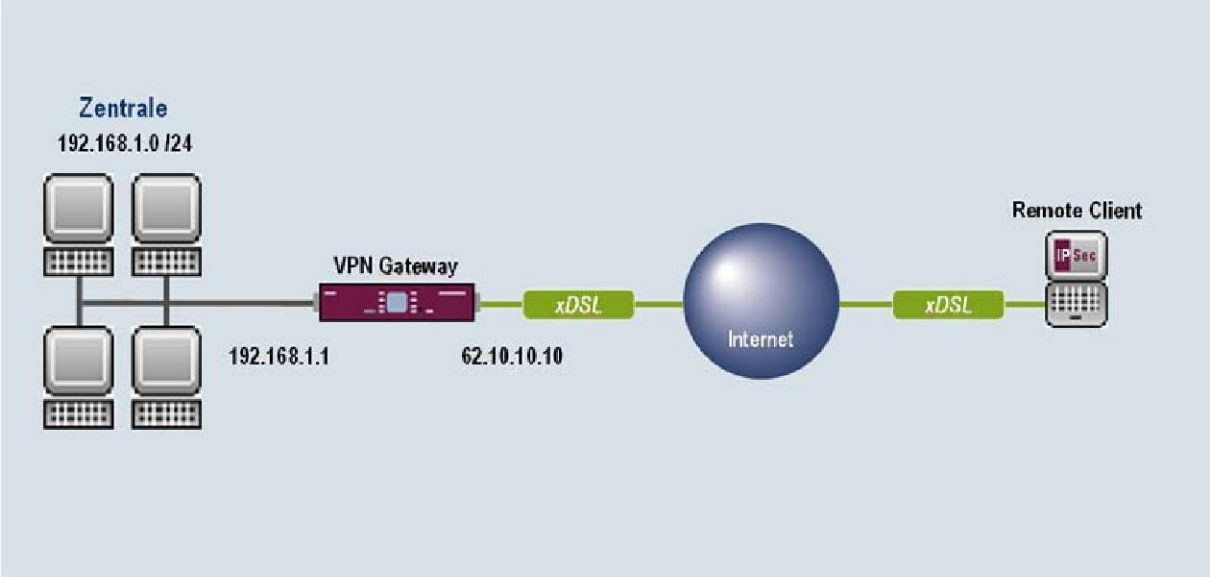
1. IPsec Verbindung zwischen Gateway und IPsec Client - Peer



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung zwischen einem Bintec IPsec Gateway und dem Bintec IPsec Client mit öffentlicher IP-Adresse beschrieben. Diese Anleitung zeigt die Konfiguration auf Release 7.1.4

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 7.1.1 zu verwenden.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider
- Der Remote PC muss sich über eine eigene Verbindung ins Internet einwählen, damit er eine öffentliche IP Adresse erhält
- Auf dem Gateway brauchen Sie eine statische IP Adresse oder Dyndns für das Internet
- Auf dem Remote PC ist der installierte IPsec Client ab Version 1.0 build 78 erforderlich

1.3 Konfiguration

Die Anleitung konfiguriert sowohl die Zentrale als auch den Client.
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

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PEERS][ADD]: Configure Peer                                  zentrale
------------------------------------------------------------------------------

     Description:       Client
     Admin Status:      up        Oper Status:   down

     Peer Address:
     Peer IDs:          Client
     Pre Shared Key:    bintec

     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: no
     Traffic List Settings >


