Networking
- Routing Protocols
- Multicast
- WAN
- VPN**
- IPSec
- L2TP
- PPTP
- GRE
- Firewall
- VoIP
- Local Services
- Maintenance
- External Reporting
- Monitoring

IPSec Peers Phase-1 Profiles Phase-2 Profiles XAUTH Profiles IP Pools Options

Peer Parameters

Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down		
Description	<input type="text" value="rs232bw_branchoffice"/>		
Peer Address	<input type="text"/>		
Peer ID	IPV4 Address	<input type="text" value="192.168.0.254"/>	
Internet Key Exchange	<input type="text" value="IKEv1"/>		
Preshared Key	<input type="text" value="*****"/>		

Interface Routes

IP Address Assignment	<input type="text" value="Static"/>		
Default Route	<input type="checkbox"/> Enabled		
Local IP Address	<input type="text" value="192.168.1.254"/>		
Route Entries	Remote IP Address	Netmask	Metric
	<input type="text" value="192.168.0.0"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="1"/>

Advanced Settings

Advanced IPsec Options

Phase-1 Profile	<input type="text" value="None (use default profile)"/>		
Phase-2 Profile	<input type="text" value="None (use default profile)"/>		
XAUTH Profile	<input type="text" value="Select one"/>		
Number of Admitted Connections	<input checked="" type="radio"/> One User <input type="radio"/> Multiple Users		
Start Mode	<input checked="" type="radio"/> On Demand <input type="radio"/> Always up		

Advanced IP Options

Back Route Verify	<input type="checkbox"/> Enabled		
Proxy ARP	<input checked="" type="radio"/> Inactive <input type="radio"/> Up or Dormant <input type="radio"/> Up only		

IPsec Callback

Mode	<input type="text" value="Both"/>		
Incoming Phone Number	<input type="text" value="850"/>		
Outgoing Phone Number	<input type="text" value="50"/>		
Transfer own IP address over ISDN/GSM	<input checked="" type="checkbox"/> Enabled		
Transfer Mode	<input checked="" type="radio"/> Autodetect best mode <input type="radio"/> Autodetect only D Channel Modes <input type="radio"/> Use specific D Channel Mode <input type="radio"/> Try specific D Channel Mode, fall back to B Channel <input type="radio"/> Use only B Channel Mode		

Fig. 6: VPN -> IPSec ->IPSec Peers -> New

**Relevant fields in the IPSec Peers menu**

Field	Meaning
Description	Define a name for the IPsec peer.
Peer ID	Select the ID type and enter the peer ID.
Preshared Key	This is the secret key for IPsec negotiation.
Default Route	Select whether the route to this IPsec peer is to be defined as the default route.
Local IP Address	Enter the WAN IP address of your device.

Field	Meaning
Route entries: Remote IP Address / Netmask	Enter the networks to be set up over this IPsec tunnel.

To create an IPsec peer, proceed as follows:

- (1) Enter the description of the peer **Description**, e.g. *rs232bw\_branchoffice*.
- (2) Leave **Peer Address** blank as the IP address of the peer is assigned dynamically by the provider.
- (3) Under **Peer ID** select *IPV4 Address* and enter the ID of the remote terminal, in this example *192.168.0.254*.
- (4) Under **Preshared Key** enter, for example, *secret123*.
- (5) Deselect **Default Route**.
- (6) Enter the IP address of your device under **Local IP Address**, e.g. *192.168.1.254*.
- (7) Under **Route Entries** for **IP Address** and **Netmask** enter the IP address and the corresponding subnet mask of the network you wish to reach over the tunnel, in this example *192.168.0.0* and *255.255.255.0*.

Additional settings are required for peer configuration. For this, go to the following menu:

- (1) Go to **VPN -> IPsec -> IPsec Peers-> New-> Advanced Settings**.

#### Relevant fields in the menu Advanced Settings

Field	Meaning
Mode	Select the type of IPsec callback.
Incoming ISDN Number	Enter the subscriber number that arrives when the peer initiates the callback.
Outgoing ISDN Number	Enter the subscriber number that is dialled when the gateway initiates the callback.
Transfer own IP address over ISDN	Determines whether or not the IP address of the gateway is transferred over ISDN.
Transfer Mode	Select the transfer mode of the IP address.

Proceed as follows:

- (1) Select *Both* under **Mode**.
- (2) Under **Incoming ISDN Number** enter the MSN from which a callback is requested, in this example *850*.
- (3) Under **Outgoing ISDN Number** enter the MSN dialled for a callback, in this example *850*.
- (4) Select **Transfer Own IP Address over ISDN**.
- (5) Leave **Transfer Mode** set to *Autodetect Best Mode*.

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

Click **Save Configuration** and then confirm with **OK**.

Configure the IPsec for the gateway in the branch in the same way. Check that the IDs, IP addresses and MSN are configured correctly.




### Note

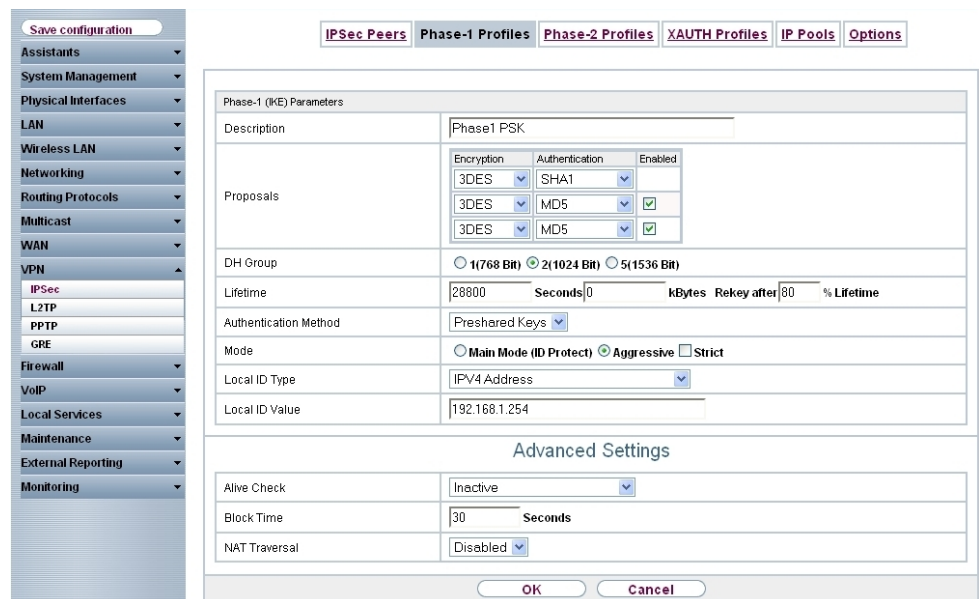
The preshared key here is kept very simple and is only intended for test purposes. In productive operation you should use a key containing at least 30 characters, unconnected words and preferably upper and lower case letters, numbers and special characters.

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.

## 1.5.2 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>** -> .



The screenshot displays the configuration interface for IPsec Phase-1 Profiles. The left sidebar contains a navigation menu with 'VPN' expanded and 'IPsec' selected. The main configuration area is titled 'Phase-1 (IKE) Parameters' and includes the following settings:

- Description:** Phase1 PSK
- Proposals:** A table with three rows:
 

Encryption	Authentication	Enabled
3DES	SHA1	<input type="checkbox"/>
3DES	MD5	<input checked="" type="checkbox"/>
3DES	MD5	<input checked="" type="checkbox"/>
- DH Group:** 2(1024 Bit) (selected)
- Lifetime:** 28800 Seconds, 0 kBytes, Rekey after 80 % Lifetime
- Authentication Method:** Preshared Keys
- Mode:** Aggressive (selected)
- Local ID Type:** IPv4 Address
- Local ID Value:** 192.168.1.254

The 'Advanced Settings' section includes:

- Alive Check:** Inactive
- Block Time:** 30 Seconds
- NAT Traversal:** Disabled

Buttons for 'OK' and 'Cancel' are located at the bottom of the configuration window.

Fig. 7: VPN -> IPsec -> Phase-1 Profiles-> <Multi-Proposal> -> 

### Relevant fields in the Phase-1 Profiles menu

Field	Meaning
Description	Define a name for the profile.
Proposal	Defines the encryption and authentication algorithm to be used.
DH Group	Defines the Diffie-Hellman group to be used.
Lifetime	Defines the time or data volume after which re-authentication is carried out.
Authentication Method	Select the authentication method.
Mode	Defines the type of tunnel negotiation.
Local ID Type	Defines the type of local ID for the gateway.
Local ID Value	This is the local ID of the gateway.

Proceed as follows to change the profile for phase-1:

- (1) Under **Description** enter the name of the profile, for example, *Phase1 PSK*.
- (2) Under **Proposal Encryption** select *3DES*, under **Authentication** select *SHA1* in the first entry. Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.
- (3) Leave **DH Group** set to *2(1024 Bit)*.
- (4) Under **Lifetime Seconds** enter a time in seconds, in this example *28800* and leave the KBytes set to *0*.
- (5) Leave the **Authentication Method** set to *Preshared Keys*.
- (6) Leave **Mode** set to *Aggressive*.
- (7) Set the **Local ID Type** to *IPV4 Address*.
- (8) Under **Local ID Value** enter the ID, in this example *192.168.1.254*.

Additional settings are required for the phase-1 configuration. For this, go to the following menu:

- (1) Go to **Phase-1 Profiles** -> **<Multi-Proposal>**  -> **Advanced Settings**.

### Relevant fields in the menu Advanced Settings

Field	Meaning
Alive Check	Defines the type of phase monitoring.
NAT Traversal	Determines whether or not the NAT traversal is used.

Proceed as follows:

- (1) Under **Alive check** select *Inactive*.
- (2) Deselect **NAT Traversal**.



(3) Confirm with **OK**.

Configure the phase 1 for the gateway in the branch in the same way.

### 1.5.3 Changing the Phase-2 profile

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


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

Fig. 8: **VPN -> IPsec -> Phase-2 Profiles-> <Multi-Proposal>** -> .

#### Relevant fields in the Phase-2 Profiles menu

Field	Meaning
Description	Define a name for the profile.
Proposal	Defines the encryption and authentication algorithm to be used.
Use PFS Group	Determines whether or not PFS (Perfect Forwarding Secrecy) is used.
Lifetime	Defines the time or data volume after which re-authentication is carried out.

Proceed as follows to change the profile for phase-2:

- (1) Under **Description** enter the name of the profile, for example, *Phase2*.
- (2) Under **Proposal Encryption** select *3DES*, under **Authentication** select *SHA1* in the first entry. Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.

- (3) Select **Use PFS Group**.
- (4) Under **Lifetime Seconds** enter the time in seconds, in this example *3600* and leave the KBytes set to *0*.

Additional settings are required for the phase-2 configuration. For this, go to the following menu:

- (1) Go to **Phase-2 Profile** -> **<Multi-Proposal>** ->  -> **Advanced Settings**.

#### Relevant fields in the menu **Advanced Settings**

Field	Meaning
Alive Check	Defines the type of phase monitoring.
Propagate PMTU	Determines whether or not the PMTU (Path Maximum Transfer Unit) is transferred.

Proceed as follows:

- (1) Under **Alive check** select *Inactive*.
- (2) Deselect **Propagate PMTU**.
- (3) Confirm with **OK**.

Configure the phase 2 for the gateway in the branch in the same way.

## 1.6 Result

You have entered a licence for transmitting the IP address in the B/D-channel. The ISDN interface has been configured to use the IPSec callback function. xDSL internet accesses have been set up at head office and at the branch offices. The IPSec tunnel has been configured on the gateway of the head office.

## 1.7 Checking the configuration

You have now configured an IPSec tunnel between two gateways; the IP addresses of the gateways are transmitted over ISDN to the remote terminal.

### 1.7.1 Testing the connection and the ISDN callback

The connection is set up by the head office, for example, with a ping. You can follow the set-up of the connection and the ISDN callback by entering the command `debug ipsec` in the command line.

```

r232bw> debug ipsec
00:01:04 INFO/IPSEC: IPSEC CB - need callback from Peer "r232bw_filiale"
00:01:04 INFO/IPSEC: IPSEC CB - trigger callback at Peer "r232bw_filiale" (do call ""->"850")
00:01:05 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", trigger call "" -> "850" is ALERTING
00:01:11 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", CB Mode LLC failed (next E) - clear trigger call ("> "850") now
00:01:11 INFO/IPSEC: P1: peer 1 (r232bw_filiale) sa 0 (-): Callback retry
00:01:11 INFO/IPSEC: IPSEC CB - need callback from Peer "r232bw_filiale"
00:01:11 INFO/IPSEC: IPSEC CB - trigger callback at Peer "r232bw_filiale" (do call ""->"850")
00:01:11 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", trigger call requested while peer triggeres ("> "850");
clearing trigger call from peer first
00:01:11 INFO/IPSEC: IPSEC CB - Peer "r232bw_filiale", trigger call "" -> "850" is ALERTING
00:01:21 INFO/IPSEC: IPSEC CB - Trigger Call by Peer "r232bw_filiale" successfully transmitted IP 84.146.201.132 /
Token 59766 via B channel
00:01:21 DEBUG/IPSEC: P1: peer 0 () sa 1 (R): new ip 84.146.201.132 <- ip 84.146.228.145
00:01:21 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 84.146.228.145:1023 (No Id) is 'BINTEC'
00:01:21 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 84.146.228.145:1023 (No Id) is 'BINTEC Heartbeats Version 1'
00:01:21 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 84.146.228.145:1023 (No Id) is 'Dead Peer Detection (DPD, RFC 3706)'
00:01:21 DEBUG/IPSEC: P1: peer 1 (r232bw_filiale) sa 1 (R): identified ip 84.146.201.132 <- ip 84.146.228.145
00:01:21 DEBUG/IPSEC: P1: peer 1 (r232bw_filiale) sa 1 (R): token payload: received token 59766
00:01:22 DEBUG/IPSEC: P1: peer 1 (r232bw_filiale) sa 1 (R): notify id ipv4(any:0,[0..3])=192.168.1.254 <- id
ipv4(any:0,[0..3])=192.168.0.254 (unencrypted): Initial contact notification proto 1 spi(16) =
[c838dcd0 28dfec79 : 6511d733 cf7dd976]
00:01:22 INFO/IPSEC: Trigger Bundle -1 (Peer 1 Traffic -1) prot 1 192.168.1.2:0->192.168.0.2:0
00:01:22 INFO/IPSEC: P1: peer 1 (r232bw_filiale) sa 1 (R): done id ipv4(any:0,[0..3])=192.168.1.254
<- id ipv4(any:0,[0..3])=192.168.0.254) AG[c838dcd0 28dfec79 : 6511d733 cf7dd976]
00:01:22 INFO/IPSEC: P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): created 192.168.1.0/24:0 < any >
192.168.0.0/24:0 rekeyed 0
00:01:23 DEBUG/IPSEC: P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): SA 1 established ESP[20893821] in[0]
Mode tunnel enc 3des-cbc (192 bit) auth sha (160 bit)
00:01:23 DEBUG/IPSEC: P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): SA 2 established ESP[34ffffb5] out[0]
Mode tunnel enc 3des-cbc (192 bit) auth sha (160 bit)
00:01:23 INFO/IPSEC: Activate Bundle -1 (Peer 1 Traffic -1)
00:01:23 INFO/IPSEC: P2: peer 1 (r232bw_filiale) traf 0 bundle -1 (I): established (84.146.201.132<->84.146.228.145)
with 2 SAs life 3600 Sec/O Kb rekey 2880 Sec/O Kb Hb none
r232bw>

```

This debug extract shows how the IPsec tunnel is initiated from head office. The system first attempts to transmit the IP address over the D-channel. However, this attempt fails as it is not supported by the PBX or the provider. Next, the IP address is transmitted in the B-channel and the tunnel is set up.

## 1.8 Overview of configuration steps

### Licence for IP address transfer over ISDN

Field	Menu	Value
Licence Serial Number	<b>System Management -&gt; Global Settings-&gt; System Licenses -&gt; New</b>	Serial number
Licence Key	<b>System Management -&gt; Global Settings-&gt; System Licenses -&gt; New</b>	Licence Key

### ISDN interfaces

Field	Menu	Value
ISDN Port	<b>Physical Interfaces -&gt; ISDN Ports-&gt; MSN Configuration -&gt; New</b>	e.g. <i>bri-0</i>
Service	<b>Physical Interfaces -&gt; ISDN Ports-&gt; MSN Configuration -&gt; New</b>	<i>IPSec</i>
MSN	<b>Physical Interfaces -&gt; ISDN Ports-&gt;</b>	e.g. <i>840</i>

Field	Menu	Value
	<b>MSN Configuration -&gt; New</b>	
MSN Recognition	<b>Physical Interfaces -&gt; ISDN Ports-&gt; MSN Configuration -&gt; New</b>	<i>Right to Left</i>
Bearer Service	<b>Physical Interfaces -&gt; ISDN Ports-&gt; MSN Configuration -&gt; New</b>	<i>Data + Voice</i>







### Internet Accesses

Field	Menu	Value
Description	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	e.g. <i>T-Online</i>
PPPoE ethernet interface	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	<i>ethoa50-0</i>
User Name	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	Your user name, e.g. <i>t-online.de</i>
Password	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	Your password
Always on (flat-rate mode)	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	<i>Disabled</i>
IP address mode	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	<i>Get IP Address</i>
Default Route	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	<i>Enabled</i>
Create NAT entry	<b>WAN -&gt; Internet + Dialup -&gt; PPPoE -&gt; New</b>	<i>Enabled</i>

### IPSec Configuration

Field	Menu	Value
Description	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt; New</b>	e.g. <i>rs232bw_branchoffice</i>
Peer ID	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt; New</b>	e.g. <i>IPV4 Address and 192.168.0.254</i>
Preshared Key	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt; New</b>	e.g. <i>secret123</i>
Default Route	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt; New</b>	<i>Disabled</i>
Local IP Address	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt; New</b>	e.g. <i>192.168.1.254</i>
Route Entries	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt; New</b>	e.g. for IP Address <i>192.168.0.0</i>

Field	Menu	Value
		and for 255.255.255 <b>Netmask . 0</b>
Mode	<b>VPN -&gt; IPsec -&gt;IPsec Peers-&gt; New -&gt; Advanced Settings</b>	<i>Both</i>
Incoming ISDN Number	<b>VPN -&gt; IPsec -&gt;IPsec Peers-&gt; New -&gt; Advanced Settings</b>	e.g. 850
Outgoing ISDN Number	<b>VPN -&gt; IPsec -&gt;IPsec Peers-&gt; New -&gt; Advanced Settings</b>	e.g. 850
Transfer own IP address over ISDN	<b>VPN -&gt; IPsec -&gt;IPsec Peers-&gt; New -&gt; Advanced Settings</b>	Enabled
Transfer Mode	<b>VPN -&gt; IPsec -&gt;IPsec Peers-&gt; New -&gt; Advanced Settings</b>	e.g. <i>Autodetect Best Mode</i>
Description	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	e.g. <i>Phase1 PSK</i>
Proposal	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	e.g. <i>3DES and SHA1</i>
DH Group	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	e.g. <i>2 (1024 Bit)</i>
Lifetime	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	e.g. <i>28800 and 0</i>
Authentication Method	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	<i>Preshared Keys</i>
Mode	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	<i>Aggressive</i>
Local ID Type	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	e.g. <i>IPV4 Address</i>
Local ID Value	<b>VPN -&gt; IPsec -&gt; Phase-1 Profiles-&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	e.g. <i>192.168.1.254</i>
Alive Check	<b>VPN -&gt; IPsec -&gt;Phase-1 Profiles -&gt; &lt;Multi-Proposal&gt; -&gt;</b>  <b>-&gt; Advanced Settings</b>	<i>Inactive</i>
NAT Traversal	<b>VPN -&gt; IPsec -&gt;Phase-1 Profiles -&gt; &lt;Multi-Proposal&gt; -&gt;</b>  <b>-&gt; Advanced Settings</b>	<i>Disabled</i>
Description	<b>VPN -&gt; IPsec -&gt; Phase-2 Profiles-&gt;</b>	e.g. <i>Phase2</i>

Field	Menu	Value
	<Multi-Proposal> -> 	
Proposal	VPN -> IPsec -> Phase-2 Profiles-> <Multi-Proposal> -> 	e.g. 3DES and SHA1
Use PFS Group	VPN -> IPsec -> Phase-2 Profiles-> <Multi-Proposal> -> 	Enabled
Lifetime	VPN -> IPsec -> Phase-2 Profiles-> <Multi-Proposal> -> 	e.g. 3600 and 0
Alive Check	VPN -> IPsec ->Phase-2 Profiles -> <Multi-Proposal> ->  -> <b>Advanced Settings</b>	Disabled
Propagate PMTU	VPN -> IPsec ->Phase-2 Profiles -> <Multi-Proposal> ->  -> <b>Advanced Settings</b>	Disabled

## Chapter 2 Security - IPsec client authentication via XAuth on Microsoft RADIUS Server (IAS)

### 2.1 Introduction

This chapter describes VPN IPsec connection of the **bintec secure IPsec clients** to a **bintec R3000** VPN gateway with advanced authentication (XAuth) on Microsoft Windows 2003 RADIUS server. A double authentication is performed at VPN tunnel setup. The VPN IPsec client authenticates itself per preshared key at the VPN gateway; in addition, user login is performed over Windows 2003 server. The VPN IPsec client is subsequently assigned a dynamic private IP address (per IKE config mode) from the local network.

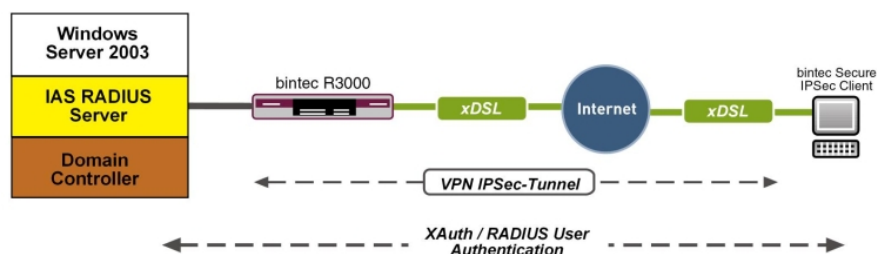


Fig. 9: Example scenario

### Requirements

The following are required for the configuration:

- A VPN gateway e.g. **bintec R3000** with system software 7.8.7 (XAuth support)
- A **bintec secure IPsec client**
- A Microsoft Windows 2003 Server with installed Internet Authentication Service (IAS)
- VPN gateway and VPN client each require an independent Internet connection

### 2.2 Configuration

## 2.2.1 Configuration of the VPN gateway

### Configuring the local IP address

The VPN gateway is operated here with IP address 192.168.10.254. To assign the VPN client an IP address from this network range, the option **Proxy ARP** must be enabled.

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

Fig. 10: LAN -> IP Configuration -> Interfaces -> Edit

#### Relevant fields in the Interfaces menu

Field	Meaning
Address mode	Select how an IP address is assigned to the interface.
IP Address/Netmask	Here, enter the <b>IP address</b> and the corresponding <b>Netmask</b> of the interface.
Interface Mode	Here, select the configuration mode of the interface.
Proxy ARP	Enable the option <b>Proxy ARP</b> .

### VPN Configuration

An IP address pool is specified in the **IP Pools** menu, from which an address is assigned to the VPN client at tunnel setup. In our example, a range from the local network is selected, e.g. 192.168.10.150 to 192.168.10.180.

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



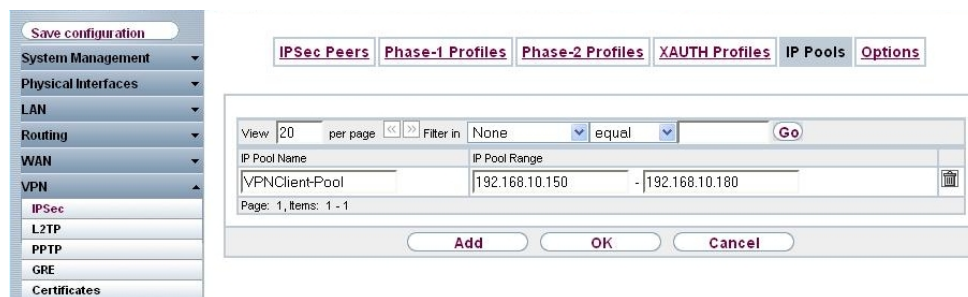


Fig. 11: VPN -> IPsec -> IP Pools -> Add

### Relevant fields in the IP Pools menu

Field	Meaning
IP pool name	Enter the name of the IP pool.
IP pool range	In the first field, enter the first IP address from the local network.  In the second field, enter the last IP address from the local network.

### XAUTH Configuration

A RADIUS server must be used for advanced IPsec authentication (XAuth). Perform all necessary settings in the **XAuth Profile** menu.

- (1) Go to **VPN -> IPsec -> XAUTH Profiles -> New**.

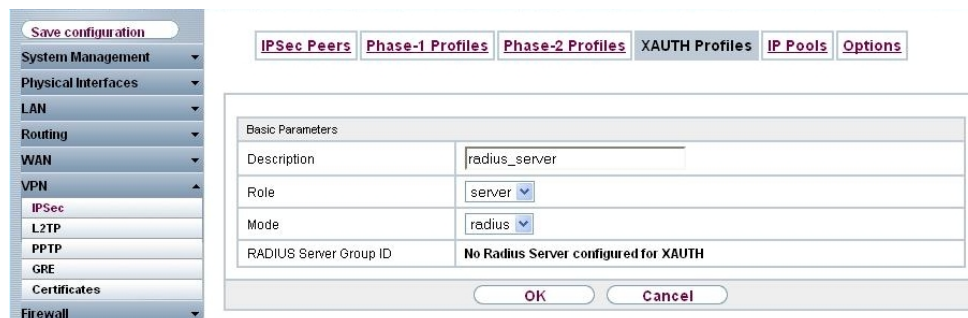


Fig. 12: VPN -> IPsec -> XAUTH Profiles -> New

### Relevant fields in the XAUTH Profiles menu

Field	Meaning
Description	Enter a description for the IPsec authentication.
Role	Here, select <i>Server</i> .


Field	Meaning
Mode	Under <b>Mode</b> select <i>RADIUS</i> .

### IPsec peers configuration

You can now configure **IPsec Peers**. Create one entry per VPN client connection. The **pre-shared key** as well as the **local ID** must be differently saved for every user or tunnel.

Choose the **New** button to set up more IPsec peers.

- (1) Go to **VPN -> IPsec -> IPsec Peers ->** .

Fig. 13: **VPN -> IPsec -> IPsec Peers ->** 

#### Relevant fields in the Peer Parameter menu

Field	Meaning
Administrative Status	Set Administrative Status to <b>Active</b> . The peer is available for setting up a tunnel immediately after saving the configuration.

Field	Meaning
Description	Enter a description of the peer that identifies it.
Peer ID	Select the ID type and enter the peer ID. On the peer device, this ID corresponds to the parameter <b>Local ID Value</b> .  Possible ID types: <ul style="list-style-type: none"> <li>• Full Qualified Domain Name (FQDN)</li> <li>• E-mail Address</li> <li>• IVP4 address</li> <li>• ASN.1-DN (Distinguished Name)</li> </ul>
Preshared Key	Under <b>Preshared Key</b> enter the password agreed with the peer.
IP Address Assignment	Select the configuration mode of the interface.  When selecting the option <i>IKE Config Mode</i> choose an IP address from the configured IP pool.
IP Assignment Pool	Select an IP pool configured in the <b>VPN -&gt; IP Pools</b> menu. If an IP pool has not been configured here yet, the message <i>Not yet defined</i> appears in this field.
Local IP Address	Enter the WAN IP address of your IPsec tunnel. This can be the same IP address as the address configured on your router as the LAN IP address.


The **Advanced Settings** menu consists of the following fields:


#### Relevant fields in the menu Advanced Settings

Field	Meaning
Phase 1 Profile	If selecting <i>None (use standard profile)</i> the profile indicated as standard in <b>Phase 1 Profiles</b> is used.
Phase 2 Profile	When selecting <i>None (use standard profile)</i> the profile indicated as standard in <b>Phase 2 Profiles</b> is used.
XAUTH Profile	Here, select a configured XAUTH profile (e.g. <i>radius_server</i> ).
Start mode	Here, you can select how the peer is to be switched to the active state. By selecting <i>On Demand</i> the peer is switched to the active state with a trigger.
Back Route Verify	Here, it is determined whether a check on the back route should be enabled for the interface to the connection partner.

Field	Meaning
Proxy ARP	Set <b>Proxy ARP</b> to <i>Up</i> or <i>Dormant</i> . Your device only responds to an ARP request if the status of the connection to the IPsec peer is up or dormant.
Mode	Set the <b>Mode</b> of the <b>IPsec callback</b> to <i>Inactive</i> . The local device neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote device.

### 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 ->** .

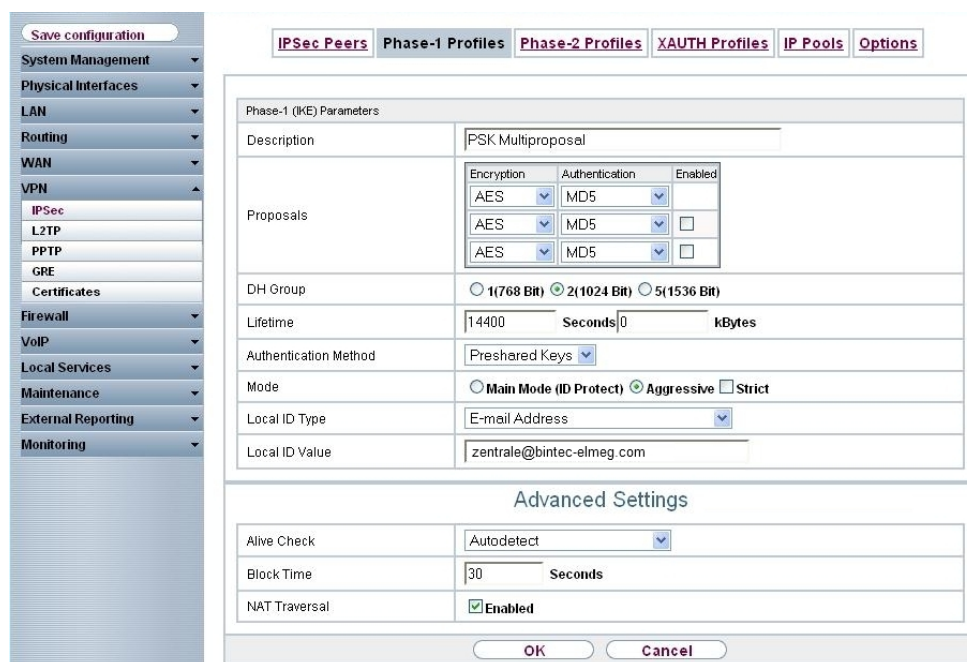



Fig. 14: **VPN -> IPsec -> Phase 1 Profiles ->** 

### Relevant fields in the Phase 1 Parameters (IKE) menu

Field	Meaning
Mode	Select Phase 1 mode <i>Aggressive</i> .

Field	Meaning
	The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication; it requires only three messages for configuring a secure channel.
Local ID Type	Select the local ID type.  Possible values: <ul style="list-style-type: none"> <li>• Full Qualified Domain Name (FQDN)</li> <li>• E-mail Address</li> <li>• IVP4 address</li> <li>• ASN.1-DN (Distinguished Name)</li> </ul>
Local ID Value	Enter the VPN gateway ID, e.g. <i>headoffice@bintec-elmeg.com</i>

### Phase-2 Profiles

Settings in the **VPN -> IPsec -> Phase 2 Profiles** menu can be taken over unchanged.

### RADIUS settings

Settings in the **RADIUS** menu enable advanced IPsec authentication (XAuth) with the Windows 2003 RADIUS server (IAS). You must set **Authentication Type** to *XAuth* as well as save the **Server IP address** of the Microsoft Windows 2003 RADIUS server (IAS). Communication with the RADIUS server is password-protected.

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

The screenshot shows a configuration window for RADIUS. On the left is a navigation menu with categories like System Management, Physical Interfaces, and Local Services. The main area is titled 'RADIUS' and has sub-tabs for 'TACACS+' and 'Options'. It is divided into two sections: 'Basic Parameters' and 'Advanced Settings'. The 'Basic Parameters' section includes fields for Authentication Type (set to XAUTH), Server IP Address (192.168.10.100), RADIUS Secret (masked), Priority (0), Entry active (checked), and Group Description (xauth). The 'Advanced Settings' section includes Policy (Authoritative), UDP Port (1812), Server Timeout (1000 milliseconds), Alive Check (checked), Retries (1), and a section for RADIUS Dialout with options for Enabled (checked), Reload Interval (0 seconds), and Default User Password (masked). At the bottom are 'OK' and 'Cancel' buttons.

