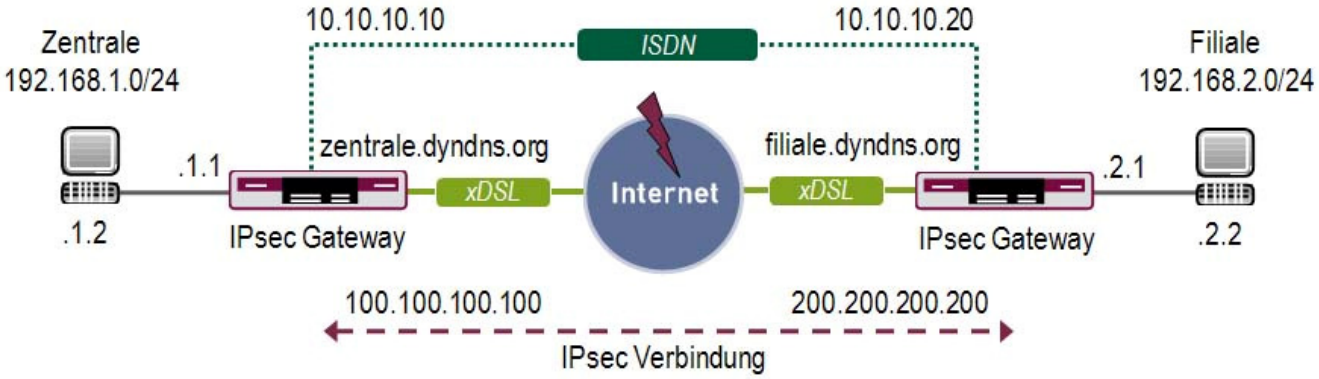
Konfigurationsanleitung
IPsec mit ISDN Backup und dynamischen IP-Adressen
Funkwerk / Bintec

Version 1.0

1. IPsec Verbindung mit ISDN Backup und dynamischen IP Adressen



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung 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 Internet Zugang hat dynamische IP-Adressen und Sie verwenden Dyndns. 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.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang
- Auf beiden Gateways müssen Sie Dyndns konfiguriert haben
- 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:       filiale.dyndns.org
     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 **filiale.dyndns.org** an
- Bei Peer IDs geben Sie **filiale** 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                 :    aggressiv
   Alive Check          :    Heartbeats (send and expect)
   Block Time           :    30
   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
Alive Check	Baut den Tunnel ab, wenn der 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**, da Sie dynamische IP Adressen haben

- Alive Check stellen Sie auf: **Heartbeats (send and expect)**
- Die Block Time setzen Sie auf **30**
- 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
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 Co**
- 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. Über die wird später eine zweite IPsec Verbindung als Backup laufen. 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                  10.10.10.10

  Default Route                     no

  Remote IP Address                 10.10.10.20
  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	Bestimmen Sie hier die Subnetmask

Konfigurieren Sie die Einstellungen mit folgenden Parametern:

- Das Transit Network stellen Sie auf : **no**
- Unter Local IP Address tragen Sie Ihre WAN IP Adresse ein **10.10.10.10**
- Bei Remote IP Address tragen Sie die WAN IP Adresse des Partners ein **10.10.10.20**
- Remote Netmask steht auf **255.255.255.255**

1.3.2b Backup IPsec Peer

Wenn die erste IPsec Verbindung nicht zustande kommt, soll eine Backup IPsec Verbindung über eine Direkteinwahl zum VPN Partner aufgebaut werden. Dafür konfigurieren Sie nochmals die Abschnitte **1.3.1a** und **1.3.1b**. Alle Parameter sind soweit identisch, bis auf folgende Werte unter **1.3.1a**:

- Benennen Sie den Eintrag **Filiale2**
- Bei Peer Address geben Sie **10.10.10.20** an
- Im Pre Shared Key tragen Sie **123456** als Passwort ein

INFO

Optional können Sie auch in dem Peer unter „Peer specific Settings" eigene PHASE 1 Parameter konfigurieren. Die Parameter sind identisch, wie unter Abschnitt **1.3.1c** beschrieben. Optimal wären hier die folgenden veränderten Werte:

- Den Mode stellen Sie auf **id_protect**
- Block Time stellen Sie auf: **0**
- Bei Local ID setzen Sie Ihre eigene WAN IP rein: **10.10.10.10**

Nachdem Sie den zweiten IPsec Peer konfiguriert haben, setzen Sie das Interface auf den Status DOWN. Geben Sie dazu an der Shell folgendes ein:

Ifconfig 100002 down

In der Routing Tabelle haben Sie zwei IPsec Routen, die zum gleichen Partner-Netz zeigen. Verändern Sie die Metrik1 von der ersten IPsec Verbindung auf den Wert **5**.

Gehen Sie folgendermaßen vor:

- Rufen Sie die **iproutetable** an der Shell auf
- Bearbeiten Sie Metric1 Ihrer ersten IPsec Verbindung z.B. **metric1:05=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)

 04 10.10.10.20        10001             0                 -1
    -1                 0                 10.10.10.10       direct
    local              3768              255.255.255.255   0
    .0.0

 05 192.168.2.0        100001            5                 -1
    -1                 5                 192.168.1.1       direct
    local              3768              255.255.255.0     536870912
    .0.0

 06 192.168.2.0        100002            0                 -1
    -1                 0                 192.168.1.1       direct
    local              3768              255.255.255.0     536870912
    .0.0
```

Für Keepalive Monitoring brauchen Sie auf beiden Seiten eine weitere IP Adresse im LAN Interface, die Sie nur über den ersten IPsec Tunnel erreichen dürfen. Gehen Sie dazu in Ihr LAN Interface und Konfigurieren Sie eine weitere IP Adresse **100.100.100.100**

1.3.2c Keepalive Monitoring

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                 200.200.200.200
          Interval                  5
          Source IP                 100.100.100.100
          DownAction                up
          FirstIfIndex              100002
          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
Source IP	Tragen Sie hier die Absender IP ein
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 : **200.200.200.200**
- Den Interval stellen Sie auf **5** (nach 20 Sek. führt er die DownAction durch)
- Die Source IP konfigurieren Sie auf : **100.100.100.100**
- DownAction setzen Sie auf **up**
- FirstIfIndex setzen Sie auf **100002**
- Range stellen Sie auf **0**

1.3.2d IP-Routing

Damit die Keepalive Pakete über die erste IPsec Verbindung geschickt werden, müssen Sie noch eine Route zur zweiten IP Adresse auf dem LAN Interface des Partners hinzufügen. Konfigurieren Sie die Route in folgendem Menü:

IP -> Routing -> ADD

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Route Type	Bestimmen Sie hier den Typ der Route
Network	Geben Sie hier den Netzwerktyp an
Destination IP-Address	Geben Sie hier die zweite IP des VPN Partners an
Partner / Interface	Wählen Sie hier die zweite IPsec Verbindung

Konfigurieren Sie die folgenden Parameter:

- Stellen Sie Route Type auf **Host route**
- Network stellen Sie auf **WAN without transit network**
- Die Destination IP-Address konfigurieren Sie auf **200.200.200.200**
- Das Partner / Interface stellen Sie auf **Filiale**

1.4 Ergebnis

Sie haben eine IPsec Verbindung zwischen 2 Gateways mit dynamischen 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.