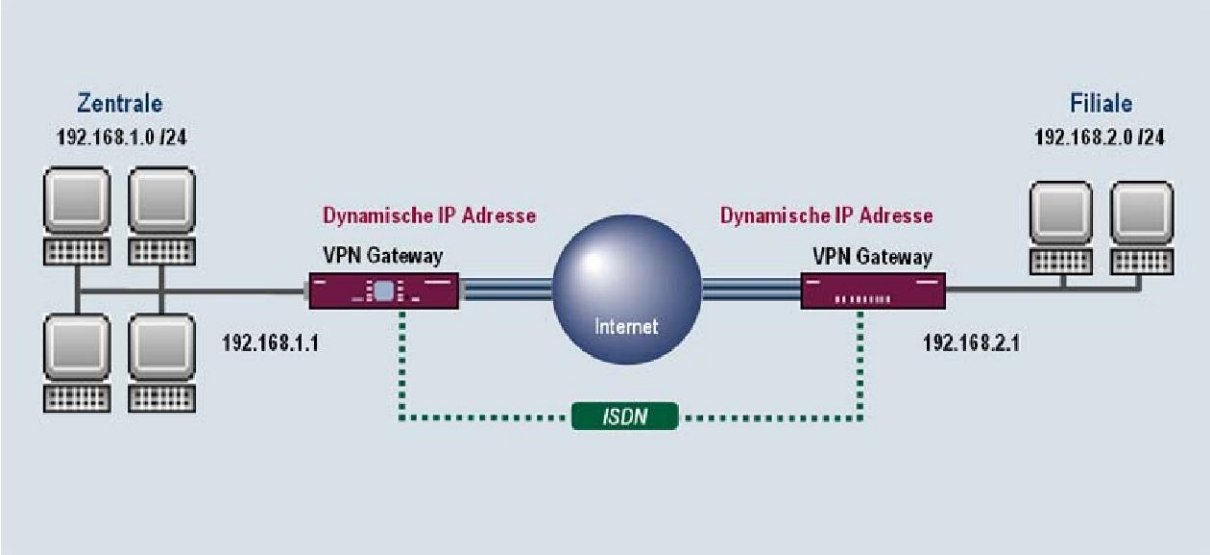
1. IPsec Verbindung mit Übertragung der IP-Adresse im D-/B-Kanal



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung mit dynamischen IP Adressen beschrieben. Die IP-Adresse wird vor dem Verbindungsaufbau über ISDN zum VPN Partner übertragen. Die Anleitung zeigt einmal die Konfigurationsschritte für Traffic Lists und den Unterschied zu Interface basierender Konfiguration. Diese Anleitung zeigt die Konfiguration auf Release 7.1.4

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:
- Grundkonfiguration des Gateways
- Für das IPsec Gateway ist ein Bootimage ab Version 7.1.4 zu verwenden.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider
- Beide Geräte müssen am ISDN angeschlossen sein und eine MSN für IPsec zur Verfügung haben

1.3 Konfiguration

Die Anleitung konfiguriert ein Beispiel auf Seiten der Zentrale.
Sie müssen Einstellungen in folgenden Menüs vornehmen:

Hauptmenü -> IPSEC
Hauptmenü -> ISDN S0

In dem Untermenü "Configure Peers" vom "IPSEC" haben Sie die Möglichkeit mit "APPEND" Verbindungspartner für IPsec hinzuzufügen.

INFO
Bei der Erstkonfiguration von IPsec startet der Wizard. Den sollten Sie ausführen, um Default Parameter für IPsec zu generieren. Die Vorgehensweise beim Anlegen von Verbindungen ist jedoch beim Wizard und beim manuellen Konfigurieren fast identisch.

