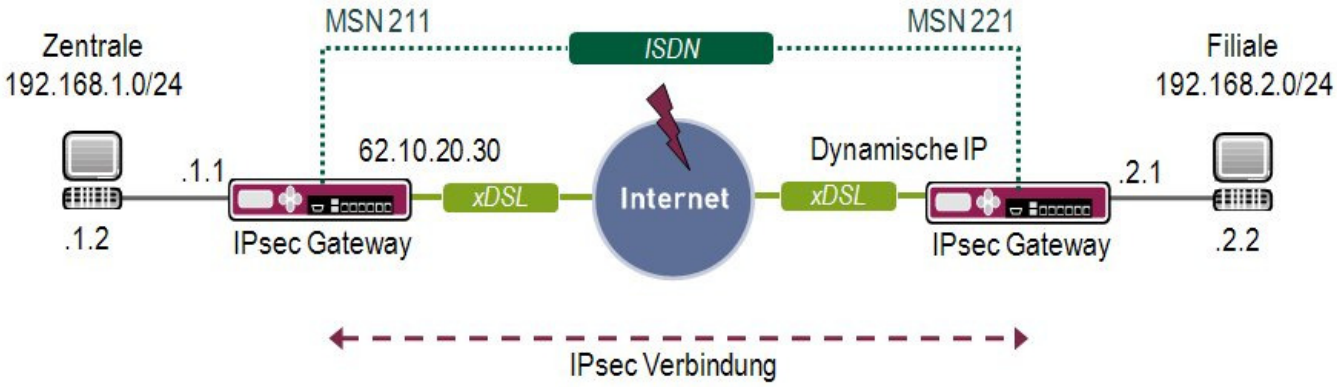
Konfigurationsanleitung
IPsec Verbindung mit ISDN Backup und Callback
Funkwerk / Bintec

Version 1.0

1. IPsec Verbindung mit ISDN Backup und Callback



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung beschrieben. Auf der Seite der Zentrale haben Sie eine statische und in der Filiale eine dynamische IP Adresse. Sollte der Internetzugang ausfallen oder das Routing nicht mehr funktionieren, wird eine Backup Verbindung direkt zum Partner über ISDN aufgebaut. Die Zentrale wird per Keepalive Monitoring überwacht. Aufgrund des Callbacks kann die Verbindung von beiden Seiten aus aufgebaut werden. Der Datenverkehr über die Backup-Verbindung wird nicht mit IPsec verschlüsselt.

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
- Eine Lan-Kopplung zwischen beiden Netzen ist zusätzlich erforderlich

1.3 IPsec Verbindung anlegen

Gehen Sie in folgendes Menü, um eine IPsec Verbindung anzulegen:

IPsec → Configure Peers → APPEND

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.

1.3.1a Configure Peer Parameter

```
R1200 Setup Tool                          Funkwerk Enterprise Communications GmbH
[IPSEC][PEERS][ADD]: Configure Peer                                      zentrale
------------------------------------------------------------------------------


     Description:       Filiale
     Admin Status:      up          Oper Status:   down

     Peer Address:
     Peer IDs:          filiale
     Pre Shared Key:    bintec

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: yes
     Interface IP 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 (In der Filiale unter Local ID eingetragen)

Pre Shared Key	Das gemeinsame Passwort von beiden Gateways
Virtual Interface	Bestimmen Sie hier, ob Sie Traffic List oder Interface Routing konfigurieren
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**
- Bei Peer Address geben Sie nichts an
- Bei Peer IDs geben Sie **filiale** an
- Im Pre Shared Key tragen Sie **bintec** als Passwort ein

INFO
In der Filiale kommt bei Peer Address die statische IP Adresse rein: **62.10.20.30**

1.3.1b 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)

```
R1200 Setup Tool                    Funkwerk Enterprise Communications 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
```

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 vom Ethernet 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**.

1.3.1c IPsec Anpassungen

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

IPSEC → IKE (Phase 1) Defaults → EDIT

```
R1200 Setup Tool                    Funkwerk Enterprise Communications 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                :  aggressiv
   Alive Check         :  Heartbeats (send and expect)
   Block Time          :  20
   Local ID            :  zentrale
   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
Heartbeats	Baut den Tunnel ab, wenn VPN Partner nicht mehr reagiert
Block Time	Setzt den Tunnel auf BK, wenn dieser fehlschlägt
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 stellen Sie auf **aggressiv**
- Alive Check stellen Sie auf **Heartbeats (send and expect)**
- Die Block Time setzen Sie auf **20**
- Unter Local ID geben Sie **zentrale** ein (Ihre Local ID steht beim Partner unter Peer IDs)

