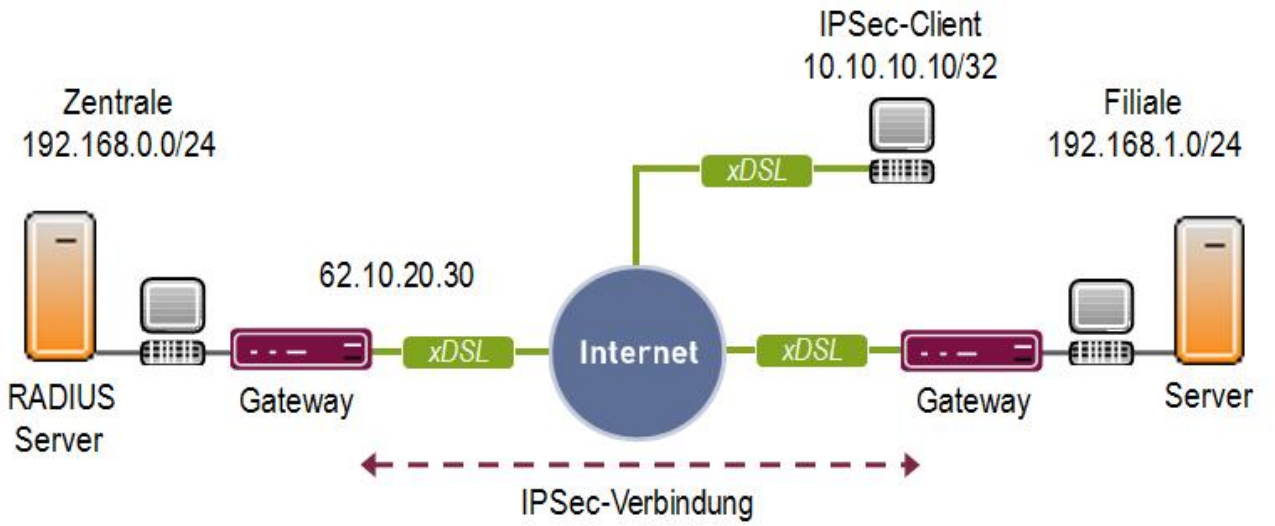
8. IPSec über RADIUS-Server (onDemand / Preload)



8.1 Einleitung

Im Folgenden wird die Konfiguration von IPSec-Verbindungen über einen RADIUS-Server beschrieben. Die Anleitung beschreibt die Konfiguration des RADIUS-Servers im LAN der Zentrale für die Einwahl von IPSec-Clients (onDemand) und Verbindungen zu Außenstellen (Preload). Diese Anleitung zeigt die Konfiguration der Zentrale auf Basis eines RS232bw und den bintec IPSec Client in der Software Version 2.20.

Zur Konfiguration wird das Graphical User Interface (GUI) verwendet.

