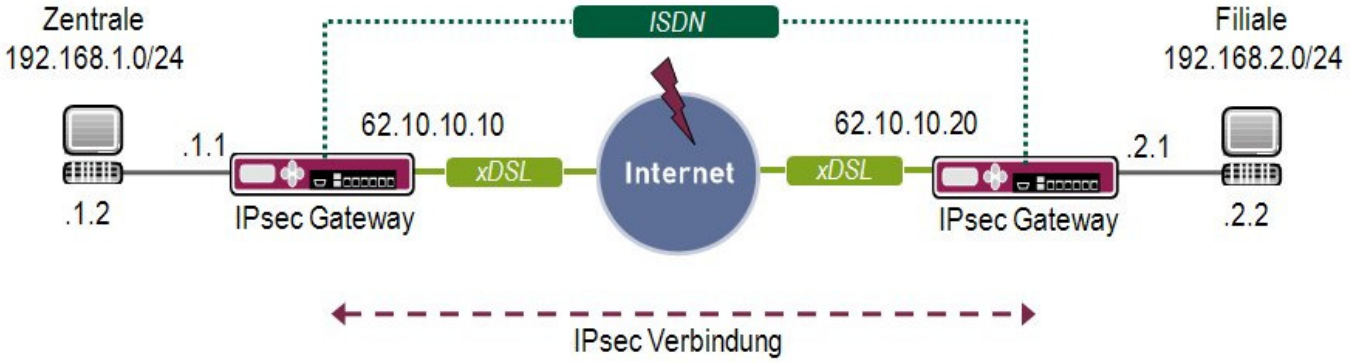
Konfigurationsanleitung
IPsec mit ISDN Backup und statischen IP-Adressen
Funkwerk / Bintec

Version 1.0

1. IPsec Verbindung mit ISDN Backup und statischen IP-Adressen



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung mit statischen IP-Adressen beschrieben. Sollte der Internetzugang ausfallen, wird eine Backup Verbindung direkt zum Partner über ISDN aufgebaut. Dabei spielt es keine Rolle, ob das Routing oder das Interface ausfällt, da der VPN Partner mit Keepalive Monitoring überwacht wird. Der Datenverkehr über die Backup-Verbindung wird 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.
- Einen funktionsfähigen Internetzugang mit statischen Adressen
- Eine Lan-Kopplung zwischen beiden Netzen ist zusätzlich erforderlich

1.3 Konfiguration

Die Anleitung konfiguriert ein Beispiel auf Seiten der Zentrale.
Um IPsec zu konfigurieren, müssen Sie im Folgenden Menü Einstellungen vornehmen:

Hauptmenü -> IPSEC

In dem Untermenü "Configure Peers" 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

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


     Description:       Filiale
     Admin Status:      up        Oper Status:   down

     Peer Address:      62.10.10.20
     Peer IDs:          62.10.10.20
     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
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 **62.10.10.20** an
- Bei Peer IDs geben Sie **62.10.10.20** an
- Im Pre Shared Key tragen Sie **bintec** als Passwort ein

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

------------------------------------------------------------------------------
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.

1.3.1c 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                :  id_protect
   Alive Check         :  Heartbeats (send and expect)
   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
Alive Check	Baut den Tunnel ab, wenn der Partner nicht mehr reagiert
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 **id_protect** da Sie dynamische IP Adressen haben
- Alive Check stellen Sie auf: **Heartbeats (send and expect)**
- 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

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

   Description (Idx 1) :     *autogenerated*

   Proposal              :   1 (ESP(Blowfish/MD5) no Comp)
   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
Alive Check	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 Comp)**
- Alive Check stellen Sie auf: **Heartbeats (send and expect)**