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

IPSEC → IPsec (Phase 2) Defaults → EDIT

```
R1200 Setup Tool                    Funkwerk Enterprise Communications GmbH
[IPSEC][PHASE2][EDIT]                                              zentrale
-------------------------------------------------------------------------------

   Description (Idx 1) :     *autogenerated*

   Proposal              :   1 (ESP(Blowfish/MD5) no Co
   Lifetime              :   use default
   Use PFS               :   none
   Alive Check           :   Heartbeats (send and expect)
   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**
- Alive Check stellen Sie auf **Heartbeats (send and expect)**

1.3.2 Anpassungen für Callback

Sie brauchen für den Callback 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

```
R1200 Setup Tool                    Funkwerk Enterprise Communications GmbH
[SLOT 0 UNIT 4 ISDN BRI][INCOMING][EDIT]                          zentrale
------------------------------------------------------------------------------


      Item                          IPSec
      Number                        211
      Mode                          right to left

      Bearer                        any



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

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

```
R1200 Setup Tool                     Funkwerk Enterprise Communications GmbH
[IPSEC][PEERS][EDIT][CALLBACK]: ISDN Callback Peer (filiale)           zentrale
------------------------------------------------------------------------------

     ISDN Callback:       active

     Outgoing ISDN Number:221

     Transfer own IP Address over ISDN:  no




                          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)

Gehen Sie folgendermaßen vor, um Ihren Eintrag in der Zentrale zu konfigurieren:

- ISDN Callback stellen Sie auf **active**
- Bei Outgoing ISDN Number kommt die Rufnummer des Partners rein z.B. **221**

Gehen Sie folgendermaßen vor, um Ihren Eintrag in der Filiale zu konfigurieren:

- ISDN Callback stellen Sie auf **passiv**
- Bei Incoming ISDN Number kommt die Rufnummer des Partners rein z.B. **211**

1.3.3 Backup Verbindung

1.3.3a Routing

Sie müssen eine normale Lan-Kopplung ohne Transit-Netz z.B. über ISDN zum Partner konfiguriert haben, die als Backup genutzt wird. Die Konfiguration unter IP erfolgt genauso wie schon unter **1.3.1b** gezeigt.
Die Backup Verbindung, die hier als WAN Partner mit der Nummer 10002 dargestellt wird, muss in der Zentrale eine schlechtere und in der Filiale eine bessere Metrik haben als die IPsec Verbindung. Daher bearbeiten Sie den Eintrag in der Routingtabelle und setzen den Parameter Metric1 auf den Wert **5**.

Gehen Sie für die Zentrale folgendermaßen vor:

- Rufen Sie die **iproutetable** an der Shell auf
- Bearbeiten Sie Metric1 Ihrer Backup Verbindung z.B. **metric1:01=5**
- Rufen Sie die **iproutetable** noch mal auf und kontrollieren Sie Ihre Eingabe

Jetzt sollte die Routing Tabelle den veränderten Wert anzeigen:

```
inx Dest(*rw)          IfIndex(rw)       Metric1(rw)       Metric2(rw)
    Metric3(rw)        Metric4(rw)       NextHop(rw)       Type(-rw)
    Proto(ro)          Age(rw)           Mask(rw)          Metric5(rw)
    Info(ro)

 00 192.168.1.0        100               0                 -1
    -1                 0                 192.168.1.1       direct
    local              256194            255.255.255.0     536870912
    .0.0

 01 192.168.2.0        10002             5                 -1
    -1                 3                 192.168.1.1       direct
    local              2762              255.255.255.0     536870912
    .0.0

 02 0.0.0.0            300               1                 -1
    -1                 1                 62.10.10.20       indirect
    local              2762              0.0.0.0           -2147483648
    .0.0

 03 192.168.2.0        100001            0                 -1
    -1                 0                 192.168.1.1       direct
    local              22                255.255.255.0     536870912
    .0.0
```

1.3.3b Keepalive Monitoring (Filiale)

Jetzt müssen Sie in der Filiale Keepalive Monitoring konfigurieren. Gehen Sie dazu in dieses Menü:

System → Schedule & Monitor → Keepalive Monitoring (Hosts & Ifc) → ADD

```
R1200 Setup Tool                        Funkwerk Enterprise Communications GmbH
[SYSTEM][KEEPALIVE MONITORING][EDIT]: Host Monitoring                    zentrale
------------------------------------------------------------------------------


          Group                     0
          IPAddress                 62.10.20.30
          Interval                  5
          Source IP
          DownAction                up
          FirstIfIndex              10002
          Range                     0