8.2 Voraussetzungen

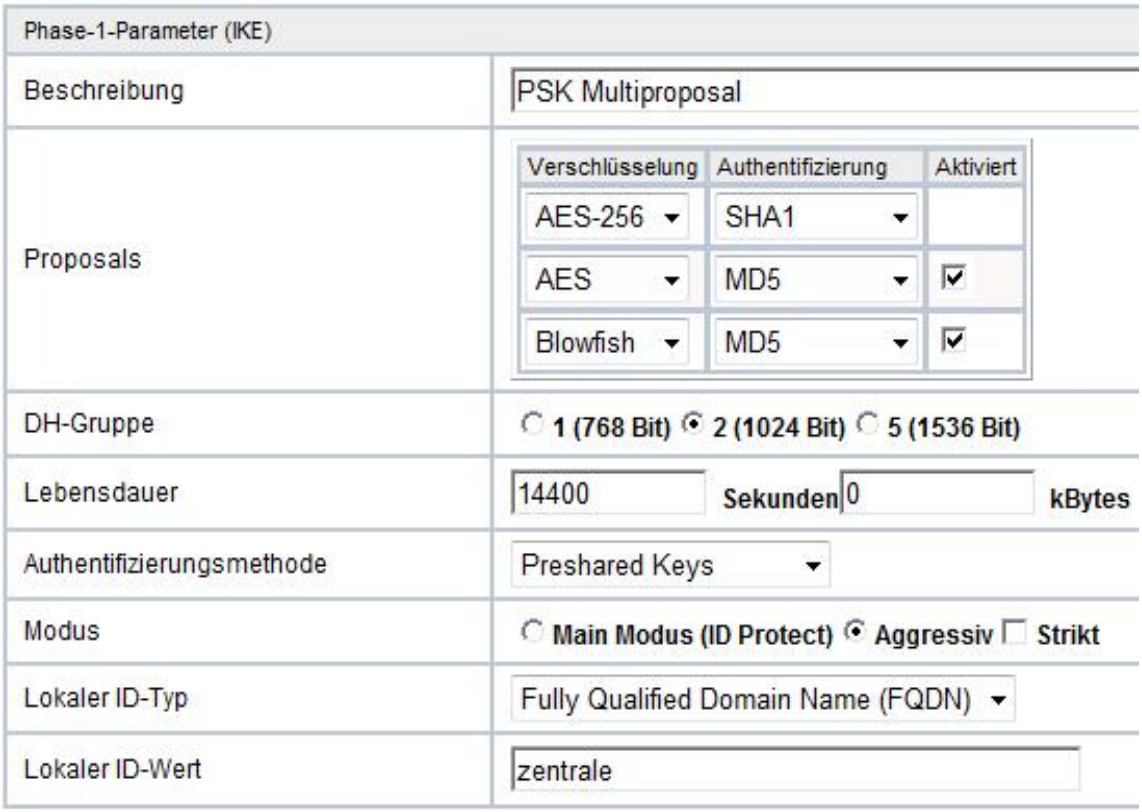
Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Eine Grundkonfiguration des Gateways.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang.
- Installierter bintec IPSec Client Version 2.20.
- Ein RADIUS-Server z.B. FreeRadius 1.1.7.

8.3 Phase-1 konfigurieren

Die Phase-1 gibt an, wie und mit welchen Parametern der Partner und das eigene Gateway die IPSec-Verbindung aufbauen und absichern soll. Um die Phase-1 zu konfigurieren erstellen Sie einen neuen Eintrag:

GUI → VPN → IPSec → Phase-1 Profile → Neu



Folgende Punkte sind hier relevant:

Feld	Bedeutung
Beschreibung	Die Bezeichnung des Phase-1 Profils.
Proposals	Die Phase-1 Verschlüsselungs- / Authentifizierungs-Algorithmen.
Authentifizierungsmethode	Die Art, wie die Identität vom Partner überprüft wird.
Modus	Der Mechanismus für den Tunnelaufbau.
Lokaler ID-Typ	Die Art der eigenen Identität.
Lokaler ID-Wert	Die eigene Identität.

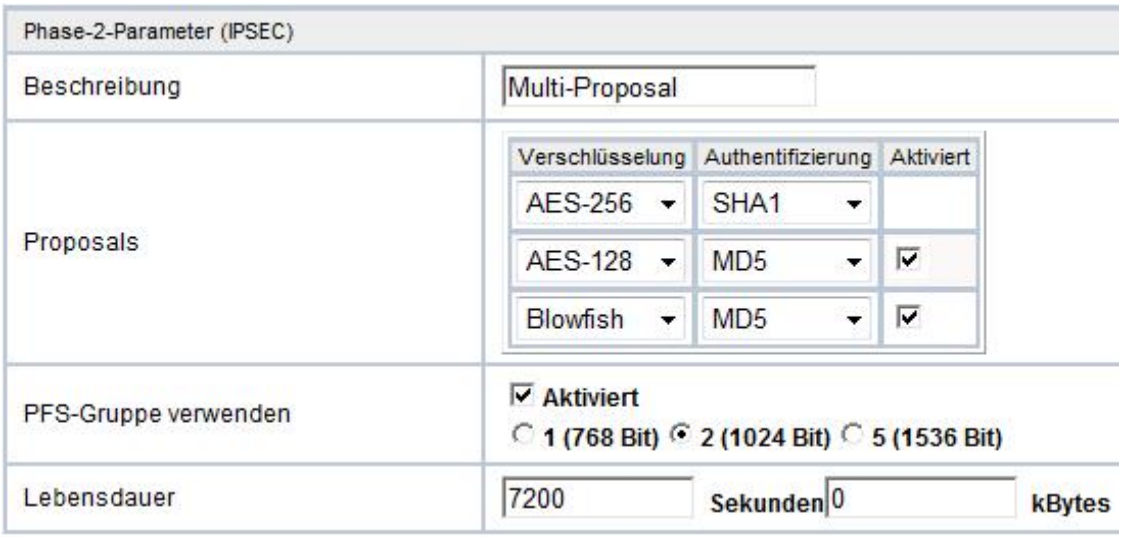
Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Als Beschreibung verwenden Sie z.B. PSK Multiproposal.
- Bei Proposals wählen Sie z.B. AES-256 / SHA1.
- Als Authentifizierungsmethode wählen Sie z.B. Preshared Keys.
- Den Modus setzen Sie auf z.B. Aggressiv.
- Unter Lokaler ID-Typ wählen Sie z.B. Fully Qualified Domain Name (FQDN).
- Unter Lokaler ID-Wert tragen Sie z.B. zentrale ein.

