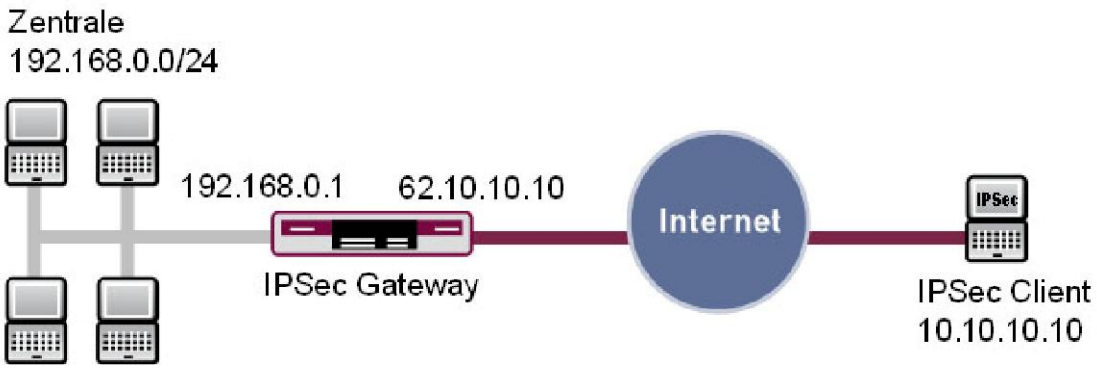
# 1. IPSec Verbindung zwischen IPSec Client und Gateway




## 1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPSec Verbindung vom Bintec IPSec Client zum Gateway gezeigt. Dabei spielt es keine Rolle, ob Sie sich vom Client direkt ins Internet eingewählt haben oder sich hinter einem Router befinden. Diese Anleitung zeigt die Konfiguration auf Release 7.4.4.

Zur Konfiguration wird hierbei das FCI verwendet.

## 1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:
- Grundkonfiguration des Gateways.
- Für das IPSec Gateway ist ein Bootimage ab Version 7.4.4 zu verwenden.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider.
- In der Zentrale brauchen Sie eine statische IP Adresse oder DynDNS für das Internet.
- Auf dem Remote PC ist der installierte IPSec Client ab Version 1.1 build 108 erforderlich.

## 1.3 Konfiguration

Um IPSec zu konfigurieren, müssen Sie im Folgenden Menü Einstellungen vornehmen:

**VPN -> IPSec**

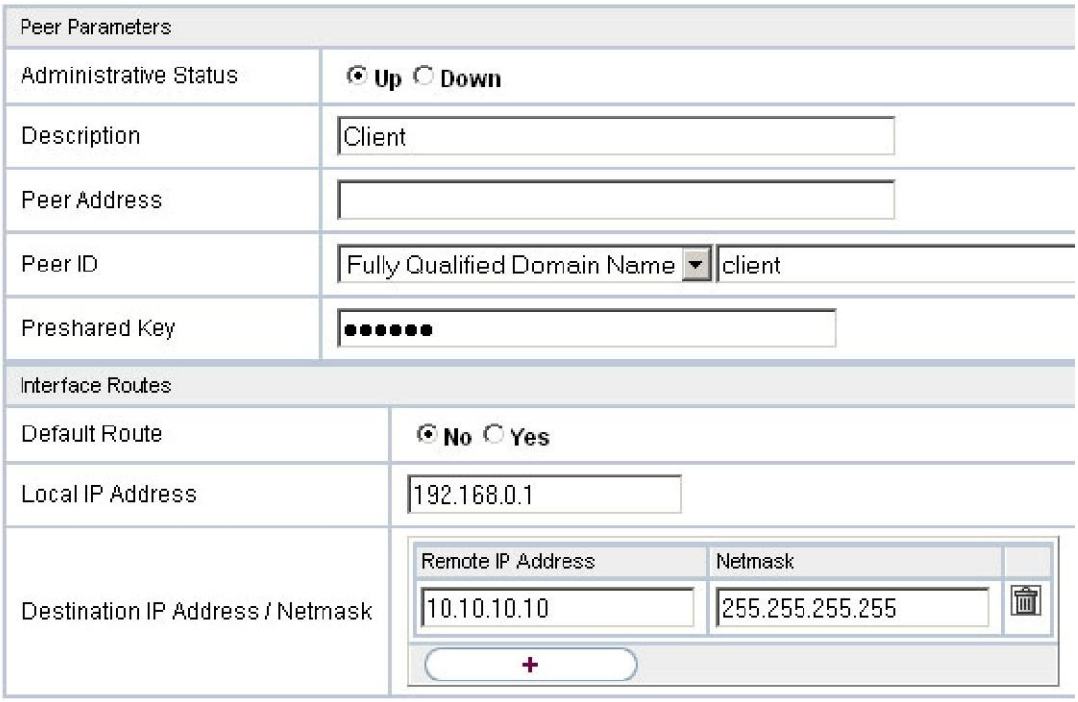
In dem Untermenü "IPSec Peers" haben Sie die Möglichkeit mit **New** Verbindungspartner für IPSec hinzuzufügen.