1.3.2 Backup Verbindung

1.3.2a WAN-Partner - IP Settings

Sie müssen eine normale Lan-Kopplung ohne Transit-Netz z.B. über ISDN zum Partner konfiguriert haben, die als Backup genutzt wird. Unter IP im WAN-Partner konfigurieren Sie folgendes:

```
R1200 Setup Tool                    Funkwerk Enterprise Communications GmbH
[WAN][EDIT][IP][BASIC]: IP-Settings (Backup)                        zentrale
------------------------------------------------------------------------------

  IP Transit Network                no


  Local IP Address                  62.10.10.10


  Default Route                     no

  Remote IP Address                 62.10.10.20
  Remote Netmask                    255.255.255.255


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

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
IP Transit Network	Wählen Sie hier aus, ob Sie ein Transit Netz möchten
Local IP Address	Hier tragen Sie Ihre eigene IP Adresse ein
Remote IP Address	Hier tragen Sie die Partner IP Adresse ein
Remote Netmask	Die Subnetmask, die zur Remote IP gehört

Gehen Sie folgendermaßen vor, um Ihren Eintrag zu konfigurieren:

- Das Transit Network stellen Sie auf : **no**
- Unter Local IP Address tragen Sie Ihre statische IP Adresse **62.10.10.10** ein
- Bei Remote IP Address tragen Sie die statische Partner IP Adresse des ein: **62.10.10.20**
- Die Remote Netmask steht auf **255.255.255.255**

1.3.2b Keepalive Monitoring

In der Routingtabelle finden Sie jetzt eine Hostroute die zum VPN Partner über die Backupverbindung zeigt. Konfigurieren Sie eine weitere **Hostroute** im Menü

IP -> Routing -> ADD

über Ihr Internet Interface zum Ziel **62.10.10.20**. Achten Sie darauf, dass die Metrik der Route schlechter ist als die der Backup Verbindung. Jetzt müssen Sie 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                 62.10.10.20
          Interval                  5
          Source IP
          DownAction                up
          FirstIfIndex              10001
          Range                     1

                    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 : **62.10.10.20**
- 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 **10001**
- Range stellen Sie auf **1**

1.3.2c Extended Routing

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

Ifconfig 10001 down

Damit die Keepalive Pakete nicht über die Backup Verbindung geschickt werden, wenn diese aufgebaut ist, müssen Sie noch eine Extended Route konfigurieren. Dort sagen Sie, dass alle ICMP Pakete die zum Partner Gateway geschickt werden, nur über die Internetverbindung gerouted werden sollen. Konfigurieren Sie die Route in folgendem Menü:

IP -> Routing -> ADDEXT

```
R1200 Setup Tool                    Funkwerk Enterprise Communications GmbH
[IP][ROUTING][ADD]: IP Routing - Extended Route                      zentrale

  Route Type                 Host route
  Network                    WAN without transit network

  Destination IP-Address     62.10.10.20

  Partner / Interface        Internet                  Mode  always

  Metric                     1
  Source Interface           dont verify
  Source IP-Address
  Source Mask
  Type of Service (TOS)      00000000                  TOS Mask  00000000
  Protocol                   icmp

                  SAVE                              CANCEL
```

Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Route Type	Bestimmen Sie hier den Typ der Route
Destination IP-Address	Geben Sie hier die IP des VPN Partners an
Protocol	Das Protokoll, welches explizit gerouted werden soll

Konfigurieren Sie die folgenden Parameter:

- Stellen Sie Route Type auf **Host route**
- Die Destination IP-Address konfigurieren Sie auf **62.10.10.20**
- Das Protocol verändern Sie auf **ICMP**

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 unter:

IP -> Network Address Translation -> Edit-> requested from OUTSIDE -> ADD

```
R1200 Setup Tool                    Funkwerk Enterprise Communications GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT - sessions from OUTSIDE (Internet)  zentrale
------------------------------------------------------------------------------


  Service                   user defined
  Protocol                  icmp

  Remote Address
  Remote Mask


  External Address
  External Mask
  External Port             any

  Internal Address          127.0.0.1
  Internal Mask             255.255.255.255
  Internal Port             any

                  SAVE                                CANCEL

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

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**

1.4 Ergebnis

Sie haben eine IPsec Verbindung zwischen 2 Gateways mit statischen IP Adressen konfiguriert und als Backup eine direkte Einwahl zum Partner konfiguriert. Mit Keepalive Monitoring überprüfen Sie die Gegenstelle auf Erreichbarkeit. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite konfigurieren.