8.4 Phase-2 konfigurieren

Die Phase-2 bestimmt die Algorithmen zur Abgesicherung der Nutzdaten. Gehen Sie in folgendes Menü, um ein Neues Profil zu erstellen:

GUI → VPN → IPSec → Phase-2 Profile → Neu



Folgende Punkte sind hier relevant:

Feld	Bedeutung
Beschreibung	Die Bezeichnung des Phase-2 Profils.
Proposals	Die Phase-2 Verschlüsselungs- / Authentifizierungs-Algorithmen.
PFS-Gruppe verwenden	Perfect Forward Secrecy erstellt für die Phase-2 neue Schlüssel.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Als Beschreibung verwenden Sie z.B. PSK Multi-Proposal.
- Bei Proposals wählen Sie z.B. AES-256 / SHA1.
- Wählen Sie bei PFS-Gruppe verwenden z.B. Aktiviert / 2 (1024 Bit).

8.5 IPSec und RADIUS einschalten

Um IPSec über RADIUS zu nutzen, müssen Sie in folgendem Menü die Dienste einschalten:

GUI → VPN → IPSec → Optionen

Folgende Punkte sind hier relevant:

Feld	Bedeutung
IPSec aktivieren	Schaltet den IPSec-Dienst ein.
Dynamische RADIUS-Authentifizierung	Schaltet die Nutzung des RADIUS-Servers ein.

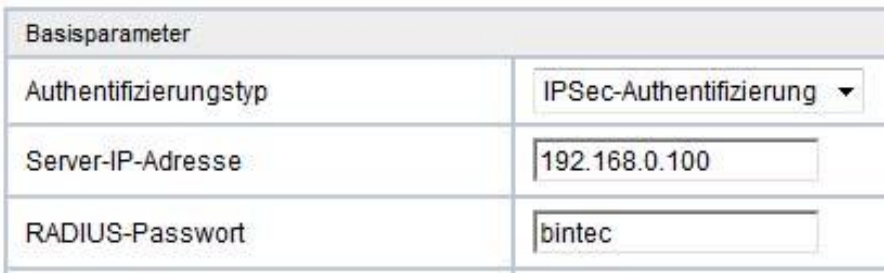
Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Der Haken bei IPSec aktivieren ist z.B. aktiviert.
- Der Haken bei Dynamische RADIUS-Authentifizierung ist z.B. aktiviert.