Fig. 15: System Management->Remote Authentication->RADIUS->New

Relevant fields in the RADIUS menu

Field	Meaning
Authentication Type	Select <b>Authentication Type</b> <i>XAUTH</i> .
Server IP Address	Enter the <b>Server IP address</b> of the Microsoft Windows 2003 RADIUS server (IAS).
RADIUS Password	Enter the shared password used for communication between the RADIUS server and your device (e.g. <i>bintec elmeg</i> ).
Group description	<p>Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS servers for a group are queried according to <b>priority</b> and <b>policy</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>New</i> (default value): Enter a new group description in the text field, e.g. <i>xauth</i></li> <li>&lt;Group Name&gt;: Select a predefined group from the list.</li> </ul>

## 2.2.2 Configuration of the Windows 2003 RADIUS Server

In our example, a Windows 2003 RADIUS server is used for advanced IPsec authentication (XAuth). **Internet Authentication Service (IAS)** must be installed on this server. The RADIUS server accesses the Microsoft Active Directory Service and uses Windows logon data for advanced IPsec authentication (XAuth).

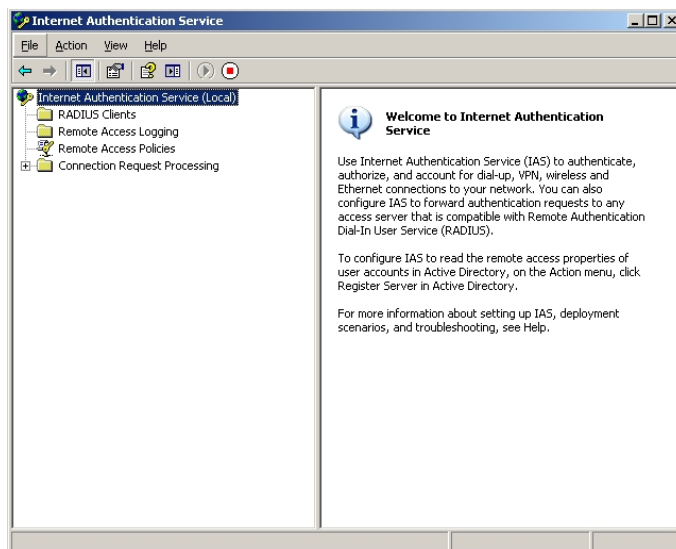


Fig. 16: Internet Authentication Service

In the Microsoft Management Console **Internet Authentication Service** the *R3000* must be created in the **New RADIUS Client** submenu as a RADIUS client. Enter the designation and IP address of the VPN gateway.

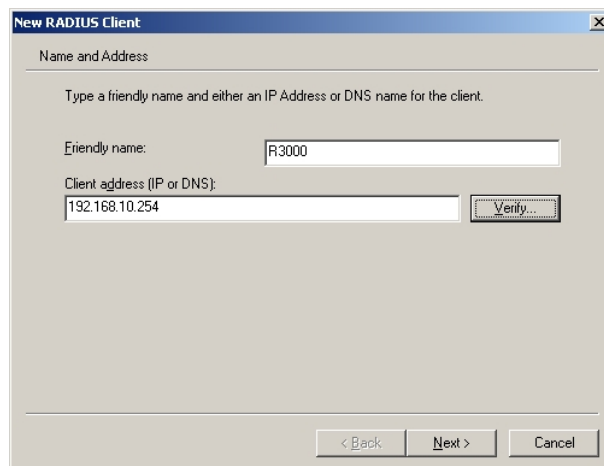


Fig. 17: New RADIUS Client

Here, the password for RADIUS communication (e.g. *bintec elmeg*) is saved.

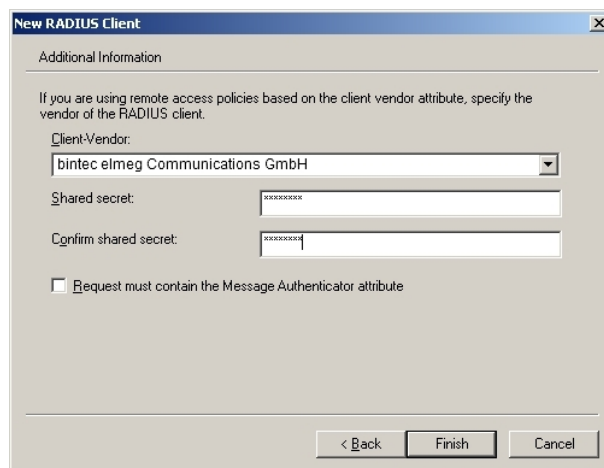


Fig. 18: Password

Then, a new policy is created in the **New Remote Access Policy Wizard**.



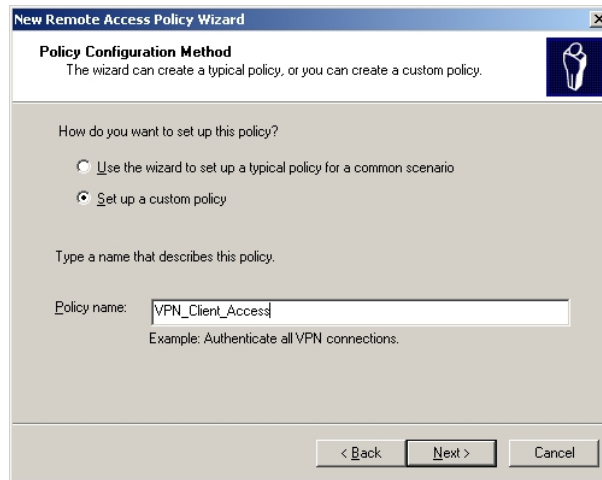


Fig. 19: Policy Name

When creating the **Remote Access Policy**, conditions to which this dial-in policy shall apply must be saved. In our example, the corresponding client provider is saved. For example, it would also be possible to save a specific time-span during which the dial-in policy should be used.

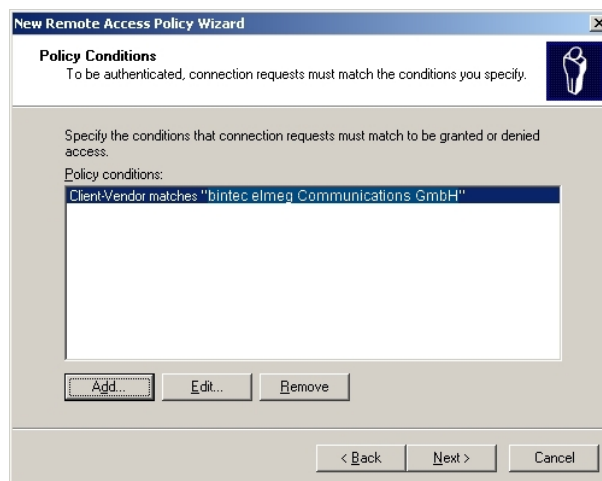


Fig. 20: Policy Conditions

The dial-in policy should allow VPN access or access to the network. For this, enable *Grant remote access permission*.

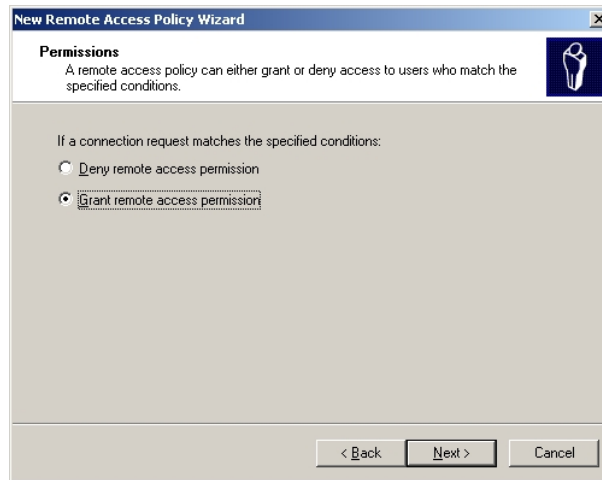


Fig. 21: Permissions

The other steps for creating a new dial-in policy can be taken over, as shown in the following steps.

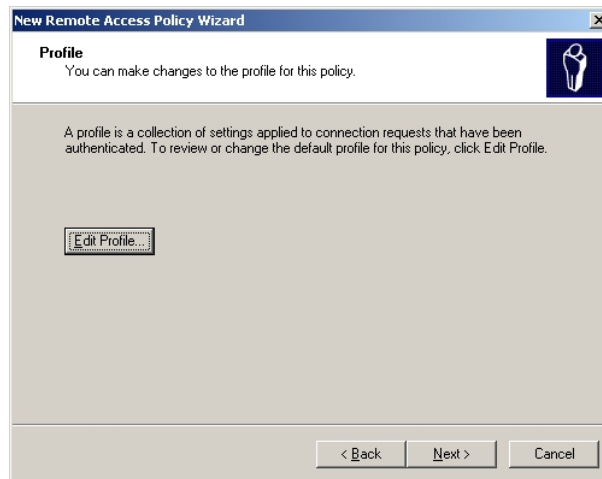


Fig. 22: Profiles

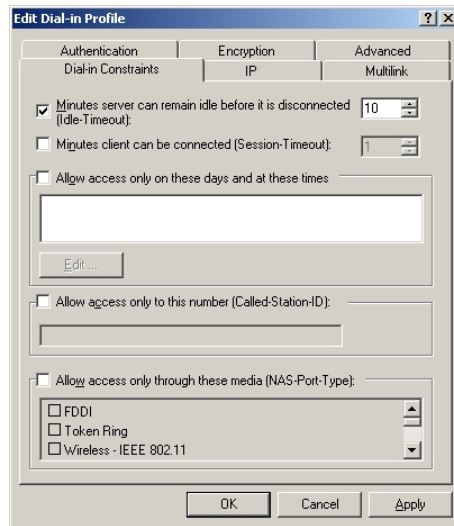


Fig. 23: Dial-in constraints

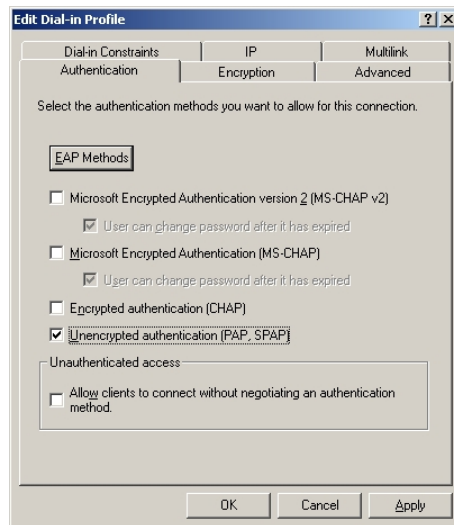


Fig. 24: Authentication

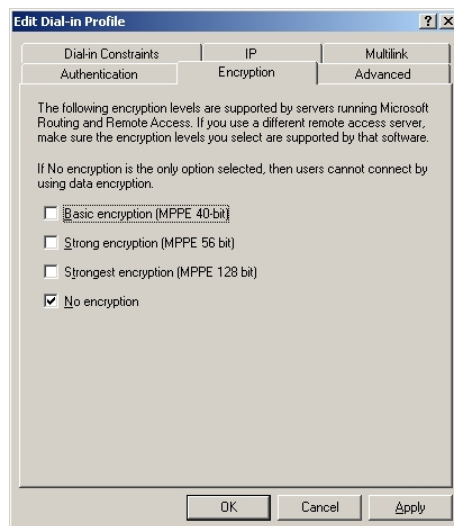


Fig. 25: Encryption

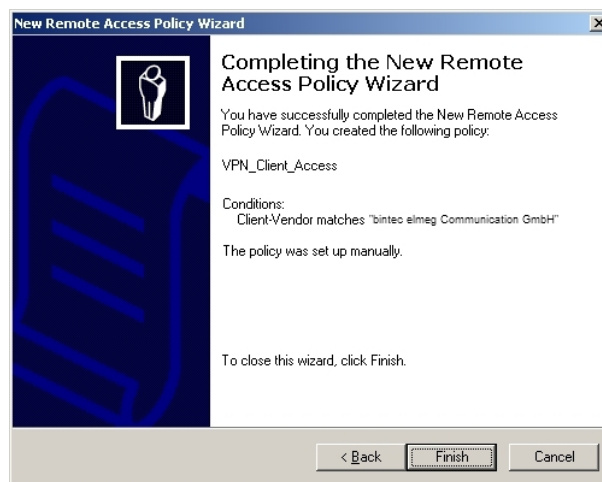


Fig. 26: New remote access policy wizard

Via user administration of **Active Directory Services** there is the option of allowing, or preventing, VPN dial-in per user.

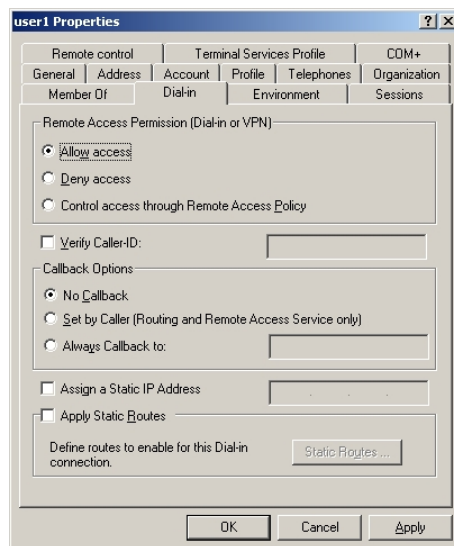


Fig. 27: dial-in

### 2.2.3 Configuration of bintec secure IPsec clients

The **bintec secure IPsec client** is called up with **Start -> Program -> FEC Secure IPsec Client -> Secure Client Mode**. Configuration of the **bintec secure IPsec clients** is performed with the assistant. At first launch of the **bintec secure IPsec client** the **new assistant profile** starts automatically. Select **Company Network Connection over IPsec**.

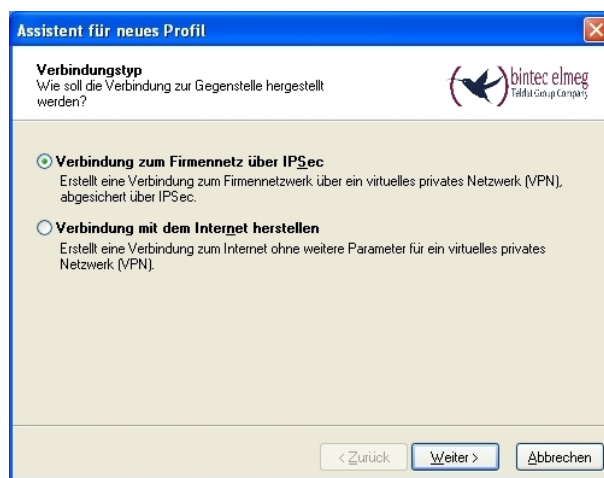


Fig. 28: Connector Type

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

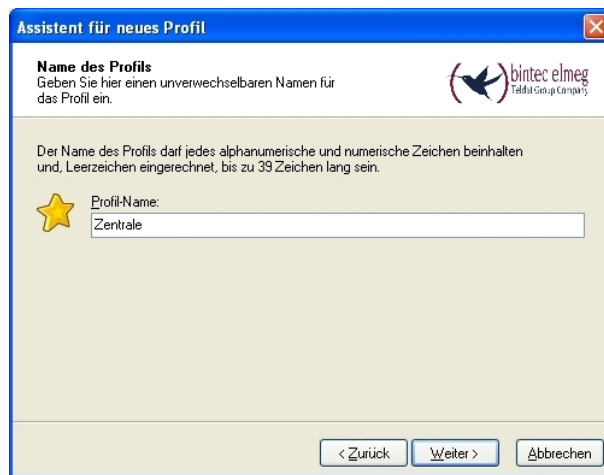


Fig. 29: Profile Name

In the next step of the assistant, 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.

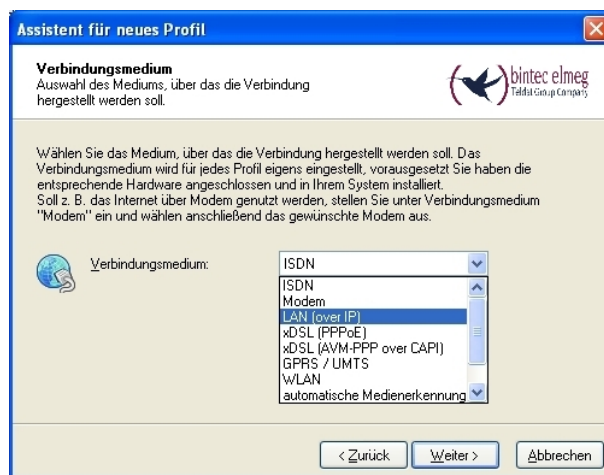


Fig. 30: Connection Medium

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)*.

**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:  
Passwort:  
Passwort (Wiederholung):

< Zurück Weiter > Abbrechen

Fig. 31: VPN gateway parameters

Next, *Aggressive Mode* is used as **Exchange Mode** because the **bintec R3000 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 Richtlinien der IPSec-Verhandlung wird die Einstellung "Automatischer Modus" verwendet. Sollen bestimmte IKE / IPSec-Richtlinien 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

< Zurück Weiter > Abbrechen

Fig. 32: IPSec Configuration

In the next step of the assistant, the **preshared key** saved in the VPN gateway, along with its **peer ID**, are saved. In the **Type** field, use of the option *Fully Qualified Username* is recommended.

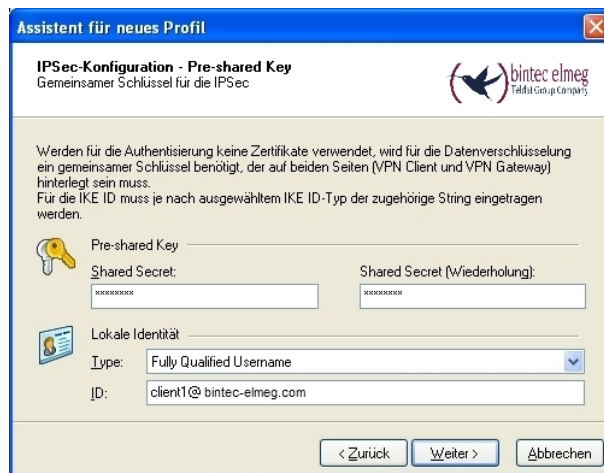


Fig. 33: Pre-shared key

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.

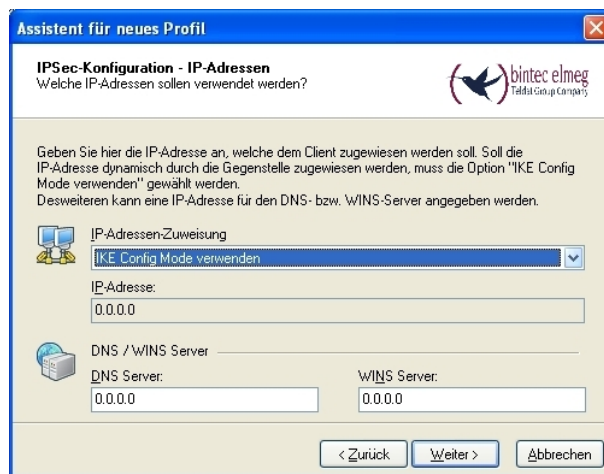


Fig. 34: IKE Config Mode

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



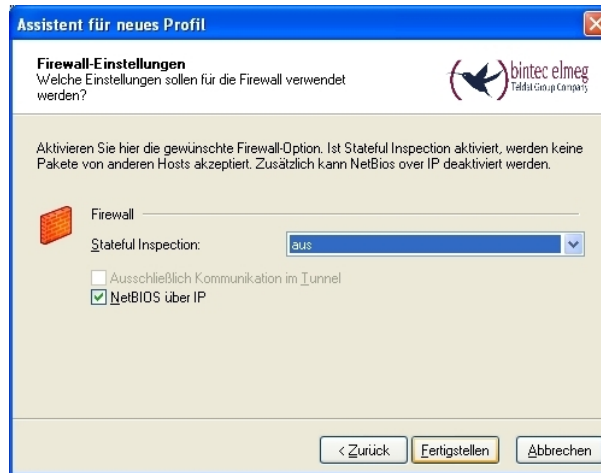


Fig. 35: Firewall

## 2.3 Checking the connection

At setup of the VPN IPsec tunnel, a user password request appears on the **bintec secure IPsec client**. The Windows logon data must be entered there. Besides IPsec authentication, there is an additional authentication at the RADIUS server. Next, an IP address is assigned to the **bintec secure IPsec client**.

## VPN gateway system messages

```

13:38:37 DEBUG/IPSEC: P1: peer 0 () sa 78 (R): new ip 10.1.1.2 <- ip 10.1.1.3
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'da8e937880010000'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsra-isakmp-xauth-06'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsec-nat-t-ike-03'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsec-nat-t-ike-02'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'draft-ietf-ipsec-nat-t-ike-00'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is '4a131c81070358455c5728f20e95452f'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'Dead Peer Detection (DPD, RFC 3706)'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'cb1ed48b6d68269bb411b61a07bce24a'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is 'c61bacaf1a60cc10800000000000000'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is '4048b7d56ebce88525e7de7f00d6c2d3c0000000'
13:38:37 INFO/IPSEC: P1: peer 0 () sa 78 (R): Vendor ID: 10.1.1.3:669 (No Id) is '12f5f28c457168a9702d9fe274cc0100'
13:38:37 DEBUG/IPSEC: P1: peer 1 (VPNClient) sa 78 (R): identified ip 10.1.1.2 <- ip 10.1.1.3
13:38:38 DEBUG/IPSEC: P1: peer 1 (VPNClient) sa 78 (R): notify id usr@fqdn(any:0,[0..23]=zentrale@funkwerk-ec.com) <- id
usr@fqdn(any:0,[0..22]=client1@funkwerk-ec.com): Initial contact notification proto 1 spi(16) =
[f8c1c782 5235a083 : aa54a587 ea60d83d]
13:38:38 DEBUG/IPSEC: P1: peer 1 (VPNClient) sa 78 (R): [Aggr] NAT-T: port change: local: 10.1.1.2:500->10.1.1.2:4500,
remote: 10.1.1.3:669->10.1.1.3:56542
13:38:38 INFO/IPSEC: XAUTH: peer 1 (VPNClient) sa 78 (I): request extended authentication
13:38:38 INFO/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 48 (R): deleted (Initial contact), Pkts: 123/98 Hb: 0/1 Bytes:
40856(48984)/18600(25840) rekeyed by 0
13:38:38 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 48 (R): SA 106 deleted errors 0/0/0
13:38:38 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 48 (R): SA 105 deleted errors 0/0/0
13:38:38 INFO/IPSEC: Destroy Bundle 48 (Peer 1 Traffic -1)
13:38:38 INFO/IPSEC: P1: peer 1 (VPNClient) sa 78 (R): done id usr@fqdn(any:0,[0..23]=zentrale@funkwerk-ec.com) <- id
usr@fqdn(any:0,[0..22]=client1@funkwerk-ec.com) AG[f8c1c782 5235a083 : aa54a587 ea60d83d]
13:38:38 DEBUG/IPSEC: RADIUS: requested user user1
13:38:38 INFO/IPSEC: XAUTH: peer 1 (VPNClient) sa 78 (I): extended authentication for user 'user1' succeeded
13:38:40 INFO/IPSEC: CFG: peer 1 (VPNClient) sa 78 (R): request for ip address received
13:38:40 INFO/IPSEC: CFG: peer 1 (VPNClient) sa 78 (R): ip address 192.168.10.166 assigned
13:38:40 INFO/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 49 (R): created 0.0.0.0/0:0 < any > 192.168.10.166/32:0 rekeyed 0
13:38:40 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 49 (R): SA 107 established ESP[490750e9] in[0] Mode tunnel enc
aes-cbc (128 bit) auth md5 (128 bit)
13:38:40 DEBUG/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 49 (R): SA 108 established ESP[56954d49] out[0] Mode tunnel enc
aes-cbc (128 bit) auth md5 (128 bit)
13:38:40 INFO/IPSEC: Activate Bundle 49 (Peer 1 Traffic -1)
13:38:40 INFO/IPSEC: P2: peer 1 (VPNClient) traf 0 bundle 49 (R): established (10.1.1.2<->10.1.1.3) with 2 SAs life 28800
Sec/0 Kb rekey 25920 Sec/0 KbHb none PMTU

```

## Log book of the bintec secure IPsec client

```

3/12/2009 1:34:36 PM IPsec: Start building connection
3/12/2009 1:34:36 PM Ike: phase1.name(Zentrale) - outgoing connect request - aggressive mode.
3/12/2009 1:34:36 PM Ike: XMIT_MSG1_AGGRESSIVE - Zentrale
3/12/2009 1:34:36 PM Ike: RECV_MSG2_AGGRESSIVE - Zentrale
3/12/2009 1:34:36 PM IPsec: Final Tunnel EndPoint is:010.001.001.002
3/12/2009 1:34:36 PM Ike: IKE phase I: Setting LifeTime to 28800 seconds
3/12/2009 1:34:36 PM Ike: Turning on XAUTH mode - Zentrale
3/12/2009 1:34:36 PM Ike: IkeSa negotiated with the following properties -
3/12/2009 1:34:36 PM Authentication=XAUTH_INIT_PSK,Encryption=AES,Hash=MD5,DHGroup=2,KeyLen=128
3/12/2009 1:34:36 PM Ike: Zentrale ->Support for NAT-T version - 3
3/12/2009 1:34:36 PM Ike: Turning on NATD mode - Zentrale - 1
3/12/2009 1:34:36 PM Ike: XMIT_MSG3_AGGRESSIVE - Zentrale
3/12/2009 1:34:36 PM Ike: IkeSa negotiated with the following properties -
3/12/2009 1:34:36 PM Authentication=XAUTH_INIT_PSK,Encryption=AES,Hash=MD5,DHGroup=2,KeyLen=128
3/12/2009 1:34:36 PM Ike: Turning on DPD mode - Zentrale
3/12/2009 1:34:36 PM Ike: phase1.name(Zentrale) - connected
3/12/2009 1:34:36 PM SUCCESS: IKE phase 1 ready
3/12/2009 1:34:36 PM IPsec: Phase1 is Ready - IkeIndex=3
3/12/2009 1:34:36 PM IkeXauth: RECV_XAUTH_REQUEST
3/12/2009 1:34:36 PM IkeXauth: XMIT_XAUTH_REPLY
3/12/2009 1:34:36 PM IkeXauth: RECV_XAUTH_SET
3/12/2009 1:34:36 PM IkeXauth: XMIT_XAUTH_ACK
3/12/2009 1:34:36 PM IkeCfg: name <Zentrale> - IkeXauth: enter state open
3/12/2009 1:34:36 PM SUCCESS: Ike Extended Authentication is ready
3/12/2009 1:34:38 PM IkeCfg: XMIT_IKECFG_REQUEST - Zentrale
3/12/2009 1:34:38 PM IkeCfg: RECV_IKECFG_REPLY - Zentrale
3/12/2009 1:34:38 PM IkeCfg: name <Zentrale> - enter state open
3/12/2009 1:34:38 PM SUCCESS: IkeCfg ready
3/12/2009 1:34:38 PM IPsec: Quick Mode is Ready: IkeIndex = 00000003 , VpnSrcPort = 4500
3/12/2009 1:34:38 PM IPsec: Assigned IP Address: 192.168.10.167
3/12/2009 1:34:38 PM IPsec: DNS Server: 192.168.10.100
3/12/2009 1:34:38 PM IkeQuick: XMIT_MSG1_QUICK - Zentrale
3/12/2009 1:34:38 PM IkeQuick: RECV_MSG2_QUICK - Zentrale
3/12/2009 1:34:38 PM IkeQuick: Turning on PFS mode(Zentrale) with group 2
3/12/2009 1:34:38 PM IkeQuick: XMIT_MSG3_QUICK - Zentrale
3/12/2009 1:34:38 PM IkeQuick: phase2.name(Zentrale) - connected
3/12/2009 1:34:38 PM SUCCESS: Ike phase 2 [quick mode] ready
3/12/2009 1:34:38 PM IPsec: Created an IPSEC SA with the following characteristics -
3/12/2009 1:34:38 PM IpSrcRange=[192.168.10.167-192.168.10.167],IpDstRange=[0.0.0.0-255.255.255.255],IpProt...
3/12/2009 1:34:38 PM IPsec: connected: LifeDuration in Seconds = 20160 and in KiloBytes = 0
3/12/2009 1:34:38 PM IPsec: Connected to Zentrale on channel 1.
3/12/2009 1:34:38 PM PPP(lcp): connected to Zentrale with IP Address: 192.168.010.167. : 192.168.010.168.
3/12/2009 1:34:38 PM SUCCESS: IpSec connection ready
3/12/2009 1:34:41 PM SUCCESS: Link -> <Zentrale> IP address assigned to IP stack - link is operational.

```

In addition, there is an entry in the Windows 2003 Server syslog.

```

User user1 was granted access.
Fully-Qualified-User-Name = virtualnet.funkwerk-ec.com/FEC_QA_users/user1
NAS-IP-Address = <not present>
NAS-Identifier = r3000
Client-Friendly-Name = R3000
Client-IP-Address = 192.168.10.254
Calling-Station-Identifier = <not present>
NAS-Port-Type = <not present>
NAS-Port = <not present>
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = VPN_Client_Access
Authentication-Type = PAP
EAP-Type = <undetermined>

```

## 2.4 Windows login per VPN (optional)

The **bintec secure IPSec client** offers the option of performing a Windows login. For this, the VPN connection is already established at OS startup or at Windows login. Then, windows login occurs via this VPN connection.

The Windows login (per VPN connection) is activated in the **bintec secure IPSec client** in the **Configuration -> Logon Options** menu.

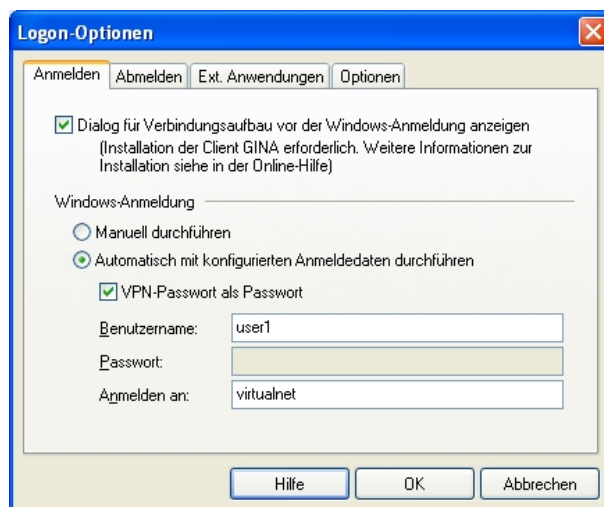


Fig. 36: Logon options

At OS startup, **FEC Secure IPSec Client - Windows Login** then appears.