                          SAVE                          CANCEL
------------------------------------------------------------------------------
```

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Description	Geben Sie eine Beschreibung für die Verbindung an.
Peer Address	Die IP Adresse des IPsec Partners (Bleibt bei einer Client Einwahl frei)
Peer IDs	Hier tragen Sie eine Identifikation des Partners ein
Pre Shared Key	Das gemeinsame Passwort von beiden IPsec Partnern
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)

Gehen Sie folgendermassen vor, um die Einstellungen im Peer vorzunehmen:

- Benennen Sie den Eintrag **Client**
- Bei Peer Address geben Sie nichts an. Der Eintrag bleibt leer.
- Bei Peer IDs geben Sie **Client** an
- Im Pre Shared Key tragen Sie **bintec** als Passwort ein
- Virtual Interface steht auf: **no**

1.3.1b Traffic List Settings

- 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)

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PEERS][EDIT][TRAFFIC][ADD]: Traffic Entry (Client)          zentrale
-------------------------------------------------------------------------------

     Description:    Client

     Protocol:       dont-verify

     Local:
          Type: net    Ip: 192.168.1.0     / 24

     Remote:
          Type: peer

     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 Type	Geben Sie hier an, ob der IPsec Partner ein Netz darstellt oder nur ein Host ist

Gehen Sie folgendermassen vor um Ihren Eintrag zu konfigurieren:

- Als Beschreibung geben Sie **Client** an
- Unter Lokal IP tragen Sie **192.168.1.0** mit der Mask **24** ein
- Den Remote Type stellen Sie auf **peer**
- 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

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                                                zentrale
------------------------------------------------------------------------------

   Description (Idx 1) :    *autogenerated*
   Proposal            :  19 (Rijndael/MD5)
   Lifetime            :  use default
   Group               :  2 (1024 bit MODP)
   Authentication Method :  Pre Shared Keys
