funkwerk)))

enterprise communications

bintec Workshop

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

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

1   Introduction

The configuration of IPSec callback with IP address transfer in the B/D-channel 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 IPSec 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.

Head Office

VPN Access 25
ETH1 192.168.1.0
S0 dynamic IP address

ISDN

Branch

VPN Access 25
ETH1 192.168.0.0
S0 dynamic IP address
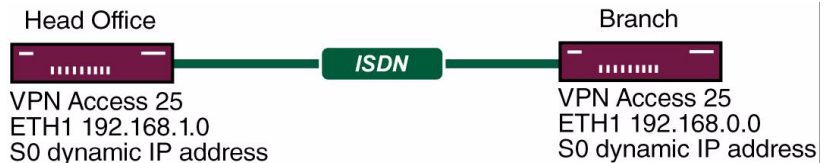
1.2   Requirements

■   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.

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][EDIT]                         vpn25


          Item                    IPSec
          Number                  100
          Mode                    right to left

          Bearer                  any



           SAVE                              CANCEL

Use <Space> to select
```

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 Connection

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                        vpn25


     Description:      Branch office
     Admin Status:     up        Oper Status:   dormant

     Peer Address:
     Peer IDs:         Branch office
     Pre Shared Key:   *

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: yes
     Interface IP Settings >



              SAVE                           CANCEL

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.

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.

Note

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              Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][IP][BASIC]: IP Settings (Head Office)     vpn25

  IP Transit Network                 no


  Local IP Address                   192.168.1.1


  Default Route                      no

  Remote IP Address                  192.168.0.0
  Remote Netmask                     255.255.255.0


         SAVE                             CANCEL

Use <Space> to select
```

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 Setup Tool              Bintec Access Networks GmbH
[IP][ROUTING]: IP Routing                                   vpn25

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   Gateway       Mask           Flags Met.   Interface Pro
192.168.1.0   192.168.1.1   255.255.255.0          0    en0-1     loc
192.168.0.0   192.168.1.1   255.255.255.0   DG     0    Branch Of loc
default                     0.0.0.0         DI     1    Internet  loc




     ADD                ADDEXT              DELETE            EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return>
to edit
```

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                  Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][CALLBACK]: ISDN Callback Peer            vpn25
                              (Head Office)

     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
```

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 transferred 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.

Note

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 trans-ferred over the ISDN network. If this is not the case, you must switch to trans-mission 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                 Bintec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                                          vpn25

   Description (Idx 1)   : *autogenerated*
   Proposal             : 1 (Blowfish/MD5)
   Lifetime             : use default
   Group                : 2 (1024-bit MODP)
   Authentication Method : Pre Shared Keys
   Mode                 : id_protect
   Heartbeats           : none
   Block Time           : 0
   Local ID             : Head Office
   Local Certificate    : none
   CA Certificates      :
   Nat Traversal        : enabled

   View Proposals >
   Edit Lifetimes >

            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.

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 set-up 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-ietf-
ipsec-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-ietf-
ipsec-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-ietf-
ipsec-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-ietf-
ipsec-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,,O,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]
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.

5.2 Overview of Configuration Steps

Field	Menu	Description	Compulsory field
Item	**ISDN S0 ➜ INCOMING CALL ANSWERING ➜ ADD**	*IPSec*	Yes
Number	**ISDN S0 ➜ INCOMING CALL ANSWERING ➜ ADD**	e.g. *100*	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. *Test*	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

Field	Menu	Description	Compulsory field
ISDN Callback	*IPSEC* ➜ *CONFIGURE PEERS* ➜ *IPSEC CALLBACK*	*both*	Yes
Incoming ISDN Number	*IPSEC* ➜ *CONFIGURE PEERS* ➜ *IPSEC CALLBACK*	e.g. *101*	Yes
Outgoing ISDN Number	*IPSEC* ➜ *CONFIGURE PEERS* ➜ *IPSEC CALLBACK*	e.g. *101*	Yes
Transfer own IP Address over ISDN	*IPSEC* ➜ *CONFIGURE PEERS* ➜ *IPSEC CALLBACK*	*yes*	Yes
Mode	*IPSEC* ➜ *CONFIGURE PEERS* ➜ *IPSEC CALLBACK*	*autodetect best possible mode (D or B channel)*	Yes
Authentication Method	*IPSEC* ➜ *IKE (PHASE 1) DEFAULTS* ➜ *EDIT* ➜ *AUTOGENERATED*	*ip_protect*	Yes