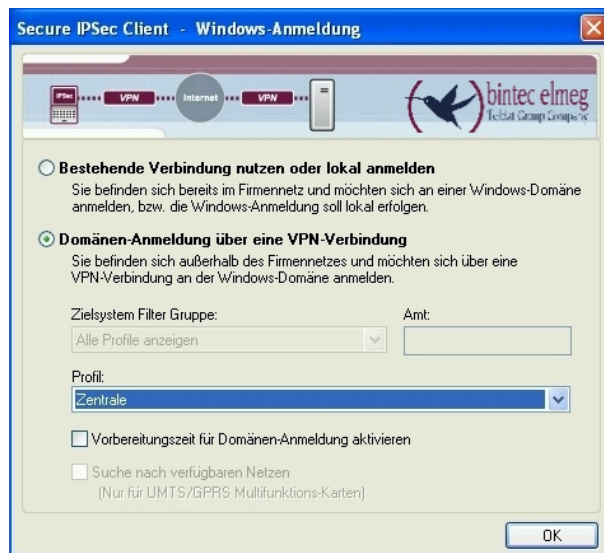


Fig. 37: Windows application

## 2.5 Overview of configuration steps

### Configuring the local IP address

Field	Menu	Value
Address mode	LAN -> IP Configuration-> Interfaces -> Edit	Static
IP Address/Netmask	LAN -> IP Configuration-> Interfaces -> Edit	e.g. 192.168.10.254 / 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Interfaces -> Edit	Manual
Proxy ARP	LAN -> IP Configuration-> Interfaces -> Edit	Enabled

### VPN Configuration

Field	Menu	Value
IP pool name	VPN -> IPSec -> IP Pools -> Add	e.g. VPNClient Pool
IP pool range	VPN -> IPSec -> IP Pools -> Add	e.g. 192.168.10.150 - 192.168.10.180




### XAUTH Configuration

Field	Menu	Value
Description	VPN -> IPSec -> XAUTH Profiles -> New	e.g. <i>radius_server</i>
Role	VPN -> IPSec -> XAUTH Profiles -> New	<i>Server</i>
Mode	VPN -> IPSec -> XAUTH Profiles -> New	<i>RADIUS</i>

### IPSec peers configuration

Field	Menu	Value
Administrative Status	VPN -> IPSec -> IPSec Peers -> 	<i>Active</i>
Description	VPN -> IPSec -> IPSec Peers -> 	e.g. <i>VPNClient1</i>
Peer ID	VPN -> IPSec -> IPSec Peers -> 	<i>E-mail Address / cli-ent1@bintec-elmeg.com</i>
Preshared Key	VPN -> IPSec -> IPSec Peers -> 	e.g. <i>bintec elmeg</i>
IP Address Assignment	VPN -> IPSec -> IPSec Peers -> 	<i>IKE Config Mode</i>
IP Assignment Pool	VPN -> IPSec -> IPSec Peers -> 	<i>VPNClient Pool</i>
Local IP Address	VPN -> IPSec -> IPSec Peers -> 	e.g. <i>192.168.10.254</i>
Phase 1 Profile	VPN -> IPSec -> IPSec Peers ->  -> <b>Advanced Settings</b>	<i>None (use Default Profile)</i>
Phase 2 Profile	VPN -> IPSec -> IPSec Peers ->  -> <b>Advanced Settings</b>	<i>None (use Default Profile)</i>
XAUTH Profile	VPN -> IPSec -> IPSec Peers ->  -> <b>Advanced Settings</b>	<i>radius_server</i>
Start mode	VPN -> IPSec -> IPSec Peers ->  -> <b>Advanced Settings</b>	<i>On Demand</i>
Back Route Verify	VPN -> IPSec -> IPSec Peers ->  -> <b>Advanced Settings</b>	<i>Disabled</i>
Proxy ARP	VPN -> IPSec -> IPSec Peers ->  -> <b>Advanced Settings</b>	<i>Up or Dormant</i>
Mode	VPN -> IPSec -> IPSec Peers ->  -> <b>Advanced Settings</b>	<i>Inactive</i>

**Configuration of Phase 1 Profiles**

Field	Menu	Value
Mode	VPN -> IPsec ->Phase 1 Profiles -> 	Aggressive
Local ID Type	VPN -> IPsec ->Phase 1 Profiles -> 	E-mail Address
Local ID Value	VPN -> IPsec ->Phase 1 Profiles -> 	e.g. headoffice@bintec-elmeg.com

**RADIUS settings**

Field	Menu	Value
Authentication Type	System Administration -> Remote Authentication -> RADIUS -> New	XAuth
Server IP Address	System Administration -> Remote Authentication -> RADIUS -> New	e.g. 192.168.10.100
RADIUS Password	System Administration -> Remote Authentication -> RADIUS -> New	e.g. bintec elmeg
Group description	System Administration -> Remote Authentication -> RADIUS -> New	e.g. xauth

**Configuration of the Windows 2003 RADIUS Server**

Field	Menu	Value
Friendly name	New RADIUS Client	R3000
Client address (IP or DNS)	New RADIUS Client	192.168.10.254
Client-Vendor	New RADIUS Client	e.g. bintec elmeg Communications GmbH
Shared secret	New RADIUS Client	e.g. bintec elmeg
Confirm shared secret	New RADIUS Client	e.g. bintec elmeg
Policy Name	New Remote Access Policy Wizard	e.g. VPN_Client_Access
Policy Conditions	New Remote Access Policy Wizard	e.g. Client-Vendor matches "BinTec Communications GmbH"
Grant remote access permission	New Remote Access Policy Wizard	Enabled

Field	Menu	Value
Edit Profile	<b>New Remote Access Policy Wizard</b>	Enabled
Idle Timeout	<b>Edit Dial-in Profile</b>	<i>10 minutes</i>
Authentication	<b>Edit Dial-in Profile</b>	<i>Unencrypted authentication (PAP, SPAP)</i>
Encryption	<b>Edit Dial-in Profile</b>	<i>No encryption</i>
dial-in	<b>user 1 Properties</b>	<i>Allowed access</i>

### Configuration of bintec secure IPSec clients

Field	Menu	Value
Connector Type	<b>Assistant for new profile</b>	<i>Connection to company network via IPSec</i>
Profile Name	<b>Assistant for new profile</b>	<i>Head Office</i>
Connection Medium	<b>Assistant for new profile</b>	<i>LAN (over IP)</i>
Gateway (Tunnel Endpoint)	<b>Assistant for new profile</b>	<i>e.g. vpn-gateway.bintec-elmeg.com</i>
Advanced authentication (XAUTH)	<b>Assistant for new profile</b>	Enabled
Exchange Mode	<b>Assistant for new profile</b>	Aggressive Mode
PFS Group	<b>Assistant for new profile</b>	DH Group 2 (1024 Bit)
Shared secret	<b>Assistant for new profile</b>	<i>e.g. bintec elmeg</i>
Shared Secret (Retry)	<b>Assistant for new profile</b>	<i>e.g. bintec elmeg</i>
Type	<b>Assistant for new profile</b>	<i>e.g. Fully Qualified Username</i>
ID	<b>Assistant for new profile</b>	<i>e.g. client1@bintec-elmeg.com</i>
IP address assignment	<b>Assistant for new profile</b>	<i>Use IKE Config Mode</i>
Stateful Inspection	<b>Assistant for new profile</b>	<i>off</i>
NetBIOS over IP	<b>Assistant for new profile</b>	Enabled



## Chapter 3 Security - VPN IPSec authentication with KOBIL SecOVID one-time password request

### 3.1 Introduction

This chapter describes VPN IPSec connection of the **bintec secure IPSec client** to a **bintec R3000** VPN gateway with advanced authentication (XAuth) over a one-time password on the **KOBIL SecOVID** server. At VPN tunnel setup, a double authentication per one-time password is performed, generated over a **KOBIL SecOVID** token. When the VPN connection is set up, the **bintec secure IPSec client** is assigned a dynamic IP address (per IKE-Config Mode) from the local network. The **bintec R3000** VPN gateway is configured with a multiuser VPN peer allowing connections of several VPN clients.

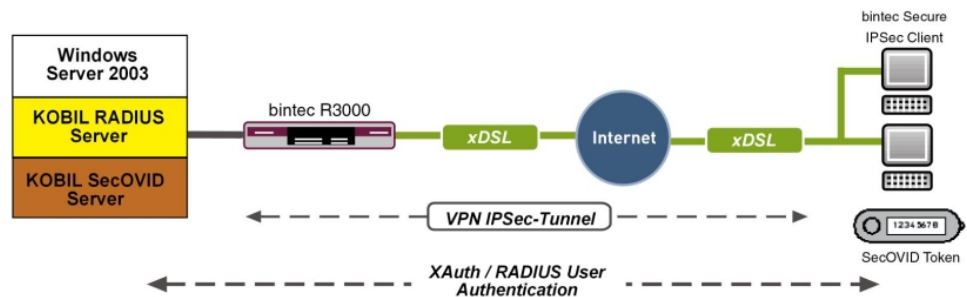


Fig. 38: Example scenario

### Requirements

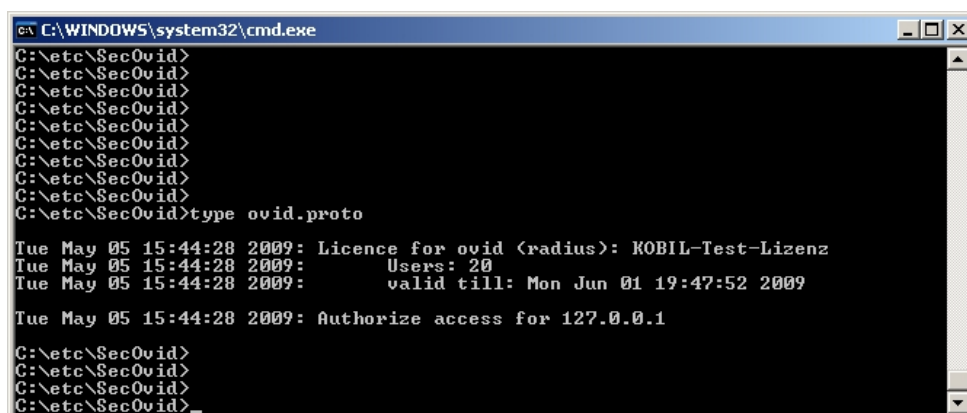
- A bintec VPN gateway e.g. **bintec R3000** with system software 7.8.7 (XAuth support)
- A **bintec secure IPSec client**
- A **KOBIL SecOVID** server installed on a Microsoft Windows computer (e.g. Server 2003 (32 Bit))
- A **KOBIL SecOVID** token
- VPN gateway and VPN client each require an independent Internet connection

## 3.2 Configuration

### 3.2.1 Installation of the KOBIL SecOVID server

#### Installation of the KOBIL SecOVID servers on a 32Bit Windows 2003 server

The installation program of the **KOBIL SecOVID** server is launched on the CD by opening the `win32\server\SECOVID Server.exe` file. Please read the setup outputs for your information and follow the instructions and recommendations of the installation routine. At conclusion of the installation routine, the logfile of the **KOBIL SecOVID** server should be checked to insure that the server started up.



```
C:\WINDOWS\system32\cmd.exe
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>type ovid.proto
Tue May 05 15:44:28 2009: Licence for ovid (radius): KOBIL-Test-Lizenz
Tue May 05 15:44:28 2009: Users: 20
Tue May 05 15:44:28 2009: valid till: Mon Jun 01 19:47:52 2009
Tue May 05 15:44:28 2009: Authorize access for 127.0.0.1
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
```

Fig. 39: Installation of the **KOBIL SecOVID**

#### Installation of the KOBIL SecOVID administration tool

For installation of the **KOBIL SecOVID** administration tool under Win32 systems, proceed as follows:

- Launch the setup program for the drivers of your KOBIL chip card terminal via `/Driver Setup/KOBILDriverSetup.exe`
- Follow setup program instructions and close the chip card terminal when prompted. The chip card terminal is required to administer the **KOBIL SecOVID** server per remote console. The KOBIL chip card terminal is not required for local administration of the **KOBIL SecOVID** server.

For installation of the **KOBIL SecOVID** administration tool, the setup program `win32/admin/Setup_admintools.exe` on the installation CD must be launched. At installation, please follow additional instructions of the setup program.

## Launching the KOBIL SecOVID administration tool

The **KOBIL SecOVID** administration tool is launched over the **Start -> Programs -> SecOVID Admintools -> WxOvid** menu. After initial startup of **SecOVID Admintools**, the secret token data can be imported and added to the SecOVID data bank. At a second SecOVID testing, token data are displayed in clear text. If you've bought the SecOVID tokens, the token data are generally provided in encrypted form. Token data import (e.g. `tokendata_firm.db`) occurs via the **Other Tokens -> Import Tokens** menu.

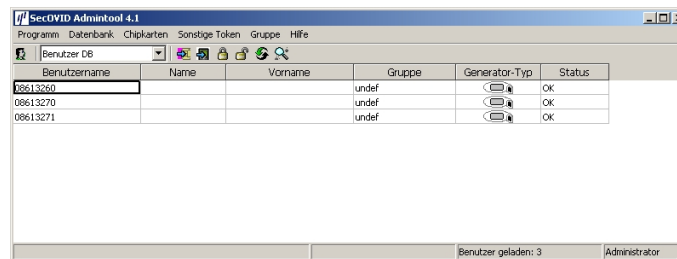


Fig. 40: Launching **KOBIL SecOVID** admintools

## Token personalisation

For assignment of tokens to a user, token sets must be blocked. After temporary blocking of a token data set, user information can be saved by editing the entry. The information in the **User Name** field is used after configuration of the **bintec secure IPSec client** for advanced IPSec authentication.

Fig. 41: User information

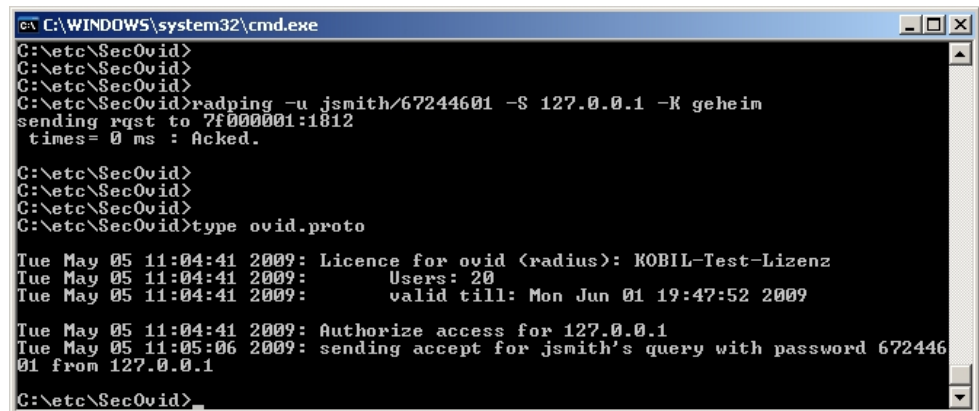
The data set must subsequently be unblocked.

Benutzername	Name	Vorname	Gruppe	Generator-Typ	Status
08613270			undef	OK	OK
jsmith	John	Smith	undef	OK	OK
mmustermann	Max	Mustermann	undef	OK	OK

Fig. 42: Unblock

### First function test

An initial function test can be performed with the command line tool `radping.exe`. With the one-time password, `Radping` initiates an authentication request on the SecOVID RADIUS server. During installation, the tool was saved in the `\etc\SecOVID\` directory. With the `-u` option, the user name and the one-time password are transmitted to the SecOVID server. The one-time password must be generated with the user token. The SecOVID server is addressed with the `-s` option. For the first function test, `radping` must be executed directly on the server. The RADIUS password is sent with the `-k` option. The default value is `secret`. The SecOVID logfile (`\etc\SecOVID\ovid.proto`) displays the following message in case of successful authentication:



```
C:\WINDOWS\system32\cmd.exe
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>radping -u jsmith/67244601 -S 127.0.0.1 -K geheim
sending rqst to 7f000001:1812
  times= 0 ms : Acked.

C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>type ovid.proto

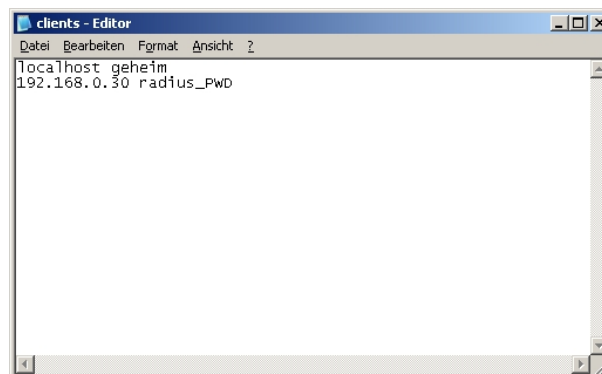
Tue May 05 11:04:41 2009: Licence for ovid (radius): KOBIL-Test-Lizenz
Tue May 05 11:04:41 2009:           Users: 20
Tue May 05 11:04:41 2009:           valid till: Mon Jun 01 19:47:52 2009

Tue May 05 11:04:41 2009: Authorize access for 127.0.0.1
Tue May 05 11:05:06 2009: sending accept for jsmith's query with password 672446
01 from 127.0.0.1
C:\etc\SecOvid>
```

Fig. 43: Function test

### Configuration of the RADIUS client on the SecOVID server

All RADIUS clients (e.g. the bintec VPN gateway, or the test application `radping`) must be saved on the SecOVID server as RADIUS client. For this, configuration file `\etc\SecOVID\clients` is edited. In our example, the bintec VPN gateway with the IP address `192.168.0.30` and the RADIUS password `radius_PWD` is added. This password is subsequently also saved on the VPN gateway in the RADIUS settings. The SecOVID server service must be restarted for these changes to become effective.



```
clients - Editor
Datei Bearbeiten Format Ansicht ?
localhost geheim
192.168.0.30 radius_PWD
```

Fig. 44: Clients-Editor

## 3.2.2 Configuration of the VPN gateway

### Local IP address of the VPN gateway

In our example, the VPN gateway is operated with IP address `192.168.0.30`. To assign

the **bintec secure IPsec client** an IP address from this network range, the option **Proxy ARP** must be enabled.

For this, go to the following menu:

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

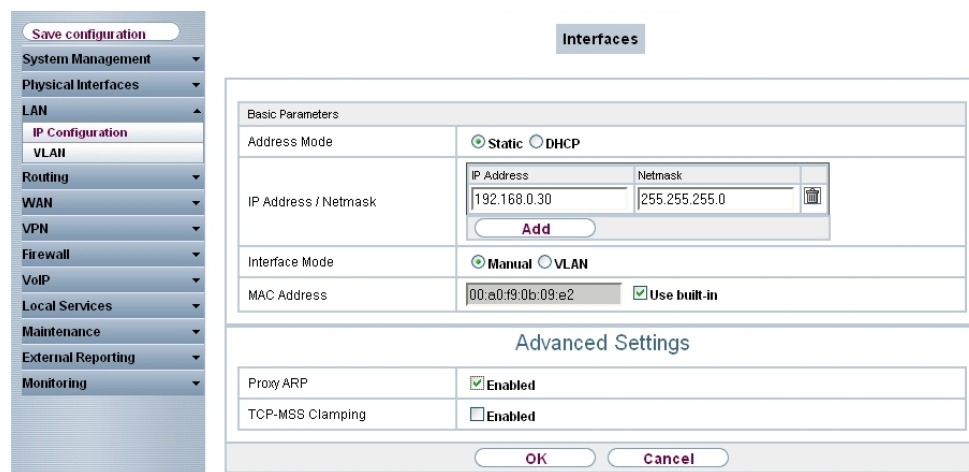


Fig. 45: **LAN -> IP Configuration -> Interfaces -> <en1-0>** 

#### Relevant fields in the Interfaces menu

Field	Description
IP Address/Netmask	With <b>Add</b> , add a new address entry and enter the <b>IP Address</b> and corresponding <b>Netmask</b> of the interface.
Proxy ARP	Enable the option <b>Proxy ARP</b> .

#### RADIUS settings

With the settings in the **RADIUS** menu, advanced IPsec authentication (XAuth) with the RADIUS server of the **KOBIL SecOVID** server is enabled. You must set the authentication type to the *XAUTH* value, and save the IP address of the **KOBIL SecOVID** server. Communication with the RADIUS server is password-protected. Here, please use the RADIUS password saved on the SecOVID server (configuration file `\etc\SecOVID\clients`).

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

The screenshot shows the RADIUS configuration window with the following settings:

- Basic Parameters:**
  - Authentication Type: XAUTH
  - Server IP Address: 192.168.0.111
  - RADIUS Secret: [Masked]
  - Priority: 0
  - Entry active:  Enabled
  - Group Description: xauth
- Advanced Settings:**
  - Policy: Authoritative
  - UDP Port: 1812
  - Server Timeout: 1000 Milliseconds
  - Alive Check:  Enabled
  - Retries: 1
  - RADIUS Dialout:  Enabled
    - Reload Interval: 0 Seconds
    - Default User Password: [Masked]

Fig. 46: System Management-> Remote Authentication -> RADIUS  
Relevant fields in the RADIUS menu

Field	Description
Authentication Type	Select <b>Authentication Type</b> <i>XAUTH</i> .
Server IP Address	Enter the <b>server IP address</b> of the <b>KOBIL SecOVID</b> server.
RADIUS Password	Enter the shared password used for communication between the RADIUS server and your device, e.g. <i>radius_PWD</i> .
Group description	<p>Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS servers for a group are queried according to <b>priority</b> and <b>policy</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>New</i> (default value): Enter a new group description in the text field</li> <li>&lt;Group Name&gt;: Select a predefined group from the list. e.g. <i>xauth</i>.</li> </ul>

## VPN Configuration

An IP address pool is specified in the **IP Pools** menu, from which an address is assigned to all VPN clients at tunnel setup. In our example, a range from the local network is selected,

e.g. 192.168.0.150 to 192.168.0.180.

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

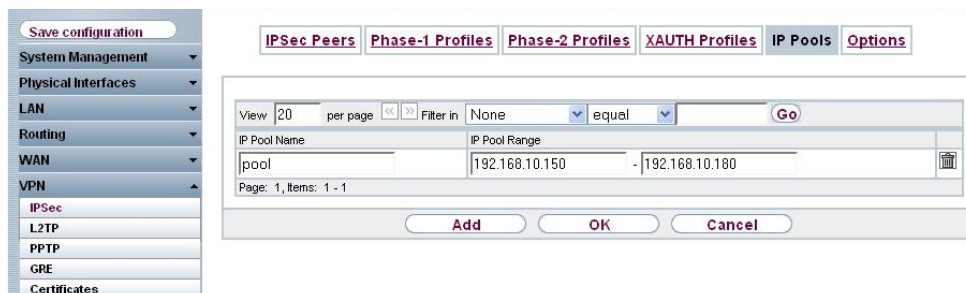


Fig. 47: VPN -> IPSec -> IP Pools -> Add

### Relevant fields in the IP Pools menu

Field	Meaning
IP pool name	Enter the name of the IP pool.
IP pool range	In the first field, enter the first IP address from the local network. In the second field, enter the last IP address from the local network.

### XAUTH Configuration

A RADIUS server must be used for advanced IPSec authentication (XAuth). Perform all necessary settings in the **XAuth Profile** menu.

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

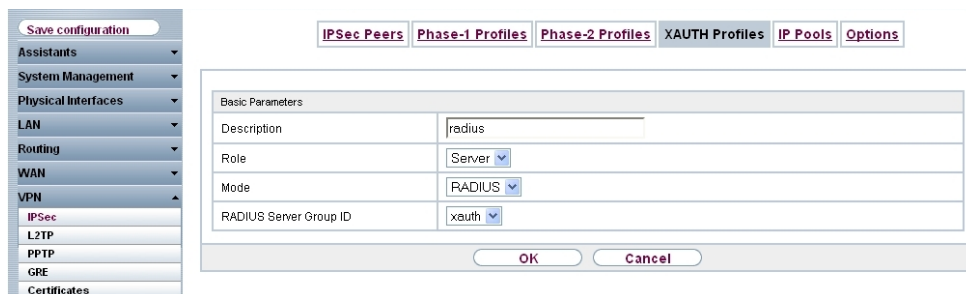


Fig. 48: VPN -> IPSec -> XAUTH Profiles -> New

### Relevant fields in the XAUTH Profiles menu



Field	Meaning
Description	Enter a description for the IPSec authentication, e.g. <i>radius</i> .
Role	Here, select <i>Server</i> .
Mode	Under <b>Mode</b> select <i>RADIUS</i> .
RADIUS Server Group ID	Select RADIUS server <i>xauth</i> .

### IPSec peers configuration

In the **IPSec Peers** menu, a multiuser VPN connection is configured, allowing connection setup of several **bintec secure IPSec clients**. If the VPN IPSec connection with preshared keys is to be authenticated, the same preshared key is used on all **bintec secure IPSec clients**. For the multiuser VPN connections, no ID information is saved in the **Peer ID** field.

Choose the **New** button to set up the IPSec peer.

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

Fig. 49: VPN -> IPsec -> IPsec Peers ->

**Relevant fields in the IPsec Peers menu**

Field	Meaning
Administrative Status	Set Administrative Status to <b>Active</b> . The peer is available for setting up a tunnel immediately after saving the configuration.
Description	Enter a description of the peer that identifies it.
Peer ID	Select the ID type.  Possible ID types: <ul style="list-style-type: none"> <li>• Full Qualified Domain Name (FQDN)</li> <li>• E-mail Address</li> <li>• IVP4 address</li> <li>• ASN.1-DN (Distinguished Name)</li> </ul>
Preshared Key	Under <b>Preshared Key</b> enter the password agreed with the peer.

Field	Meaning
IP Address Assignment	Select the configuration mode of the interface.  When selecting the option <i>IKE Config Mode</i> choose an IP address from the configured IP pool.
IP Assignment Pool	Select an IP pool configured in the <b>VPN -&gt; IP Pools</b> menu. If an IP pool has not been configured here yet, the message <i>Not yet defined</i> appears in this field.
Local IP Address	Enter the WAN IP address of your IPsec tunnel. This can be the same IP address as the address configured on your router as the LAN IP address.


The **Advanced Settings** menu consists of the following fields:

#### Relevant fields in the menu Advanced Settings

Field	Meaning
Phase 1 Profile	If selecting <i>None (use standard profile)</i> the profile indicated as standard in <b>Phase 1 Profiles</b> is used.
Phase 2 Profile	When selecting <i>None (use standard profile)</i> the profile indicated as standard in <b>Phase 2 Profiles</b> is used.
XAUTH Profile	Here, select a configured XAUTH profile (e.g. <i>radius</i> ).
Start mode	Here, you can select how the peer is to be switched to the active state. By selecting <i>On Demand</i> the peer is switched to the active state with a trigger.
Back Route Verify	Here, it is determined whether a check on the back route should be enabled for the interface to the connection partner.
Proxy ARP	Set <b>Proxy ARP</b> to <i>Up or Dormant</i> . Your device only responds to an ARP request if the status of the connection to the IPsec peer is up or dormant.  In the case of <i>Dormant</i> , your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route.
Mode	Set the <b>Mode</b> of the <b>IPsec callback</b> to <i>Inactive</i> . The local device neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote device.

#### Phase-1 Profiles

In the **Phase 1 Profiles** menu, aggressive mode is enabled and the **local ID value** of the

VPN gateway is set. Click on the  icon to edit existing entries. Select the **New** button to create new profiles.


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

Fig. 50: **VPN -> IPSec -> Phase 1 Profiles -> Edit** 

### Relevant fields in the Phase 1 Profiles menu

Field	Meaning
Mode	Select Phase 1 mode <i>Aggressive</i> .  The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication; it requires only three messages for configuring a secure channel.
Local ID Value	Enter the VPN gateway ID, e.g. <i>vpngate-way.bintec-elmeg.com</i>

### Phase-2 Profiles

Settings in the **VPN -> IPSec -> Phase 2 Profiles-> Edit**  can be taken over unchanged.

The screenshot shows the configuration window for Phase 2 Profiles. The left sidebar contains a navigation menu with categories like System Management, Physical Interfaces, Routing, WAN, VPN, and Firewall. The main window has tabs for IPsec Peers, Phase-1 Profiles, Phase-2 Profiles, XAUTH Profiles, IP Pools, and Options. The Phase-2 Profiles tab is active, showing a table of proposals and advanced settings.

Phase-2 (IPSEC) Parameters		
Description	Multi-Proposal	
Proposals	Encryption	Authentication Enabled
	3DES	MD5
	AES-128	MD5 <input checked="" type="checkbox"/>
	Blowfish	MD5 <input checked="" type="checkbox"/>
Use PFS Group	<input checked="" type="checkbox"/> Enabled <input type="radio"/> 1(768 Bit) <input checked="" type="radio"/> 2(1024 Bit) <input type="radio"/> 5(1536 Bit)	
Lifetime	7200	Seconds 0 kBytes
Advanced Settings		
IP Compression	<input type="checkbox"/> Enabled	
Alive Check	Autodetect	
Propagate PMTU	<input checked="" type="checkbox"/> Enabled	

Buttons: OK, Cancel

Fig. 51: VPN -> IPsec -> Phase 2 Profiles -> Edit 

### 3.2.3 Configuration of bintec secure IPsec clients

The **bintec secure IPsec client** is called up with **Start -> Program -> FEC Secure IPsec Client -> Secure Client Mode**. Configuration of the **bintec secure IPsec clients** is performed with the assistant. At first launch of the **bintec secure IPsec client** the **new assistant profile** starts automatically.

Select **Company Network Connection over IPsec**.

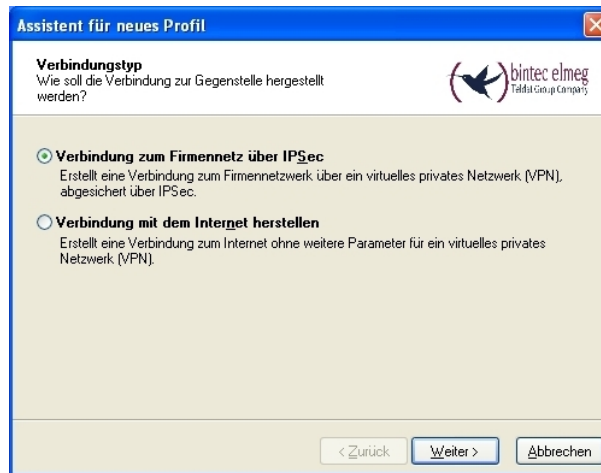


Fig. 52: Connector Type

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



Fig. 53: Profile Name

In the next step of the assistant, 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 **bintec secure IPSec client** establishes no direct Internet access but uses an Internet access router.

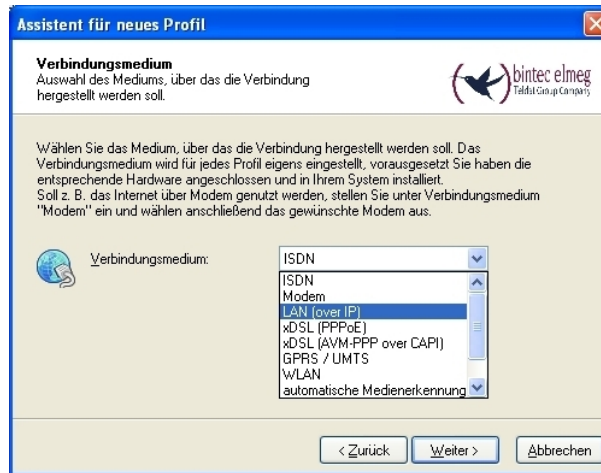


Fig. 54: Connection Medium

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)* to transfer the user name and password to the **KOBIL SecOVID** server.

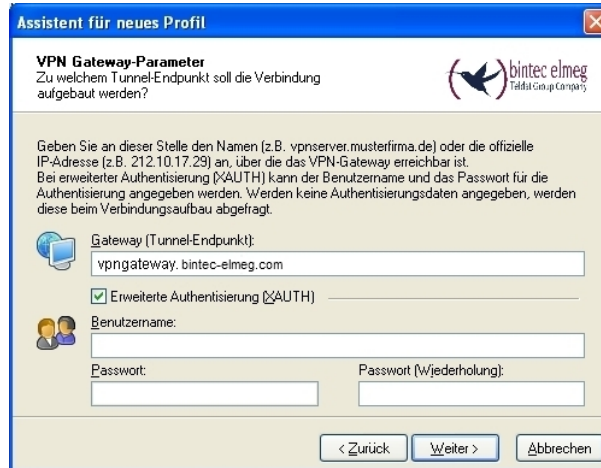


Fig. 55: VPN Gateway Parameters

Next, *Aggressive Mode* is used as **exchange mode** because the **bintec R3000** gateway 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.

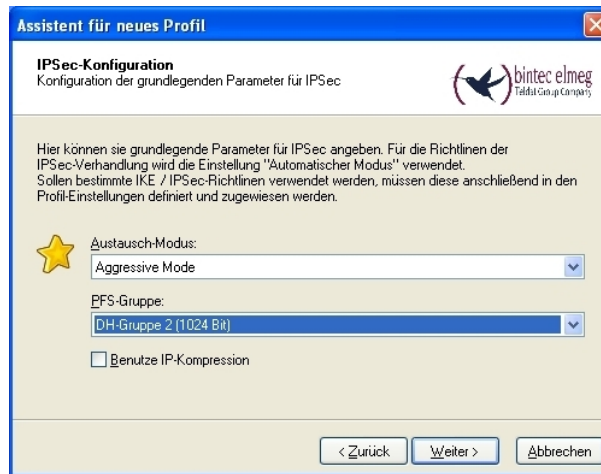


Fig. 56: IPSec Configuration

In the next assistant step, the **preshared key** configured on the VPN gateway is saved. The user e-mail address should be used as **local identity** under **Type Fully Qualified Username**.

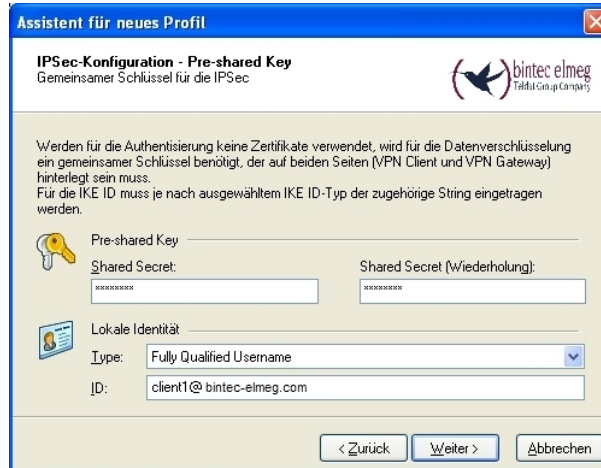


Fig. 57: Pre-shared key

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.



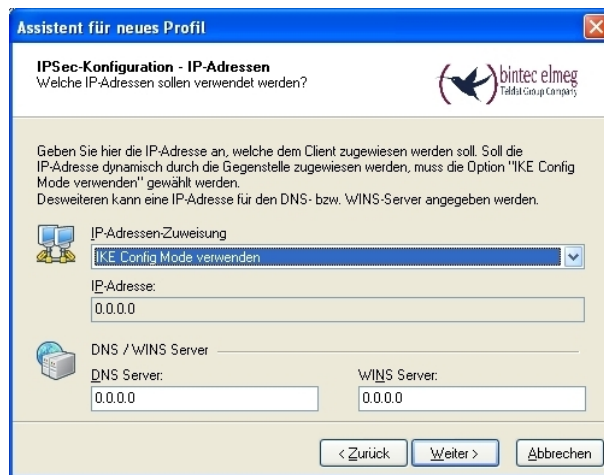


Fig. 58: IKE Config Mode

In the final step, the **firewall** of the **bintec secure IPsec client** is configured. If the client is directly connected to the Internet, the firewall should be enabled.