1.3.1 Einstellungen im Menü IPSEC -> Configure Peers -> APPEND

1.3.1a Configure Peer Parameter

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PEERS][ADD]: Configure Peer                                  zentrale
_____________________________________________________________________________


     Description:       Filiale
     Admin Status:      up        Oper Status:    down

     Peer Address:
     Peer IDs:
     Pre Shared Key:    bintec

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: no
     Traffic List Settings >



                          SAVE                          CANCEL
_____________________________________________________________________________
Enter string, max length = 255 chars
```

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Description	Geben Sie eine Beschreibung für die Verbindung an.
Peer Address	Hier geben Sie die Gateway IP Adresse oder Dyndns Namen des Verbindungspartners ein
Peer IDs	Hier tragen Sie eine Identifikation des Partners ein
Pre Shared Key	Das gemeinsame Passwort von beiden Gateways
Virtual Interface	Bestimmen Sie hier, ob Sie Traffic List oder Interface Routing konfigurieren.
Traffic List Settings	Hier konfigurieren Sie die Traffic List Einträge (Virtual Interface steht auf: no)
Interface IP Settings	Hier konfigurieren Sie die Interface IP Einträge (Virtual Interface steht auf: yes)

Gehen Sie folgendermassen vor, um die Einstellungen im Peer vorzunehmen:

- Benennen Sie den Eintrag **Filiale**
- Das Feld Peer Address bleibt leer
- Bei Peer IDs geben Sie ebenfalls nichts an
- Im Pre Shared Key tragen Sie **bintec** als Passwort ein

Wenn Sie Ihre Verbindung mit Traffic List konfigurieren möchten, dann gehen Sie zu Abschnitt **1.3.1b**
Wenn Sie Ihre Verbindung mit Interface Routing konfigurieren möchten, dann gehen Sie zu Abschnitt **1.3.1c**

1.3.1b Traffic List Settings

- Virtual Interface belassen Sie auf: **no**
- Gehen Sie in das Untermenü "Traffic List Settings -> APPEND" um die Traffic List zu bearbeiten. (Sollten Sie den Wizard benutzen, verlassen Sie das Menü mit **SAVE**, um die Traffic List Einträge zu erstellen)

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PEERS][EDIT][TRAFFIC][EDIT]: Traffic Entry (Filiale)          zentrale
------------------------------------------------------------------------------

     Description:    Filiale

     Protocol:       dont-verify

     Local:
          Type: net    Ip: 192.168.1.0     / 24

     Remote:
          Type: net    Ip: 192.168.2.0     / 24

     Action:         protect

     Profile           *autogenerated*       edit >


                     SAVE                                  CANCEL
------------------------------------------------------------------------------
```

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Description	Geben Sie eine Beschreibung für den Eintrag an
Local IP	Geben Sie hier das lokale Netz mit zugehöriger Subnetmask (in BIT) an
Remote IP	Geben Sie hier das Remote Netz mit zugehöriger Subnetmask (in BIT) an

Gehen Sie folgendermassen vor um, Ihren Eintrag zu konfigurieren:

- Als Beschreibung geben Sie **Filiale** an
- Unter Lokal IP tragen Sie **192.168.1.0** mit der Mask **24** ein
- Unter Remote IP tragen Sie **192.168.2.0** mit der Mask **24** ein
- Speichern Sie mit **SAVE** ab
- Verlassen Sie alle weiteren Menüs mit **Save** oder **Exit**, bis Sie sich im IPsec Main Menü befinden. Konfigurieren Sie weiter ab Punkt **1.3.1d**

1.3.1c Interface IP Settings

- Virtual Interface stellen Sie auf: **yes**
- Gehen Sie in das Untermenü "Interface IP Settings -> Basic IP-Settings" um das Routing zu bearbeiten. (Sollten Sie den Wizard benutzen, verlassen Sie das Menü mit **SAVE**, um die Routing Einträge zu erstellen)

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

  IP Transit Network                    no



  Local IP Address                      192.168.1.1


  Default Route                         no

  Remote IP Address                     192.168.2.0
  Remote Netmask                        255.255.255.0