8.6 RADIUS-Server angeben

Der RADIUS-Server übergibt die IPSec Konfiguration an das Gateway und übernimmt die Authentifizierung der IPSec-Partner. Gehen Sie für die Konfiguration in folgendes Menü:

GUI → Systemverwaltung → Remote Authentifizierung → RADIUS → Neu



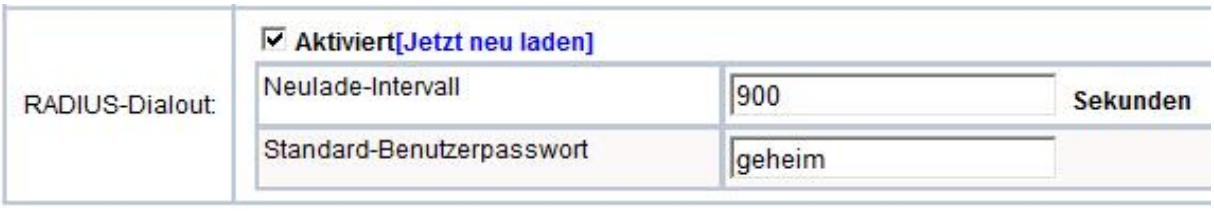
Folgende Punkte sind hier relevant:

Feld	Bedeutung
Authentifizierungstyp	Die Art der Authentifizierung.
Server-IP-Adresse	Die IP-Adresse des RADIUS-Servers.
RADIUS-Passwort	Das Passwort des RADIUS-Servers.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Als Authentifizierungstyp wählen Sie z.B. IPSec-Authentifizierung.
- Als Server-IP-Adresse geben Sie z.B. 192.168.0.100 ein.
- Als RADIUS-Passwort tragen Sie z.B. bintec ein.

Wenn das Gateway in der Zentrale selber Verbindungen zu Außenstellen aufbaut, müssen die IPSec-Verbindungen beim Router-Start oder in einem festen Intervall vom RADIUS-Server geladen werden. Für diese sogenannte Preload Konfiguration müssen Sie unter Erweiterte Einstellungen folgende Parameter angeben:



Folgende Punkte sind hier relevant:

Feld	Bedeutung
RADIUS-Dialout	Aktiviert das Laden der IPSec-Konfiguration vor dem Aufbau.
Neulade-Intervall	Wann sollen die IPSec-Verbindungen neu geladen werden.
Standard-Benutzerpasswort	Das Passwort für die zugehörigen IPSec-Verbindungen.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Der Haken bei RADIUS-Dialout ist z.B. aktiviert.
- Als Neulade-Intervall verwenden Sie z.B. 900.
- Verwenden Sie als Standard-Benutzerpasswort z.B. geheim.

8.7 RADIUS-Server konfigurieren

Nach der Installation des FreeRADIUS-Servers müssen Sie verschiedene Konfigurationsdateien bearbeiten. Öffnen Sie die folgende Datei, um die RADIUS-Clients anzugeben:

FreeRADIUS.net → etc → raddb → clients.conf

```
client 192.168.0.0/24 {
      secret       = bintec
      shortname    = bintec-ipsec
}
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
client	Die IP-Adresse (Netz) / Maske vom RADIUS-Client (Router).
secret	Das gemeinsame Passwort zwischen Router und RADIUS-Server.
shortname	Ein Alias für den Router im RADIUS-Logging.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Verwenden Sie als Subnetz vom Client z.B. 192.168.0.0/24.
- Als secret tragen Sie z.B. bintec ein.
- Als shortname verwenden Sie z.B. bintec-ipsec.

Der RADIUS-Server benötigt für die Einwahl der IPSec-Clients und die Verbindung zu den Außenstellen die IPSec-Konfigurationsparameter. Für jede Verbindung sollten Sie einen Eintrag in der Konfiguration erzeugen. Es gibt verschiedene Ansätze in der users.conf Datei, um die IPSec-Verbindungen im RADIUS-Server zu hinterlegen:

FreeRADIUS.net → etc → raddb → users.conf

Client zu Gateway mit Traffic-Listen (Preload)

Der nachfolgende Eintrag zeigt eine Verbindung zwischen Client und Gateway. Die Konfiguration wird beim ersten Kontakt zum RADIUS-Server übermittelt (Preload). Die IPSec-Konfiguration im Router erfolgt anhand der alten Traffic-Listen Methode (Setup-Tool).