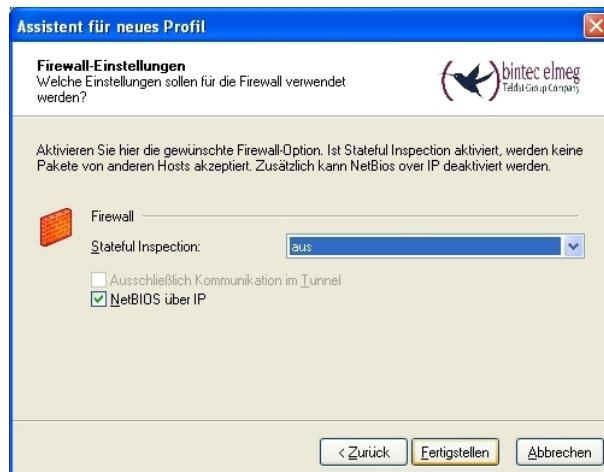


Fig. 59: Firewall

When setting up the VPN tunnel, the **bintec secure IPsec client** displays a **user ID** and **password** request. Here, the user name saved in the SecOVID admintool and the one-time password generated with the **KOBIL SecOVID** token are requested.

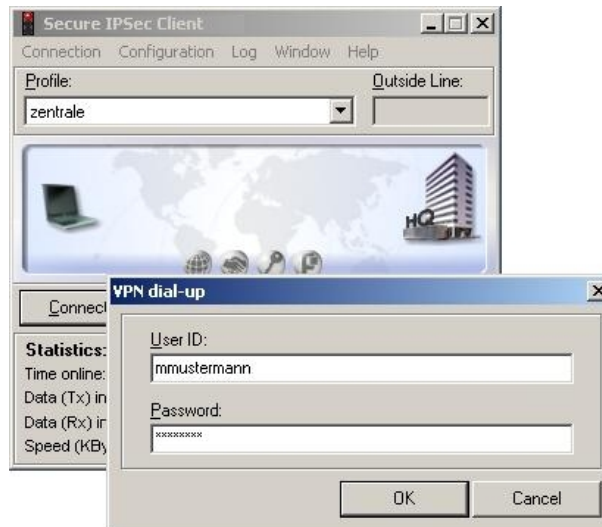


Fig. 60: User ID / Password Request

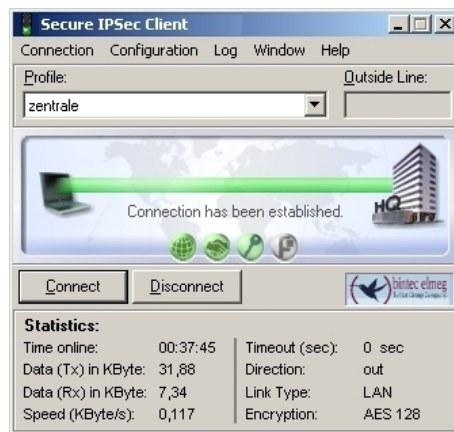






Fig. 61: FEC Secure IPSec Client

### 3.3 Overview of configuration steps

#### Configuration of the VPN gateway

Field	Menu	Value
Address mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Static
IP Address/Netmask	LAN -> IP Configuration-> Interfaces -> <en1-0> 	e.g. 192.168.0.30 / 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Manual
Proxy ARP	LAN -> IP Configuration-> Interfaces -> <en1-0> 	Enabled

#### RADIUS settings

Field	Menu	Value
Authentication Type	System Administration -> Remote Authentication -> RADIUS -> New	XAUTH
Server IP Address	System Administration -> Remote Authentication -> RADIUS -> New	e.g. 192.168.0.111
RADIUS Password	System Administration -> Remote Authentication -> RADIUS -> New	e.g. radius_PWD
Group description	System Administration -> Remote Authentication -> RADIUS -> New	xauth

#### VPN Configuration

Field	Menu	Value
IP pool name	VPN -> IPsec -> IP Pools -> Add	e.g. pool.
IP pool range	VPN -> IPsec -> IP Pools -> Add	e.g. 192.168.0.150 - 192.168.0.180

#### XAUTH Configuration


Field	Menu	Value
Description	VPN -> IPsec -> XAUTH Profiles -> New	e.g. radius
Role	VPN -> IPsec -> XAUTH Profiles -> New	Server
Mode	VPN -> IPsec -> XAUTH Profiles ->	RADIUS


Field	Menu	Value
	<b>New</b>	
RADIUS Server Group ID	<b>VPN -&gt; IPSec -&gt; XAUTH Profiles -&gt; New</b>	<i>xauth</i>

### IPSec peers configuration

Field	Menu	Value
Administrative Status	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt;</b> 	<i>Active</i>
Description	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt;</b> 	<i>e.g. vpnclient.</i>
Peer ID	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt;</b> 	<i>Fully Qualified Domain Name (FQDN)</i>
Preshared Key	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt;</b> 	<i>e.g. bintec elmeg</i>
IP Address Assignment	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt;</b> 	<i>IKE Config Mode</i>
IP Assignment Pool	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt;</b> 	<i>pool</i>
Local IP Address	<b>VPN -&gt; IPSec -&gt;IPSec Peers -&gt;</b> 	<i>e.g. 192.168.0.30</i>
Phase 1 Profile	<b>VPN -&gt; IPSec -&gt; IPSec Peers -&gt;</b>  -> <b>Advanced Settings</b>	<i>None (use Default Profile)</i>
Phase 2 Profile	<b>VPN -&gt; IPSec -&gt; IPSec Peers -&gt;</b>  -> <b>Advanced Settings</b>	<i>None (use Default Profile)</i>
XAUTH Profile	<b>VPN -&gt; IPSec -&gt; IPSec Peers -&gt;</b>  -> <b>Advanced Settings</b>	<i>radius</i>
Start mode	<b>VPN -&gt; IPSec -&gt; IPSec Peers -&gt;</b>  -> <b>Advanced Settings</b>	<i>On Demand</i>
Back Route Verify	<b>VPN -&gt; IPSec -&gt; IPSec Peers -&gt;</b>  -> <b>Advanced Settings</b>	<i>Disabled</i>
Proxy ARP	<b>VPN -&gt; IPSec -&gt; IPSec Peers -&gt;</b>  -> <b>Advanced Settings</b>	<i>Up or Dormant</i>
Mode	<b>VPN -&gt; IPSec -&gt; IPSec Peers -&gt;</b>  -> <b>Advanced Settings</b>	<i>Inactive</i>

### Configuration of Phase 1 Profiles

Field	Menu	Value
Mode	<b>VPN -&gt; IPSec -&gt;Phase 1 Profiles -&gt; Edit</b> 	<i>Aggressive</i>

Field	Menu	Value
Local ID Value	<b>VPN -&gt; IPSec -&gt;Phase 1 Profiles -&gt; Edit</b> 	e.g. <i>vpngate-way.bintec-elmeg.com</i>

### Configuration of bintec secure IPSec clients

Field	Menu	Value
Connector Type	<b>Assistant for new profile</b>	<i>Connection to company network via IPSec</i>
Profile Name	<b>Assistant for new profile</b>	<i>Head Office</i>
Connection Medium	<b>Assistant for new profile</b>	<i>LAN (over IP)</i>
Gateway (Tunnel Endpoint)	<b>Assistant for new profile</b>	e.g. <i>vpngate-way.bintec-elmeg.com</i>
Advanced authentication (XAUTH)	<b>Assistant for new profile</b>	Enabled
Exchange Mode	<b>Assistant for new profile</b>	Aggressive Mode
PFS Group	<b>Assistant for new profile</b>	DH Group 2 (1024 Bit)
Shared secret	<b>Assistant for new profile</b>	e.g. <i>bintec elmeg</i>
Shared Secret (Retry)	<b>Assistant for new profile</b>	e.g. <i>bintec elmeg</i>
Type	<b>Assistant for new profile</b>	e.g. <i>Fully Qualified Username</i>
ID	<b>Assistant for new profile</b>	e.g. <i>cli-ent1@bintec-elmeg.com</i>
IP address assignment	<b>Assistant for new profile</b>	<i>Use IKE Config Mode</i>
Stateful Inspection	<b>Assistant for new profile</b>	<i>off</i>
NetBIOS over IP	<b>Assistant for new profile</b>	Enabled

## Chapter 4 Security - Certificate-based VPN IPsec with optional KOBIL SecOVID one-time password request

### 4.1 Introduction

This chapter describes a certificate-based VPN IPsec connection of the **bintec secure IPsec client** to a **bintec R3000** VPN gateway. An owned certification authority (OpenSSL CA) is set up to generate the required certificates in PKCS#12 format. When the VPN tunnel is set up, a dynamic IP address is assigned to the **bintec secure IPsec client** (per IKE config mode). The solution can be optionally upgraded with one-time password request. Here, a one-time password is generated with a **KOBIL SecOVID** token authenticated on the **KOBIL SecOVID** server.

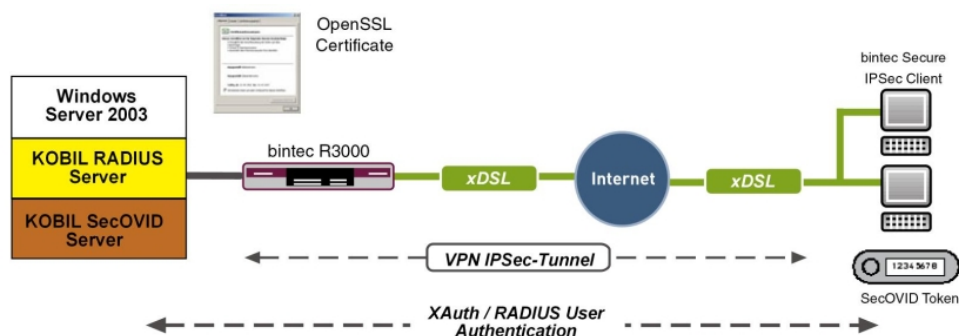


Fig. 62: Example scenario

### Requirements

- A bintec VPN gateway e.g. **bintec R3000** with system software 7.8.7 (XAuth support)
- A **bintec secure IPsec client**
- VPN gateway and VPN client each require an independent Internet connection
- Optionally, a **KOBIL SecOVID** server installed on a Microsoft Windows computer (e.g. Server 2003 (32 Bit))

### 4.2 Configuration

## 4.2.1 Setting up the OpenSSL certification authority

In our example, the certificates for VPN IPsec authentication are generated using the DemoCA included with OpenSSL. Here, OpenSSL version 0.9.8g is used. To set up the certification authority and generate the certificates, the `CA.sh` script included with OpenSSL is used (found at Debian under `/usr/lib/ssl/misc/CA.sh`). The command for setup of a new certification authority `CA.sh -newca` need only be executed once. On the basis of this certification authority, the user certificates are generated and exported in PKCS#12 format.

If OpenSSL standard settings (`openssl.cnf`) are used, a `demoCA` directory is created when setting up a new certification authority; the former contains the following information:

<code>private/cakey.pem</code>	private key of certification authority (CA)
<code>cacert.pem</code>	self-certified certificate of the certification authority (CA)
<code>index.txt</code>	List of previously-issued certificates
<code>serial</code>	Serial number for the following certificate
<code>newcerts</code>	Directory for issued certificates

The following provides an example for setup of new certification authority using OpenSSL, or the script `CA.sh -newca`:

```
root@server:/usr/lib/ssl/misc# ./CA.sh -newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:bavaria
Locality Name (eg, city) []:nuernberg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:funkwerk-ec
Organizational Unit Name (eg, section) []:dev
Common Name (eg, YOUR name) []:demo
Email Address []:demo@funkwerk-ec.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 0 (0x0)
    Validity
        Not Before: Jun  8 07:52:39 2009 GMT
        Not After  : Jun  7 07:52:39 2012 GMT
    Subject:
        countryName           = DE
        stateOrProvinceName   = bavaria
        organizationName      = funkwerk-ec
        organizationalUnitName = dev
        commonName            = demo
        emailAddress          = demo@funkwerk-ec.com
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            8C:4A:25:72:E5:43:B2:BD:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13
        X509v3 Authority Key Identifier:
            keyid:8C:4A:25:72:E5:43:B2:BD:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13
            DirName:/C=DE/ST=bavaria/O=funkwerk-ec/OU=dev/CN=demo/emailAddress=demo@funkwerk-ec.com
            serial:00
        X509v3 Basic Constraints:
            CA:TRUE
Certificate is to be certified until Jun  7 07:52:39 2012 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
root@server:/usr/lib/ssl/misc#
```



## 4.2.2 Generation of user certificates

After setup of the certification authority (CA), user certificates of the VPN gateway and those of the VPN client can be created. To generate a user certificate, three steps are necessary:

- (a) Generation of a new key along with a certificate request (`CA.sh -newreq`)
- (b) Signing of the certificate request with the certification authority (`CA.sh -sign`)
- (c) Export of certificates (CA certificate and customer certificate), incl. keys (public and private customer key) in PKCS#12 format using OpenSSL.

In the first step, a new certificate key and certificate request are generated with the command `CA.sh -newreq`:

```
newkey.pem = RSA Key Pair (public and private key)
```

```
newreq.pem = certificate request (contains the public key along with the required data for certificate request)
```

In the second step, this certificate request is signed by the certification authority with the command `CA.sh -sign`. This generates the `newcert.pem` file. Now, a separate folder should be created in which the certification key, certification request and the signed certificate are stored:

- create a new folder `mkdir ./vpn-gateway`
- copy the temporary files into the folder
- Move the following files into this folder

```
mv newreq.pem vpn-gateway/hinz_req.pem
```

```
mv newkey.pem vpn-gateway/hinz_key.pem
```

```
mv newcert.pem vpn-gateway/hinz_cert.pem
```

In the third step, the certificate of the certification authority, the just created user certificate including the certification key is exported in a file in PKCS#12 format. This file is protected with a password and allows transmission of the certificates to the VPN gateway, or a VPN client. For this, the following command is used:

```
openssl pkcs12 -export -in vpn-gateway/newcert.pem -inkey vpn-gateway/newkey.pem -certfile demoCA/cacert.pem -name vpn-gateway -out vpn-gateway/vpn-gateway1.p12
```

The described steps for generation of a user certificate are illustrated through the example of the certificate created for the VPN gateway.

These steps must be similarly performed for each of the **bintec secure IPsec clients**.

Creation of a new key along with a certificate request:

```
root@server:/usr/lib/ssl/misc# ./CA.sh -newreq
Generating a 1024 bit RSA private key
.+++++
.....+++++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:bavaria
Locality Name (eg, city) []:nuernberg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:fec
Organizational Unit Name (eg, section) []:dev
Common Name (eg, YOUR name) []:vpn-gateway
Email Address []:vpn-gateway@funkwerk-ec.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request is in newreq.pem, private key is in newkey.pem
root@tp2h1:/usr/lib/ssl/misc#
```

Signing of the certificate request with the certification authority:

```
root@server:/usr/lib/ssl/misc# ./CA.sh -sign
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 1 (0x1)
    Validity
        Not Before: Jun  8 08:54:05 2009 GMT
        Not After  : Jun  8 08:54:05 2010 GMT
    Subject:
        countryName           = DE
        stateOrProvinceName   = bavaria
        localityName          = nuernberg
        organizationName       = fec
        organizationalUnitName = dev
        commonName             = vpn-gateway
        emailAddress           = vpn-gateway@funkwerk-ec.com
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            48:65:44:7A:45:B4:68:03:8C:C9:00:67:E2:E5:54:E2:7B:7D:4A:5B
        X509v3 Authority Key Identifier:
            keyid:8C:4A:25:72:E5:43:B2:B0:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13

Certificate is to be certified until Jun  8 08:54:05 2010 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, ST=bavaria, O=funkwerk-ec, OU=dev, CN=demo/emailAddress=demo@funkwerk-ec.com
        Validity
            Not Before: Jun  8 08:54:05 2009 GMT
            Not After  : Jun  8 08:54:05 2010 GMT
        Subject: C=DE, ST=bavaria, L=nuernberg, O=fec, OU=dev,
        CN=vpn-gateway/emailAddress=vpn-gateway@funkwerk-ec.com
        Subject Public Key
```

```
Info:
      Public Key Algorithm:
rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):

00:dc:de:3f:5f:f8:09:08:3b:a0:4d:9d:3d:c2:70:
02:98:ac:68:1d:4f:f9:47:b4:2c:6b:68:6e:a6:b2:
4a:87:16:57:29:e7:d7:83:b5:5e:c6:ba:44:34:03:
2b:90:f3:e9:7a:b2:3b:9c:99:70:ba:f6:55:27:eb:
51:5c:f7:5d:a7:bc:46:12:9e:24:f8:ba:3c:c1:37:
87:ef:a6:ec:62:9c:fc:5b:f6:3e:4d:27:db:11:54:
8d:38:39:8a:79:eb:86:cd:3e:55:77:2d:94:ef:59:

15:4c:32:36:8a:9b:08:0d:23:36:20:0f:e8:50:7a:
      43:5a:2f:0d:3b:77:0b:8e:59
      Exponent: 65537 (0x10001)
X509v3 extensions:
      X509v3 BASIC Constraints:
      CA:FALSE
      Netscape Comment:
      OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
      48:65:44:7A:45:B4:68:03:8C:C9:00:67:E2:E5:54:E2:7B:7D:4A:5B
X509v3 Authority Key Identifier:
      keyid:8C:4A:25:72:E5:43:B2:B0:44:1C:F6:E8:5C:6C:FC:58:DA:90:12:13

Signature Algorithm: sha1WithRSAEncryption
a0:2b:df:23:6b:5a:4e:ac:4d:71:b8:b7:ca:ad:3e:49:4c:55:
72:14:e0:a0:1f:d5:21:3e:f3:98:0a:51:86:fe:c2:02:2b:81:
88:76:cd:69:a3:88:75:ed:c2:5c:43:64:14:cc:9e:b1:c8:88:
ee:b0:e7:f4:c5:b4:2f:a0:b5:55:e9:61:1b:9d:ec:7a:25:95:
a7:d8:53:65:7a:04:f3:b7:b8:7a:f3:af:62:88:46:b9:a6:a3:
48:93:a9:d4:ff:2b:4e:3c:3b:d4:74:cc:45:dd:c4:30:8e:c6:
de:ac:e0:57:b3:ae:7b:03:f8:aa:c8:cc:34:0c:45:ef:8a:8d:
93:66

-----BEGIN CERTIFICATE-----
MIIC+jCCAmOgAwIBAgIBATANBgkqhkiG9w0BAQUFAADB3MQswCQYDVQQGEwJERTEQ
MA4GA1UECBMHYmF2eXJpYTEUMBIGA1UEChMLZnVua3dlcmstZWMMxDDAKBgNVBAsT
A2RldjENMAsGA1UEAxMEZGVtbzEjMCEGCSqGSIb3DQEJARYUZGVtb0BmdW5rd2Vy
ay1lYy5jb20wHhcNMjM0MDg1NDM0NDM0NDM0NDM0NDM0NDM0NDM0NDM0NDM0NDM0
A1UEBmHCREUxEDA0BgNVBAGTB2JhdnFyaWEeXjAQBgNVBACTCU51ZXJlYmV5ZzEM
MAoGA1UEChMDZmVjMjQwYDQLEwNkZXYxZDAsBgNVBAMTC3Zwbi1nYXRld2F5
MSowKAYJKoZIhvcNAQkBFht2cG4tZ2FOZXdheUJmdW5rd2Vyay1lYy5jb20wZDZw
DQYJKoZIhvcNAQEBBQADGYYoAMIGJAoGBANzeP1/4CQg7cE2dPcJwApisaB1P+Ue0
LGTobqaySocWVynn1401Xsa6RDQDK5dz6XqyO5yZcLr2V8frUVz3Xae8RhKeJP16
PME3h+m7GKc/Fv2PkOn2xFUjTg5innrth0+VXct109ZFUwyNoqbCA0jNiAP6FB6
Q1ovDt3C45ZAgMBAAGjczB5MAkGA1UdEwQCAAAwLAYjYlZiAYb4QgENBBSWHU9w
ZW5TU0wR2VuZXJhdGVkIENlcnRp2mljYXR1MBOGA1UdDgQWBBRIZUR6RbRoA4zJ
AGfi5VTie31KWzAfBgNVHSMGDAWgBSMSiVy5UOysEQc9uhcbPxY2pASzANBgkq
hkiG9w0BAQUFAAOBgQCgK98ja1pOrE1xuLfrT5JTFVvFOCGH9UhpVoyC1GG/sIC
K4GIds1po4h17cJcQ2QUzJ6xyIjusOf0xbQvoLVV6WEbnex6JZWn2FN1egTzt7h6
869i1Ea5pqNk6nU/ytOPDvUdMx3cQwjsberOBXs657A/igyMw0DEXvio2T2g==
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
root@server:/usr/lib/ssl/misc#
```

Export of certificates (CA certificate and customer certificate), incl. keys (public and private customer key) in PKCS#12 format using OpenSSL:

```

root@server:/usr/lib/ssl/misc# openssl pkcs12 -export -in newcert.pem -inkey newkey.pem -certfile
demoCA/cacert.pem
-name vpn-gateway -out vpn-gateway.p12
Enter pass phrase for newkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
root@server:/usr/lib/ssl/misc# ls -l vpn-gateway/
insgesamt 16
-rw-r--r-- 1 root root 3249 2009-06-08 10:58 newcert.pem
-rw-r--r-- 1 root root 963 2009-06-08 10:28 newkey.pem
-rw-r--r-- 1 root root 708 2009-06-08 10:28 newreq.pem
-rw-r--r-- 1 root root 2732 2009-06-08 11:07 vpn-gateway.p12

```

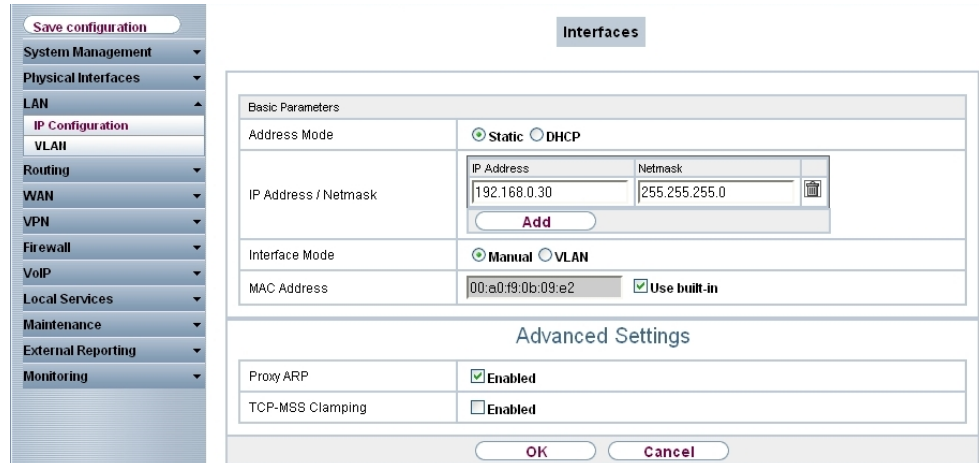
## 4.2.3 Configuration of the VPN gateway

### Local IP address of the VPN gateway

In this example, the VPN gateway is operated with IP address `192.168.0.30`. To assign the **bintec secure IPsec client** an IP address from this network range, the option **Proxy ARP** must be enabled.

For this, go to the following menu:

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



The screenshot shows a web-based configuration interface for network interfaces. On the left is a navigation menu with options like 'System Management', 'Physical Interfaces', 'LAN', 'IP Configuration', 'VLAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Local Services', 'Maintenance', 'External Reporting', and 'Monitoring'. The main area is titled 'Interfaces' and shows configuration for a specific interface, 'en1-0'. Under 'Basic Parameters', 'Address Mode' is set to 'Static' (radio button selected). The 'IP Address / Netmask' field contains '192.168.0.30' and '255.255.255.0' respectively, with an 'Add' button below. 'Interface Mode' is set to 'Manual' (radio button selected). The 'MAC Address' is '00:a0:f9:0b:09:e2' and 'Use built-in' is checked. Under 'Advanced Settings', 'Proxy ARP' is checked and 'Enabled', and 'TCP-MSS Clamping' is unchecked and 'Enabled'. At the bottom are 'OK' and 'Cancel' buttons.

Fig. 63: LAN -> IP Configuration -> Interfaces -> <en1-0> 

### Relevant fields in the Interfaces menu

Field	Meaning
IP Address/Netmask	With <b>Add</b> , add a new address entry and enter the <b>IP Address</b> and corresponding <b>Netmask</b> of the interface.
Proxy ARP	Enable the option <b>Proxy ARP</b> .

## Definition of an IP address pool

An IP address pool is specified in the **IP Pools** menu, from which an address is assigned all VPN clients at tunnel setup. In our example, a range from the local network is selected, e.g. *192.168.0.150* to *192.168.0.180*.

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

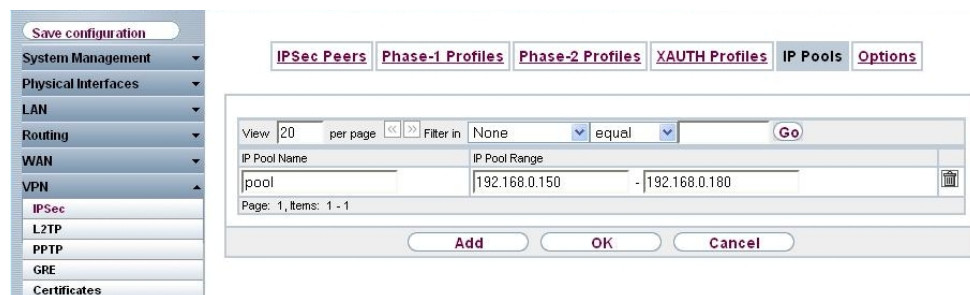


Fig. 64: **VPN -> IPsec -> IP Pools -> Add**

### Relevant fields in the IP Pools menu

Field	Meaning
IP pool name	Enter the name of the IP pool, e.g. <i>pool</i> .
IP pool range	In the first field, enter the first IP address from the local network.  In the second field, enter the last IP address from the local network.

### Import of certificates

For VPN IPsec authentication, a PKCS#12 certificate was generated for each of the **bintec secure IPsec clients** as well as the VPN gateway. The certificate of the VPN gateway is imported over the **Certificate List** Menu.

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

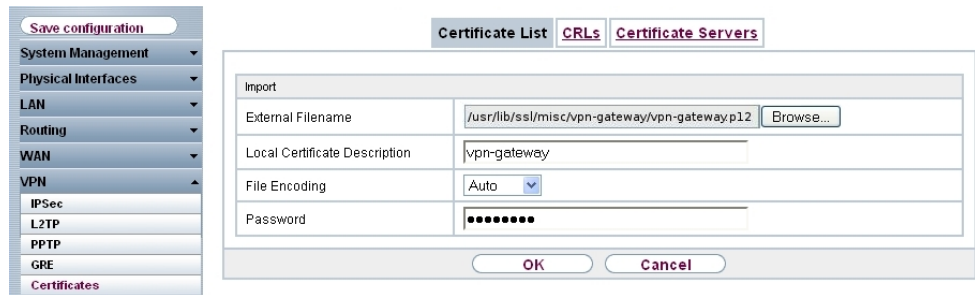


Fig. 65: VPN->Certificates->Certificate List->Import

### Relevant fields in the Certificate List menu

Field	Meaning
External Filename	With <b>Browse...</b> , select the file path or data name of the PKCS#12 certificate.
Local Certificate Description	Enter a name under which the certificate is saved in the VPN gateway, e.g. <i>vpn-gateway</i> .
Password	Enter the password issued at creation of the PKCS#12 certificate.

After importing the PKCS#12 container, you see the inserted certificate of the VPN gateway and the root certificate of the certification authority in the **certificate list**.

- (1) Go to **VPN -> Certificate -> Certificate List**.

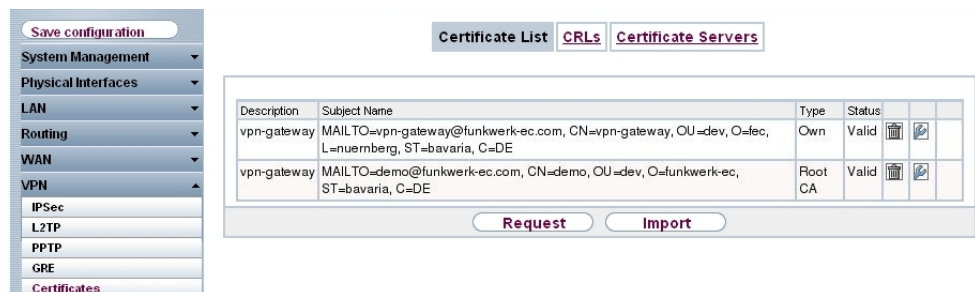



Fig. 66: VPN -> Certificates -> Certificate List

### Configuration of IPsec Phase 1 parameters

In the **Phase 1 Profile** menu, the imported certificate (e.g. vpn-gateway) is then selected as **Local Certificate**.

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

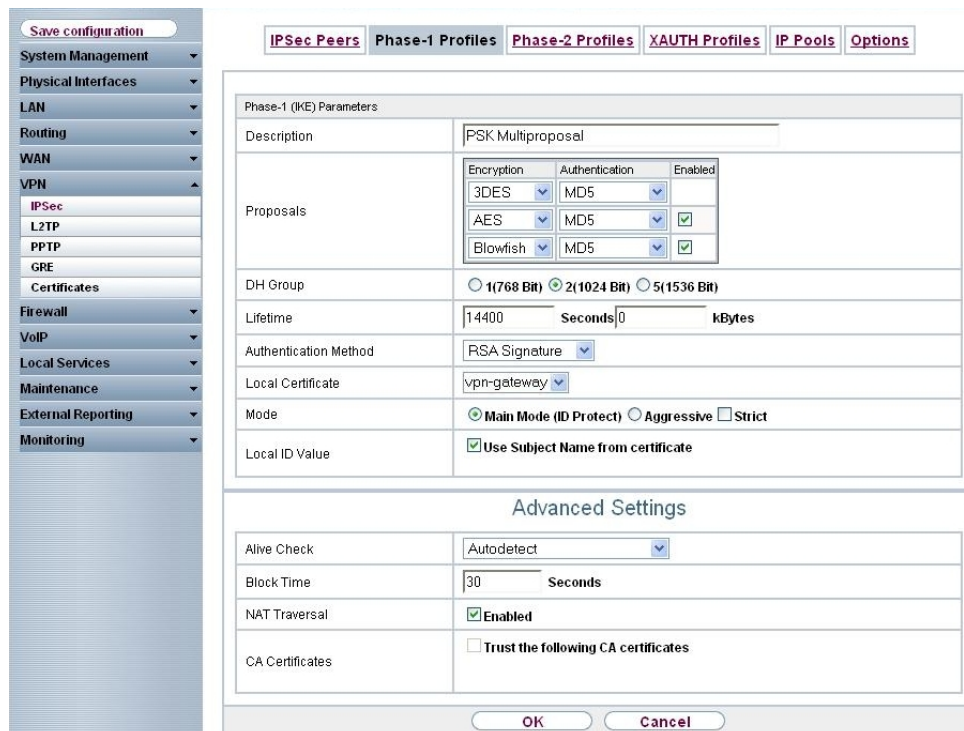


Fig. 67: VPN -> IPsec -> Phase 1 Profiles -> Edit 

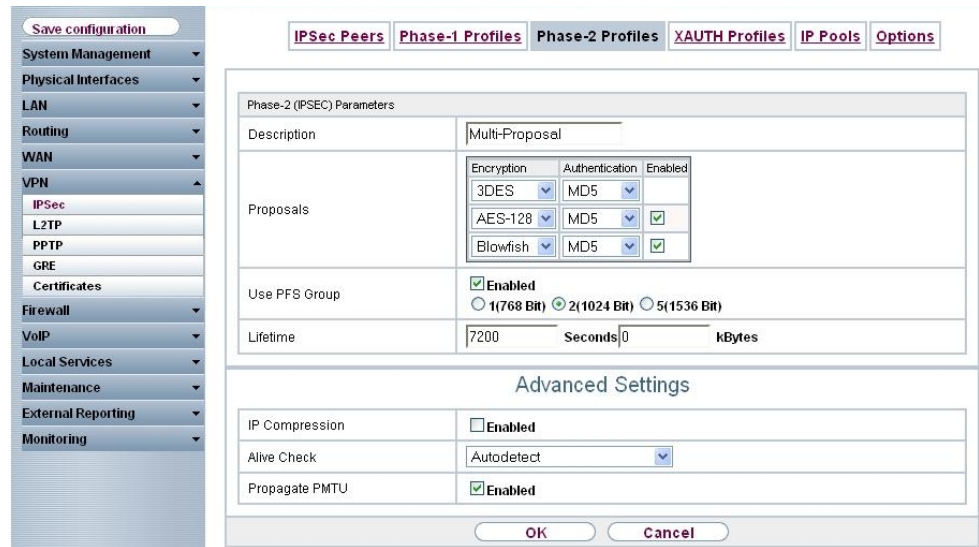
### Relevant fields in the Phase 1 Profiles menu

Field	Meaning
Authentication Method	Under <b>Authentication Method</b> select <i>RSA Signature</i> . Phase 1 key calculations are authenticated using the RSA algorithm.
Local Certificate	This field allows you to select the imported certificate (e.g. vpn-gateway) as local certificate.
Mode	With the option <b>Main Mode (ID Protect)</b> it is insured that the data for negotiation of the IPSec Phase 1 are transmitted in encrypted form.
Local ID Value	If you enable the option <b>Use subject name from certificate</b> , the subject name of the VPN gateway certificate (in our example: "MAILTO=vpn-gateway@bintec-elmeg.com, CN=vpn-gateway, OU=dev, O=fec, L=nuernberg, ST=bavaria, C=DE") is used as a local IPSec ID.