   Mode                :  aggressiv
   Heartbeats          :  none
   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

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals verändern Sie auf: **19 (Rijndael/MD5)**
- Den Mode stellen Sie auf **aggressiv**, da Sie mindestens eine dynamische IP Adresse haben

In folgendem Untermenü können Sie PHASE 2 Vorlagen verändern oder mit ADD hinzufügen:

IPSEC -> IPsec (Phase 2) Defaults -> EDIT

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][PHASE2][EDIT]                                                zentrale
------------------------------------------------------------------------------

   Description (Idx 1) :     *autogenerated*

   Proposal              :   23 (ESP(Rijndael/MD5))
   Lifetime              :   use default
   Use PFS               :   none
   Heartbeats            :   none
   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

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals verändern Sie auf: **23 (ESP(Rijndael/MD5))**

1.3.2 Einstellungen im Bintec IPsec Client

Nach der ersten Installation des Clients müssen Sie über den Secure Client Monitor Ihre Verbindung konfigurieren. Legen Sie für jede Verbindung ein Profil an. Der Wizard startet nach der Installation automatisch. Gehen Sie folgendermassen vor, um eine Verbindung zur Zentrale zu konfigurieren:

- Starten Sie den Wizard ggf. unter Konfiguration –> Profil-Einstellungen -> Neuer Eintrag

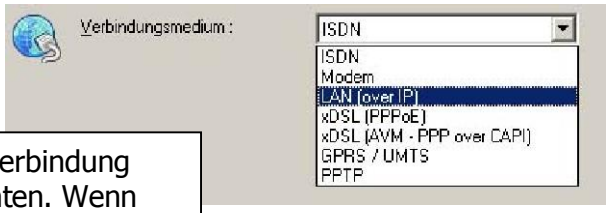
1.

Wählen Sie die Konfiguration einer IPsec Verbindung aus

2.

Benennen Sie den Eintrag Zentrale

3.

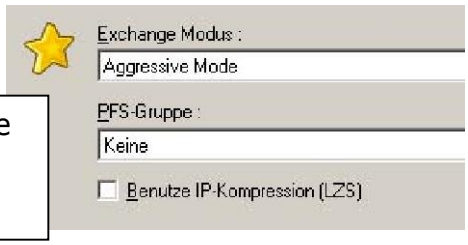


Wählen Sie hier Ihre Internet Verbindung aus, die Sie konfigurieren möchten. Wenn Sie bereits eine Verbindung konfiguriert haben (z. B. DFÜ) wählen Sie LAN (over IP)

4.

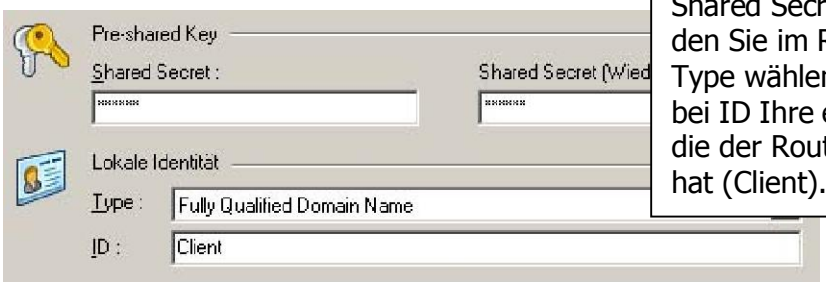
Hier geben Sie die Gateway IP Adresse oder Dyndns Namen der Zentrale an

5.



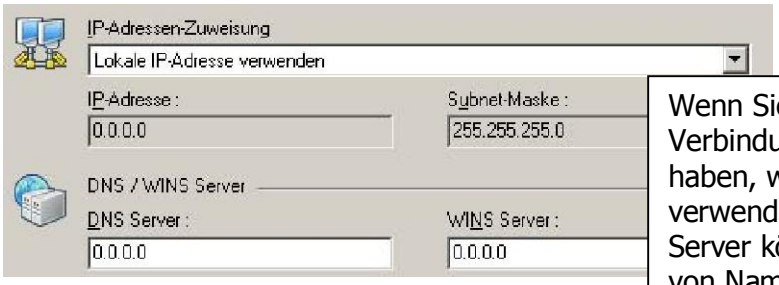
Den IKE Modus setzen Sie auf Aggressive Mode, da Sie auf mindestens einer Seite dynamische IP Adressen haben

6.



