

bintec Workshop IPSec VPN with Callback (IP-Address in B/D channel)

Copyright [©] November 8, 2005 Funkwerk Enterprise Communications GmbH Version 0.9

| Purpose | This document is part of the user's guide to the installation and configuration of bintec gateways run- ning software release 7.1.4 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our Release Notes , especially when carrying out a software update to a later release level. The latest Release Notes can be found at www.funkwerk- ec.com. | | |
|--|---|---|--|
| Liability | While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery. | | |
| | The information in this manual is subject to change Release Notes for bintec gateways can be found a | without notice. Additional information, changes and at www.funkwerk-ec.com. | |
| | As multiprotocol gateways, bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product. | | |
| Trademarks | bintec and the bintec logo are registered trademark | s of Funkwerk Enterprise Communications GmbH. | |
| | Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers. | | |
| Copyright | All rights are reserved. No part of this publication may be reproduced or transmitted in any form or by any means – graphic, electronic, or mechanical – including photocopying, recording in any medium, taping, or storage in information retrieval systems, without the prior written permission of Funkwerk En- terprise Communications GmbH. Adaptation and especially translation of the document is inadmissible without the prior consent of Funkwerk Enterprise Communications GmbH. | | |
| Guidelines and standards | bintec gateways comply with the following guidelines and standards: | | |
| | R&TTE Directive 1999/5/EG | | |
| | CE marking for all EU countries and Switzerland | | |
| You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com. | | | |
| How to reach Funkwerk | | | |
| Enterprise Communications GmbH | Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany | Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France | |
| | Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com | Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr | |

| 1 | Introd | uction |
|---|--------|---|
| | 1.1 | Scenario |
| | 1.2 | Requirements |
| 2 | Config | guration of ISDN Interface 5 |
| 3 | Config | guration of Internet Connection (WAN Partner) |
| 4 | Config | guration of IPSec Connection9 |
| | 4.1 | Configuration of IPSec Peer 9 |
| | 4.2 | Configuration of Virtual Interface 10 |
| | 4.3 | Configuration of ISDN Callback Mechanism |
| | 4.4 | Configuration of Parameters for IPSec Phase 1 |
| 5 | Resul | t 17 |
| | 5.1 | Test of Connection and ISDN Callback |
| | 5.2 | Overview of Configuration Steps 19 |

1 Introduction

The configuration of IPSec callback with IP address transfer in the B/Dchannel is described in the following chapters using two Bintec VPN Access 25 gateways (software version 7.1.6 patch 3).

This feature has only been available since firmware version 7.1.4. It enables dynamically assigned IP addresses to be transferred in the B-/D-channel.

1.1 Scenario

A branch office of a company is to be connected to the head office over an IP-Sec tunnel. An ISDN connection is available for the Internet connection in both the branch office and head office. Both devices receive their IP address dynamically from the ISP.



1.2 Requirements

- Two Bintec VPN Access 25 gateways.
- At least firmware version 7.1.4.
- An ISDN S0 connection per Bintec VPN Access 25 gateway.
- Connect your LAN to the ETH1 interface of your gateway.
- ISDN Internet connection.

Introduction

2 Configuration of ISDN Interface

You must configure "Incoming Call Answering" so that for a call to a certain number, this is used for ISDN callback.

```
■ Go to ISDN S0 → INCOMING CALL ANSWERING → ADD.
```

| VPN Access 25 Setup Tool | Bintec Access Networks GmbH |
|--------------------------------------|-----------------------------|
| [SLOT 0 UNIT 4 ISDN BRI][INCOMING][E | DIT] vpn25 |
| Item | IPSec |
| Number | 100 |
| Mode | right to left |
| Bearer | any |
| SAVE | CANCEL |
| Use <space> to select</space> | |

The following fields are relevant:

| Field | Meaning |
|--------|--|
| Item | Service for which this number is to be used. |
| Number | Number for the service. |
| Mode | Type of number check. |
| Bearer | Is to respond to a voice or data call or both. |

Table 2-1: Relevant fields in ISDN S0 -> INCOMING CALL ANSWERING -> ADD

Proceed as follows to define the necessary settings:

- Set ITEM to IPSec.
- Enter the desired number under **NUMBER**, e.g. 100.
- Set **Mode** to right to left.