### Configuration of IPSec Phase 2 parameters



Settings in the **VPN -> IPsec -> Phase 2 Profiles-> Edit**  can be taken over unchanged.



The screenshot shows the configuration interface for Phase 2 Profiles. The left sidebar contains a navigation menu with options like System Management, Physical Interfaces, LAN, Routing, WAN, VPN, IPsec, L2TP, PPTP, GRE, Certificates, Firewall, VoIP, Local Services, Maintenance, External Reporting, and Monitoring. The main area has tabs for IPsec Peers, Phase-1 Profiles, Phase-2 Profiles, XAUTH Profiles, IP Pools, and Options. The Phase-2 Profiles tab is active, showing a form for editing a profile named 'Multi-Proposal'.

**Phase-2 (IPSEC) Parameters**

Description	Multi-Proposal		
Proposals	Encryption	Authentication	Enabled
	3DES	MD5	<input type="checkbox"/>
	AES-128	MD5	<input checked="" type="checkbox"/>
	Blowfish	MD5	<input checked="" type="checkbox"/>
Use PFS Group	<input checked="" type="checkbox"/> Enabled <input type="radio"/> 1(768 Bit) <input checked="" type="radio"/> 2(1024 Bit) <input type="radio"/> 5(1536 Bit)		
Lifetime	7200	Seconds	0 kBytes

**Advanced Settings**

IP Compression	<input type="checkbox"/> Enabled
Alive Check	Autodetect
Propagate PMTU	<input checked="" type="checkbox"/> Enabled

Buttons: OK, Cancel

Fig. 68: VPN -> IPsec -> Phase 2 Profiles -> Edit 

## Setup of VPN IPsec peers

In the **IPsec Peers** menu, a VPN connection is set up for every **bintec secure IPsec client**.



- (1) Go to **VPN -> IPsec -> IPsec Peers -> Edit** .

Fig. 69: VPN -> IPsec -> IPsec Peers -> Edit 

### Relevant fields in the IPsec Peers menu

Field	Meaning
Description	Enter a description of the peer which identifies it, e.g. <i>vpnclient1</i> .
Peer ID	As <b>Peer ID</b> the <b>Subject Name</b> of the VPN client certificate with the type <i>ASN.1-DN (Distinguished Name)</i> is saved. This <b>subject name</b> was issued at creation of the certificates generated for the <b>bintec secure IPsec clients</b> . In this example, for the first VPN peer the following subject name is saved: MAILTO=vpnclientuser@bintec-elmeg.com, CN=vpnclientuser, OU=sales, O=FEC, L=nuernberg, ST=bavaria, C=DE.
IP Address Assignment	Here, choose the configuration mode  <i>IKE Config Mode</i> off.

Field	Meaning
IP Assignment Pool	Select an IP pool configured in the <b>VPN -&gt; IP Pools</b> menu.
Local IP Address	Assign an IP address to the <b>bintec secure IPsec client</b> .

The **Advanced Settings** menu consists of the following fields:

#### Relevant fields in the menu **Advanced Settings**

Field	Meaning
Phase 1 Profile	For phase 1, select a profile already configured in the <b>Phase 1 Profiles</b> menu, e.g. <i>RSA Multiproposal</i> .
Phase 2 Profile	For phase 1, select a profile already configured in the <b>Phase 2 Profiles</b> menu, e.g. <i>Multiproposal</i> .
Proxy ARP	<p>Set <b>Proxy ARP</b> to <i>Up or Dormant</i>. Your device only responds to an ARP request if the status of the connection to the IPsec peer is up or dormant.</p> <p>In the case of <i>Dormant</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route.</p>

### 4.2.4 Configuration of bintec secure IPsec clients

The **bintec secure IPsec client** is called up with **Start -> Program -> FEC Secure IPsec Client -> Secure Client Mode**. Configuration of the **bintec secure IPsec clients** is performed with the assistant. At first launch of the **bintec secure IPsec client** the **new assistant profile** starts automatically.

Under **Connection Type**, select **Company Network Connection over IPsec**.

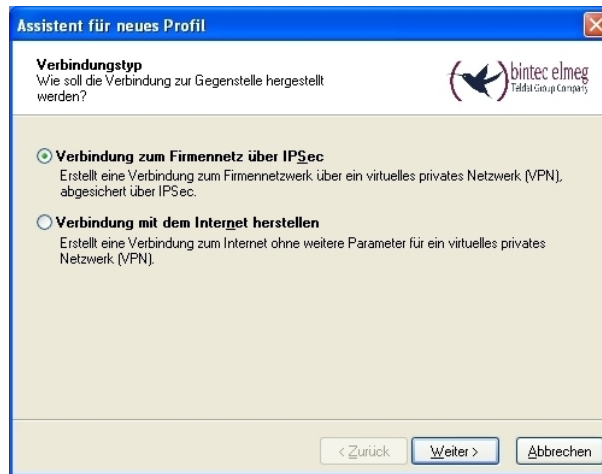


Fig. 70: Connector Type

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

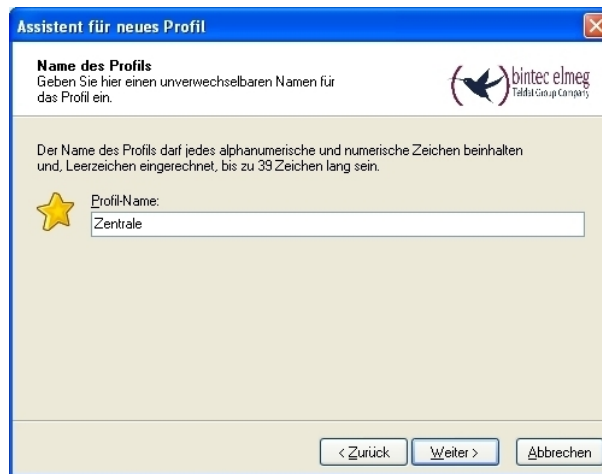


Fig. 71: Profile Name

In the next step of the assistant, 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 **bintec secure IPSec client** establishes no direct Internet access but uses an Internet access router.



Fig. 72: Connection Medium

In the option **Access data for Internet service providers** the address at which the VPN gateway is accessible from the Internet, e.g. `vpngateway.bintec-elmeg.com`, is saved under **user name**.

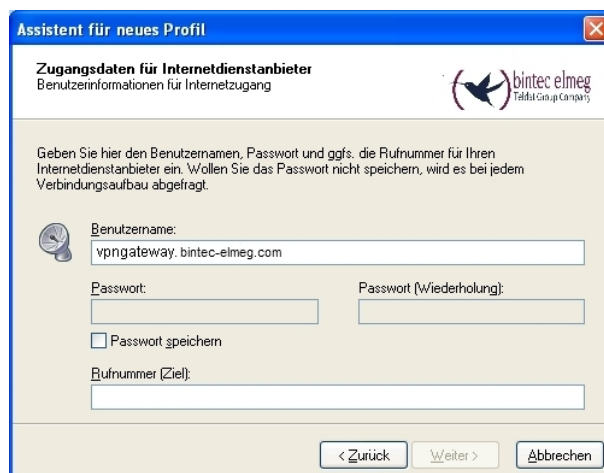


Fig. 73: User Name

Then, *Main Mode* is used as **Exchange Mode**. If *main mode* is used, data for setup of the IPsec Phase1 is already transmitted in encrypted form, in contrast to aggressive mode. For **PFS group**, as already at the VPN gateway, the *DH Group 2 (1024 Bit)* is selected and the option *Use IP Compression* enabled.

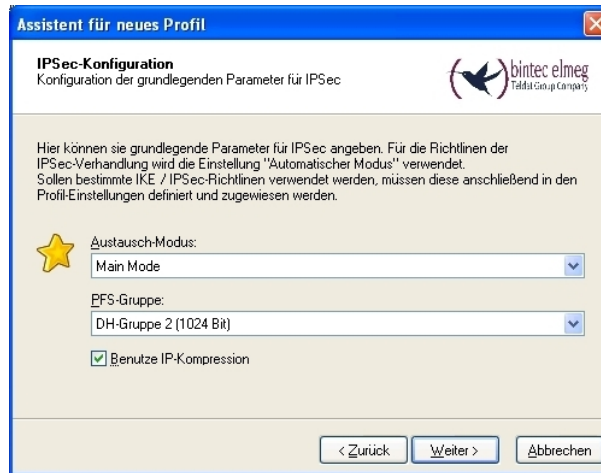


Fig. 74: IPSec Configuration

As authentication of the **bintec secure IPSec client** occurs with certificates, no **pre-shared key** is saved. The **Type of Local Identity** is set to *ASN1 Distinguished Name*.

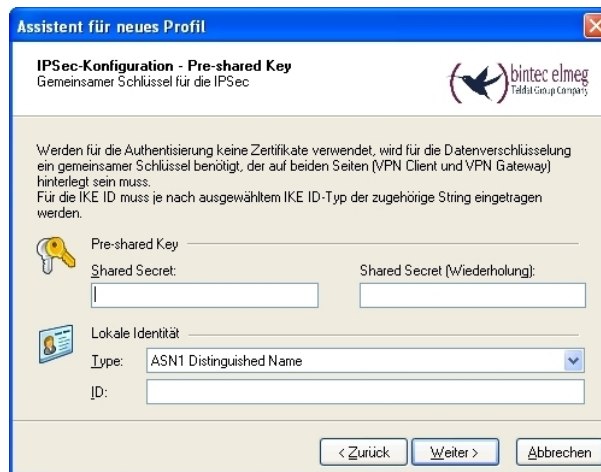


Fig. 75: Pre-shared key

In this example, a dynamic VPN IP address is assigned to the VPN IPSec client. *IKE Config Mode* must also be enabled.

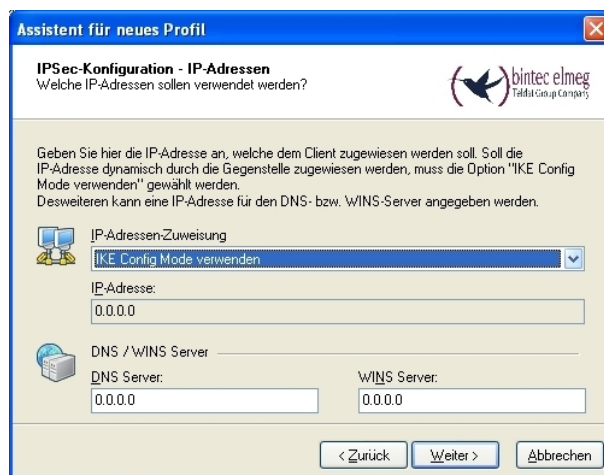


Fig. 76: IKE Config Mode

In the final step, the **firewall** of the **bintec secure IPsec client** is configured. If the client is directly connected to the Internet, the firewall should be enabled.

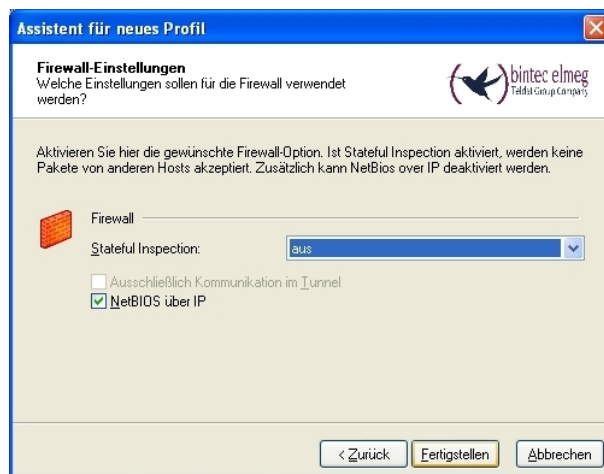


Fig. 77: Firewall

After the assistant for setup of a new VPN tunnel is run, the certificate (PKCS#12 file) of the first VPN client must be copied on this computer. Then, the user certificate is selected in menu **Configuration -> Certificate -> Add** of the **bintec secure IPsec client**.

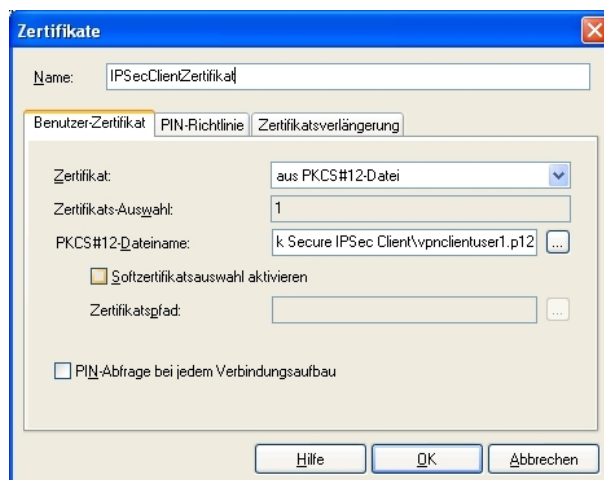


Fig. 78: Certificates

After this, certain adjustments are still required in the VPN connection profile.

In menu **Configuration -> Profile -> Edit -> IPSec Settings** the predefined **IKE Policy RSA Signature** and the **IPSec Policy ESP - AES128 - MD5** are selected .



Fig. 79: IPSec Settings

The previously-created certificate policy is selected in menu **Configuration -> Profile -> Edit -> Identity**. The certificate/certificate profile saved here is used for authentication at VPN IPSec tunnel setup.



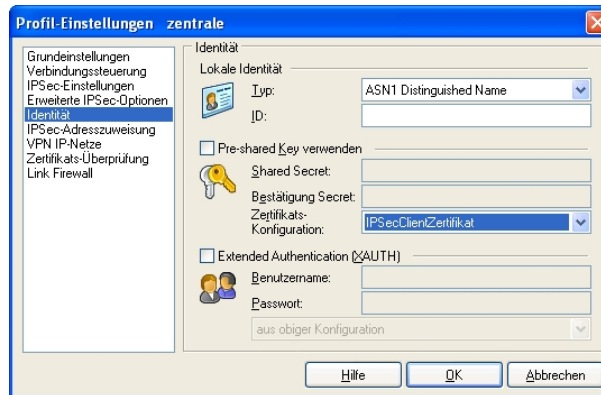


Fig. 80: Identity

## 4.2.5 Setup of the VPN IPsec tunnel

At setup of the VPN IPsec tunnel, there is a PIN request. The **PIN** is used to open the PKCS#12 certificate container. Here, the password issued when generating the PKCS#12 certificate must be used.

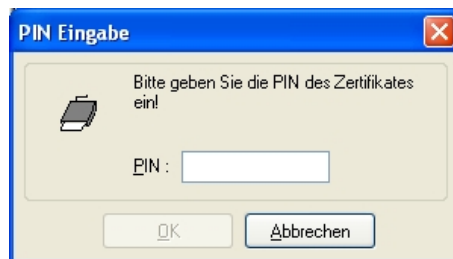


Fig. 81: PIN Entry



Fig. 82: FEC Secure IPsec Client

## 4.2.6 Additional securing of the VPN IPsec tunnel with a one-time password (optional)

To further secure the VPN IPsec tunnel, there is the option of enabling a one-time password request. This example describes the **KOBIL SecOVID** one-time password solution. The one-time password is generated with a token. At setup of the VPN IPsec tunnel, this one-time password is authenticated on the **KOBIL SecOVID** Radius Server.

### Installation of the **KOBIL SecOVID** servers on a 32Bit Windows 2003 server

The installation program of the **KOBIL SecOVID** server is launched on the CD by opening the `win32\server\SECOVID Server.exe` file. Please read the setup outputs for your information and follow the instructions and recommendations of the installation routine. At conclusion of the installation routine, the logfile of the **KOBIL SecOVID** server should be checked to insure that the server started up.

```

C:\WINDOWS\system32\cmd.exe
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>type ovid.proto

Tue May 05 15:44:28 2009: Licence for ovid (radius): KOBIL-Test-Lizenz
Tue May 05 15:44:28 2009:           Users: 20
Tue May 05 15:44:28 2009:           valid till: Mon Jun 01 19:47:52 2009

Tue May 05 15:44:28 2009: Authorize access for 127.0.0.1

C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>

```

Fig. 83: Installation of the **KOBIL SecOVID**

### Installation of the **KOBIL SecOVID** administration tool

For installation of the **KOBIL SecOVID** administration tool under Win32 systems, proceed as follows:

- Launch the setup program for the drivers of your KOBIL chip card terminal via `/Driver Setup/KOBILDriverSetup.exe`
- Follow setup program instructions and close the chip card terminal when prompted. The chip card terminal is required to administer the **KOBIL SecOVID** server per remote console. The KOBIL chip card terminal is not required for local administration of the **KOBIL SecOVID** server.

For installation of the **KOBIL SecOVID** administration tool, the setup program `/win32/admin/Setup_admintools.exe` on the installation CD must be launched. At installation, please follow additional instructions of the setup program.

### Launching the **KOBIL SecOVID** administration tool

The **KOBIL SecOVID** administration tool is launched over the **Start ->Programs-> SecOVID Admintools-> WxOvid** menu. After initial startup of **KOBIL SecOVID** Admintools, the secret token data can be imported and added to the SecOVID data bank. At a second SecOVID testing, token data are displayed in clear text. If you've bought the SecOVID tokens, the token data are generally provided in encrypted form. Import of token data (e.g. `tokendata_firm.db`) occurs via menu **Other Tokens -> Import Tokens**.

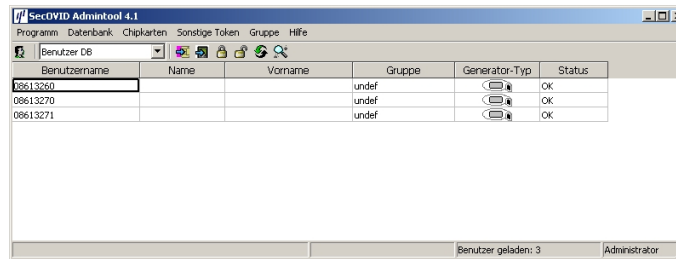


Fig. 84: Launching **KOBIL SecOVID** admintools

## Token personalisation

For assignment of tokens to a user, token sets must be blocked. After temporary blocking of a token data set, user information can be saved by editing the entry. The information in the **User Name** field is used after configuration of the **bintec secure IPsec client** for advanced IPsec authentication.

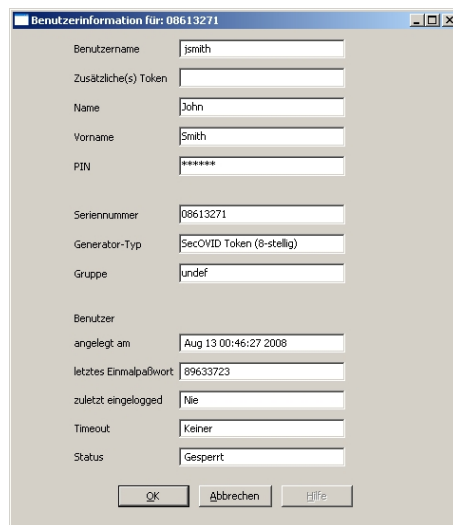
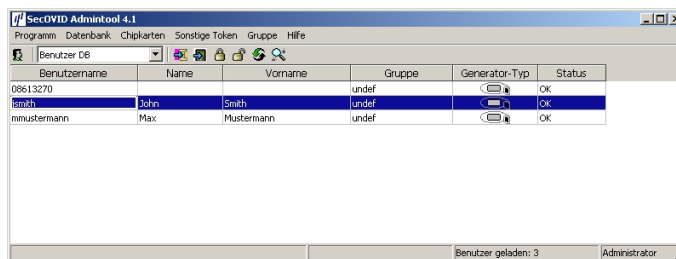


Fig. 85: User information

The data set must subsequently be unblocked.



The screenshot shows the 'SecOVID Admintool 4.1' window. At the top, there is a menu bar with 'Programm', 'Datenbank', 'Chipkarten', 'Sonstige Token', 'Gruppe', and 'Hilfe'. Below the menu is a toolbar with icons for search, refresh, and other functions. A dropdown menu shows 'Benutzer DB'. The main area contains a table with the following data:

Benutzername	Name	Vorname	Gruppe	Generator-Typ	Status
08613270			undef		OK
jsmith	John	Smith	undef		OK
mmustermann	Max	Mustermann	undef		OK

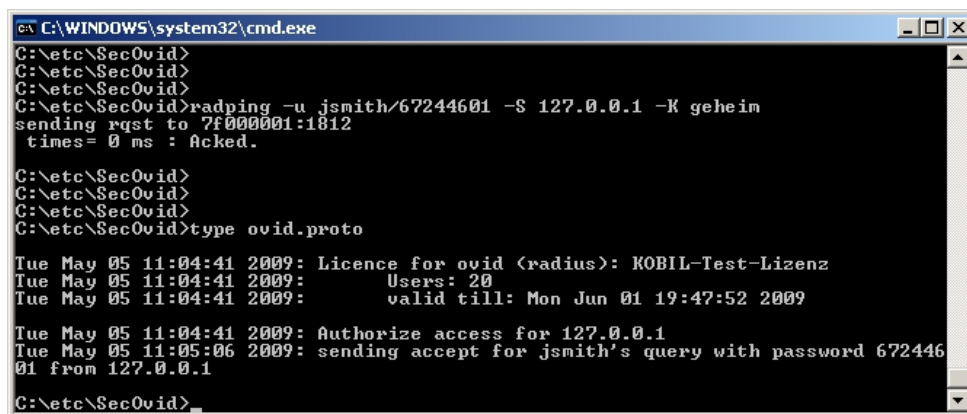
At the bottom right of the window, it says 'Benutzer geladen: 3' and 'Administrator'.

Fig. 86: Unblock

### Initial function test of the KOBIL SecOVID server

An initial function test can be performed with the command line tool `radping.exe`. With the one-time password, `Radping` initiates an authentication request on the SecOVID RADIUS server. During installation, the tool was saved in the `\etc\SecOVID\` directory.

With the `-u` option, the user name and the one-time password are transmitted to the SecOVID server. The one-time password must be generated with the user token. The SecOVID server is addressed with the `-S` option. For the first function test, `radping` must be executed directly on the server. The RADIUS password is sent with the `-k` option. The default value is `secret`. The SecOVID logfile (`\etc\SecOVID\ovid.proto`) displays the following message in case of successful authentication:



```
C:\WINDOWS\system32\cmd.exe
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>radping -u jsmith/67244601 -S 127.0.0.1 -K geheim
sending rqst to 7f000001:1812
times= 0 ms : Acked.

C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>
C:\etc\SecOvid>type ovid.proto

Tue May 05 11:04:41 2009: Licence for ovid (radius): KOBIL-Test-Lizenz
Tue May 05 11:04:41 2009:      Users: 20
Tue May 05 11:04:41 2009:      valid till: Mon Jun 01 19:47:52 2009

Tue May 05 11:04:41 2009: Authorize access for 127.0.0.1
Tue May 05 11:05:06 2009: sending accept for jsmith's query with password 672446
01 from 127.0.0.1

C:\etc\SecOvid>
```

Fig. 87: Function test

### Configuration of the RADIUS client on the SecOVID server

All RADIUS clients (e.g. the bintec VPN gateway, or the test application `radping`) must be saved on the SecOVID server as RADIUS client. For this, configuration file `\etc\SecOVID\clients` is edited. In our example, the bintec VPN gateway with the IP

address `192.168.0.30` and the RADIUS password `radius_PWD` is added. This password is subsequently also saved on the VPN gateway in the RADIUS settings. The SecOVID server service must be restarted for these changes to become effective.

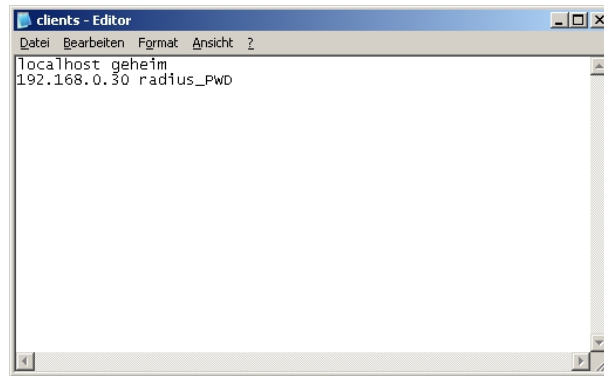


Fig. 88: Clients-Editor

## 4.2.7 Adjusting the VPN gateway configuration for one-time password request

### Radius settings at the VPN gateway

With the settings in the **RADIUS** menu, advanced IPsec authentication (XAUTH) with the RADIUS server of the **KOBIL SecOVID** server is enabled. You must set the authentication type to the *XAUTH* value, and save the IP address of the **KOBIL SecOVID** server. Communication with the RADIUS server is password-protected. Here, please use the RADIUS password saved on the SecOVID server (configuration file `\etc\SecOVID\clients`).

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

Save configuration

System Management

- Status
- Global Settings
- Interface Mode / Bridge Groups
- Administrative Access
- Remote Authentication
- Physical Interfaces
  - LAN
  - Routing
  - WAN
  - VPN
  - Firewall
  - VoIP
  - Local Services
  - Maintenance
  - External Reporting
  - Monitoring

RADIUS TACACS+ Options

Basic Parameters

Authentication Type: XAUTH

Server IP Address: 192.168.0.111

RADIUS Secret: .....

Priority: 0

Entry active:  Enabled

Group Description: xauth New: [ ]

Advanced Settings

Policy: Authoritative

UDP Port: 1812

Server Timeout: 1000 Milliseconds

Alive Check:  Enabled

Retries: 1

RADIUS Dialout:  Enabled [Reload now!]

Reload Interval: 0 Seconds

Default User: [ ]

Password: .....

OK Cancel

Fig. 89: System Management-> Remote Authentication -> RADIUS

#### Relevant fields in the RADIUS menu

Field	Description
Authentication Type	Select <b>Authentication Type</b> <i>XAUTH</i> .
Server IP Address	Enter the <b>server IP address</b> of the <b>KOBIL SecOVID</b> server, e.g. <i>192.168.0.111</i> .
RADIUS Password	Enter the shared password used for communication between the RADIUS server and your device, e.g. <i>radius_PWD</i> .
Group description	<p>Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS servers for a group are queried according to <b>priority</b> and <b>policy</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>New</i> (default value): Enter a new group description in the text field</li> <li>&lt;Group Name&gt;: Select a predefined group from the list. e.g. <i>xauth</i>.</li> </ul>

## XAUTH Configuration

A RADIUS server must be used for advanced IPSec authentication (XAuth). Perform all necessary settings in the **XAuth Profile** menu.

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

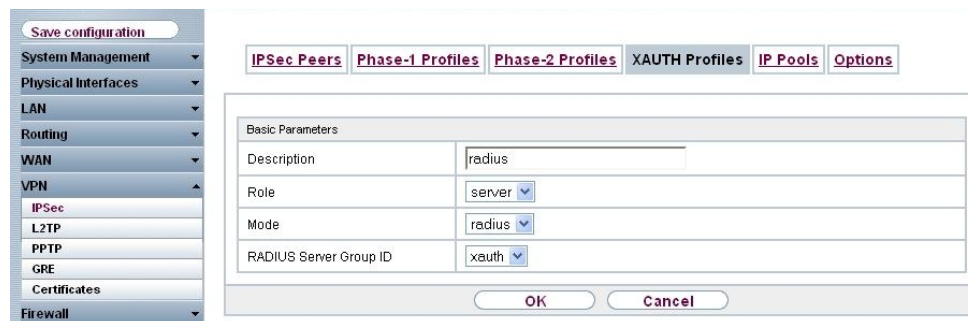


Fig. 90: VPN -> IPSec -> XAUTH Profiles -> New

### Relevant fields in the XAUTH Profiles menu

Field	Meaning
Description	Enter a description for the IPSec authentication, e.g. <i>radius</i> .
Role	Here, select <i>Server</i> .
Mode	Under <b>Mode</b> select <i>RADIUS</i> .
RADIUS Server Group ID	Select RADIUS server <i>xauth</i> .

### Activating the one-time password request on the VPN peer

To activate the one-time password request in the corresponding VPN peer configuration, the previously-configured Radius server profile is selected.

Under the option **XAUTH Profil** the Radius server profile of the **KOBIL SecOVID** server is selected. At the next setup of a VPN IPSec tunnel, the one-time password is requested and matched with the **KOBIL SecOVID**.

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



Save configuration

System Management

Physical Interfaces

LAN

Routing

WAN

VPN

IPsec

L2TP

PPTP

GRE

Certificates

Firewall

VoIP

Local Services

Maintenance

External Reporting

Monitoring

IPsec Peers Phase-1 Profiles Phase-2 Profiles XAUTH Profiles IP Pools Options

Peer Parameters

Administrative Status  Up  Down

Description vpnclient1

Peer Address

Peer ID ASN.1-DN (Distinguished Name) MAILTO=vpnclientuser@bintec-elmeg.com, CN=vpnclient

Preshared Key

Interface Routes

IP Address Assignment  Static  IKE Config Mode

IP Assignment Pool pool

Local IP Address 192.168.0.30

Advanced Settings

Advanced IPsec Options

Phase-1 Profile \* RSA Multiproposal

Phase-2 Profile \* Multi-Proposal

XAUTH Profile radius

Start Mode  On Demand  Always up

Advanced IP Options

Back Route Verify  Enabled

Proxy ARP  Inactive  Up or Dormant  Up only

IPsec Callback

Mode Inactive

OK Cancel

Fig. 91: VPN -> IPsec -> IPsec Peers ->

#### Relevant fields in the IPsec Peers menu

Field	Meaning
XAUTH	Select the Radius server profile of the <b>KOBIL SecOVID</b> server.

### 4.2.8 Adjusting the bintec Secure IPsec configuration for one-time password request

The one-time password is transmitted at VPN IPsec tunnel setup via the XAuth mechanism (advanced authentication). For this, the VPN IPsec tunnel profile must be edited. In menu **Configuration -> Profile -> Edit -> Identity** an administrator saved in **KOBIL SecOVID** is entered.

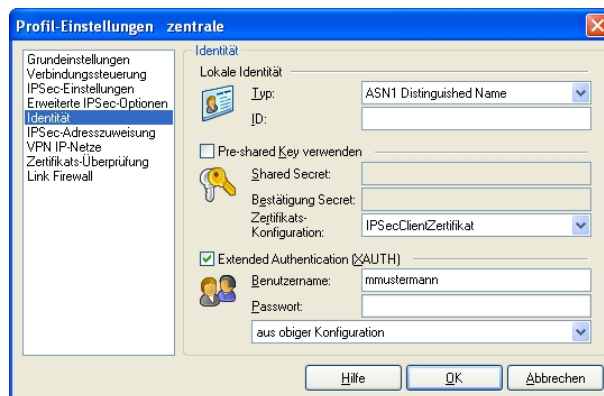


Fig. 92: Identity

The one-time password is requested at the next setup of the VPN IPSec tunnel.

