funkwerk
enterprise communications

bintec Workshop

IPSec VPN mit Callback (IP-Adresse im B-/D-Kanal)

Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.funkwerk-ec.com.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für bintec-Gateways finden Sie unter www.funkwerk-ec.com.

Als Multiprotokollgateways bauen bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

bintec und das bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

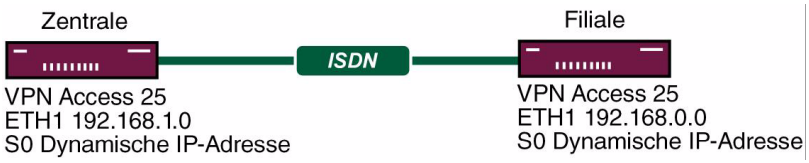
1 Einleitung

Im Folgenden wird die Konfiguration des IPSec Callback mit Übermittlung der IP-Adresse im B/D-Kanal anhand von zwei Bintec VPN Access 25 Gateways (Software Version 7.1.6 Patch 3) beschrieben.

Diese Funktion steht erst seit Firmware Version 7.1.4 zur Verfügung. Dadurch können dynamisch zugewiesene IP-Adressen im B-/D-Kanal übertragen werden.

1.1 Szenario

Eine Filiale eines Unternehmens soll über einen IPSec-Tunnel mit der Zentrale verbunden werden. Für die Internetverbindung steht sowohl in der Filiale als auch in der Zentrale ein ISDN-Anschluss zur Verfügung. Beide Geräte erhalten ihre IP-Adresse dynamisch vom ISP.



1.2 Voraussetzungen

- Zwei Bintec **VPN Access 25** Gateways.
- Mindestens Firmware Version 7.1.4.
- Pro Bintec **VPN Access 25** Gateway ein ISDN S0 Anschluss.
- Verbinden Sie Ihr LAN mit dem Interface ETH1 Ihres Gateways.
- ISDN Internetverbindung.

2 Konfiguration des ISDN Interfaces

Sie müssen das "Incoming Call Answering" so konfigurieren, dass bei einem Anruf auf eine bestimmte Nummer diese für den ISDN Callback verwendet wird.

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Item	Dienst, für den diese Nummer verwendet werden soll.
Number	Rufnummer für den Dienst.
Mode	Art der Nummernüberprüfung.
Bearer	Soll auf einen Sprach-, Datenanruf oder beide reagiert werden.

Tabelle 2-1: Relevante Felder in ***ISDN S0*** ➜ ***INCOMING CALL ANSWERING*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***ITEM*** *IPSec*.
- Tragen Sie unter ***NUMBER*** die gewünschte Rufnummer ein, z.B. *100*.
- Wählen Sie unter ***MODE*** *right to left*

Hinweis

Sollte sich Ihr Gateway an einem Point-to-Point ISDN Anschluss befinden, ist es eventuell erforderlich *left to right* zu wählen!

- Wählen Sie unter ***BEARER*** *any*.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Sie haben nun konfiguriert, dass das Gateway Anrufe über die Nummer 100 für IPSec verwendet.

3 Konfiguration der Internetverbindung (WAN Partner)

Verwenden Sie dazu das Bintec Handbuch oder die Bintec FAQs.

4 Konfiguration der IPSec Verbindung

Dieses FAQ beschreibt die für die Einrichtung des ISDN Callback relevanten Konfigurationsschritte. Genauere Erläuterungen zum Einrichten einer IPSec Verbindung finden Sie im Bintec Benutzerhandbuch oder den entsprechenden FAQs.

4.1 Konfiguration des IPSec Peers

- Gehen Sie zu ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT]: Configure Peer                              vpn25


     Description:       Filiale
     Admin Status:      up          Oper Status:   dormant

     Peer Address:
     Peer IDs:          Filiale
     Pre Shared Key:    *

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: yes
     Interface IP Settings >



               SAVE                              CANCEL

Enter string, max length = 255 chars
```

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Frei wählbare Beschreibung des Peers.
Peer Address	IP-Adresse der Gegenstelle.
Peer IDs	Identität (Name) der Gegenstelle.

Feld	Bedeutung
Pre Shared Key	Geheimer Schlüssel für die IPSec Aushandlung.
Virtual Interface	Virtuelle Interfaces können verwendet werden.

Tabelle 4-1: Relevante Felder in ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***PEER ADDRESS*** einen Namen ein, z.B. *Filiale.*
- Tragen Sie einen ***PRE SHARED KEY*** ein, z.B. *test*.
- Wählen Sie unter ***VIRTUAL INTERFACE*** z.B. *yes*.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Hinweis

Der ***PRE SHARED KEY*** sollte im Wirkbetrieb mindestens 25 bis 30 Zeichen lang sein und keine bekannten Wörter oder Zahlenkombinationen enthalten. Es sollten am besten Groß- und Kleinschreibung, Zahlen und Sonderzeichen in zufälligem Wechsel eingesetzt werden.

Sie haben nun die Grundeinrichtung eines IPSec Peers abgeschlossen.

4.2 Konfiguration des virtuellen Interfaces

- Gehen Sie zu ***IPSEC ➜ CONFIGURE PEERS ➜ ENTSPRECHENDER PEER ➜ INTERFACE IP-SETTINGS ➜ BASIC IP-SETTINGS***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][IP][BASIC]: IP-Settings (Zentrale)          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
```

