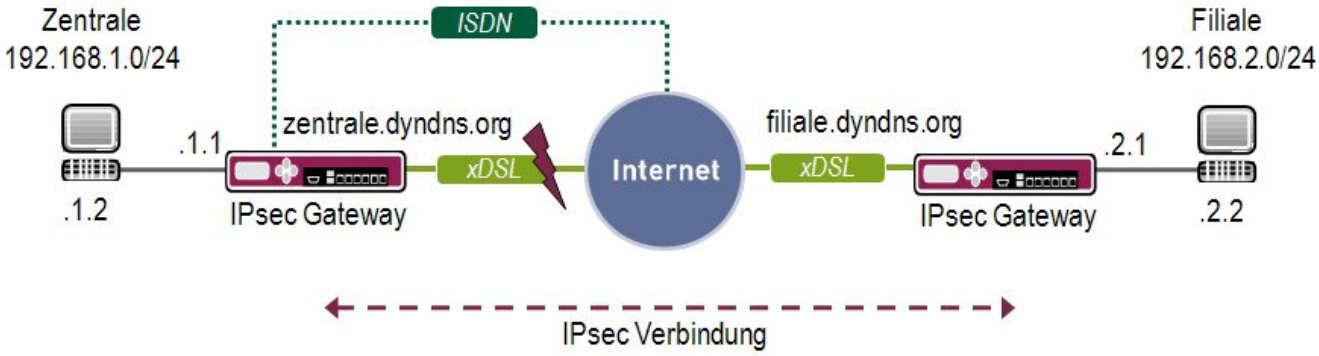
Konfigurationsanleitung
IPSec Verbindung mit Provider Backup
Funkwerk / Bintec

Version 1.0

1. IPsec Verbindung mit Provider 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 zu einem Ersatz Provider aufgebaut. Der Internet Zugang hat dynamische IP-Adressen und Sie verwenden Dyndns.

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 zwei funktionsfähige Internetzugänge auf jeder Seite
- Auf beiden Gateways müssen Sie Dyndns für beide Internet Zugänge konfiguriert haben

1.3 IPsec Verbindung anlegen

Gehen Sie in folgendes Menü, um eine IPsec Verbindung zu erstellen:

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:      filiale.dyndns.org
     Peer IDs:          filiale
     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 (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.
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**
- 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

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)

```
R1200 Setup Tool                          Funkwerk Enterprise Communications 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:

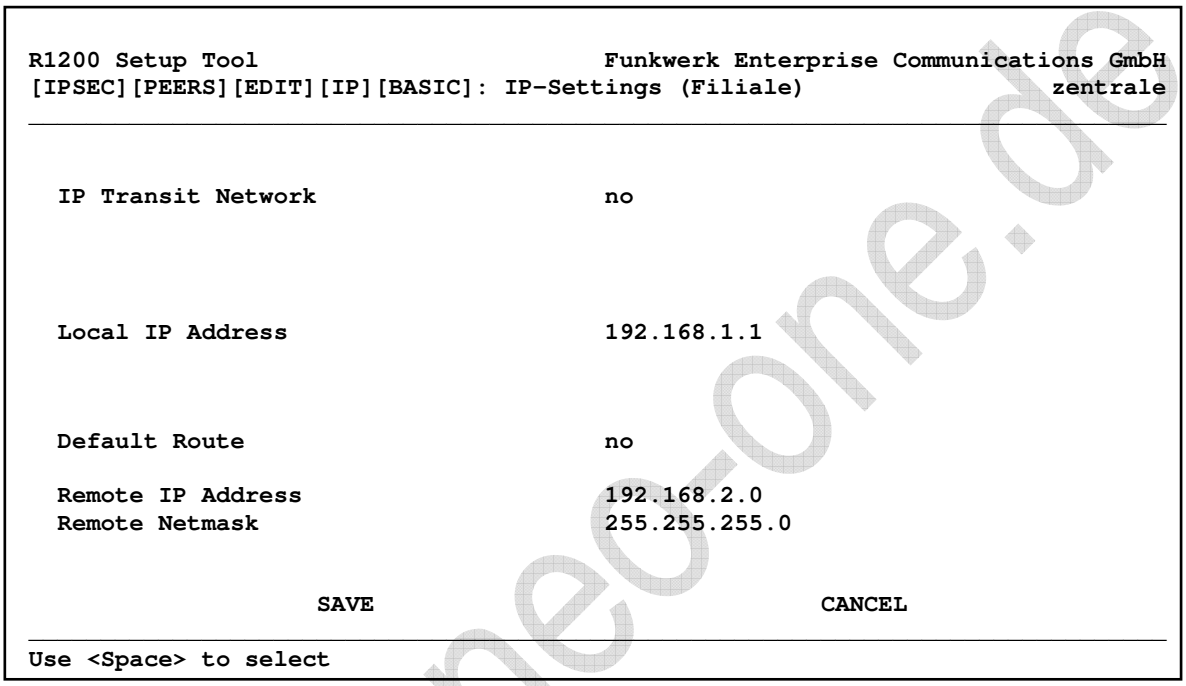
Feld	**Bedeutung**
Description	Geben Sie eine Beschreibung für den Eintrag an
Local IP	Geben Sie hier das lokale Netz mit zugehöriger Subnetmask (in BIT) an
Remote IP	Geben Sie hier das Remote Netz mit zugehöriger Subnetmask (in BIT) an

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**
- 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)



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