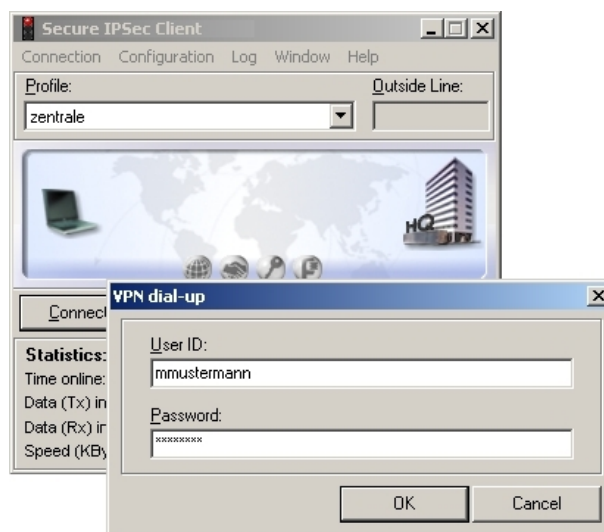


Fig. 93: User ID / Password Request

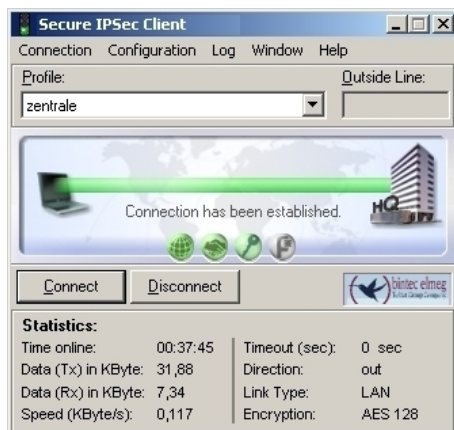


Fig. 94: Connection Setup

## 4.3 Overview of configuration steps

### Configuration of the VPN gateway

Field	Menu	Value
Address mode	LAN -> IP Configuration-> Interfaces -> <en1-0>	Static
IP Address/Netmask	LAN -> IP Configuration-> Interfaces -> <en1-0>	e.g. 192.168.0.30 / 255.255.255.0
Interface Mode	LAN -> IP Configuration-> Interfaces -> <en1-0>	Manual
Proxy ARP	LAN -> IP Configuration-> Interfaces -> <en1-0>	Enabled

### VPN Configuration





Field	Menu	Value
IP pool name	VPN -> IPsec -> IP Pools -> Add	e.g. pool.
IP pool range	VPN -> IPsec -> IP Pools -> Add	e.g. 192.168.0.150 - 192.168.0.180

### Importing Certificates





Field	Menu	Value
External Filename	VPN -> Certificates -> Certificate List -> Import	e.g. /usr/lib/






Field	Menu	Value
		<i>ssl/ misc/ vpn-gate- way/ vpn-gateway.p12</i>
Local Certificate Description	<b>VPN -&gt; Certificates -&gt; Certificate List -&gt; Import</b>	e.g. <i>vpn gateway</i>
Password	<b>VPN -&gt; Certificates -&gt; Certificate List -&gt; Import</b>	Password for PKCS#12 certificate

### Configuration of Phase 1 Profiles

Field	Menu	Value
Authentication Method	<b>VPN -&gt; IPsec -&gt;Phase 1 Profiles -&gt; Edit</b> 	<i>RSA Signature</i>
Local Certificate	<b>VPN -&gt; IPsec -&gt;Phase 1 Profiles -&gt; Edit</b> 	e.g. <i>vpn gateway</i>
Mode	<b>VPN -&gt; IPsec -&gt;Phase 1 Profiles -&gt; Edit</b> 	<i>Main Mode (ID Protect)</i>
Local ID Value	<b>VPN -&gt; IPsec -&gt;Phase 1 Profiles -&gt; Edit</b> 	<i>Enable Use Subject Name from Certificate</i>

### IPsec peers configuration

Field	Menu	Value
Administrative Status	<b>VPN -&gt; IPsec -&gt;IPsec Peers -&gt;</b> 	<i>Active</i>
Description	<b>VPN -&gt; IPsec -&gt;IPsec Peers -&gt;</b> 	e.g. <i>vpnclient1</i>
Peer ID	<b>VPN -&gt; IPsec -&gt;IPsec Peers -&gt;</b> 	<i>ASN.1-DN (Distinguished Name) and MAILTO=vpnclientuser@bintec-elmeg.com, CN=vpnclientuser, OU=sales, O=FEC, L=nuernberg, ST=bavaria, C=DE</i>
IP Address Assignment	<b>VPN -&gt; IPsec -&gt;IPsec Peers -&gt;</b> 	<i>IKE Config Mode</i>

Field	Menu	Value
IP Assignment Pool	VPN -> IPsec -> IPsec Peers -> 	<i>pool</i>
Local IP Address	VPN -> IPsec -> IPsec Peers -> 	e.g. <i>192.168.0.30</i>
Phase 1 Profile	VPN -> IPsec -> IPsec Peers ->  -> <b>Advanced Settings</b>	* <i>RSA Multiproposal</i>
Phase 2 Profile	VPN -> IPsec -> IPsec Peers ->  -> <b>Advanced Settings</b>	* <i>Multi-Proposal</i>
Proxy ARP	VPN -> IPsec -> IPsec Peers ->  -> <b>Advanced Settings</b>	<i>Up or Dormant</i>

### Configuration of bintec secure IPsec clients

Field	Menu	Value
Connector Type	<b>Assistant for new profile</b>	<i>Connection to company network via IPsec</i>
Profile Name	<b>Assistant for new profile</b>	<i>Head Office</i>
Connection Medium	<b>Assistant for new profile</b>	<i>LAN (over IP)</i>
User Name	<b>Assistant for new profile</b>	e.g. <i>vpngateway.bintec-elmeg.com</i>
Exchange Mode	<b>Assistant for new profile</b>	Main Mode
PFS Group	<b>Assistant for new profile</b>	DH Group 2 (1024 Bit)
Local Identity	<b>Assistant for new profile</b>	<i>ASN1 Distinguished Name</i>
IP address assignment	<b>Assistant for new profile</b>	<i>Use IKE Config Mode</i>
Stateful Inspection	<b>Assistant for new profile</b>	<i>off</i>
NetBIOS over IP	<b>Assistant for new profile</b>	Enabled

### Copy certificates

Field	Menu	Value
Name	<b>Configuration -&gt; Certificates -&gt; Add</b>	<i>IPsecClientCertificate</i>
Certificate	<b>Configuration -&gt; Certificates -&gt; Add</b>	<i>from PKCS#12 file</i>
PKCS#12 data name	<b>Configuration -&gt; Certificates -&gt; Add</b>	<i>bintec secure IPsec client\vpnclientuser1</i>

Field	Menu	Value
		<i>.p12</i>

### Profile Settings

Field	Menu	Value
Gateway (Tunnel Endpoint)	<b>Configuration -&gt; Profile -&gt; Edit -&gt; IPSec Settings</b>	<i>vpngate-way.bintec-elmeg.com</i>
IKE Policy	<b>Configuration -&gt; Profile -&gt; Edit -&gt; IPSec Settings</b>	<i>RSA Signature</i>
IPSec Guideline	<b>Configuration -&gt; Profile -&gt; Edit -&gt; IPSec Settings</b>	<i>ESP - AES128 - MD5</i>
Exchange Mode	<b>Configuration -&gt; Profile -&gt; Edit -&gt; IPSec Settings</b>	<i>Main Mode</i>
PFS Group	<b>Configuration -&gt; Profile -&gt; Edit -&gt; IPSec Settings</b>	<i>DH Group 2 (1024 Bit)</i>
Type	<b>Configuration -&gt; Profile -&gt; Edit -&gt; Identity</b>	ASN1 Distinguished Name
Certificate Configuration	<b>Configuration -&gt; Profile -&gt; Edit -&gt; Identity</b>	IPSecClientCertificate

### Setup of the VPN IPSec tunnel

Field	Menu	Value
PIN	<b>PIN Entry</b>	<i>Password for PKCS#12 certificate</i>


### RADIUS settings

Field	Menu	Value
Authentication Type	<b>System Administration -&gt; Remote Authentication -&gt; RADIUS -&gt; New</b>	<i>XAUTH</i>
Server IP Address	<b>System Administration -&gt; Remote Authentication -&gt; RADIUS -&gt; New</b>	<i>e.g. 192.168.0.111</i>
RADIUS Password	<b>System Administration -&gt; Remote Authentication -&gt; RADIUS -&gt; New</b>	The Radius password saved on the SecOVID server
Group description	<b>System Administration -&gt; Remote Authentication -&gt; RADIUS -&gt; New</b>	<i>xauth</i>

### XAUTH Configuration

Field	Menu	Value
Description	<b>VPN -&gt; IPsec -&gt; XAUTH Profiles -&gt; New</b>	e.g. <i>radius</i>
Role	<b>VPN -&gt; IPsec -&gt; XAUTH Profiles -&gt; New</b>	<i>Server</i>
Mode	<b>VPN -&gt; IPsec -&gt; XAUTH Profiles -&gt; New</b>	<i>RADIUS</i>
RADIUS Server Group ID	<b>VPN -&gt; IPsec -&gt; XAUTH Profiles -&gt; New</b>	<i>xauth</i>

#### IPsec peers configuration

Field	Menu	Value
XAUTH Profile	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt;  -&gt; Advanced Settings</b>	<i>radius</i>

#### Profile Settings

Field	Menu	Value
Type	<b>Configuration -&gt; Profile -&gt; Edit -&gt; Identity</b>	ASN1 Distinguished Name
Certificate Configuration	<b>Configuration -&gt; Profile -&gt; Edit -&gt; Identity</b>	IPsecClientCertificate
User Name	<b>Configuration -&gt; Profile -&gt; Edit -&gt; Identity</b>	e.g. <i>jeveryman.</i>

## Chapter 5 Security - VPN IPSec tunnel via HTTPS between the bintec Secure IPSec Client and a bintec router

### 5.1 Introduction

This workshop describes the VPN IPSec Client connection of the **bintec Secure IPSec Client** to an **bintec R3502** VPN gateway via the HTTPS protocol. The use of a VPN should be prevented in public hotspots or in hotels, for example, by blocking the typical ports UDP500 and UDP4500. In such cases, the VPN IPSec tunnel is tunneled via the HTTPS port (TCP 443) if the IPSec Pathfinder function is enabled.

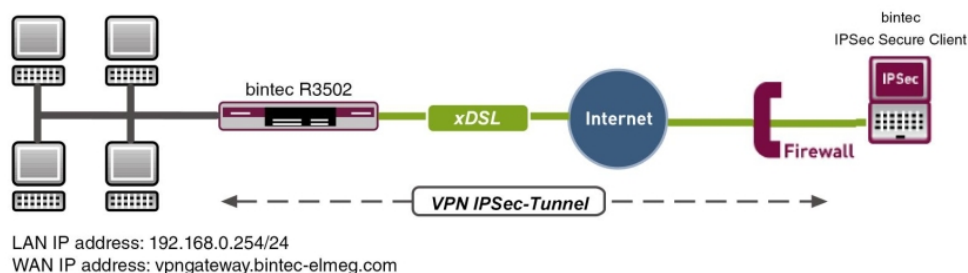


Fig. 95: Example scenario

### Requirements

The following prerequisites for configuration must be met:

- A VPN gateway, e.g. **bintec R3502** with system software 7.10.1 (IPSec Pathfinder support)
- A **bintec Secure IPSec Client**
- VPN gateway and VPN client each require an independent Internet connection

### 5.2 Configuration



## 5.2.1 Configuration of the VPN gateway

A dynamic IP address is assigned to the **bintec Secure IPsec Client** when establishing the VPN IPsec connection. An IP address pool is created for this purpose. To do this, go to the following menu:

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

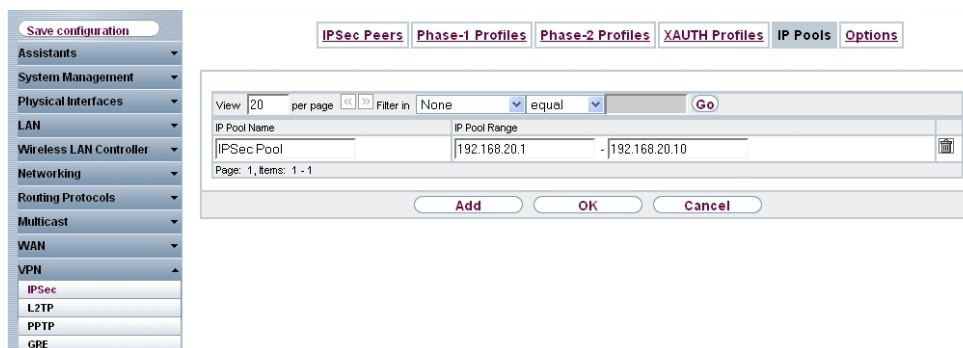


Fig. 96: VPN -> IPsec -> IP Pools -> Add

Proceed as follows to set up an IP pool:

- (1) Enter the name of the IP pool under **IP Pool Name**, e.g. *IPsec Pool*.
- (2) In our example for VPN IPsec Client connections, the addresses *192.168.20.1* to *192.168.20.10* are assigned for **IP Pool Range**.
- (3) Confirm with **OK**.

## 5.2.2 Configuration of the VPN IPsec tunnel

The actual VPN connection is configured in the **IPsec Peers** menu.

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

Fig. 97: VPN -> IPSec -> IPSec Peers -> New

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

- (1) For **Description**, enter a description of the peer which identifies it, e.g. *VPN\_Client1*.
- (2) Leave the field empty under **Peer Address**.
- (3) The **Peer-ID** must match the local ID value of the remote terminal, e.g. *E-mail Address* type, and enter *User1@bintec-elmeg.com*.
- (4) For **Preshared Key**, enter the password for the encrypted connection, e.g. *test*.
- (5) For **IP Address Assignment**, select the *Server in IKE Configuration Mode* setting. An IP address is then assigned to the bintec Secure IPSec Client when a connection is established.
- (6) Select *IPSec Pool* for **IP Assignment Pool**.
- (7) Under **Local IP Address**, enter the IP address of the LAN interface of the router, e.g. *192.168.0.254*.
- (8) Press **OK** to confirm your entries.

### 5.2.3 Enable IPSec Pathfinder function

The IPSec Pathfinder function is disabled in the ex works state. When the IPSec Pathfinder is switched on, the VPN gateway also responds to the HTTPS port to any VPN IPSec requests.

- (1) Go to **VPN -> IPSec -> Options -> Advanced Settings**.

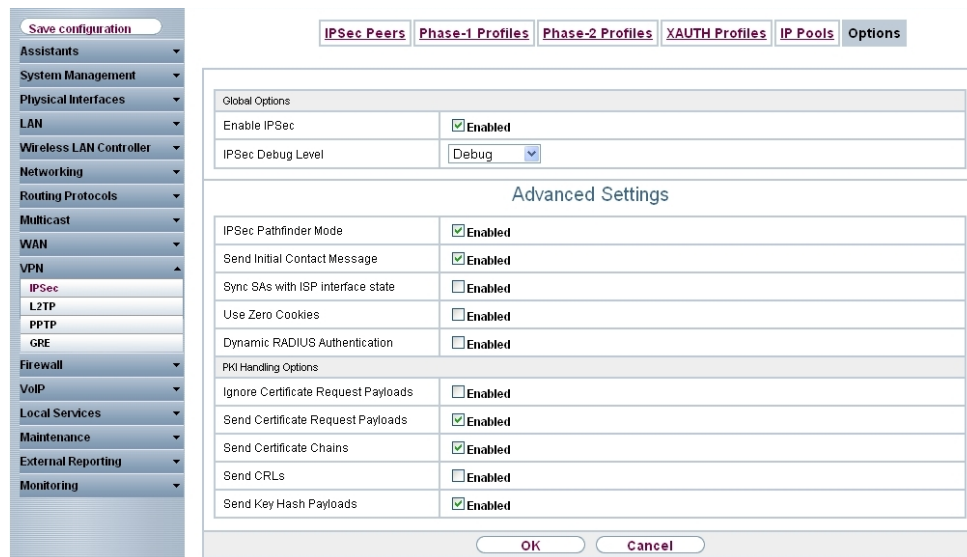


Fig. 98: VPN -> IPsec -> Options -> Advanced Settings

Proceed as follows:

- (1) Enable **IPsec Pathfinder mode**.
- (2) Leave the remaining settings unchanged and confirm them with **OK**.

## 5.2.4 Configuration of bintec Secure IPsec Client

The **bintec Secure IPsec Client** is called up via **Start -> Program -> FEC Secure IPsec Client -> Secure Client Mode**. 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**.



Fig. 99: Connection Type

Enter a name for the profile, e.g. *VPN Company Head Office*.

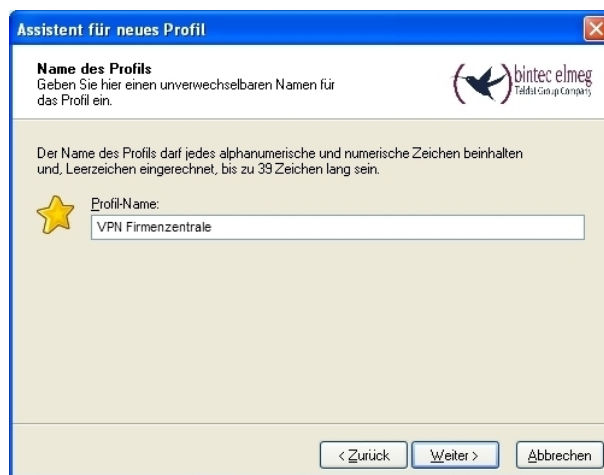


Fig. 100: Profile Name

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 **bintec Secure IPSec Client** establishes no direct Internet access but uses an Internet access router.

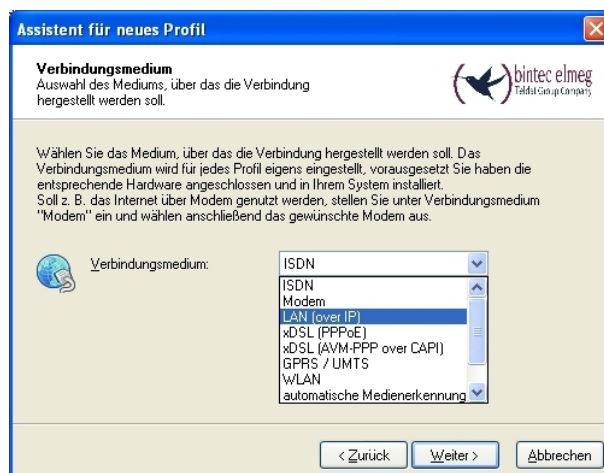


Fig. 101: Connection Medium

In the **VPN Gateway Parameters** window, the official static IP address or the DynDNS name of the remote terminal to which the IPsec tunnel is to be built must be entered, e.g. `vpngateway.bintec-elmeg.com`.

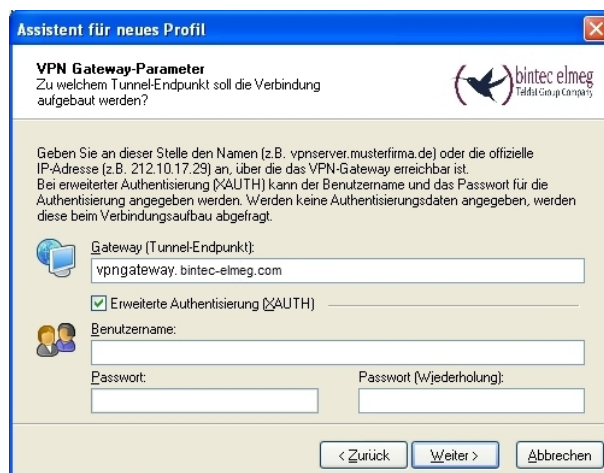


Fig. 102: VPN Gateway Parameters

Next, *Aggressive Mode* is used as **Exchange Mode** because the **bintec R3502** router and the **bintec Secure IPsec Client** are assigned dynamic IP addresses by the Internet provider. Set **PFS Group** to *DH Group 2 (1024 Bit)*, for example. The option *Use IP Compression* is not employed in this configuration.

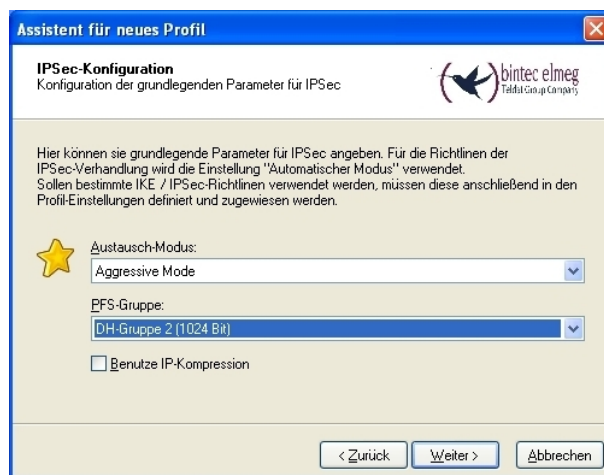


Fig. 103: IPSec Configuration

In the next Wizard step, the **Preshared Key** configured on the VPN gateway is saved, e.g. *test*.

The user e-mail address should be used as **Local Identity** under **Type** *Fully Qualified Username*, along with the **ID** *User1@bintec-elmeg.com* . This type and the ID must match the peer ID configured on the VPN gateway.

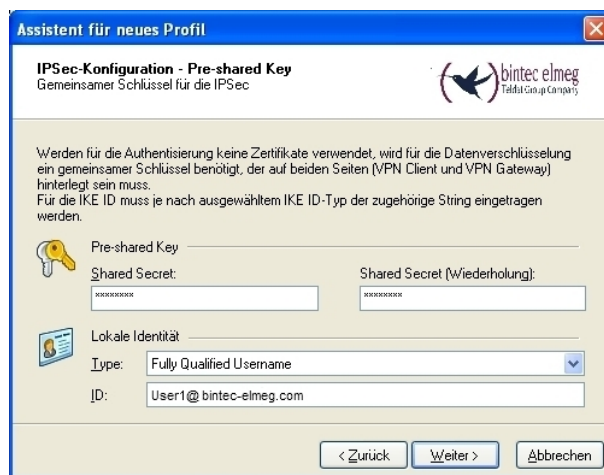


Fig. 104: Preshared Key

In this example, the **bintec Secure IPSec Client** derives an IP address from the IP pool configured on the VPN gateway. For this, the option *Use IKE Config Mode* must be selected under **IP Address Assignment**.

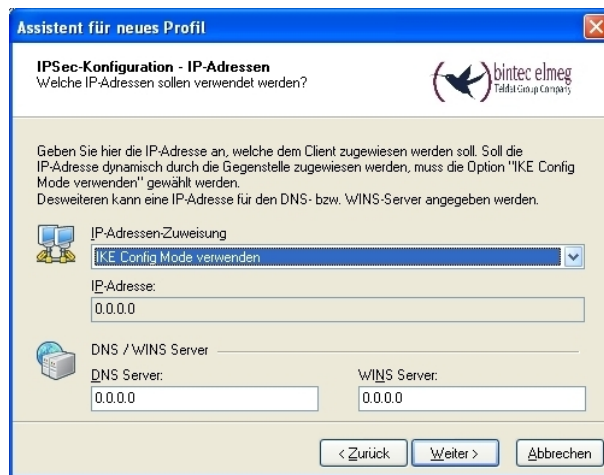


Fig. 105: IKE Config Mode

In the next 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. If the firewall is enabled, then it can also be specified whether traffic is permitted outside the IPSec tunnel or not.



Fig. 106: Firewall

The IPSec Pathfinder function must still be enabled separately by editing the newly created profile.

- (1) Go to **Configuration -> Profiles**.

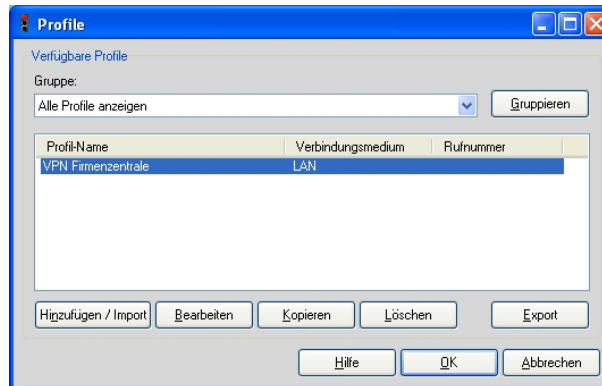


Fig. 107: Available Profiles

The option *IPSec Pathfinder Function* is enabled in the **Advanced IPSec Options** menu.

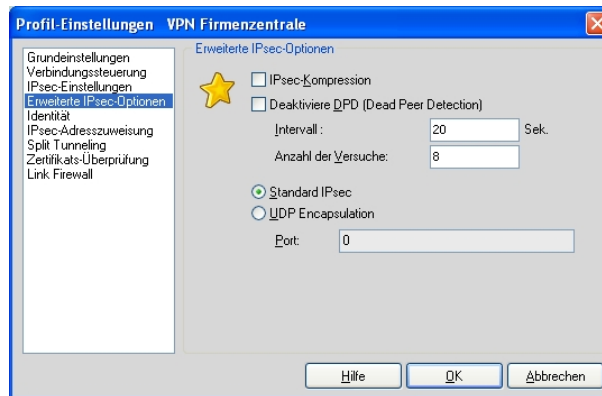


Fig. 108: IPSec Options

If a proxy server is used to connect to the Internet, then the **bintec Secure IPSec Client** offers the option to save proxy server settings in the **Configuration -> Proxy for VPN Pathfinder** menu.



## 5.3 Overview of Configuration Steps

### Create IP Pool

Field	Menu	Value
IP Pool Name	<b>VPN -&gt; IPsec -&gt; IP Pools -&gt; Add</b>	e.g. <i>IPsec Pool</i>
IP Pool Range	<b>VPN -&gt; IPsec -&gt; IP Pools -&gt; Add</b>	e.g. <i>192.168.20.1 - 192.168.20.10</i>

### Configuration of the VPN IPsec tunnel

Field	Menu	Value
Administrative Status	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	<i>Active</i>
Description	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	e.g. <i>VPNClient1</i>
Peer Address	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	empty field
Peer ID	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	<i>E-mail Address / User1@bintec-elmeg.com</i>
Preshared Key	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	e.g. <i>test</i>
IP Address Assignment	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	<i>Server In IKE Configuration Mode</i>
IP Assignment Pool	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	<i>IPsec Pool</i>
Local IP Address	<b>VPN -&gt; IPsec -&gt; IPsec Peers -&gt; New</b>	e.g. <i>192.168.0.254</i>

### Enable IPsec Pathfinder function

Field	Menu	Value
IPsec Pathfinder Mode	<b>VPN -&gt; IPsec -&gt; Options -&gt; Advanced Settings</b>	<i>Enabled</i>

### Configuration of bintec Secure IPsec Client

Field	Menu	Value
Connection Type	<b>Wizard for new profile</b>	<i>Connection to company network via IPsec</i>
Profile Name	<b>Wizard for new profile</b>	<i>VPN Company Head Office</i>
Connection Medium	<b>Wizard for new profile</b>	<i>LAN (over IP)</i>
Gateway (Tunnel Endpoint)	<b>Wizard for new profile</b>	e.g. <i>vpngateway.bintec-elmeg.c</i>

Field	Menu	Value
		<i>om</i>
Exchange Mode	<b>Wizard for new profile</b>	Aggressive Mode
PFS Group	<b>Wizard for new profile</b>	DH Group 2 (1024 Bit)
Shared Secret	<b>Wizard for new profile</b>	e.g. <i>test</i>
Shared Secret (Retry)	<b>Wizard for new profile</b>	e.g. <i>test</i>
Type	<b>Wizard for new profile</b>	e.g. <i>Fully Qualified Username</i>
ID	<b>Wizard for new profile</b>	e.g. <i>User1@bintec-elmeg.com</i>
IP address assignment	<b>Wizard for new profile</b>	<i>Use IKE Config Mode</i>
Stateful Inspection	<b>Wizard for new profile</b>	<i>off</i>
IPSec Pathfinder Function	<b>Wizard for new profile</b>	Enabled

## Chapter 6 Security - IPSec with certificates

### 6.1 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).

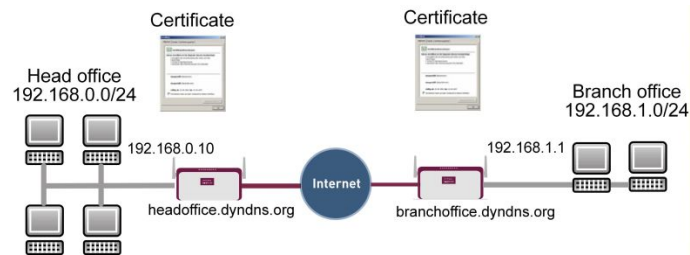


Fig. 109: Example scenario IPSec with certificates

### 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.

### 6.2 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.

## 6.2.1 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**.

The screenshot displays two side-by-side configuration panels for an IPSec peer. The left panel, titled 'Peer Parameters', includes fields for 'Administrative Status' (set to 'Up'), 'Description' ('Branch Office'), 'Peer Address' (IP Version: 'IPv4 Preferred', address: 'branchoffice.dyndns.org'), 'Peer ID' (Fully Qualified Domain Name (FQDN): 'Branch Office'), 'Internet Key Exchange' (set to 'IKEv1'), 'Preshared Key' (masked with dots), and 'IP Version of the tunneled Networks' (set to 'IPv4'). The right panel, titled 'IPv4 Interface Routes', includes 'Security Policy' (set to 'Trusted'), 'IPv4 Address Assignment' (set to 'Static'), 'Default Route' (set to 'Disabled'), 'Local IP Address' ('192.168.0.10'), and a 'Route Entries' table with one entry: Remote IP Address '192.168.1.0', Netmask '255.255.255.0', and Metric '1'. An 'ADD' button is located below the table.

Fig. 110: **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.

## 6.2.2 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 ▼	<input type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>
Blowfish ▼	MD5 ▼	<input checked="" type="checkbox"/>

DH Group 2(1024 Bit) ▼

Lifetime  Seconds  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


Fig. 112: 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**.

### 6.2.3 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 ▼	<input type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>

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

Propagate PMTU  Enabled

Fig. 114: VPN -> IPsec -> Phase-2 Profiles-> <Multi-Proposal> -> 



Configure the phase-2 profile with the following parameters:

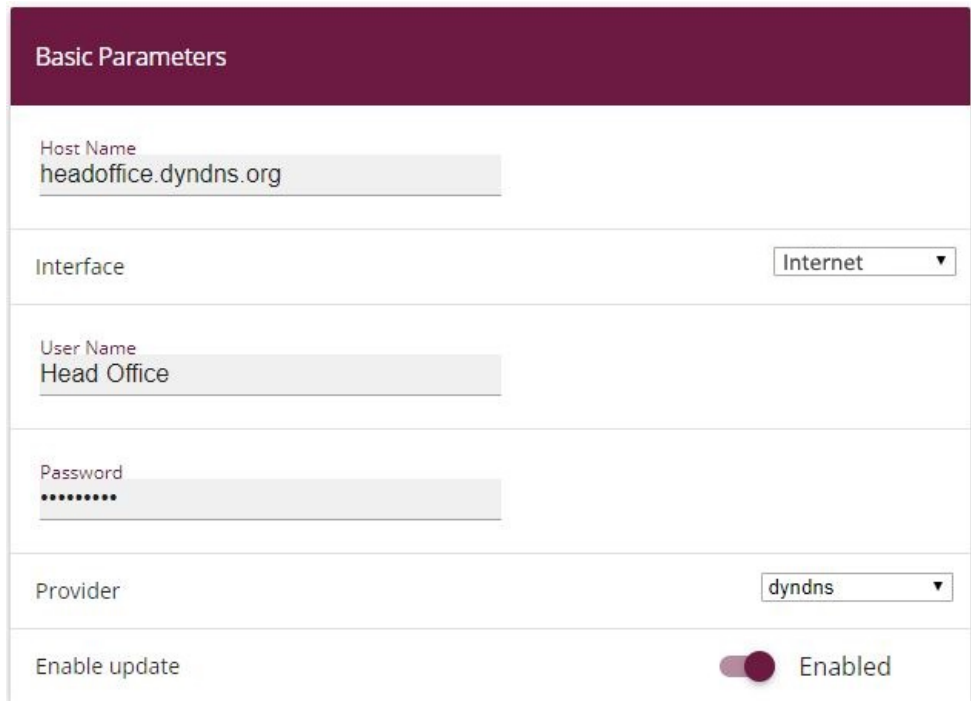
- (1) Under **Description** define a name for the profile, e.g. *Branch Office*.
- (2) Under **Proposal Encryption** select *AES-128*, under **Authentication** select *MD5*.  
Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.
- (3) Click **Advanced Settings**.
- (4) Set **Alive Check** to *Inactive*.
- (5) Confirm with **OK**.

## 6.2.4 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**.



The screenshot displays a configuration window titled "Basic Parameters" for a DynDNS client. The form includes the following fields and controls:

- Host Name:** A text input field containing "headoffice.dyndns.org".
- Interface:** A dropdown menu currently set to "Internet".
- User Name:** A text input field containing "Head Office".
- Password:** A text input field with masked characters (dots).
- Provider:** A dropdown menu currently set to "dyndns".
- Enable update:** A toggle switch that is currently turned on, labeled "Enabled".

Fig. 115: **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.

## 6.2.5 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	Subject Name
Certificate Request Description Head Office	Custom <span style="float: right;">Disabled</span>
Mode <input checked="" type="radio"/> Manual <input type="radio"/> SCEP	Common Name Head Office
Generate Private Key <span style="float: right;">RSA / 1024 Bits</span>	E-mail
	Organizational Unit
	Organization
	Locality
	State/Province
	Country

Fig. 116: **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. 117: 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:

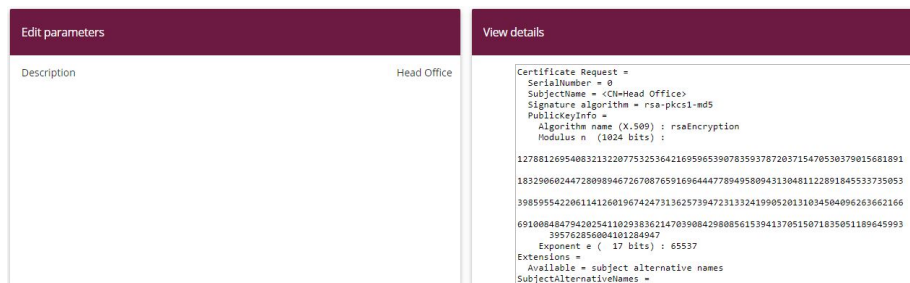


Fig. 118: System Management -> Certificates -> Certificate List

- (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**.

Fig. 119: 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.

## 6.2.6 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 ▼	<input type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>
3DES ▼	MD5 ▼	<input checked="" type="checkbox"/>

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

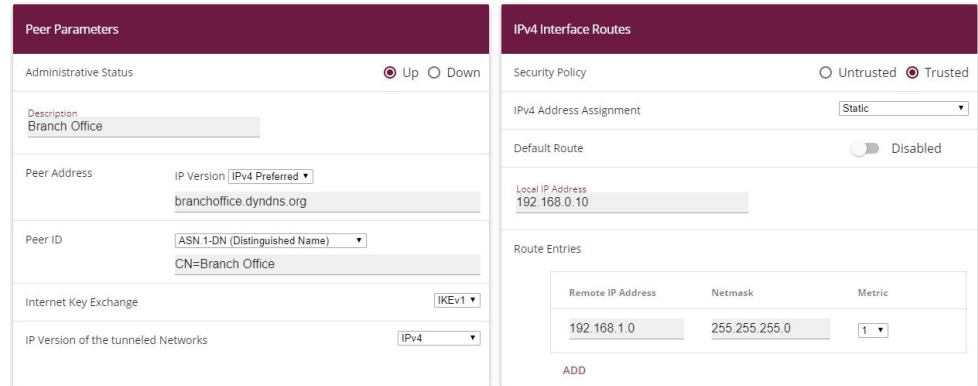
Fig. 120: VPN -> IPSec ->Phase-1 Profiles -> <Branch Office>->

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>->** .