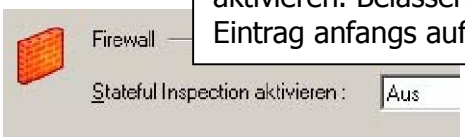
Shared Secret ist der Preshared Key den Sie im Router hinterlegt haben. Bei Type wählen Sie FQDN aus und geben bei ID Ihre eigene Identifikation an, die der Router unter Peer IDs stehen hat (Client).

7.



Wenn Sie sich mit einer eigenen Verbindung ins Internet eingewählt haben, wählen Sie „Lokale IP-Adresse verwenden" aus. Unter DNS und WINS Server können Sie optional IP Adressen von Name Servern aus dem Zentralnetz eintragen

8.

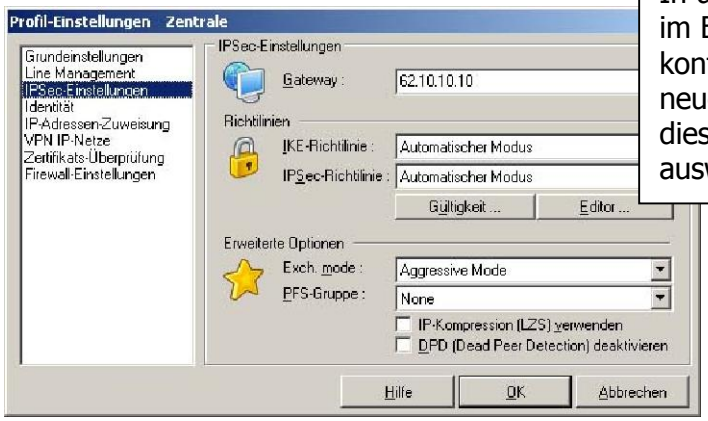


Optional können Sie die Stateful Inspection Firewall aktivieren. Belassen Sie den Eintrag anfangs auf AUS

Wenn Sie den Wizard ausgeführt haben müssen Sie die Verbindungs-Parameter noch anpassen. Gehen Sie wie folgt vor:

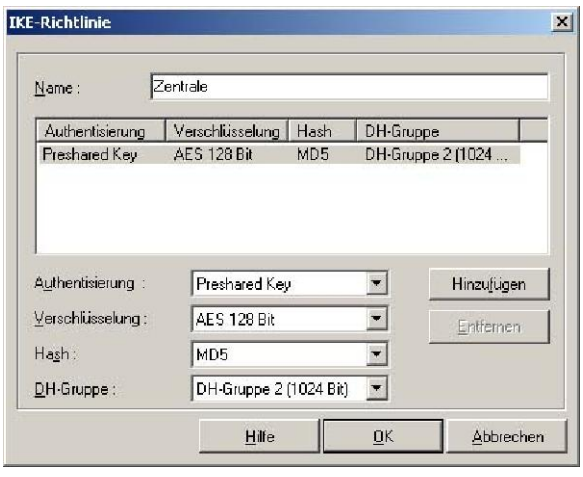
- Konfiguration –> Profil-Einstellungen -> Konfigurieren

9.



In den IPsec Einstellungen müssen Sie im Editor die IKE und IPsec Richtlinien konfigurieren. Erstellen Sie unter Editor neue Einträge, die Sie im Anschluss in diesem Menü für die Verbindung auswählen

10.



Benennen Sie den Eintrag Zentrale. Wählen Sie in der Reihenfolge aus:

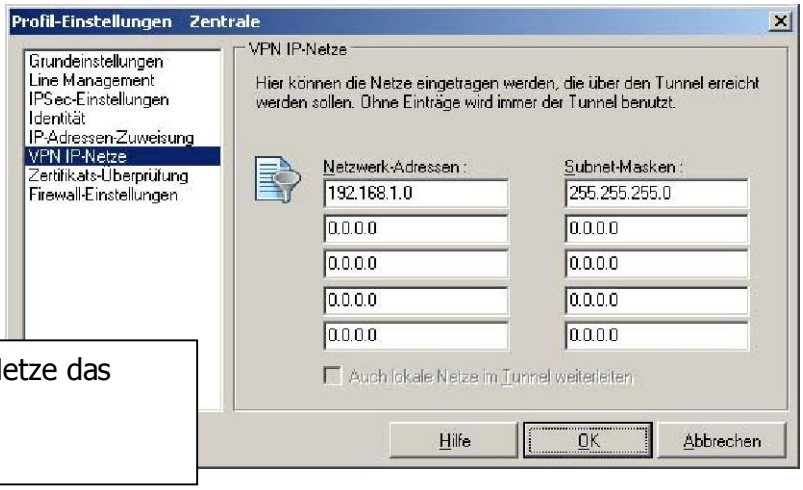
- **Preshared Key**
- **AES 128**
- **MD5**
- **DH-Gruppe2**

11.

Benennen Sie den Eintrag Zentrale.
Wählen Sie in der Reihenfolge aus:

- AES 128
- MD5

12.



Geben Sie unter VPN IP-Netze das Netzwerk der Zentrale an. (192.168.1.0)

1.4 Ergebnis

Sie haben eine IPsec Verbindung zwischen einem IPsec Gateway und einem Bintec IPsec Client konfiguriert. Der Client hat sich direkt ins Internet eingewählt und eine dynamische Adresse erhalten. Die Zentrale besitzt eine statische IP Adresse. Das Szenario ist wahlweise auch mit Angabe der Dyndns Adresse im Client für die Zentrale zu realisieren.

1.5 Kontrolle

Um die IPsec Verbindung zu testen, gehen Sie wie folgt beschrieben vor:

- Geben Sie an der Shell des Gateways folgendes ein: **ipsecGlobMaxSysLogLevel=debug**
- Danach starten Sie den Debug Modus mit : **debug all&**
- Verbinden Sie sich vom Client aus zur Zentrale
- Geben Sie einen Ping von Ihrer Eingabeaufforderung zum Remotenetz des Partners ab