```
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          :  0
   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
Local ID	Hier tragen Sie die eigene Identifikation für das Gateway ein
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 (Blowfish/MD5)**
- Den Mode stellen Sie auf **aggressiv** da Sie dynamische IP Adressen haben
- Unter Local ID geben Sie **zentrale** ein (Ihre Local ID steht beim Partner unter Peer IDs)
- Alive Check stellen Sie auf: **Heartbeats (send and expect)**

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

Sie müssen zwei Internet Verbindungen konfiguriert haben. Die Backup Verbindung, die hier als WAN Partner mit der Nummer 10002 dargestellt wird, muss eine schlechtere Metrik haben. 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 die Default Route Ihrer Backup Verbindung z.B. **metric1:02=5**
- Rufen Sie die **iproutetable** nochmal 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 0.0.0.0            10001             1                 -1
    -1                 1                 0.0.0.0           indirect
    local              88873             0.0.0.0           -2147483648
    .0.0

 02 0.0.0.0            10002             5                 -1
    -1                 1                 0.0.0.0           indirect
    local              88873             0.0.0.0           -2147483648
    .0.0
```

Um das Fallback auf die Backup Verbindung zu beschleunigen haben Sie die Möglichkeit, der ersten Verbindung zu sagen, dass Sie nur zweimal versuchen soll die Verbindung aufzubauen. Danach setzt sich das Interface auf den Status Blocked und die Backup Verbindung wählt sich ins Internet.

Gehen Sie folgendermaßen vor, um die Veränderung im Internet Interface zu konfigurieren:

- Rufen Sie die **biboppptable** an der Shell auf
- Verändern Sie die Maxretries von 5 auf 2: **MaxRetries:00=2**
- Rufen Sie die **biboppptable** nochmal auf und kontrollieren Sie Ihre Eingabe

Jetzt sollte die biboppptable den veränderten Wert anzeigen:

```
inx IfIndex(ro)              Type(*rw)              Encapsulation(-rw)
    Keepalive(rw)            Timeout(rw)            Compression(rw)
    Authentication(rw)       AuthIdent(rw)          AuthSecret(rw)
    IpAddress(rw)            RetryTime(rw)          BlockTime(rw)
    MaxRetries(rw)           ShortHold(rw)          InitConn(rw)
    MaxConn(rw)              MinConn(rw)            Callback(rw)
    Layer1Protocol(rw)       LoginString(rw)        VJHeaderComp(rw)
    Layer2Mode(rw)           DynShortHold(rw)       LocalIdent(rw)
    DNSNegotiation(rw)       Encryption(rw)         LQMonitoring(rw)
    IpPoolId(rw)             SessionTimeout(rw)     Layer1DiscDelay(rw)

 00 10001                    isdn_dialup            ppp
    off                      3000                   none
    both                                            "Internet"
    dynamic_client           4                      10
    2                        -1                     1
    1                        1                      disabled
    data_64k                                        disabled
    auto                     0                      "Internet"
    enabled                  none                   off
    0                        0                      enabled
```

INFO

Der Delay after Connection Failure in den Internet WAN Partnern unter Advanced Settings sollte nicht unter 30 Sec stehen

Die Sync-SA-Funktion löscht alle zu einer dynamischen IP-Adresse gehörigen Tunnel, wenn die zugrunde liegende Verbindung ausfällt oder abgebaut wird. Daher schalten Sie diese Funktion im folgenden Menü auf den Wert **yes**.

IPSEC → Advanced Settings

```
R1200 Setup Tool                          Funkwerk Enterprise Communications GmbH
[IPSEC][ADVANCED]: IPsec Configuration - Advanced Settings                zentrale
--------------------------------------------------------------------------------

  Ignore Cert Req Payloads :  no
  Dont send Cert Req Payl. :  no
  Dont Send Cert Chains    :  no
  Dont send CRLs           :  yes

  Dont send Key Hash Payl. :  no
  Trust ICMP Messages      :  no
  Dont Send Initial Contact:  no
  Sync SAs With Local Ifc  :  yes
  Max. Symmetric Key Length:  1024
  Use Zero Cookies         :  no

  RADIUS Authentication    :  disabled



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

1.4 Ergebnis

Sie haben eine IPsec Verbindung zwischen 2 Gateways mit dynamischen IP Adressen konfiguriert und als Backup einen zweiten Internet Provider gewählt. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite konfigurieren.