Folgende Felder sind relevant:

Feld	Bedeutung
IP Transit Network	Soll ein Transitnetzwerk verwendet werden?
Local IP Address	Lokale IP-Adresse des virtuellen Interfaces.
Default Route	Soll das virtuelle Interface als Default Gateway verwendet werden?
Remote IP Address	IP-Adresse oder Netzwerk, das über den Tunnel erreicht werden soll.
Remote Netmask	Netzmaske des Hosts oder des Netzwerks.

Tabelle 4-2: Relevante Felder in ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***ENTSPRECHENDER PEER*** ➜ ***INTERFACE IP-SETTINGS*** ➜ ***BASIC IP-SETTINGS***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***IP TRANSIT NETWORK*** *no*.
- Tragen Sie unter ***LOCAL IP ADDRESS*** Ihr lokale IP-Adresse ein, z.B. *192.168.1.1*.
- Wählen Sie unter ***DEFAULT ROUTE*** *no*.

- Tragen Sie unter ***REMOTE IP ADDRESS*** die Netzadresse der Gegenstelle ein, z.B. *192.168.0.0*.
- Tragen Sie unter ***REMOTE NETMASK*** die Netzmaske der Gegenstelle ein, z.B. *255.255.255.0*.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

- Gehen Sie zu ***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    Filiale   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
```

Sie sehen, dass in der Routingtabelle ein zusätzlicher Eintrag erstellt worden ist. Durch diesen kann das Netzwerk 192.168.0.0 über das IPSec Interface die Filiale erreichen.

Sie haben nun ein virtuelles IPSec Interface konfiguriert, über das ein entferntes Netzwerk erreicht werden kann.

4.3 Konfiguration des ISDN Callback Mechanismus

- Gehen Sie zu ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***IPSEC CALLBACK***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[IPSEC][PEERS][EDIT][CALLBACK]: ISDN Callback Peer (Zentrale)    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
```

Folgende Felder sind relevant:

Feld	Bedeutung
ISDN Callback	Aktiviert bzw. deaktiviert den ISDN Callback.
Incoming ISDN Number	Rufnummer, die ankommt, wenn der Peer den Callback anstösst.
Outgoing ISDN Number	Rufnummer, die gewählt wird, wenn ein ISDN Callback initiiert wird.
Transfer own IP Address over ISDN	Bestimmt, ob die IP-Adresse über ISDN übertragen wird oder nicht.
Mode	Bestimmt, wie die IP-Adresse über ISDN übertragen wird.

Tabelle 4-3: Relevante Felder in ***IPSEC → CONFIGURE PEERS → IPSEC CALLBACK***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***ISDN CALLBACK*** *both*.
- Tragen Sie unter ***INCOMING ISDN NUMBER*** die von der Gegenstelle kommende Rufnummer ein, z.B. *101*.
- Tragen Sie unter ***OUTGOING ISDN NUMBER*** die Rufnummer ein, unter welcher die Gegenstelle erreichbar ist, z.B. *101*.

- Wählen Sie unter ***TRANSFER OWN IP ADDRESS OVER ISDN*** *yes*.
- Wählen Sie unter ***MODE*** *autodetect best possible mode* (*D or B channel*).
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Hinweis

Wenn Sie die IP-Adresse ausschließlich im D-Kanal übermitteln wollen, muss sichergestellt werden, dass LLC (Low Layer Compatibility) und/oder SUBADDR (SubAddress) über das ISDN Netz übertragen werden. Sollte dies nicht der Fall sein, müssen Sie auf eine Übertragung im B-Kanal ausweichen. Den Wert ***MODE*** sollten Sie daher auf *autodetect best possible mode (D or B channel)* setzen, da bei fehlgeschlagener D-Kanal Übertragung alternativ ein B-Kanal aufgebaut wird.

Sie haben nun den ISDN Callback Mechanismus aktiviert, so das beide Seiten ihre IP-Adressen übermitteln und so einen IPSec Tunnel aufbauen können.

4.4 Konfiguration der Parameter für IPSec Phase 1

- Gehen Sie zu ***IPSEC*** ➜ ***IKE (PHASE 1) DEFAULTS*** ➜ ***EDIT***.