**INFO**
Bei der Erstkonfiguration von IPSec konfiguriert das Gateway automatisch für Sie einige Standard Parameter. Diese sind für den weiteren Verlauf der IPSec Konfiguration notwendig und werden in den Tabellen hinterlegt.

### 1.3.1 IPSec Peer Parameter

Erstellen Sie in folgendem Menü eine neue Verbindung für IPSec:

**VPN -> IPSec -> IPSec Peers -> New**




Folgende Felder sind hierbei relevant:

| **Feld** | **Bedeutung** |
|---|---|
| Description | Geben Sie eine Beschreibung für die Verbindung an. |
| Peer ID | Hier tragen Sie eine Identifikation des Partners ein (In dem Client unter Local ID eingetragen). |
| Preshared Key | Das gemeinsame Passwort von Gateway und Client. |
| Local IP Address | Hier steht Ihre lokale IP Adresse vom Ethernet Interface. |
| Destination IP Address / Netmask | Hier konfigurieren Sie die Virtuelle IP-Addresse vom IPSec Client |

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

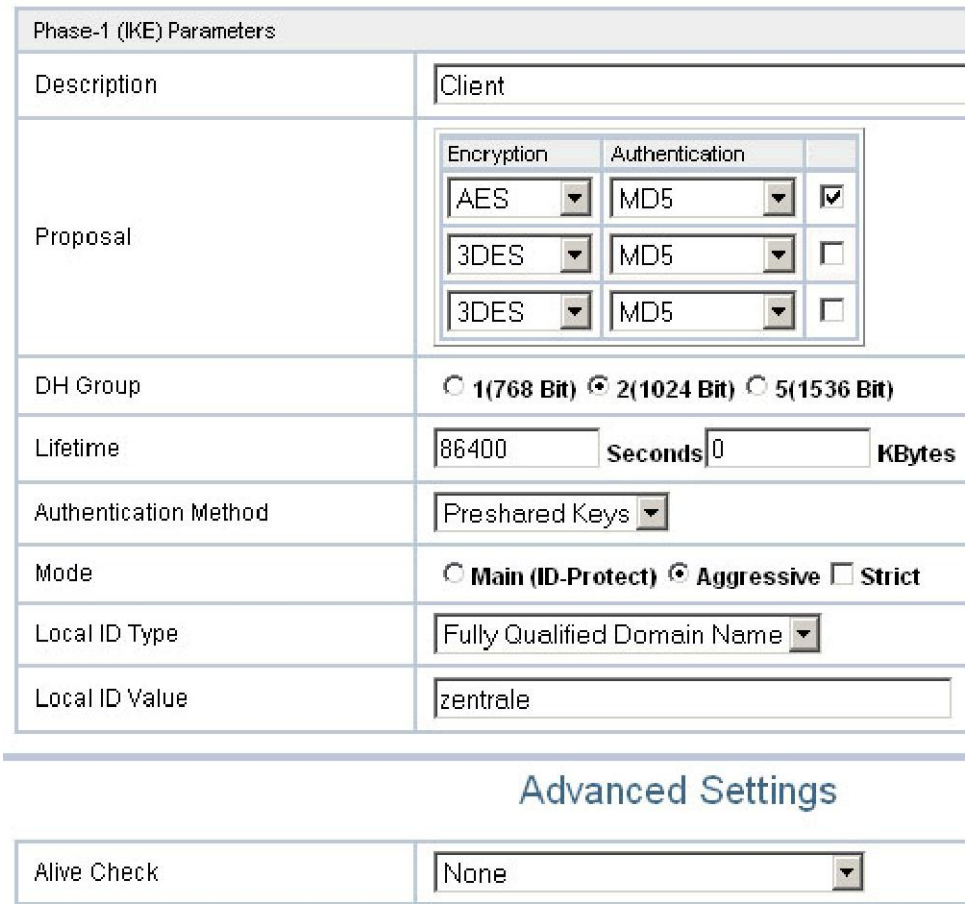
- Benennen Sie den Eintrag unter Description: **z.B. Client**.
- Bei Peer ID geben Sie: **Fully Qualified Domain Name / client** an.
- Im Preshared Key tragen Sie **z.B. bintec** als Passwort ein.
- Unter Local IP Address tragen Sie **192.168.0.1** ein.
- Unter Destination IP Address / Netmask fügen Sie mit **+** einen Eintrag hinzu.
- Tragen Sie in die Felder **10.10.10.10 / 255.255.255.255** ein.
- Bestätigen Sie Ihre Eingaben mit **OK**.