```
ipsecpre-0 User-Password=geheim
       BinTec-ipsecPeerTable=" ipsecPeerPeerIds=client0@teldat.de
       ipsecPeerPreSharedKey=sehrsicher0 ",
       BinTec-ipsecTrafficTable=" ipsecTrLocalAddress=192.168.0.0
       ipsecTrLocalMaskLen=24 ipsecTrRemoteAddress=10.10.10.10
       ipsecTrRemoteMaskLen=32 ipsecTrAction=protect "
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
ipsecpre-0	Jede IPSec-Verbindung als Preload benötigt als Standard-Benutzernamen eine fortlaufende Nummer begonnen bei 0.
User-Password	Das Standard-Benutzerpasswort des RADIUS-Eintrags.
BinTec-ipsecPeerTable	Die IPSec Parameter für die bintec Tabelle ipsecPeerTable.
BinTec-ipsecTrafficTable	Die IPSec Parameter für die bintec Tabelle ipsecTrafficTable.

Client zu Gateway mit virtuellen Interfacen (Preload)

Der nachfolgende Eintrag zeigt eine Verbindung zwischen Client und Gateway. Die Konfiguration wird beim ersten Kontakt zum RADIUS-Server übermittelt (Preload). Die IPSec-Konfiguration im Router erfolgt anhand der virtuellen Interface (Routing).

```
ipsecpre-1 User-Password=geheim
       BinTec-ipsecPeerTable=" ipsecPeerPeerIds=client1@teldat.de
       ipsecPeerPreSharedKey=sehrsicher1 ipsecPeerVirtualInterface=enabled ",
       BinTec-ipRouteTable=" ipRouteDest=10.10.10.10 ipRouteNextHop=192.168.0.1
       ipRouteMask=255.255.255.255 "
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
ipsecpre-1	Jede IPSec-Verbindung als Preload benötigt als Standard-Benutzernamen eine fortlaufende Nummer begonnen bei 0.
User-Password	Das Standard-Benutzerpasswort des RADIUS-Eintrags.
BinTec-ipsecPeerTable	Die IPSec Parameter für die bintec Tabelle ipsecPeerTable.
BinTec-ipRouteTable	Die Routing Einträge für die bintec Tabelle ipRouteTable.

IPSec zwischen Gateways mit Phase-1 / -2 Anpassungen (Preload)

Der nachfolgende Eintrag zeigt eine Verbindung zwischen Gateway und Gateway. Die Konfiguration wird beim ersten Kontakt zum RADIUS-Server übermittelt (Preload). Die IPSec-Konfiguration im Router erfolgt anhand der virtuellen Interface (Routing). Die Phase-1 und Phase-2 Parameter werden optional angepasst.

```
ipsecpre-2 User-Password=geheim
       BinTec-ipsecPeerTable=" ipsecPeerPeerIds=filiale
       ipsecPeerPreSharedKey=sehrsicher2 ipsecPeerVirtualInterface=enabled ",
       BinTec-ipRouteTable=" ipRouteDest=192.168.1.0 ipRouteNextHop=192.168.0.1
       ipRouteMask=255.255.255.0 ",
       BinTec-ikeProfileTable=" ikePrfMode=aggressive ikePrfProposal=2 ",
       BinTec-ipsecProfileTable=" ipsecPrfProposal=2 ipsecPrfPfsGroup=2 "
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
ipsecpre-2	Jede IPSec-Verbindung als Preload benötigt als Standard-Benutzernamen eine fortlaufende Nummer begonnen bei 0.
User-Password	Das Standard-Benutzerpasswort des RADIUS-Eintrags.
BinTec-ipsecPeerTable	Die IPSec Parameter für die bintec Tabelle ipsecPeerTable.
BinTec-ipRouteTable	Die Routing Einträge für die bintec Tabelle ipRouteTable.
BinTec-ikeProfileTable	Die Phase-1 Parameter für die bintec Tabelle ikeProfileTable.
BinTec-ipsecProfileTable	Die Phase-2 Parameter für die bintec Tabelle ipsecProfileTable.