```
C:\>ping 192.168.1.1

Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:

Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62

Ping-Statistik für 192.168.1.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms

C:\>
```

Jetzt sollten Sie folgende Meldungen erhalten:

```
zentrale:>
zentrale:> ipsecGlobMaxSysLogLevel=debug
ipsecGlobMaxSysLogLevel( rw):        debug
zentrale:> debug all&
02:25:58 DEBUG/IPSEC: IKE_INVALID_COOKIE: 19700105022558:   Source addr:0.0.0.0
 Destination addr:62.151.213.165
02:25:58 DEBUG/IPSEC: IKE_INVALID_COOKIE: 19700105022558:   Source addr:0.0.0.0
 Destination addr:62.151.213.165
02:25:58 DEBUG/IPSEC: P1: peer 0 () sa 1 (R): new ip 62.10.10.10 <- ip 62.151.21
3.165
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsra-isakmp-xauth-06'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-nat-t-ike-03'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-nat-t-ike-02'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-nat-t-ike-00'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-dpd-00.txt'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'cb1ed48b6d68269bb411b61a07bce24f'
02:25:58 DEBUG/IPSEC: P1: peer 1 (client) sa 1 (R): identified ip 62.10.10.10 <-
ip 62.15.213.65
02:25:58 DEBUG/IPSEC: P1: peer 1 (client) sa 1 (R): notify id ipv4(any:0,[0..3]=
62.10.10.10) <- id fqdn(any:0,[0..5]=Client) (unencrypted): Initial contact
notification proto 1 spi(16) = [62257e0b d10f904c : 3bee1cce 1d524fde]
02:25:58 INFO/IPSEC: P1: peer 1 (client) sa 1 (R): done id ipv4(any:0,[0..3]=62.
10.10.10) <- id fqdn(any:0,[0..5]=Client) AG[62257e0b d10f904c : 3bee1cce 1d524f
de]
02:25:58 INFO/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): created 192.168.1.
0/192.168.1.0:0 < any > 62.151.213.165/62.151.213.165:0 rekeyed 0
02:25:58 DEBUG/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): SA 1 established
ESP[03554571] in[0] Mode tunnel enc rijndael-cbc(16) auth md5(16)
02:25:58 DEBUG/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): SA 2 established
ESP[2b0c42ed] out[0] Mode tunnel enc rijndael-cbc(16) auth md5(16)
02:25:58 INFO/IPSEC: Activate Bundle 1 (Peer 1 Traffic 2)
02:25:58 DEBUG/INET: NAT: new outgoing session on ifc 100 prot 50 62.10.10.10:0/
62.10.10.10:0 -> 62.151.213.165:0
02:25:58 INFO/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): established  (62.1
10.10.10<->62.151.213.165) with 2 SAs life 28800 Sec/0 Kb rekey 25920 Sec/0 Kb H
b both
```

1.6 Konfigurationsschritte im IPSEC Menü im Überblick

---------- Configure Peer ----------

Feld	Menü	Wert
Description	Configure Peers > APPEND	Client
Peer IDs	Configure Peers > APPEND	Client
Pre Shared Key	Configure Peers > APPEND	bintec

---------- Traffic List ----------

Feld	Menü	Wert
Description	Configure Peers > Traffic List Settings > APPEND	Client
Local IP	Configure Peers > Traffic List Settings > APPEND	192.168.1.0 /24
Remote Type	Configure Peers > Traffic List Settings > APPEND	peer

---------- Phase 1 ----------

Feld	Menü	Wert
Proposal	IKE (Phase 1) Defaults > edit > ADD	19 (Rijndael/MD5)
Mode	IKE (Phase 1) Defaults > edit > ADD	aggressiv

---------- Phase 2 ----------

Feld	Menü	Wert
Proposal	IPsec (Phase 2) Defaults > edit > ADD	23 (ESP(Rijndael/MD5))