**INFO**
Bedenken Sie bitte, dass Sie in Ihrer Produktiv-Umgebung einen bedeutend längeren PreShared Key nutzen sollten. Empfehlenswert ist eine Länge von 20 Zeichen bei der Verwendung von Sonderzeichen, Zahlen und Klein/Groß Buchstaben.

### 1.3.2 Phase 1 Profil

Im folgenden Untermenü können Sie Phase 1 Vorlagen verändern oder mit **New** hinzufügen:

**VPN -> IPSec -> Phase-1 Profiles**



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 Type | Wählen Sie hier die Art der Identifikation aus. |
| Local ID Value | Hier tragen Sie die eigene Identifikation für das Gateway ein. |
| Alive Check | Schalten Sie hier die Tunnelüberwachung ein oder aus. |

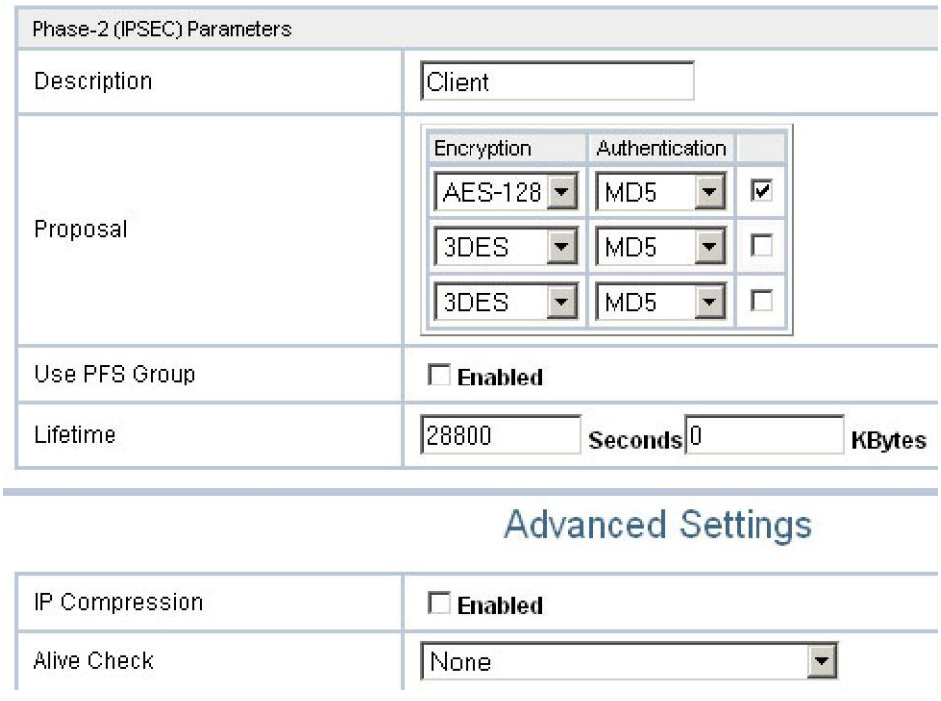
Konfigurieren Sie das Phase 1 Profil mit folgenden Parametern:

- Bei Description geben Sie: **z.B. Client** ein.
- Die Proposal markieren Sie mit einem **haken** und stellen Sie auf: **AES/MD5**.
- Den Mode stellen Sie auf **aggressiv** da Sie dynamische IP Adressen nutzen.
- Unter Local ID Type wählen Sie: **Fully Qualified Domain Name** aus.
- Unter Local ID Value geben Sie: **zentrale** ein (Steht beim Partner unter Peer ID).
- Alive Check setzen Sie auf: **None**.