The screenshot shows two panels for configuring an IPSec peer named 'Branch Office'.

**Peer Parameters Panel:**

- Administrative Status:** Up (selected), Down
- Description:** Branch Office
- Peer Address:** IP Version: IPv4 Preferred; Address: branchoffice.dyndns.org
- Peer ID:** ASN 1-DN (Distinguished Name); Value: CN=Branch Office
- Internet Key Exchange:** IKEv1
- IP Version of the tunneled Networks:** IPv4

**IPv4 Interface Routes Panel:**

- Security Policy:** Untrusted, Trusted (selected)
- 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

Fig. 121: **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.

## 6.3 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.

## 6.4 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:

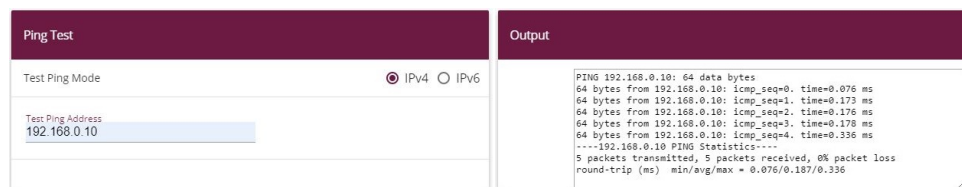


Fig. 122: Maintenance -> Diagnosis -> Ping Test



### 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.

## 6.5 Overview of configuration steps







### Creating an IPSec peer

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




### Changing the Phase-1 profile

Field	Menu	Value
Description	VPN -> IPSec -> Phase-1	e.g. <i>Branch Office</i>



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

### Changing the Phase-2 profile

Field	Menu	Value
<b>Description</b>	<b>VPN -&gt; IPSec -&gt; Phase-2 Profiles -&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	e.g. <i>Branch Office</i>
<b>Proposal</b>	<b>VPN -&gt; IPSec -&gt; Phase-2 Profiles -&gt; &lt;Multi-Proposal&gt; -&gt;</b> 	<i>AES-128/MD5</i>
<b>Alive Check</b>	<b>VPN -&gt; IPSec -&gt; Phase-2 Profiles -&gt; &lt;Multi-Proposal&gt; -&gt;</b>  <b>Advanced Settings</b>	<i>Inactive</i>

### DynDNS


Field	Menu	Value
<b>Hostname</b>	<b>Local Services -&gt; DynDNS Client -&gt; DynDNS Update -&gt; New</b>	e. g. <i>headoffice.dyndns.org</i>
<b>Interface</b>	<b>Local Services -&gt; DynDNS</b>	e.g. <i>Internet</i>




Field	Menu	Value
	Client -> DynDNS Update -> New	
User Name	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>Head Office</i>
Password	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>password</i>
Provider	Local Services -> DynDNS Client -> DynDNS Update -> New	<i>dyndns</i>
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. <i>Head Office</i>
Mode	System Management-> Certificates -> Request	<i>Manual</i>
Common Name	System Management -> Certificates -> Request	e.g. <i>Head Office</i>
External Filename	System Management -> Certificates -> Import	e.g. <i>C:\Headoffice.crt</i>
Local Certificate Description	System Management -> Certificates -> Import	e.g. <i>Head Office</i>
External Filename	System Management -> Certificates -> Import	e.g. <i>C:\Ca.crt</i>
Local Certificate Description	System Management -> Certificates -> Import	e.g. <i>CA</i>

#### Changing the IPSec tunnel

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

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 7 Security - IPsec with dynamic IP addresses and DynDNS

### 7.1 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.

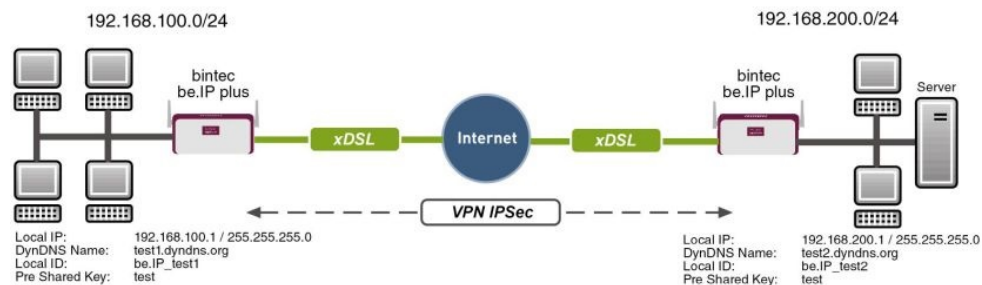


Fig. 123: Example scenario

### 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 via A-DLS flatrate
- Both routers are dynamically assigned an official IP address, and have configured a DynDNS account.

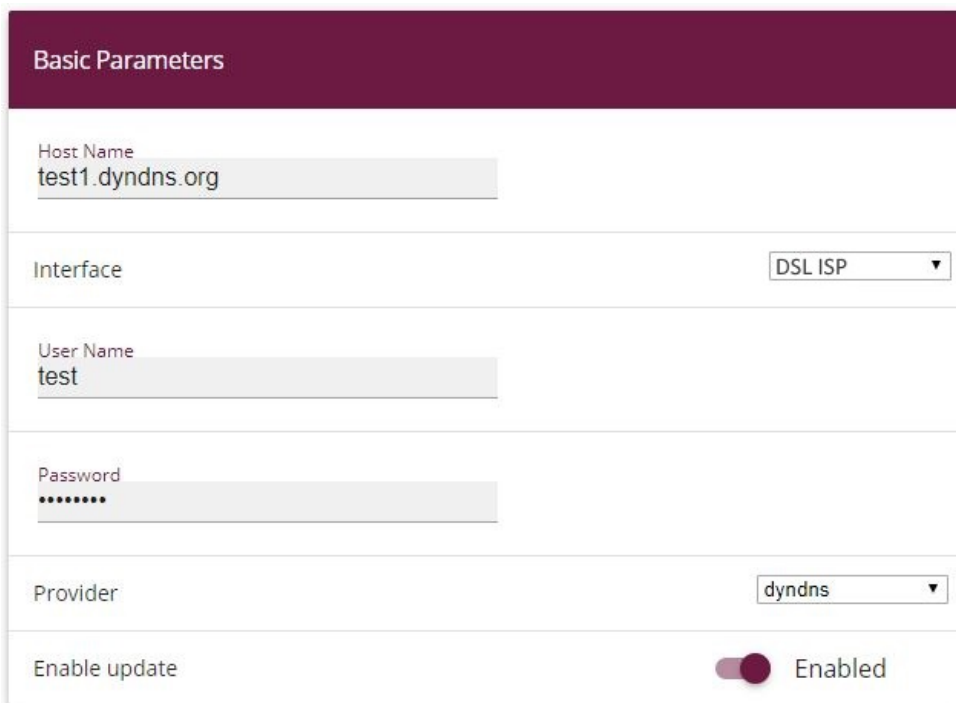
## 7.2 Configuration

### 7.2.1 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**.



The screenshot shows a web interface for configuring a DynDNS client. The page has a dark red header with the text "Basic Parameters". Below the header, there are several input fields and dropdown menus:

- Host Name:** A text input field containing "test1.dyndns.org".
- Interface:** A dropdown menu with "DSL ISP" selected.
- User Name:** A text input field containing "test".
- Password:** A text input field with masked characters (dots).
- Provider:** A dropdown menu with "dyndns" selected.
- Enable update:** A toggle switch that is currently turned on, labeled "Enabled".

Fig. 124: **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**.

The screenshot displays two configuration panels for an IPSec peer. The left panel, titled 'Peer Parameters', includes fields for:
 

- Administrative Status:** Radio buttons for 'Up' (selected) and 'Down'.
- Description:** Text input field containing 'be.IP\_test2'.
- Peer Address:** Includes a dropdown for 'IP Version' (set to 'IPv4 Preferred') and a text input field with 'test2.dyndns.org'.
- Peer ID:** Includes a dropdown for 'Fully Qualified Domain Name (FQDN)' and a text input field with 'be.IP\_test2'.
- Internet Key Exchange:** A dropdown menu set to 'IKEv1'.
- Preshared Key:** A text input field with masked characters '\*\*\*\*\*'.
- IP Version of the tunneled Networks:** A dropdown menu set to 'IPv4'.

 The right panel, titled 'IPv4 Interface Routes', includes:
 

- Security Policy:** Radio buttons for 'Untrusted' and 'Trusted' (selected).
- IPv4 Address Assignment:** A dropdown menu set to 'Static'.
- Default Route:** A toggle switch set to 'Disabled'.
- Local IP Address:** A text input field containing '192.168.100.1'.
- Route Entries:** A table with columns 'Remote IP Address', 'Netmask', and 'Metric'. One entry is shown: Remote IP Address '192.168.200.0', Netmask '255.255.255.0', and Metric '1'. Below the table is an 'ADD' button.


Fig. 125: **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 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>

DH Group 2(1024 Bit) ▼

Lifetime  Seconds  kBytes

Authentication Method Preshared Keys ▼

Mode  Main Mode (ID Protect)  Aggressive  Strict

Local ID Type Fully Qualified Domain Name (FQDN) ▼

Local ID Value



## Advanced Settings

The screenshot shows a configuration window titled 'Advanced Parameter'. It contains three main sections:


- Alive Check:** A dropdown menu currently showing 'Dead Peer Detection (Idle)'.
- Block Time:** A text input field containing the number '30', followed by the label 'Seconds'.
- NAT Traversal:** A dropdown menu currently showing 'Enabled'.

Fig. 127: 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* KBytes.
- (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 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>

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. 129: VPN -> IPsec -> Phase-2 Profiles -> New

Proceed as follows:

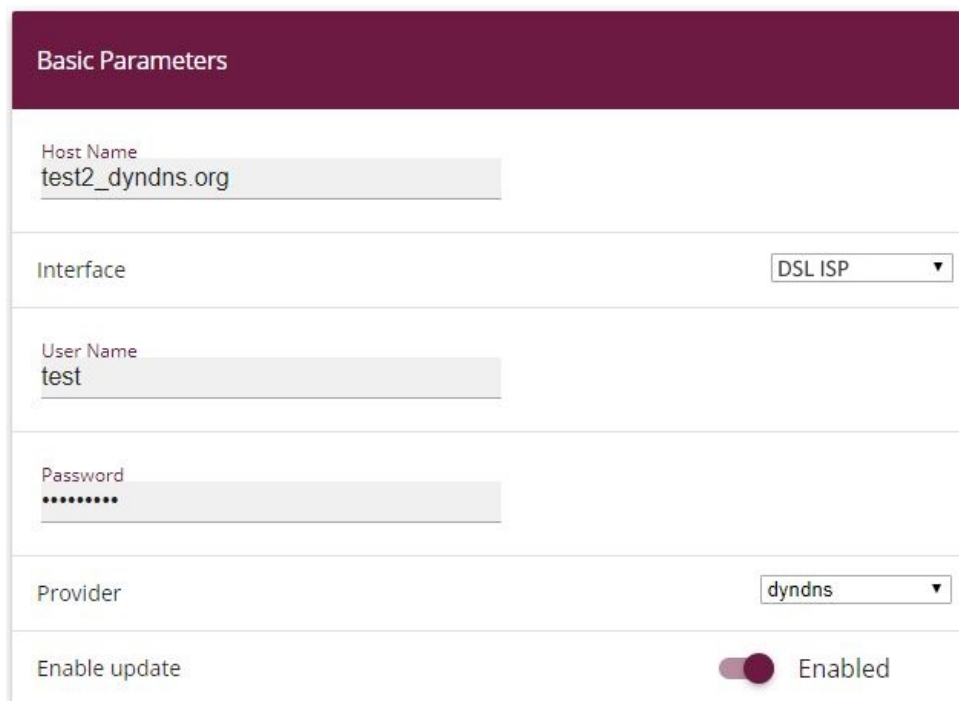
- (1) Enter a **Description** that uniquely identifies the profile.
- (2) Under **Proposal Encryption** select *Blowfish*, under **Authentication** select *MD5*. Since at least one proposal must be configured at any one time, the first entry in the list is enabled by default.
- (3) Activate the **Use 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) Activate the option **Propagate PMTU**.
- (8) Confirm with **OK**.

## 7.2.2 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. 130: **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**.


The screenshot displays two configuration panels for an IPsec peer. The left panel, titled 'Peer Parameters', includes fields for Administrative Status (set to 'Up'), 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 (masked with asterisks), and IP Version of the tunneled Networks (IPv4). The right panel, titled 'IPv4 Interface Routes', shows Security Policy (Trusted), IPv4 Address Assignment (Static), Default Route (Disabled), Local IP Address (192.168.200.1), and a Route Entries table with one entry: Remote IP Address 192.168.100.0, Netmask 255.255.255.0, and Metric 1.

Fig. 131: 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 ▼	<input type="checkbox"/>
AES ▼	SHA1 ▼	<input type="checkbox"/>
AES ▼	SHA1 ▼	<input type="checkbox"/>

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

The screenshot shows a configuration window titled "Advanced Parameter". It contains three sections:


- Alive Check:** A dropdown menu is set to "Dead Peer Detection (Idle)".
- Block Time:** A text input field contains the number "10", followed by the label "Seconds".
- NAT Traversal:** A dropdown menu is set to "Enabled".

Fig. 133: 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* KBytes.
- (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 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>
AES ▼	MD5 ▼	<input type="checkbox"/>

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. 135: 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* KBytes.
- (5) Click **Advanced Settings**.
- (6) Set **Alive Check** to *Heartbeats (send & expect)*.
- (7) Activate the option **Propagate PMTU**.
- (8) Confirm with **OK**.

## 7.3 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 **Gobutton**. 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**.

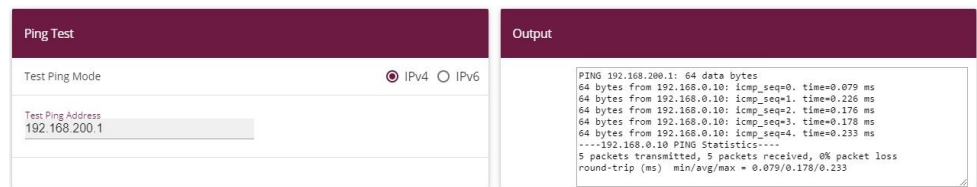


Fig. 136: Maintenance->Diagnostics->Ping Test

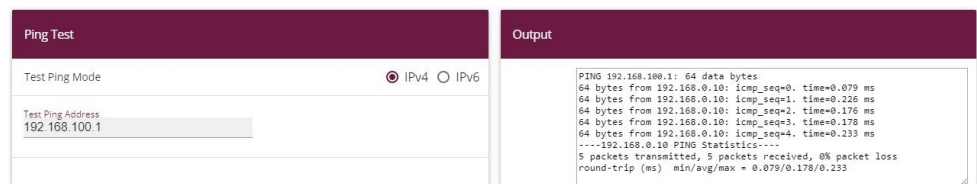


Fig. 137: Maintenance->Diagnostics->Ping Test

## 7.4 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. <i>test1.dyndns.org</i>
Interface	Local Services -> DynDNS Client -> DynDNS Update -> New	<i>DSL ISP</i>
User Name	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>test</i>
Password	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>test</i>
Provider	Local Services -> DynDNS Client -> DynDNS Update -> New	<i>dyndns</i>
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. <i>be.IP_test2</i>
Peer Address	VPN -> IPSec -> IPSec Peers -> New	e.g. <i>test2.dyndns.org</i>
Peer ID	VPN -> IPSec -> IPSec Peers -> New	<i>Fully Qualified Domain Name (FQDN) / be.IP_test2</i>
Preshared Key	VPN -> IPSec -> IPSec Peers -> New	e.g. <i>test</i>
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	<i>192.168.100.1</i>
Route Entries	VPN -> IPSec -> IPSec Peers -> New	<i>192.168.200.0 / 255.255.255.0</i>

### IPSec configuration - Phase 1

Field	Menu	Value
Description	VPN -> IPSec ->Phase-1 Profiles -> New	e.g. <i>*autogenerated*</i>
Proposals	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Blowfish, MD5</i>
DH Group	VPN -> IPSec ->Phase-1 Profiles -> New	<i>2 (1024 Bit)</i>
Lifetime	VPN -> IPSec ->Phase-1 Profiles -> New	<i>900 seconds, 0 kBytes</i>
Authentication Method	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Preshared Keys</i>
Mode	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Aggressive</i>
Local ID Type	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Fully Qualified Domain Name (FQDN)</i>
Local ID Value	VPN -> IPSec ->Phase-1 Profiles -> New	<i>be.IP_test1</i>
Alive Check	VPN -> IPSec ->Phase-1 Profiles -> New -> Advanced Settings	<i>Dead Peer Detection (idle)</i>
Block Time	VPN -> IPSec ->Phase-1 Profiles -> New -> Advanced Settings	<i>10 seconds</i>
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. <i>*autogenerated*</i>
Proposals	VPN -> IPSec ->Phase-2 Profiles -> New	<i>Blowfish, MD5</i>
Use PFS Group	VPN -> IPSec ->Phase-2 Profiles -> New	<i>2 (1024 Bit)</i>
Lifetime	VPN -> IPSec ->Phase-2 Profiles -> New	<i>900 seconds, 0 kBytes</i>
IP Compression	VPN -> IPSec ->Phase-2 Profiles -> New -> Advanced Settings	<i>Disabled</i>
Alive Check	VPN -> IPSec ->Phase-2 Profiles -> New -> Advanced Settings	<i>Heartbeats (send &amp; expect)</i>

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. <i>test2.dyndns.org</i>
Interface	Local Services -> DynDNS Client -> DynDNS Update -> New	<i>DSL ISP</i>
User Name	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>test</i>
Password	Local Services -> DynDNS Client -> DynDNS Update -> New	e.g. <i>test</i>
Provider	Local Services -> DynDNS Client -> DynDNS Update -> New	<i>dyndns</i>
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. <i>be.IP_test1</i>
Peer Address	VPN -> IPSec ->IPSec Peers -> New	e.g. <i>test1.dyndns.org</i>
Peer ID	VPN -> IPSec ->IPSec Peers -> New	<i>Fully Qualified Domain Name (FQDN)/ be.IP_test1</i>
Preshared Key	VPN -> IPSec ->IPSec Peers -> New	e.g. <i>test</i>
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	<i>192.168.200.1</i>
Route Entries	VPN -> IPSec ->IPSec Peers -> New	<i>192.168.100.0 / 255.255.255.0</i>

#### IPSec configuration - Phase 1

Field	Menu	Value
Description	VPN -> IPSec ->Phase-1 Profiles -> New	e.g. <i>*autogenerated*</i>
Proposals	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Blowfish, MD5</i>
DH Group	VPN -> IPSec ->Phase-1 Profiles -> New	<i>2 (1024 Bit)</i>
Lifetime	VPN -> IPSec ->Phase-1 Profiles -> New	<i>900 seconds, 0 kBytes</i>
Authentication Method	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Preshared Keys</i>
Mode	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Aggressive</i>
Local ID Type	VPN -> IPSec ->Phase-1 Profiles -> New	<i>Fully Qualified Domain Name (FQDN)</i>
Local ID Value	VPN -> IPSec ->Phase-1 Profiles -> New	<i>be.IP_test2</i>
Alive Check	VPN -> IPSec ->Phase-1 Profiles -> New -> Advanced Settings	<i>Dead Peer Detection (idle)</i>
Block Time	VPN -> IPSec ->Phase-1 Profiles -> New -> Advanced Settings	<i>10 seconds</i>
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. <i>*autogenerated*</i>
Proposals	VPN -> IPSec ->Phase-2 Profiles -> New	<i>Blowfish, MD5</i>
Use PFS Group	VPN -> IPSec ->Phase-2 Profiles -> New	<i>2 (1024 Bit)</i>
Lifetime	VPN -> IPSec ->Phase-2 Profiles -> New	<i>900 seconds, 0 kBytes</i>
IP Compression	VPN -> IPSec ->Phase-2 Profiles -> New -> Advanced Settings	<i>Disabled</i>
Alive Check	VPN -> IPSec ->Phase-2 Profiles -> New -> Advanced Settings	<i>Heartbeats (send &amp; expect)</i>

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

## Chapter 8 Security - Bridging over an IPSec tunnel

### 8.1 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.

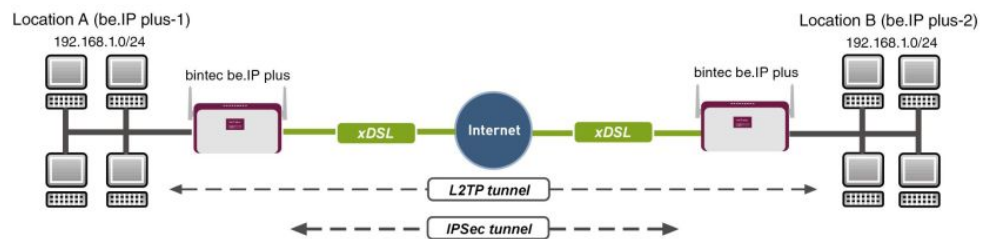


Fig. 138: Example scenario

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

## 8.2 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**.



Fig. 139: **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	Enter IP settings:
Description IPSec-Peer1	IPSec Peer IPv4 Address 10.1.1.4
Local IPsec ID be.ip_plus-1	Remote IPv4 Network 1.1.1.2
Remote IPsec ID be.IP_plus-2	255.255.255.0
Preshared Key *****	
IP Version of the tunneled Networks IPv4	
Local IP Address 192.168.1.253	
Define this connection as default route <input type="checkbox"/> Disabled	

Fig. 140: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

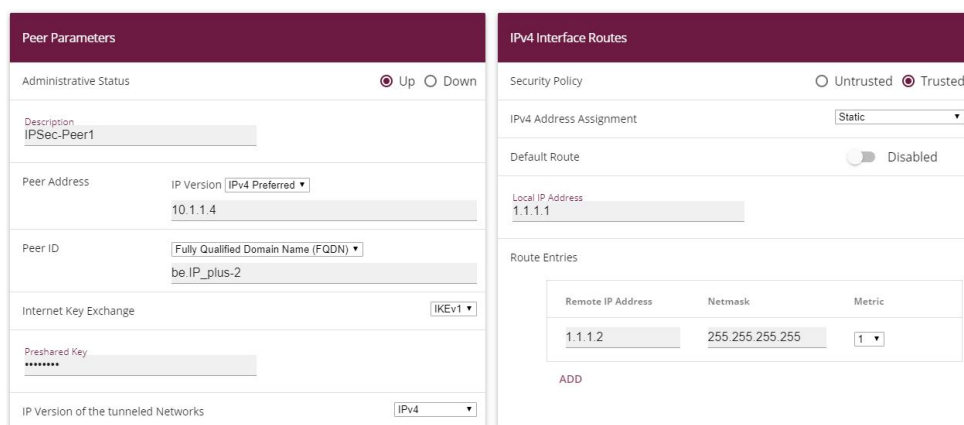
Proceed as follows to configure a new VPN connection:

- (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 -> **.



The screenshot shows two configuration panels for an IPSec peer. The left panel, titled 'Peer Parameters', includes fields for Administrative Status (Up/Down), Description (IPSec-Peer1), Peer Address (10.1.1.4), Peer ID (be.IP\_plus-2), Internet Key Exchange (IKEv1), and IP Version of the tunneled Networks (IPv4). The right panel, titled 'IPv4 Interface Routes', includes Security Policy (Trusted), IPv4 Address Assignment (Static), Default Route (Disabled), Local IP Address (1.1.1.1), and a table for Route Entries with columns for Remote IP Address, Netmask, and Metric.

Remote IP Address	Netmask	Metric
1.1.1.2	255.255.255.255	1

Fig. 141: **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	LAC Mode Parameters
Description L2TP-LAC	Remote IP Address 1.1.1.2
Local Hostname be.IP_plus-1	UDP Source Port <input type="checkbox"/> Dynamic
Remote Hostname be.IP_plus-2	UDP Destination Port 1701
Password *****	

## 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	<input type="checkbox"/> Disable

Fig. 143: 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**.

The screenshot displays two configuration panels for a new L2TP user. The left panel, titled 'Basic Parameters', includes fields for Description (L2TP-LAC), Connection Type (LAC selected), Tunnel Profile (L2TP-LAC), User Name (L2TP-User), Password (masked), Always on (disabled), and Connection Idle Timeout (300 seconds). The right panel, titled 'IP Mode and Routes', shows IP Address Mode (Static selected), Default Route (disabled), Create NAT Policy (disabled), Local IP Address (1.1.1.3), and a Route Entries table with one entry: Remote IP Address 1.1.1.4, Netmask 255.255.255.255, and Metric 1.

Advanced Settings

The bottom section shows 'Advanced Settings' with two panels. The left panel, 'Advanced Parameter', includes Block after connection failure for (300 seconds), Authentication (MS-CHAPv2), Encryption (None selected), LCP Alive Check (Enabled), and Prioritize TCP ACK Packets (disabled). The right panel, 'IP Options', includes OSPF Mode (Passive selected), Proxy ARP Mode (Inactive selected), and DNS Negotiation (Enabled).

Fig. 145: 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**.

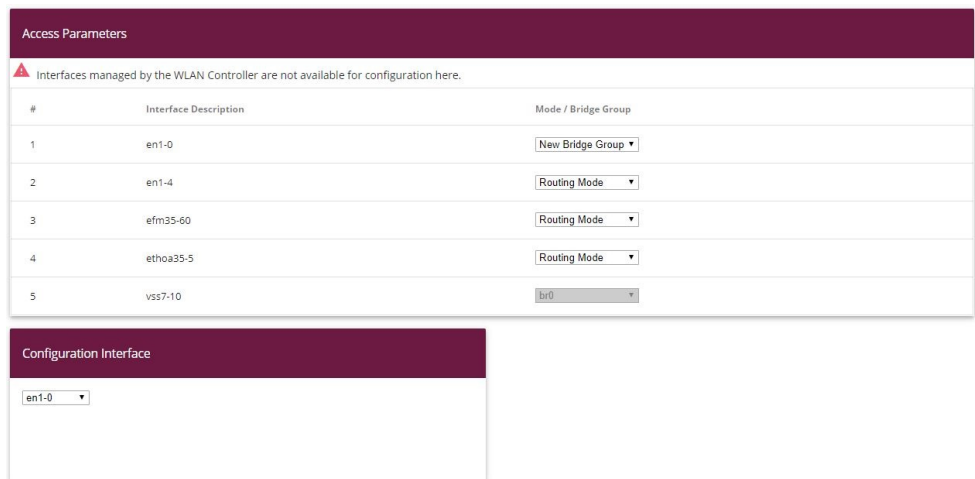


Fig. 146: **System Management -> Interface Mode / Bridge Groups -> Interfaces**

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:

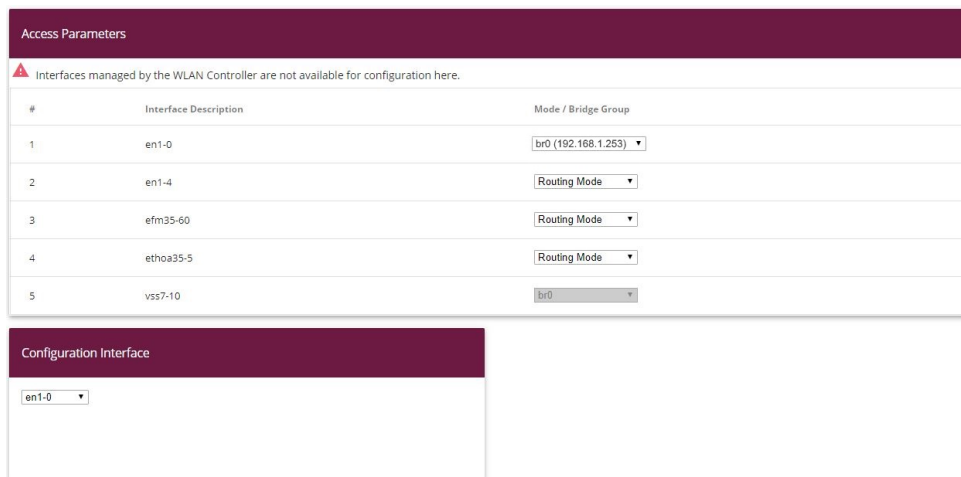


Fig. 147: **System Management -> Interface Mode / Bridge Groups -> Interfaces**

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

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



Fig. 148: **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**.

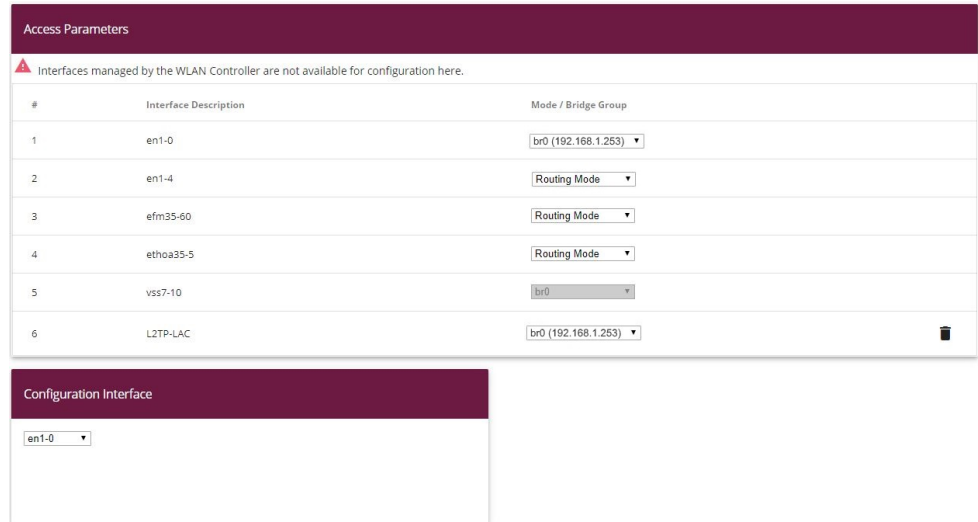


Fig. 149: System Management -> Interface Mode / Bridge Groups -> Interfaces

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.

## 8.3 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**.

Fig. 150: **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	Enter IP settings:
Description IPSec-Peer1	IPSec Peer IPv4 Address 10.1.1.1
Local IPsec ID be_ip_plus-2	Remote IPv4 Network 1.1.1.1
Remote IPsec ID be_IP_plus-1	255.255.255.255
Preshared Key *****	
IP Version of the tunneled Networks IPv4	
Local IP Address 192.168.1.254	
Define this connection as default route <input type="checkbox"/> Disabled	

Fig. 151: **Assistants** -> **VPN** -> **VPN Connections** -> **Next**

Proceed as follows to configure a new VPN connection:

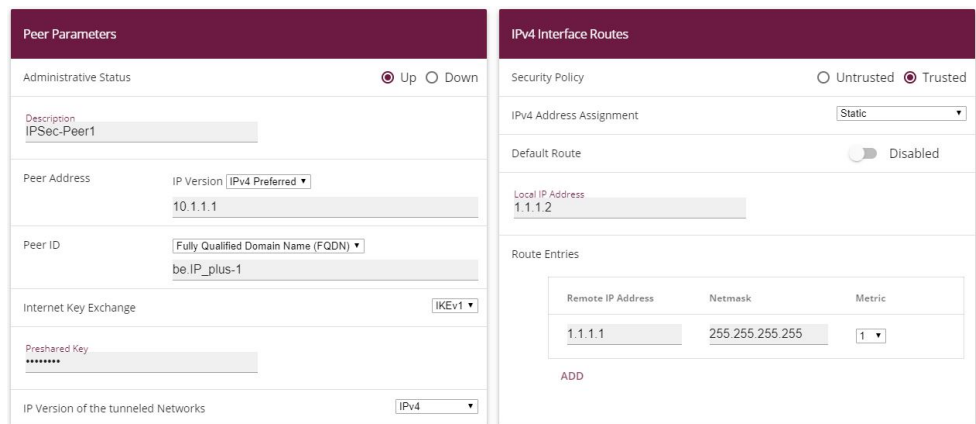
- (1) For example, under **Description** enter *IPSec Peer1*.
- (2) Enter the ID of your own IPsec gateway under **Local IPsec ID**, e.g. *be.IP\_plus-2*.
- (3) For example, under **Remote IPsec ID** enter *be.IP\_plus-1*.
- (4) Under **Preshared Key** enter, for example, *secret* for authentication. 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 ->** .



The screenshot shows two configuration panels for an IPSec peer. The left panel, titled 'Peer Parameters', includes fields for 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), and IP Version of the tunneled Networks (IPv4). The right panel, titled 'IPv4 Interface Routes', includes Security Policy (Untrusted/Trusted), IPv4 Address Assignment (Static), Default Route (Disabled), Local IP Address (1.1.1.2), and a table for Route Entries.