Note

If your gateway is connected to a point-to-point ISDN connection, it may be necessary to set to *left to right*!

- Set **BEARER** to any.
- Press **SAVE** to confirm your settings.

You have now configured the gateway for using calls via the number 100 for IP-Sec.

3 Configuration of Internet Connection (WAN Partner)

Use the Bintec manual or Bintec FAQs for this configuration.

4 **Configuration of IPSec Connec**tion

This workshop describes the relevant configuration steps for ISDN callback. A more detailed description of configuring an IPSec connection can be found in the Bintec User's Guide or the relevant FAQs.

4.1 **Configuration of IPSec Peer**

Go to IPSEC -> CONFIGURE PEERS -> APPEND.

VPN Access 25 Setup Tool Bintec Access Networks GmbH [IPSEC] [PEERS] [EDIT] : Configure Peer Description: Branch office Admin Status: up Oper Status: dormant

Peer Address: The Branch office Pre Shared Key: * IPSec Callback > Peer specific Settings > Virtual Interface: yes Interface IP Settings > CANCEL SAVE Enter string, max. length = 255 chars

The following fields are relevant:

| Field | Meaning |
|----------------|--|
| Description | Freely selectable description of peer. |
| Peer Address | IP address of remote terminal. |
| Peer IDs | Identity (name) of remote terminal. |
| Pre Shared Key | Secret key for IPSec negotiation. |

vpn25

| Field | Meaning |
|-------------------|---------------------------------|
| Virtual Interface | Virtual interfaces can be used. |

Table 4-1: Relevant fields in **IPSEC ->** CONFIGURE PEERS -> APPEND

Proceed as follows to define the necessary settings:

- Enter a name under **PEER ADDRESS**, e.g. branch office.
- Enter a **Pre Shared Key**, e.g. test.
- Set VIRTUAL INTERFACE, e.g. yes.
- Press **SAVE** to confirm your settings.



The **PRE SHARED KEY** should be at least 25 to 30 characters long in actual operation and not contain any known words or number combinations. A random sequence of upper and lower case letters, numbers and special characters should preferably be used.

You have now completed the basic configuration of an IPSec peer.

4.2 Configuration of Virtual Interface

Go to IPSEC → CONFIGURE PEERS → RELEVANT PEER → INTERFACE IP SETTINGS → BASIC IP SETTINGS.

| VPN Access 25 Setup Tool [IPSEC][PEERS][EDIT][IP][BASIC]: | Bintec Access Networks GmbH IP Settings (Head Office) vpn25 |
|--|--|
| IP Transit Network | no |
| Local IP Address | 192.168.1.1 |
| Default Route | no |
| Remote IP Address Remote Netmask | 192.168.0.0 255.255.255.0 |
| SAVE | CANCEL |
| Use <space> to select</space> | |

The following fields are relevant:

| Field | Meaning |
|--------------------|---|
| IP Transit Network | Is a transit network to be used? |
| Local IP Address | Local IP address of virtual interface. |
| Default Route | Is the virtual interface to be used as default gateway? |
| Remote IP Address | IP address or network to be reached over the tunnel. |
| Remote Netmask | Netmask of host or network. |

Table 4-2: Relevant fields in IPSEC → CONFIGURE PEERS → RELEVANT PEER → INTERFACE IP SETTINGS → BASIC IP SETTINGS

Proceed as follows to define the necessary settings:

- Set **IP TRANSIT NETWORK** to no.
- Enter your local IP address under *Local IP Address*, e.g. 192.168.1.1.
- Set **DEFAULT ROUTE** to no.
- Enter the network address of the remote terminal under **REMOTE IP ADDRESS**, e.g. 192.168.0.0.

- Enter the netmask of the remote terminal under **REMOTE NETMASK**, e.g. 255.255.255.0.
- Press SAVE to confirm your settings.