                     SAVE                                CANCEL
------------------------------------------------------------------------------
Enter integer range 0..255
```

Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
IPAddress	Tragen Sie hier die IP Adresse ein, die Sie überprüfen möchten
Interval	In welchem Intervall soll ein ICMP Paket geschickt werden
DownAction	Die Aktion für die Interface bei nicht Erreichbarkeit
FirstIfIndex	Das erste Interface was administriert wird
Range	Wie viele Interface sind betroffen

Konfigurieren Sie die folgenden Parameter:

- Die IPAddress konfigurieren Sie auf : **62.10.20.30**
- Den Interval stellen Sie auf **5** (nach 20 Sek. führt er die DownAction durch)
- DownAction setzen Sie auf **up**
- FirstIfIndex ist die Indexnummer des Backup WAN-Partners **10002**
- Range stellen Sie auf **0**

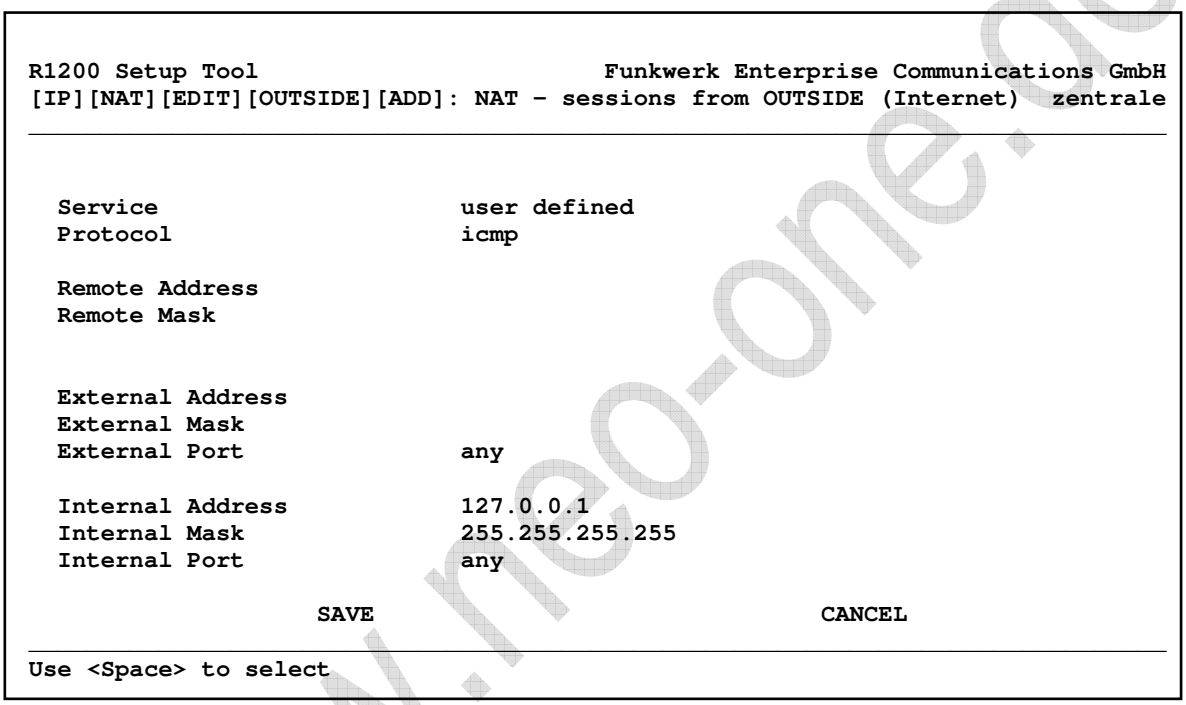
Um das Keepalive zu nutzen, müssen Sie den Backup WAN-Partner erstmals manuell auf den Status DOWN setzen. Dazu geben Sie an der Shell in der Filiale folgendes ein:

ifconfig 10002 down

1.3.3c Network Address Translation (Zentrale)

Weil auf dem Internet Interface NAT eingeschaltet ist, würde der VPN Partner nicht auf eingehende ICMP Requests antworten, die allerdings für Keepalive Monitoring wichtig sind. Konfigurieren Sie daher eine NAT Freigabe für ICMP in dem Internet Interface in der Zentrale unter:

IP → Network Address Translation → Edit → requested from OUTSIDE → ADD



Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Protocol	Das Protokoll, welches freigegeben wird
Internal Address	Die Ziel IP Adresse für die Umleitung

Konfigurieren Sie die folgenden Parameter:

- Das Protocol verändern Sie auf **ICMP**
- Unter Internal Address tragen Sie die loopback Adresse ein **127.0.0.1**