                   SAVE                                  CANCEL
------------------------------------------------------------------------------
Use <Space> to select
```

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
IP Transit Network	Bestimmen Sie hier, ob Sie ein Transitnetz nutzen möchten
Local IP Address	Geben Sie hier Ihre lokale IP Adresse von Ihrem Ethernet Interface an
Remote IP Address	Hier konfigurieren Sie das zu erreichende Partner Netz
Remote Netmask	Dies ist die Subnetmask, die zum Remotenetz gehört

Gehen Sie folgendermassen vor, um Ihren Eintrag zu konfigurieren:

- IP Transit Network lassen Sie auf: **no**
- Unter Local IP Address tragen Sie **192.168.1.1** ein
- Unter Remote IP Address tragen Sie **192.168.2.0** ein
- Die Remote Netmask stellen Sie auf **255.255.255.0**
- Speichern Sie mit **SAVE** ab. Verlassen Sie alle weiteren Menüs mit **Save** oder **Exit**, bis Sie sich im IPsec Main Menü befinden.

1.3.1d IPsec Anpassungen

In folgendem Untermenü können Sie PHASE 1 Vorlagen verändern oder mit ADD hinzufügen:

IPSEC -> IKE (Phase 1) Defaults -> EDIT

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                                                zentrale
-------------------------------------------------------------------------------

   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            :
   Local Certificate   :  none
   CA Certificates     :
   Nat-Traversal       :  enabled

   View Proposals >
   Edit Lifetimes >

                         SAVE                          CANCEL
-------------------------------------------------------------------------------
Enter string, max length = 255 chars
```

Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Description	Geben Sie dem PHASE 1 Profil einen Namen
Proposal	Mit diesem Algorithmus wird die PHASE 1 verschlüsselt
Mode	Der Mode bestimmt die Methode des IKE Aufbaus
Local ID	Hier tragen Sie die eigene Identifikation für das Gateway ein

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals lassen Sie auf: **1 (Blowfish/MD5)**
- Den Mode lassen Sie auf **id_protect** da die IP-Adressen im ISDN übertragen werden
- Unter Local ID geben Sie nichts ein

In folgendem Untermenü können Sie PHASE 2 Vorlagen verändern oder mit ADD hinzufügen:

IPSEC -> IPsec (Phase 2) Defaults -> EDIT

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PHASE2][EDIT]                                                zentrale
------------------------------------------------------------------------------

   Description (Idx 1) :    *autogenerated*

   Proposal              :  1 (ESP(Blowfish/MD5) no Co
   Lifetime              :  use default
   Use PFS               :  none
   Heartbeats            :  both
   Propagate PMTU        :  no