Remote IP Address	Netmask	Metric
1.1.1.1	255.255.255.255	1

Fig. 152: **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	LAC Mode Parameters
Description L2TP-LAS	Remote IP Address 1.1.1.1
Local Hostname be.IP_plus-2	UDP Source Port <input type="checkbox"/> Dynamic
Remote Hostname be.IP_plus-1	UDP Destination Port 1701
Password *****	

## 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 <input type="checkbox"/> Disable

Fig. 154: VPN-&gt;L2TP-&gt;Tunnel Profiles -&gt;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**.

The screenshot displays two panels of the VPN configuration interface. The left panel, titled "Basic Parameters", contains the following fields and controls:

- Description:** L2TP-LAS
- Connection Type:** LNS (selected), LAC
- User Name:** L2TP-User
- Password:** [Redacted]
- Always on:** Disabled
- Connection Idle Timeout:** 300 Seconds

The right panel, titled "IP Mode and Routes", contains the following fields and controls:

- IP Address Mode:** Static (selected), Provide IP Address
- Default Route:** Disabled
- Create NAT Policy:** Disabled
- Local IP Address:** 1.1.1.4
- Route Entries:**

Remote IP Address	Netmask	Metric
1.1.1.3	255.255.255.255	1

#### Advanced Settings

The screenshot displays two panels of the VPN configuration interface. The left panel, titled "Advanced Parameter", contains the following fields and controls:

- Block after connection failure for:** 300 Seconds
- Authentication:** MS-CHAPv2
- Encryption:** None (selected), Enabled, Windows compatible
- LCP Alive Check:** Enabled
- Prioritize TCP ACK Packets:** Disabled

The right panel, titled "IP Options", contains the following fields and controls:

- OSPF Mode:** Passive (selected), Active, Inactive
- Proxy ARP Mode:** Inactive (selected), Up or Dormant, Up only
- DNS Negotiation:** Enabled

Fig. 156: **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**.

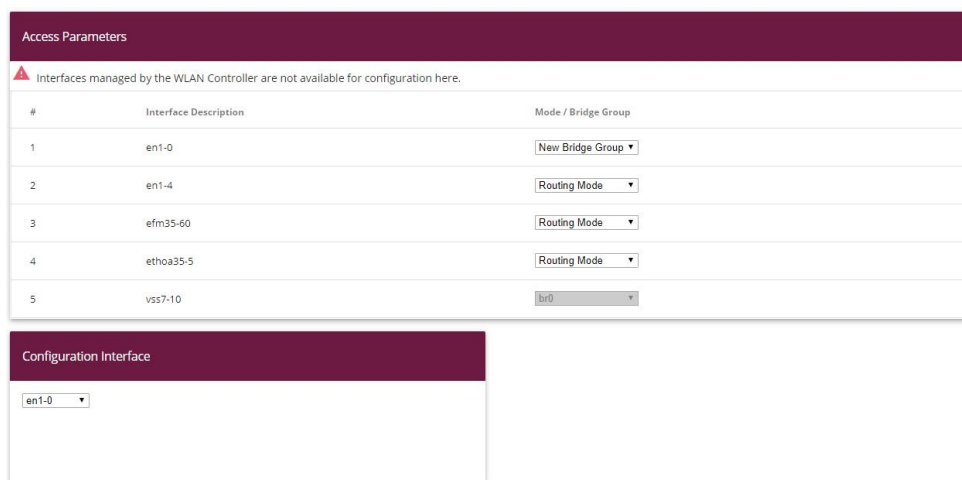


Fig. 157: **System Management -> Interface Mode / Bridge Groups -> Interfaces**

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:

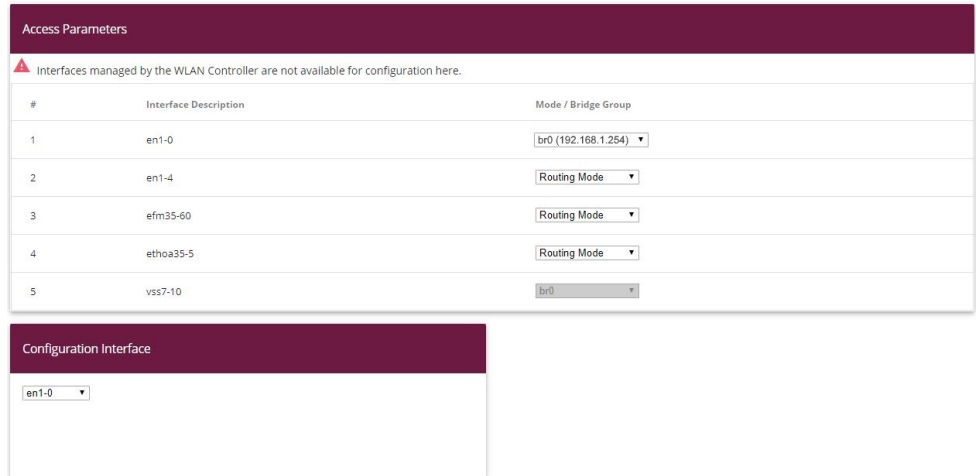


Fig. 158: **System Management -> Interface Mode / Bridge Groups -> Interfaces**

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

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



Fig. 159: **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**.

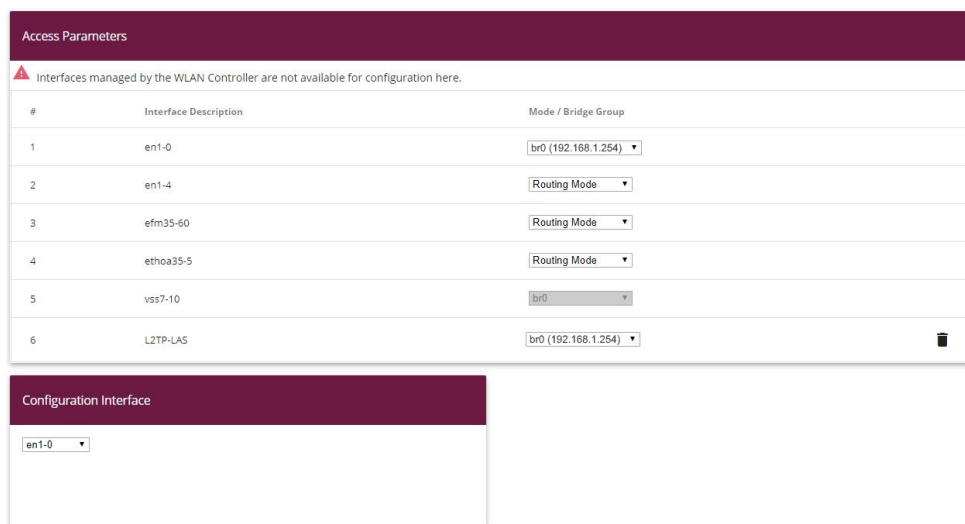


Fig. 160: System Management -> Interface Mode / Bridge Groups -> Interfaces

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.

## 8.4 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. <i>IPSec-Peer1</i>
Local IPSec ID	Assistants -> VPN -> VPN Connections -> Next	e.g. <i>be.IP_plus-1</i>
Remote IPSec ID	Assistants -> VPN -> VPN Connections -> Next	e.g. <i>be.IP_plus-2</i>
Preshared Key	Assistants -> VPN -> VPN Connections -> Next	e.g. <i>secret</i>

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	<i>New Bridge Group</i>
Configuration Interface	System Management -> Interface Mode / Bridge Groups -> Interfaces	<i>en1-0</i>

#### Assigning a L2TP interface

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

## Chapter 9 Security - Stateful Inspection Firewall (SIF)

### 9.1 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 establish 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.

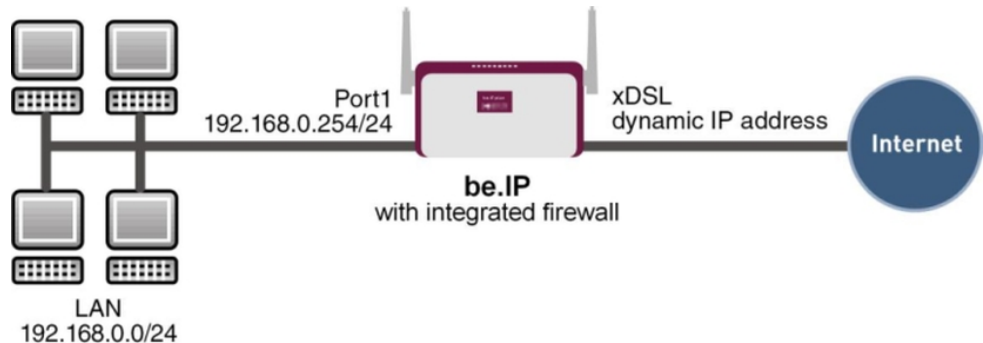


Fig. 161: Example scenario SIF

### 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.

## 9.2 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.

### 9.2.1 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. 162: 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	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Selection	
Addresses	Selection
ANY	<input type="checkbox"/>
Administrator	<input checked="" type="checkbox"/>
Director	<input checked="" type="checkbox"/>
be.IP	<input type="checkbox"/>
Network Internal	<input type="checkbox"/>

Fig. 163: 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**.

## 9.2.2 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.

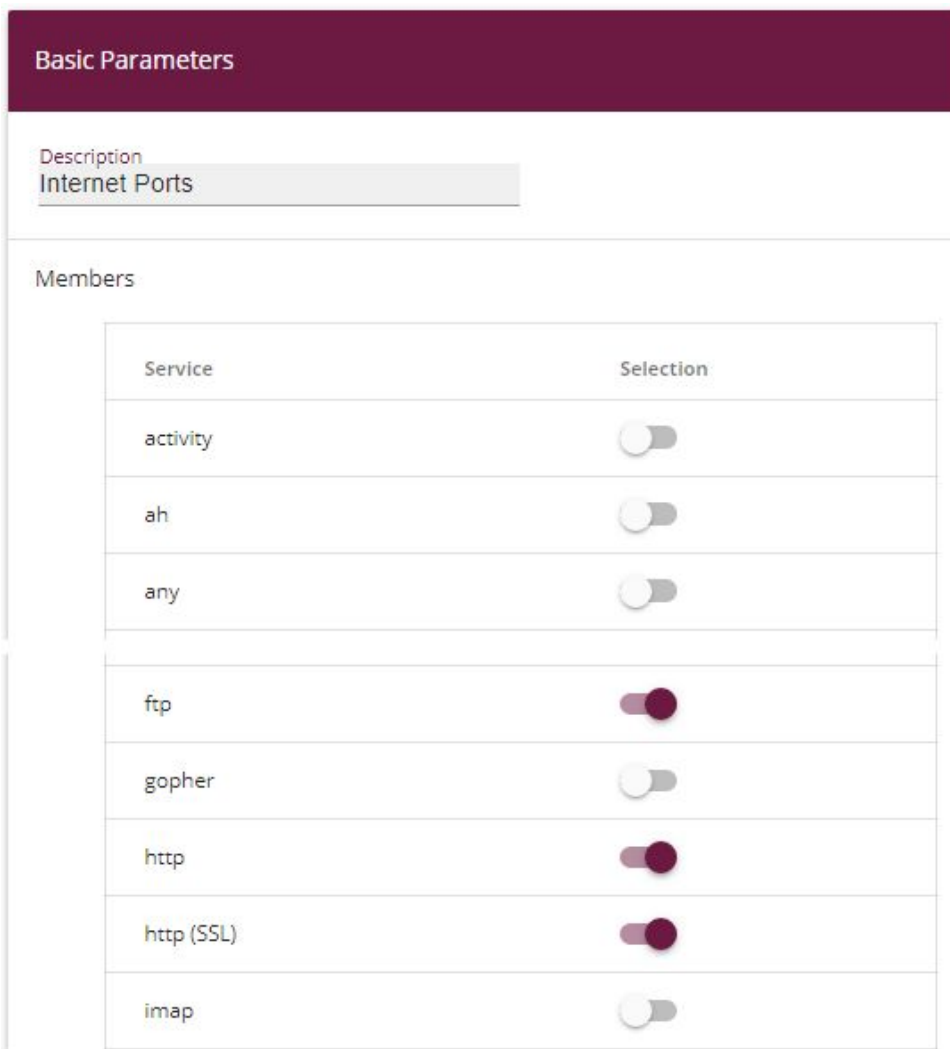
You can group together several services into groups to make it easier to configure the filter

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**.



Service	Selection
activity	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<input type="checkbox"/>
ftp	<input checked="" type="checkbox"/>
gopher	<input type="checkbox"/>
http	<input checked="" type="checkbox"/>
http (SSL)	<input checked="" type="checkbox"/>
imap	<input type="checkbox"/>

Fig. 164: **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.

### 9.2.3 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	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎	
2	LOCAL	ANY	dns	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎	
3	Network Internal	be.IP	dns	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎	
4	ANY	be.IP	any	Deny	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎	
5	Director	ANY	any	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎	
6	Network Internal	ANY	Internet Ports	Access	<input checked="" type="checkbox"/> Enabled	↑↓	≡+	🗑️	✎	

Fig. 165: 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.

## 9.3 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.

## 9.4 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] -> bc.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[1000:66.249.85.99:80] http:6
01:43:41 DEBUG/INET: SIF: No Rule, Ignore [1000:192.168.0.2:8] -> [1000:62.146.2.103:0] :1
01:44:02 DEBUG/INET: SIF: Accept Administrator[1000:192.168.0.2:2393] -> bc.IP [1:192.168.0.1:23] telnet:6
01:44:31 DEBUG/INET: SIF: Accept Netzwerk_Intern[1000:192.168.0.50:1396] -> bc.IP [1:192.168.0.1:53] dns:17
01:44:34 DEBUG/INET: SIF: Accept Geschaefsfuehrer[1000:192.168.0.50:137] -> ANY[1000:192.168.0.255:137] any:17
01:44:34 DEBUG/INET: SIF: Accept Geschaefsfuehrer[1000:192.168.0.50:123] -> ANY[1000:207.46.232.189:123] any:17
01:44:41 DEBUG/INET: SIF: Accept Geschaefsfuehrer[1000:192.168.0.50:8] -> ANY[1000:62.146.2.103:0] any:1
01:44:43 DEBUG/INET: SIF: Accept Geschaefsfuehrer[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.

## 9.5 Overview of configuration steps

### Aliases for IP addresses and network address

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

### Address groups

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

## Service Sets

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

## Filter Rules

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

Field	Menu	Value
	<b>Rules -&gt; New</b>	
<b>Destination</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>be.IP</i>
<b>Service</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>any</i>
<b>Action</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>Deny</i>
<b>Source Location</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>Director</i>
<b>Destination</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>ANY</i>
<b>Service</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>any</i>
<b>Action</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>Access</i>
<b>Source Location</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>Network_Internal</i>
<b>Destination</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>ANY</i>
<b>Service</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>Internet Ports</i>
<b>Action</b>	<b>Firewall -&gt; Policies -&gt; Filter Rules -&gt; New</b>	<i>Access</i>

## Chapter 10 Security - VPN connection via a SMS PASSCODE server

### 10.1 Introduction

This workshop describes the VPN IPsec Client connection of the **bintec Secure IPsec Clients** 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.

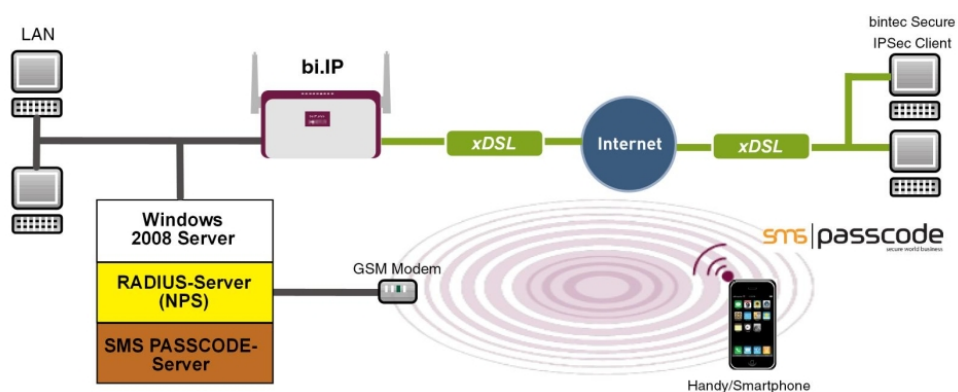


Fig. 166: Example scenario

### 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.smpasscode.com>)

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

## 10.2 Configuration

### 10.2.1 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.smpasscode.com>).

### 10.2.2 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.

### 10.2.3 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.



Fig. 167: SMS PASSCODE

## 10.2.4 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**.

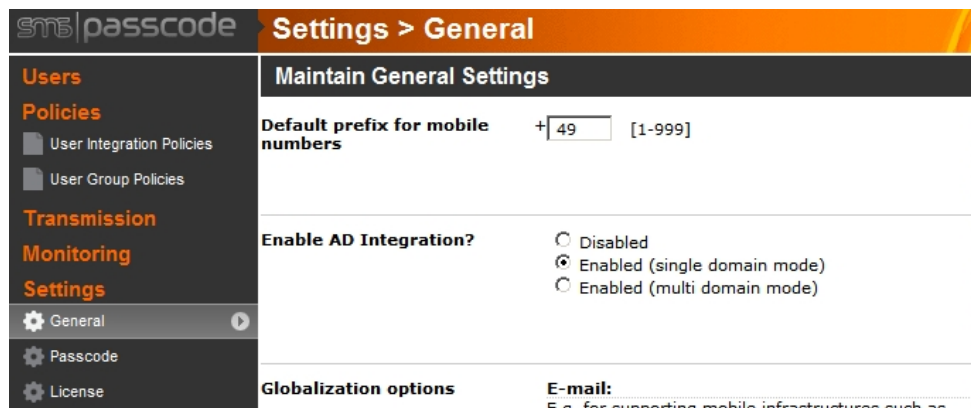


Fig. 168: Settings -&gt; General

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

Fig. 169: 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.

## 10.2.5 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.

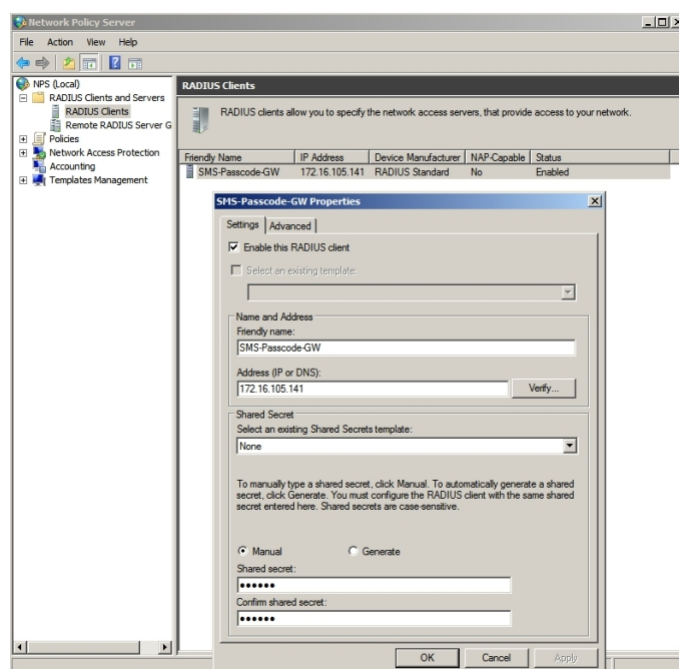


Fig. 170: Network Policy Server (NPS)

- (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.

## 10.2.6 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.



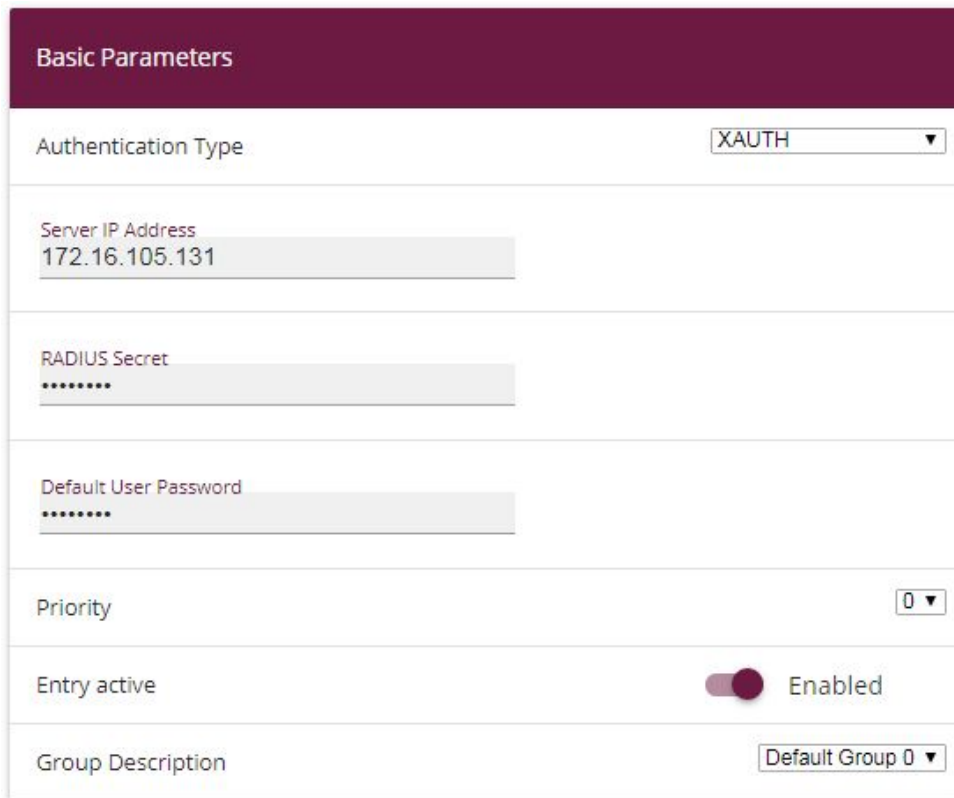
### Note

Instead of the **Multi-User IPSec configuration**, 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 RADIUS 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

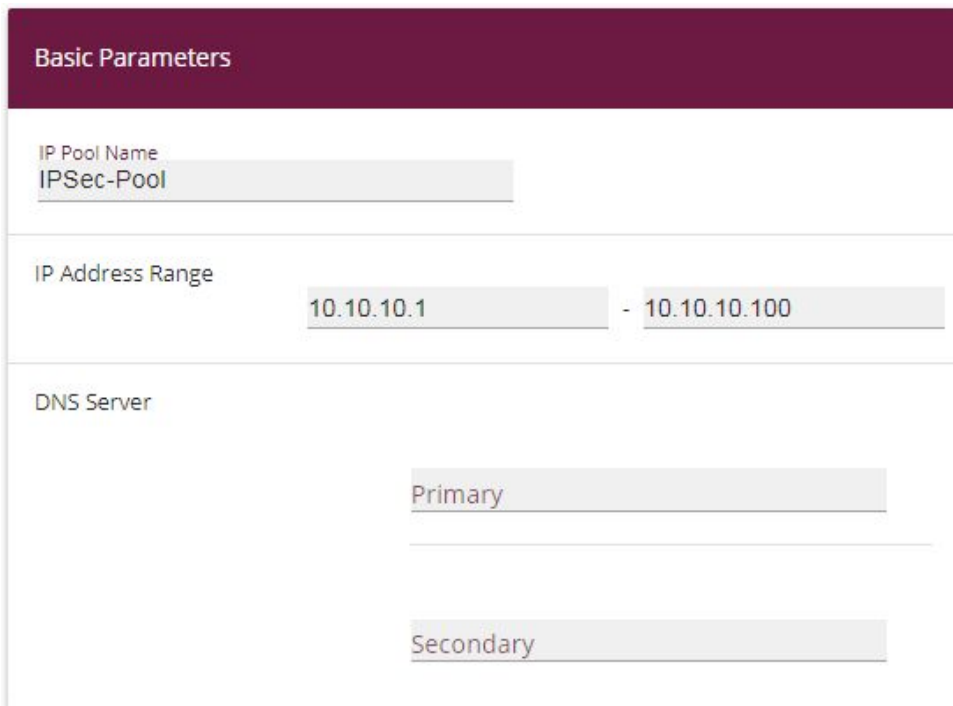
Fig. 171: **System Management->Remote Authentication->RADIUS->New**

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

Primary

Secondary

Fig. 172: 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**.

Fig. 173: 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**.

Fig. 174: 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**.

## 10.2.7 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**.

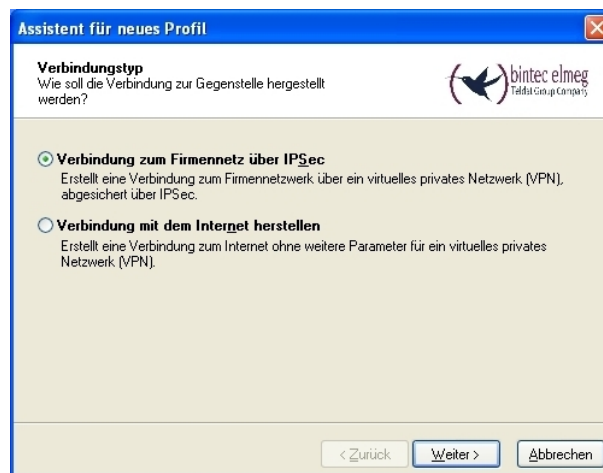


Fig. 175: Connection Type

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

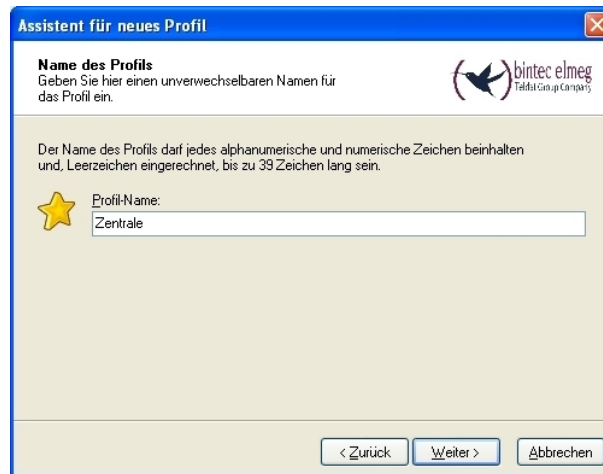


Fig. 176: Profile Name

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.

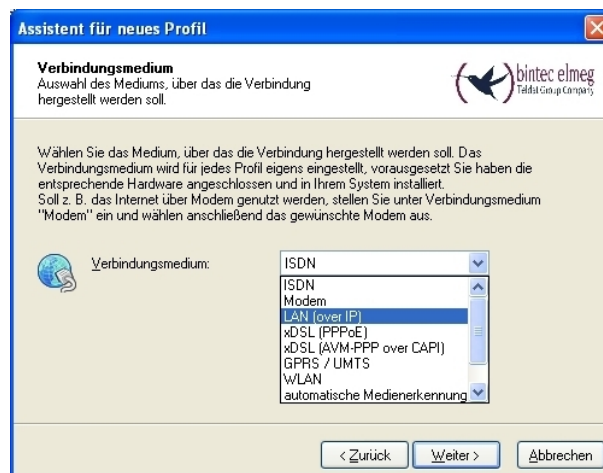


Fig. 177: Connection Medium

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:  
XXXXXXXX

Passwort (Wiederholung):  
XXXXXXXX

< Zurück Weiter > Abbrechen

Fig. 178: 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 Richtlinien der IPSec-Verhandlung wird die Einstellung "Automatischer Modus" verwendet.  
Sollen bestimmte IKE / IPSec-Richtlinien 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

< Zurück Weiter > Abbrechen

Fig. 179: 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).

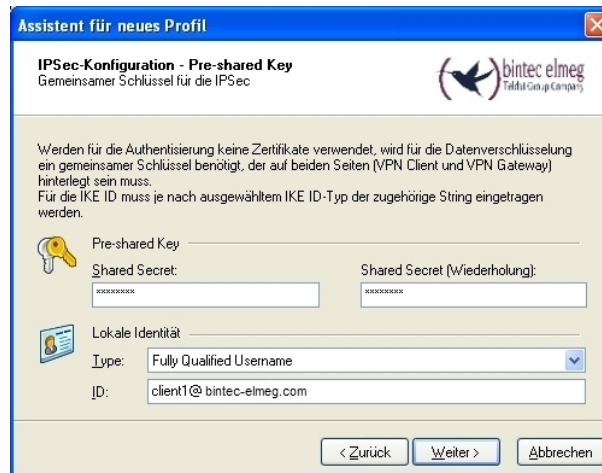


Fig. 180: Preshared Key

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.

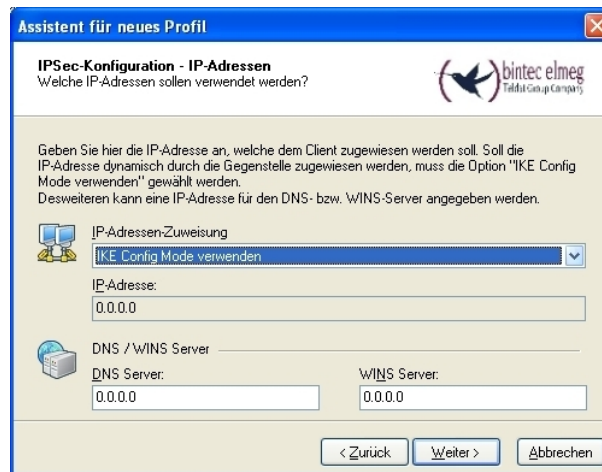


Fig. 181: IKE Config Mode

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.

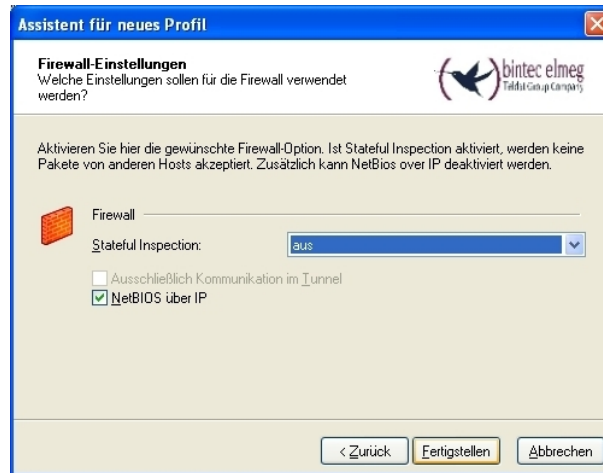


Fig. 182: Firewall

### 10.3 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.

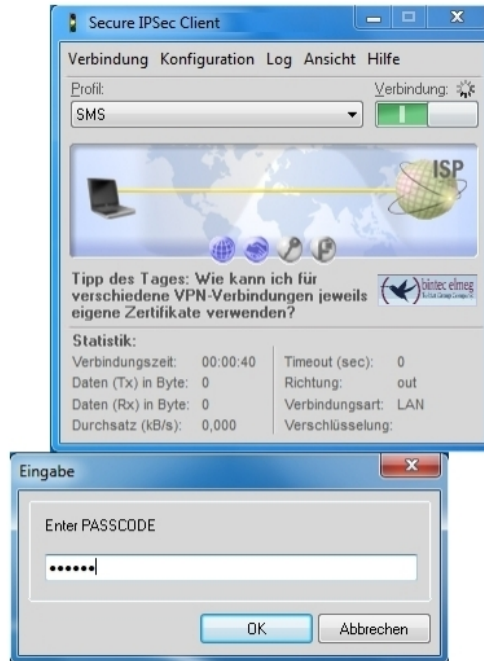


Fig. 183: Secure IP Sec Client

## 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-1sakmp-xauth-06'
P1: peer 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'draft-ietf-ipsecc-nat-t-ike-03'
P1: peer 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'draft-ietf-ipsecc-nat-t-ike-02'
P1: peer 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'draft-ietf-ipsecc-nat-t-ike-00'
P1: peer 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is '4a131c81070358459c5728f20e95452f'
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 'cbleed48b6d8269bb411b61a07bc9e07'
P1: peer 0 sa 3 (R): vendor ID: 172.16.105.130:10952 (No ID) is 'c61bacaf1a60cc10800000000000000'
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])=musermann@ldat.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 musermann@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])=musermann@ldat.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 musermann
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[3e134fc4] 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 musermann
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 musermann 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

```

## 10.4 Overview of Configuration Steps

### Installation of SMS PASSCODE server

Field	Menu	Value
RADIUS client protection	SMS PASSCODE -> Install Shield Wizard	<i>Enabled</i>

### Configuration of Web Administration Tool

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

### Configuration of RADIUS server

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

### Configuration of the VPN gateway

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

### Create IP Address Pool

Field	Menu	Value
IP Pool Name	VPN -> IPsec -> IP Pools -> Add	e.g. <i>IPsec Pool</i>



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. <i>vpngate-way.bintec-elmeg.com</i>
Advanced authentication (XAUTH)	Wizard for new profile	Enabled
Login name	Wizard for new profile	e.g. <i>mustermann</i>
Password	Wizard for new profile	e.g. <i>supersecret</i>
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. <i>bintec elmeg</i>
Shared Secret (Retry)	Wizard for new profile	e.g. <i>bintec elmeg</i>
Type	Wizard for new profile	e.g. <i>Fully Qualified Username</i>
ID	Wizard for new profile	e.g. <i>client1@bintec-elmeg.com</i>
IP address assignment	Wizard for new profile	<i>Use IKE Config Mode</i>
Stateful Inspection	Wizard for new profile	<i>off</i>
NetBIOS over IP	Wizard for new profile	Enabled