Client zu Gateway mit virtuellen Interfacen (onDemand)

Der nachfolgende Eintrag zeigt eine Verbindung zwischen Client und Gateway. Die Konfiguration wird erst beim IPSec-Verbindungsaufbau vom RADIUS-Server übermittelt (onDemand). Die IPSec-Konfiguration im Router erfolgt anhand der virtuellen Interface.

```
client@teldat.de User-Password=geheim
       BinTec-ipsecPeerTable=" ipsecPeerPeerIds=client@teldat.de
       ipsecPeerPreSharedKey=sehrsicher ipsecPeerVirtualInterface=enabled ",
       BinTec-ipRouteTable=" ipRouteDest=10.10.10.10 ipRouteNextHop=192.168.0.1
       ipRouteMask=255.255.255.255 "
```

Folgende Punkte sind hier relevant:

Feld	Bedeutung
client@teldat.de	Anhand des Benutzernamens (=ipsecPeerPeerIds) sucht der RADIUS-Server die IPSec-Verbindung aus der Konfiguration.
User-Password	Das Standard-Benutzerpasswort des RADIUS-Eintrags.
BinTec-ipsecPeerTable	Die IPSec Parameter für die bintec Tabelle ipsecPeerTable.
BinTec-ipRouteTable	Die Routing Einträge für die bintec Tabelle ipRouteTable.

INFO

Die Benutzernamen und die „ipsecPeerPeerIds“ sind bei onDemand Verbindungen identisch.

INFO

Keine BinTec-Tabelle in der RADIUS-Konfiguration darf mit einem Zeilenumbruch unterbrochen werden. Am Ende jeder Tabelle (Zeile) außer der letzten signalisiert ein Komma, dass noch weitere Tabellen zu dem Eintrag folgen.

8.8 Konfiguration überprüfen

Um Fehler zu erkennen und den Verbindungsaufbau zu überprüfen, können Sie sich die Systemmeldungen in folgendem Menü anzeigen lassen:

GUI → Monitoring → Internes Protokoll

Subsystem	Nachricht
RADIUS	client@funkwerk-ec.com: send PAP REQUEST ID 24 to <192.168.0.100:1812>
RADIUS	client@funkwerk-ec.com: got ACCESS ACCEPT ID 24 from <192.168.0.100:1812>
IPSec	set extended variable <ipsecPeerPeerIds> to <client@funkwerk-ec.com>
IPSec	set extended variable <ipsecPeerPreSharedKey> to <sehrsicher>
IPSec	set extended variable <ipsecPeerVirtualInterface> to <enabled>
IPSec	set extended variable <ipRouteDest> to <10.10.10.10>
IPSec	set extended variable <ipRouteNextHop> to <192.168.0.1>
IPSec	set extended variable <ipRouteMask> to <255.255.255.255>
IPSec	RADIUS: installed peer client@funkwerk-ec.com
IPSec	P1: peer 20003 (client@funkwerk-ec.com) sa 4 (R): identified ip 62.10.20.30 <- ip 62.10.20.31
IPSec	P1: peer 20003 (client@funkwerk-ec.com) sa 4 (R): notify id fqdn(any:0,[0..7]=zentrale) <- id usr@fqdn(any:0,[0..21]=client@funkwerk-ec.com): Initial contact notification proto 1 spi(16) = [72957f58 bdec19ab : 52b4e5d1 1e30db45]
IPSec	P1: peer 20003 (client@funkwerk-ec.com) sa 4 (R): done id fqdn(any:0,[0..7]=zentrale) <- id usr@fqdn(any:0,[0..21]=client@funkwerk-ec.com) AG[72957f58 bdec19ab : 52b4e5d1 1e30db45]
IPSec	IPSEC CB - CB mode of Peer "client@funkwerk-ec.com" changed -> reset IsdnCBNextMode
IPSec	P2: peer 20003 (client@funkwerk-ec.com) traf 0 bundle 3 (R): created 192.168.0.0/24:0 < any > 10.10.10.10/32:0 rekeyed 0
IPSec	P2: peer 20003 (client@funkwerk-ec.com) traf 0 bundle 3 (R): SA 5 established ESP [10379639] in[0] Mode tunnel enc aes-cbc (256 bit) auth sha (160 bit)
IPSec	P2: peer 20003 (client@funkwerk-ec.com) traf 0 bundle 3 (R): SA 6 established ESP [0a28f12d] out[0] Mode tunnel enc aes-cbc (256 bit) auth sha (160 bit)