■ Go to **IP** → **ROUTING**.

| VPN Access 25 Set [IP][ROUTING]: IP | up Tool Routing | E | Bintec A | ccess | Networks G vp | mbH n25 |
|---|---------------------------------|---|-------------------|----------------|---|--------------------------|
| The flags are: U (Up), D (Dormant), B (Blocked), G (Gateway Route), I (Interface Route), S (Subnet Route), H (Host Route), E (Extended Route) | | | | | | |
| Destination Gat. 192.168.1.0 192 192.168.0.0 192 default | .eway 2.168.1.1 2.168.1.1 | Mask 255.255.255.0 255.255.255.0 0.0.0.0 | Flags DG DI | Met. 0 1 | Interface en0-1 Branch Of Internet | Pro loc loc loc |
| ADD | ADDE | IXT | DELETE | 1 | EX | IT |
| Press <ctrl-n>, <c to edit</c </ctrl-n> | Ctrl-p> to s | croll, <space></space> | tag/unta | ag DEL | ETE, <retur< td=""><td>:n></td></retur<> | :n> |

You can see that an additional entry has been created in the routing table. This enables the network 192.168.0.0 to reach the branch office over the IPSec interface.

You have now configured a virtual IPSec interface, over which a remote network can be reached.

4.3 Configuration of ISDN Callback Mechanism

■ Go to IPSEC → Configure Peers → IPSec Callback.

| VPN Access 25 Setup Tool Binte [IPSEC][PEERS][EDIT][CALLBACK]: ISDN Callback Pe (Head Office) | c Access Networks GmbH er vpn25 |
|---|------------------------------------|
| ISDN Callback: both | |
| Incoming ISDN Number:101 Outgoing ISDN Number:101 | |
| Transfer own IP Address over ISDN: yes | |
| Mode : autodetect best possible mode | (D or B channel) |
| | |
| SAVE | CANCEL |
| Use <space> to select</space> | |

The following fields are relevant:

| Field | Meaning |
|--------------------------------------|---|
| ISDN Callback | Activates or deactivates ISDN callback. |
| Incoming ISDN Number | Number that arrives when the peer initiates the callback. |
| Outgoing ISDN Number | Number that is dialed when an ISDN callback is initiated. |
| Transfer own IP Address over ISDN | Determines whether the IP address is trans- ferred over ISDN or not. |
| Mode | Determines how the IP address is transferred over ISDN. |

Table 4-3: Relevant fields in IPSEC -> CONFIGURE PEERS -> IPSEC CALLBACK

Proceed as follows to define the necessary settings:

- Set **ISDN CALLBACK** to both.
- Enter the number coming from the remote terminal under INCOMING ISDN NUMBER, e.g. 101.
- Enter the number on which the remote terminal can be reached under OUTGOING ISDN NUMBER, e.g. 101.

- Set Transfer own IP Address over ISDN to yes.
- Set MODE to autodetect best possible mode (D or B channel).
- Press SAVE to confirm your settings.



If you wish to transfer the IP address only in the D-channel, you must ensure that LLC (Low Layer Compatibility) and/or SUBADDR (SubAddress) are transferred over the ISDN network. If this is not the case, you must switch to transmission in the B-channel. You should therefore set the **Mode** to autodetect best possible mode (D or B channel), as a B-channel is set up as an alternative if D-channel transmission fails.

You have now activated the ISDN callback mechanism, so that both ends can transfer their IP addresses to set up an IPSec tunnel.

4.4 Configuration of Parameters for IPSec Phase 1

Go to IPSEC → IKE (PHASE 1) DEFAULTS → EDIT.

Select the desired configuration, e.g. *autogenerated*.

| VPN Access 25 Setup Tool [IPSEC][PHASE1][EDIT] | Bintec Access Networks GmbH vpn25 |
|--|--|
| Description (Idx 1) : Proposal : Lifetime : Group : Authentication Method : Mode : Heartbeats : Block Time : Local ID : Local ID : Local Certificate : CA Certificates : Nat Traversal : View Proposals > Edit Lifetimes > | <pre>*autogenerated* 1 (Blowfish/MD5) use default 2 (1024-bit MODP) Pre Shared Keys id_protect none 0 Head Office none enabled</pre> |
| SAVE | CANCEL |
| Enter string, max. length | = 255 chars |

The following field is relevant:

| Field | Meaning |
|-------|------------------------------------|
| Mode | Mode of IPSec Phase 1 negotiation. |

Table 4-4: Relevant field in IPSEC -> IKE (PHASE 1) DEFAULTS -> EDIT

Proceed as follows to define the necessary settings:

- Set **Mode** to *id_protect*.
- Configure the other parameters according to your requirements.
- Press **SAVE** to confirm your settings.

| \sim | |
|--------|--|
| Note | |

As the IP addresses are exchanged by the ISDN callback mechanism, *id_protect* can be entered here as mode. This achieves higher security in the authentication of the IPSec connection.