   View Proposals >
   Edit Lifetimes >




                          SAVE                          CANCEL
------------------------------------------------------------------------------
Enter string, max length = 255 chars
```

Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Description	Geben Sie dem PHASE 2 Profil einen Namen
Proposal	Mit diesem Algorithmus wird die PHASE 2 verschlüsselt
Heartbeats	Baut den Tunnel ab wenn der Partner nicht mehr reagiert

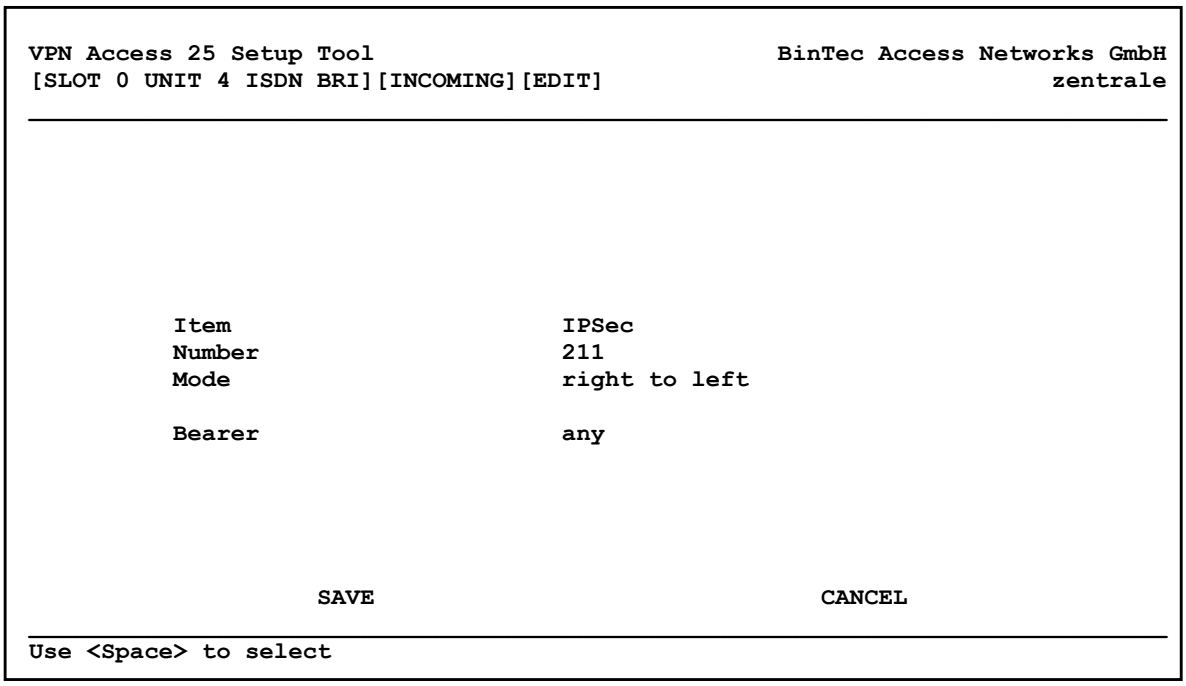
Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals lassen Sie auf: **1 (ESP(Blowfish/MD5) no Co**
- Heartbeats stellen Sie auf **both**
- Verlassen Sie das Menü mit **SAVE**

1.3.2 Anpassungen für IP-Adressen Übertragung im D-/B-Kanal

Sie brauchen für die IP-Adressen Übertragung an jedem ISDN Anschluss eine eigene Rufnummer (MSN) für IPsec. Gehen Sie in folgendes Menü, um den Eintrag für die IPsec Verbindung zu erstellen:

ISDN S0 -> Incoming Call Answering -> ADD



Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Item	Hier können Sie den Dienst bestimmen, der abnimmt
Number	Hier kommt die MSN für IPsec rein.

Gehen Sie folgendermassen vor, um Ihren Eintrag zu konfigurieren:

- Stellen Sie Item auf **IPsec**
- Bei Number kommt die Rufnummer Ihres Anschlusses rein z.B. **211**
- Verlassen Sie das Menü mit **SAVE**

Weitere Einträge müssen Sie im folgenden Menü machen:

IPSEC -> Configure Peers -> EDIT -> IPSec Callback

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PEERS][EDIT][CALLBACK]: ISDN Callback Peer (filiale)          zentrale
------------------------------------------------------------------------------

     ISDN Callback:       both

     Incoming ISDN Number:221
     Outgoing ISDN Number:221

     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 hierbei relevant:

Feld	**Bedeutung**
ISDN Callback	Hier bestimmen Sie die Richtung des Callback
Incoming ISDN Number	Eingehende Rufnummer des Partners (Calling Party Number)
Outgoing ISDN Number	Ausgehende Rufnummer zum Partner (Called Party Number)
Transfer own IP Address over ISDN	Aktivieren Sie hier die IP Adressen Übertragung im ISDN
Mode	Bestimmen Sie hier die Art der Übertragung

Gehen Sie folgendermassen vor, um Ihren Eintrag zu konfigurieren:

- ISDN Callback stellen Sie auf **both**
- Bei Incoming ISDN Number kommt die Rufnummer des Partners rein z.B. **221**
- Bei Outgoing ISDN Number kommt die Rufnummer des Partners rein z.B. **221**
- Transfer own IP Address over ISDN stellen Sie auf **yes**
- Den Mode lassen Sie auf **autodetect best possible mode (D or B channel)**

1.4 Ergebnis

Sie haben eine IPsec Verbindung mit dynamischen IP-Adressen zwischen 2 Gateways konfiguriert. Die IP-Adresse der Zentrale wurde vor dem Verbindungsaufbau über ISDN im LLC Feld zum VPN Partner übertragen. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite konfigurieren.

1.5 Kontrolle

Um die IPsec Verbindung zu testen, gehen Sie wie folgt beschrieben vor:

- Geben Sie an der Shell des Gateways folgendes ein: **ipsecGlobMaxSysLogLevel=debug**
- Danach starten Sie den Debug Modus mit : **debug all&**
- Geben Sie einen Ping von Ihrem Host in der Zentrale zum Host in der Filiale ab

Jetzt sollten Sie folgende Meldungen erhalten:

```
11:08:29 INFO/IPSEC: New Bundle -266 (Peer 1 Traffic 2)
11:08:29 INFO/IPSEC: P2: peer 1 (filiale) traf 2 bundle -266 (I): created 192.16
8.1.0/192.168.1.0:0 < any > 192.168.2.0/192.168.2.0:0 rekeyed 0
11:08:29 INFO/IPSEC: IPSEC CB - need callback from Peer "filiale"
11:08:29 INFO/IPSEC: IPSEC CB - trigger callback at Peer "filiale" (do call "*"-
>"221")
11:08:29 INFO/IPSEC: IPSEC CB - Peer "filiale", trigger call "*" -> "221" is ALE
RTING
11:08:29 DEBUG/INET: NAT: new incoming session on ifc 10001 prot 17 62.10.20.32:
500/62.10.20.32:500 <- 62.10.20.31:1023
11:08:29 DEBUG/IPSEC: P1: peer 0 () sa 1 (R): new ip 62.10.20.32 <- ip 62.10.20.
31
11:08:29 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.10.20.31:1023 (No Id)
 is 'BINTEC'
11:08:29 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.10.20.31:1023 (No Id)
 is 'BINTEC Heartbeats Version 1'
11:08:29 DEBUG/IPSEC: P1: peer 0 () sa 1 (R): token payload: received token 6184
8
11:08:29 DEBUG/IPSEC: P1: peer 1 (filiale) sa 1 (R): identified ip 62.10.20.32 <
- ip 62.10.20.31
11:08:30 DEBUG/IPSEC: P1: peer 1 (filiale) sa 1 (R): notify id No Id <- id ipv4(
any:0,[0..3]=62.10.20.31): Initial contact notification proto 1 spi(16) = [1dc61
690 efd0dbbd : 682a2653 85624ee6]
11:08:30 INFO/IPSEC: P1: peer 1 (filiale) sa 1 (R): done id ipv4(any:0,[0..3]=62
.10.20.32) <- id ipv4(any:0,[0..3]=62.10.20.31) IP[1dc61690 efd0dbbd : 682a2653
85624ee6]
11:08:30 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -266 (I): SA 1 establis
hed ESP[38172e67] in[0] Mode tunnel enc blowfish-cbc(16) auth md5(16)
11:08:30 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -266 (I): SA 2 establis
hed ESP[61ed4c36] out[0] Mode tunnel enc blowfish-cbc(16) auth md5(16)
11:08:30 INFO/IPSEC: Activate Bundle -266 (Peer 1 Traffic 2)
11:08:30 DEBUG/INET: NAT: new outgoing session on ifc 10001 prot 50 62.10.20.32:
0/62.10.20.32:0 -> 62.10.20.31:0
11:08:30 INFO/IPSEC: P2: peer 1 (filiale) traf 2 bundle -266 (I): established  (
62.10.20.32<->62.10.20.31) with 2 SAs life 28800 Sec/0 Kb rekey 23040 Sec/0 Kb H
b both
11:08:30 DEBUG/INET: NAT: new incoming session on ifc 10001 prot 50 62.10.20.32:
0/62.10.20.32:0 <- 62.10.20.31:0
```

In der Tabelle **isdncallhistorytable** können Sie überprüfen wie die IP Adresse übertragen wurde. Hier in diesem Beispiel ist das LLC Feld genutzt worden.

