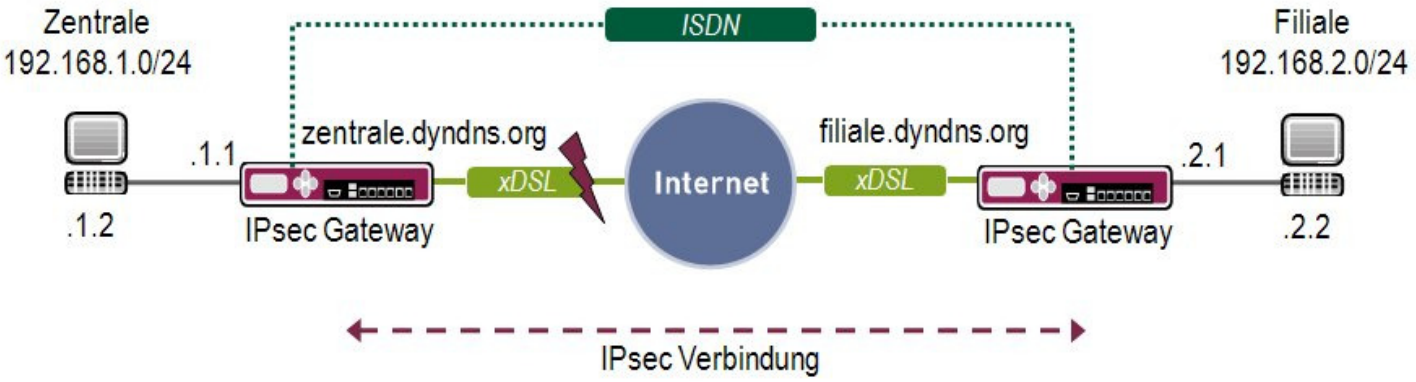
Konfigurationsanleitung
IPsec mit ISDN Backup und dynamischen IP-Adressen
Funkwerk / Bintec

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. Der Internet Zugang hat dynamische IP-Adressen und Sie verwenden Dyndns. Der Datenverkehr über die Backup-Verbindung wird nicht mit IPsec verschlüsselt. Diese

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

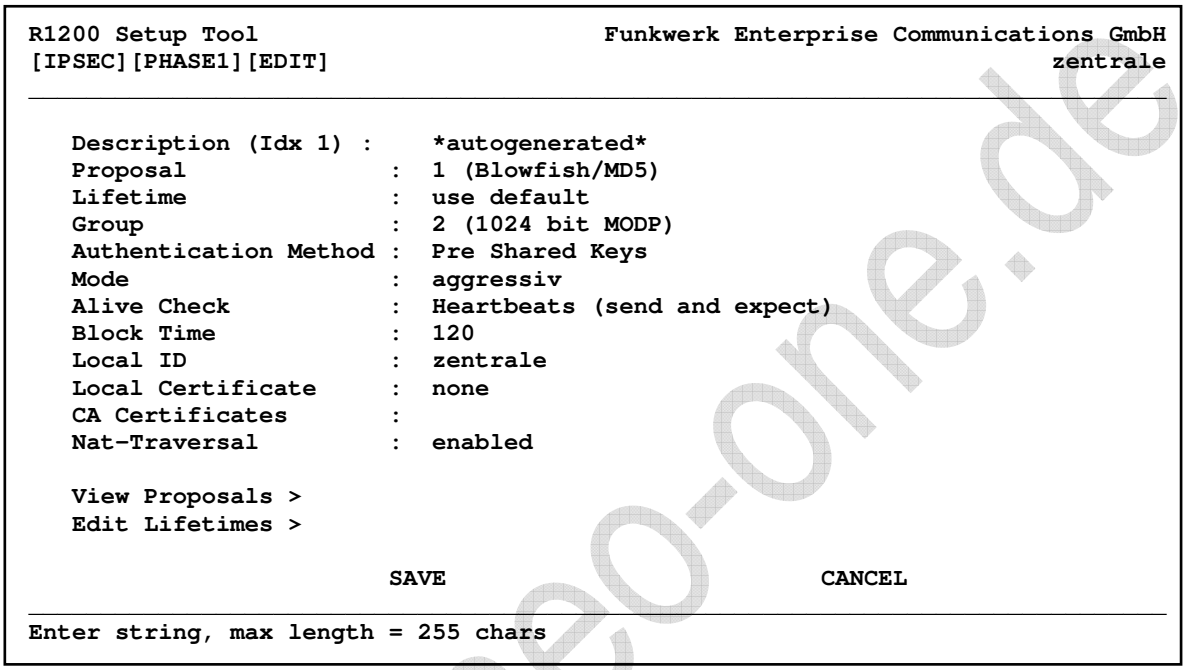
Gehen Sie folgendermaßen vor, um Ihren Eintrag zu konfigurieren:

- 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



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
- Alivecheck stellen Sie auf: **Heartbeats (send and expect)**
- Die Block Time setzen Sie auf **120**
- 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

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 eine schlechtere 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 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
```

INFO

Die Datenpakete, die über die Backupverbindung geschickt werden, sind nicht mit IPsec verschlüsselt, da über diese Verbindung kein Tunnel aufgebaut wird.