Return to the main menu and finally save your new configuration in the flash memory with *EXIT* and *Save as BOOT CONFIGURATION AND EXIT*.

5 Result

5.1 Test of Connection and ISDN Callback

The connection is set up by the head office with a ping. You can follow the setup of the connection and the ISDN callback by entering the command debug all in the command line.

00:02:28 INFO/INET: dialup if 100001 prot 1 192.168.1.2:2048->192.168.0.2:3420 00:02:28 INFO/INET: dialup if 10001 prot 17 0.0.0.0:500->0.0.0.0:500 00:02:28 DEBUG/PPP: Internet: dial number <00101901929> 00:02:31 DEBUG/PPP: Layer 1 protocol hdlc, 64000 bit/sec 00:02:31 DEBUG/PPP: Internet: set ifSpeed, number of active connections: 0/0/0 00:02:31 DEBUG/PPP: Internet: set ifSpeed, number of active connections: 1/1/1 00:02:31 DEBUG/PPP: Internet: outgoing connection established 00:02:31 INFO/PPP: Internet: local IP address is 213.7.46.137, remote is 62.104.219.41 00:02:31 DEBUG/INET: NAT: new outgoing session on ifc 10001 prot 17 192.168.1.1:4500/213.7.46.137:32769 -> 213.7.0.117:32769 00:02:31 INFO/IPSEC: IPSEC CB - need callback from Peer "branch office" 00:02:31 INFO/IPSEC: IPSEC CB - trigger callback at Peer "branch office" (do call "*"->"101") 00:02:31 INFO/IPSEC: IPSEC CB - Peer "branch office", trigger call "*" -> "101" is ALERTING 00:02:41 INFO/IPSEC: IPSEC CB - Trigger Call by Peer "branch office" successfully transmitted IP 213.7.46.137 / Token 4203 via B channel 00:02:41 DEBUG/INET: NAT: new incoming session on ifc 10001 prot 17 213.7.46.137:4500/213.7.46.137:4500 <- 213.7.0.117:32770 00:02:41 DEBUG/IPSEC: P1: peer 0 () sa 2 (R): new ip 213.7.46.137 <- ip 213.7.0.117 00:02:41 INFO/IPSEC: P1: peer 0 () sa 2 (R): Vendor ID: 213.7.0.117:32770 (No Id) is 'BINTEC' 00:02:41 INFO/IPSEC: P1: peer 0 () sa 2 (R): Vendor ID: 213.7.0.117:32770 (No Id) is 'BINTEC Heartbeats Version 1' 00:02:41 INFO/IPSEC: P1: peer 0 () sa 2 (R): Vendor ID: 213.7.0.117:32770 (No Id) is 'RFC XXXX' 00:02:41 INFO/IPSEC: P1: peer 0 () sa 2 (R): Vendor ID: 213.7.0.117:32770 (No Id) is 'draft-ietfipsec-nat-t-ike-03' 00:02:41 INFO/IPSEC: P1: peer 0 () sa 2 (R): Vendor ID: 213.7.0.117:32770 (No Id) is 'draft-ietfipsec-nat-t-ike-02 00:02:41 INFO/IPSEC: P1: peer 0 () sa 2 (R): Vendor ID: 213.7.0.117:32770 (No Id) is 'draft-ietfipsec-nat-t-ike-02' 00:02:41 INFO/IPSEC: P1: peer 0 () sa 2 (R): Vendor ID: 213.7.0.117:32770 (No Id) is 'draft-ietfipsec-nat-t-ike-00' 00:02:41 DEBUG/IPSEC: P1: peer 0 () sa 2 (R): token payload: received token 4203 00:02:41 DEBUG/IPSEC: P1: peer 1 (branch office) sa 2 (R): identified ip 213.7.46.137 <- ip 213.7.0.117 00:02:41 INFO/ACCT: ISDN: 01.01.1970,00:02:31,00:02:41,0,50,66,6,6,,0,100,101,7/0,90,0,ipsec callback 00:02:41 DEBUG/ISDN: stack 0: disconnect cause: normal call clearing (0x90) 00:02:42 INFO/IPSEC: New Bundle -2 (Peer 1 Traffic -1) 00:02:42 INFO/IPSEC: P1: peer 1 (branch office) sa 2 (R): done id fqdn(any:0,[0..7]=head office) <- id fqdn(any:0,[0..6]=branch office) IP[b08aff69 52147e68 : 2e024f96 ed2eae37]</pre> 00:02:42 INFO/IPSEC: P2: peer 1 (branch office) traf 0 bundle -2 (I): created 192.168.1.0/192.168.1.0:0 < any > 192.168.0.0/192.168.0.0:0 rekeyed 0 00:02:42 DEBUG/IPSEC: P2: peer 1 (branch office) traf 0 bundle -2 (I): SA 3 established ESP[75fc1b68] in[0] Mode tunnel enc blowfish-cbc(16) auth md5(16) 00:02:42 DEBUG/IPSEC: P2: peer 1 (branch office) traf 0 bundle -2 (I): SA 4 established ESP[4fcbcfdd] out[0] Mode tunnel enc blowfish-cbc(16) auth md5(16) 00:02:42 INFO/IPSEC: Activate Bundle -2 (Peer 1 Traffic -1) 00:02:42 INFO/IPSEC: P2: peer 1 (branch office) traf 0 bundle -2 (I): established (213.7.46.137<->213.7.0.117) with 2 SAs life 28800 Sec/0 Kb rekey 23040 Sec/0 Kb Hb none