```
zentrale:> isdncallhistorytable
inx StkNumber(*ro)          Type(*ro)              Time(ro)
    Duration(ro)            IsdnIfIndex(ro)        Channel(ro)
    DspItem(ro)             RemoteNumber(ro)       RemoteSubaddress(ro)
    LocalNumber(ro)         LocalSubaddress(ro)    ServiceIndicator(ro)
    AddInfo(ro)             BC(ro)                 LLC(ro)
    HLC(ro)                 Charge(ro)             DSS1Cause(ro)
    1TR6Cause(ro)           LocalCause(ro)         ChargeInfo(ro)
    Screening(ro)           Info(ro)               ReceivedPackets(ro)
    ReceivedOctets(ro)      ReceivedErrors(ro)     TransmitPackets(ro)
    TransmitOctets(ro)      TransmitErrors(ro)     ReceiveDiscards(ro)

 19 0                       outgoing               11/04/04 11:08:29
    0                       400                    2
    60                      "221"
    "211"                                          data_transfer
    0                       88:90                  11:c0:15:10:91:28:03:56:
                            0                      0x90
    0x80                    0
    undefined               "ipsec callback"       0
    0                       0                      0
    0                       0                      0
zentrale:>
```

1.6 Konfigurationsschritte im IPSEC Menü im Überblick

---------- Configure Peer ----------

Feld	Menü	Wert
Description	Configure Peers > APPEND	Filiale
Peer Address	Configure Peers > APPEND	(leer)
Peer IDs	Configure Peers > APPEND	(leer)
Pre Shared Key	Configure Peers > APPEND	bintec

---------- Traffic List ----------

Feld	Menü	Wert
Description	Configure Peers > Traffic List Settings > APPEND	Filiale
Local IP	Configure Peers > Traffic List Settings > APPEND	192.168.1.0 /24
Remote IP	Configure Peers > Traffic List Settings > APPEND	192.168.2.0 /24

---------- IP Routing ----------

Feld	Menü	Wert
IP Transit Network	Configure Peers > Interface IP Settings > Basic IP	no
Local IP Address	Configure Peers > Interface IP Settings > Basic IP	192.168.1.1
Remote IP Address	Configure Peers > Interface IP Settings > Basic IP	192.168.2.0
Remote Netmask	Configure Peers > Interface IP Settings > Basic IP	255.255.255.0

---------- Phase 1 ----------

Feld	Menü	Wert
Proposal	IKE (Phase 1) Defaults > edit > ADD	1 (Blowfish/MD5)
Mode	IKE (Phase 1) Defaults > edit > ADD	id_protect
Local ID	IKE (Phase 1) Defaults > edit > ADD	(leer)

---------- Phase 2 ----------

Feld	Menü	Wert
Proposal	IPsec (Phase 2) Defaults > edit > ADD	1 (ESP(Blowfish/MD5) no Co)

---------- Call Back ----------

Feld	Menü	Wert
ISDN Callback	Configure Peers > IPSec Callback	both
Incoming ISDN Number	Configure Peers > IPSec Callback	z.B. 221
Outgoing ISDN Number	Configure Peers > IPSec Callback	z.B. 221
Transfer own IP Address over ISDN	Configure Peers > IPSec Callback	yes
Mode	Configure Peers > IPSec Callback	autodetect best possible mode

---------- IPsec MSN ----------

Item	ISDN S0 > Incoming Call Answering > ADD	IPSec
Number	ISDN S0 > Incoming Call Answering > ADD	z.B. 211