Wählen Sie die gewünschte Konfiguration, z.B. **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               :  Zentrale
   Local Certificate      :  none
   CA Certificates        :
   Nat-Traversal          :  enabled

   View Proposals >
   Edit Lifetimes >

              SAVE                              CANCEL

Enter string, max length = 255 chars
```

Folgendes Feld ist relevant:

Feld	Bedeutung
Mode	Modus der IPSec Phase 1 Aushandlung.

Tabelle 4-4: Relevantes Feld in ***IPSEC ➜ IKE (PHASE 1) DEFAULTS ➜ EDIT***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie als ***MODE*** *id_protect*.
- Konfigurieren Sie die anderen Parameter je nach Ihren Anforderungen.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Hinweis

Da durch den ISDN Callback Mechanismus die IP-Adressen ausgetauscht werden, kann hier als Modus *id_protect* gewählt werden. Dadurch erreichen Sie eine höhere Sicherheit bei der Authentifizierung der IPSec-Verbindung.

Gehen Sie zurück ins Hauptmenü und sichern Sie zum Abschluss Ihre neue Konfiguration im Flashmemory mit ***EXIT*** und ***SAVE AS BOOT CONFIGURATION AND EXIT***.

5 Ergebnis

5.1 Test der Verbindung und des ISDN Callback

Die Verbindung wird von der Zentrale durch einen Ping aufgebaut. Indem Sie auf der Kommandozeile den Befehl `debug all` eingeben, können Sie den Aufbau der Verbindung und den ISDN Callback mitverfolgen.

```
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 "Filiale"
00:02:31 INFO/IPSEC: IPSEC CB - trigger callback at Peer "Filiale" (do call "*"->"101")
00:02:31 INFO/IPSEC: IPSEC CB - Peer "Filiale", trigger call "*" -> "101" is ALERTING
00:02:41 INFO/IPSEC: IPSEC CB - Trigger Call by Peer "Filiale" 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 (Filiale) 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 (Filiale) sa 2 (R): done id fqdn(any:0,[0..7]=Zentrale) <- id
fqdn(any:0,[0..6]=Filiale) IP[b08aff69 52147e68 : 2e024f96 ed2eae37]
00:02:42 INFO/IPSEC: P2: peer 1 (Filiale) 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 (Filiale) 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 (Filiale) 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 (Filiale) 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
```

Die IP-Adresse wurde hier erfolgreich im B-Kanal übermittelt und der IPSec-Tunnel konnte aufgebaut werden.

5.2 Konfigurationsschritte im Überblick

Feld	Menü	Wert	Pflichtfeld
Item	***ISDN S0*** ➜ ***INCOMING CALL ANSWERING*** ➜ ***ADD***	*IPSec*	Ja
Number	***ISDN S0*** ➜ ***INCOMING CALL ANSWERING*** ➜ ***ADD***	z.B. *100*	Ja
Mode	***ISDN S0*** ➜ ***INCOMING CALL ANSWERING*** ➜ ***ADD***	*right to left*	Ja
Bearer	***ISDN S0*** ➜ ***INCOMING CALL ANSWERING*** ➜ ***ADD***	*any*	Ja
Description	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***	z.B. *Filiale*	Ja
Peer IDs	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***	z.B. *Filiale*	Ja
Pre Shared Key	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***	z.B. *Test*	Ja
Virtual Interface	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***APPEND***	z.B. *yes*	Ja
IP Transit Network	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***ENTSPRECHENDER PEER*** ➜ ***INTERFACE IP SETTINGS*** ➜ ***BASIC IP-SETTINGS***	*no*	Ja
Local IP Address	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***ENTSPRECHENDER PEER*** ➜ ***INTERFACE IP SETTINGS*** ➜ ***BASIC IP-SETTINGS***	z.B. *192.168.1.1*	Ja
Default Route	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***ENTSPRECHENDER PEER*** ➜ ***INTERFACE IP SETTINGS*** ➜ ***BASIC IP-SETTINGS***	*no*	Ja
Remote IP Address	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***ENTSPRECHENDER PEER*** ➜ ***INTERFACE IP SETTINGS*** ➜ ***BASIC IP-SETTINGS***	z.B. *192.168.0.0*	Ja
Remote Netmask	***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ ***ENTSPRECHENDER PEER*** ➜ ***INTERFACE IP SETTINGS*** ➜ ***BASIC IP-SETTINGS***	z.B. *255.255.255.0*	Ja

Feld	Menü	Wert	Pflichtfeld
ISDN Callback	***IPSEC ➜ CONFIGURE PEERS ➜ IPSEC CALLBACK***	*both*	Ja
Incoming ISDN Number	***IPSEC ➜ CONFIGURE PEERS ➜ IPSEC CALLBACK***	z.B. *101*	Ja
Outgoing ISDN Number	***IPSEC ➜ CONFIGURE PEERS ➜ IPSEC CALLBACK***	z.B. *101*	Ja
Transfer own IP Address over ISDN	***IPSEC ➜ CONFIGURE PEERS ➜ IPSEC CALLBACK***	*yes*	Ja
Mode	***IPSEC ➜ CONFIGURE PEERS ➜ IPSEC CALLBACK***	*autodetect best possible mode (D or B channel)*	Ja
Authentication Method	***IPSEC ➜ IKE (PHASE 1) DEFAULTS ➜ EDIT ➜ AUTOGENERATED***	*ip_protect*	Ja