Here the IP address has been successfully transferred in the B-channel and the IPSec tunnel has been set up.

| Field | Menu | Description | Compulso ry field |
|--------------------|---|--------------------|----------------------|
| Item | ISDN S0 → Incoming Call Answering → ADD | IPSec | Yes |
| Number | ISDN S0 → Incoming Call Answering → ADD | e.g. <i>100</i> | Yes |
| Mode | ISDN S0 → Incoming Call Answering → ADD | right to left | Yes |
| Bearer | ISDN S0 → Incoming Call Answering → ADD | any | Yes |
| Description | IPSEC → Configure Peers → APPEND | e.g. branch office | Yes |
| Peer IDs | IPSEC → Configure Peers → APPEND | e.g. branch office | Yes |
| Pre Shared Key | IPSEC → Configure Peers → APPEND | e.g. <i>Test</i> | Yes |
| Virtual Interface | IPSEC → Configure Peers → APPEND | e.g. yes | Yes |
| IP Transit Network | IPSEC → Configure Peers → Relevant Peer → Interface IP Settings → Basic IP Settings | no | Yes |
| Local IP Address | IPSEC → Configure Peers → Relevant Peer → Interface IP Settings → Basic IP Settings | e.g. 192.168.1.1 | Yes |
| Default Route | IPSEC → Configure Peers → Relevant Peer → Interface IP Settings → Basic IP Settings | no | Yes |
| Remote IP Address | IPSEC → Configure Peers → Relevant Peer → Interface IP Settings → Basic IP Settings | e.g. 192.168.0.0 | Yes |
| Remote Netmask | IPSEC → Configure Peers → Relevant Peer → Interface IP Settings → Basic IP Settings | e.g. 255.255.255.0 | Yes |

5.2 Overview of Configuration Steps

| Field | Menu | Description | Compulso ry field |
|--------------------------------------|---|--|----------------------|
| ISDN Callback | $IPSEC \rightarrow Configure Peers \rightarrow IPSec$ $Callback$ | both | Yes |
| Incoming ISDN Number | $IPSEC \rightarrow Configure Peers \rightarrow IPSec$ $CallBack$ | e.g. 101 | Yes |
| Outgoing ISDN Number | $IPSEC \rightarrow Configure Peers \rightarrow IPSec$ $CallBack$ | e.g. 101 | Yes |
| Transfer own IP Address over ISDN | $IPSEC \rightarrow Configure Peers \rightarrow IPSec$ $CallBack$ | yes | Yes |
| Mode | $IPSEC \rightarrow Configure Peers \rightarrow IPSec$ Callback | autodetect best possible mode (D or B channel) | Yes |
| Authentication Method | $\begin{array}{l} \text{IPSEC} \rightarrow \text{IKE (Phase 1) Defaults} \rightarrow \\ \text{EDIT} \rightarrow \text{AUTOGENERATED} \end{array}$ | ip_protect | Yes |