### 1.3.3 Phase 2 Profil

Im folgenden Untermenü können Sie Phase 2 Vorlagen verändern oder mit **New** hinzufügen:

**VPN -> IPSec -> Phase-2 Profiles**



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 | Schalten Sie hier die Tunnelüberwachung ein oder aus. |

Konfigurieren Sie das Phase 2 Profil mit folgenden Parametern:

- Bei Description geben Sie: **z.B. Client** ein.
- Die Proposal markieren Sie mit einem **haken** und stellen Sie auf: **AES-128/MD5**.
- Alive Check setzen Sie auf: **None**.

### 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

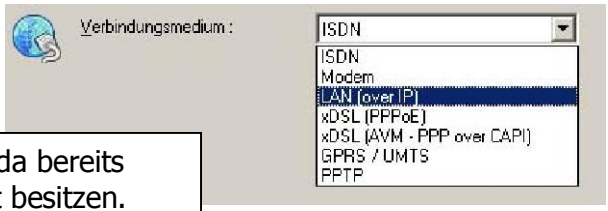
**1.**


Wählen Sie die Konfiguration einer IPSec Verbindung aus.

**2.**


Benennen Sie den Eintrag Zentrale.

**3.**

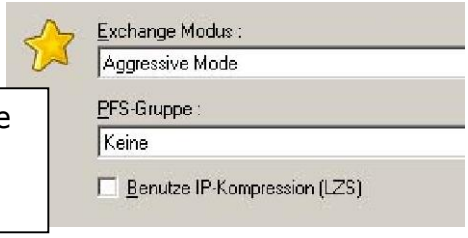



Wählen Sie LAN (over IP) aus, da bereits eine IP-Verbindung ins Internet besitzen.

**4.**

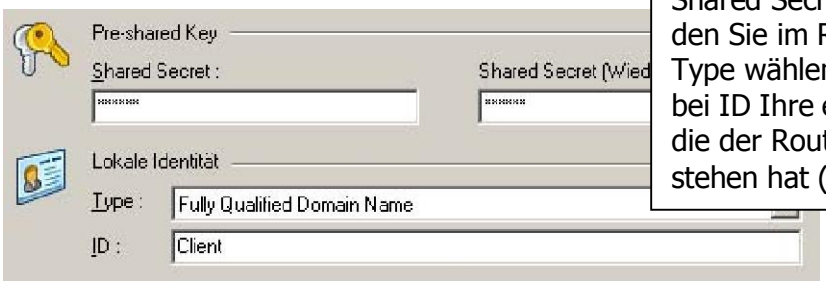

Hier geben Sie die Gateway IP Adresse oder DynDNS Namen der Zentrale an.

**5.**



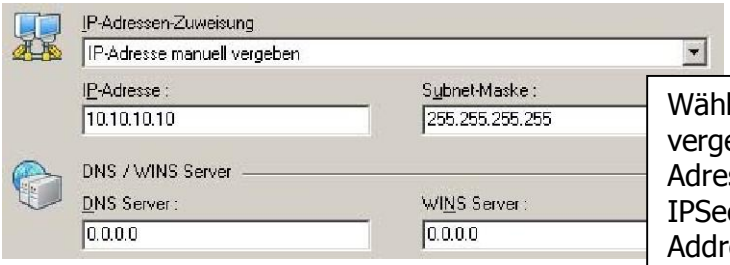

Den IKE Modus setzen Sie auf Aggressive Mode, da Sie auf mindestens einer Seite dynamische IP Adressen haben.

**6.**



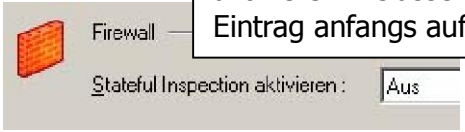

Shared Secret ist der Preshared Key den Sie im Router hinterlegt haben. Bei Type wählen Sie FQDN aus und geben bei ID Ihre eigene Identifikation an, die der Router unter Peer ID Value stehen hat (client).

**7.**




Wählen Sie „IP-Adresse manuell vergeben" aus. Geben Sie bei IP Adresse eine virtuelle IP an, die Sie im IPSec Gateway unter Destination IP-Address eingestellt haben (10.10.10.10). Unter DNS und WINS Server können Sie optional IP Adressen von Name Servern aus dem Zentralnetz eintragen.

**8.**

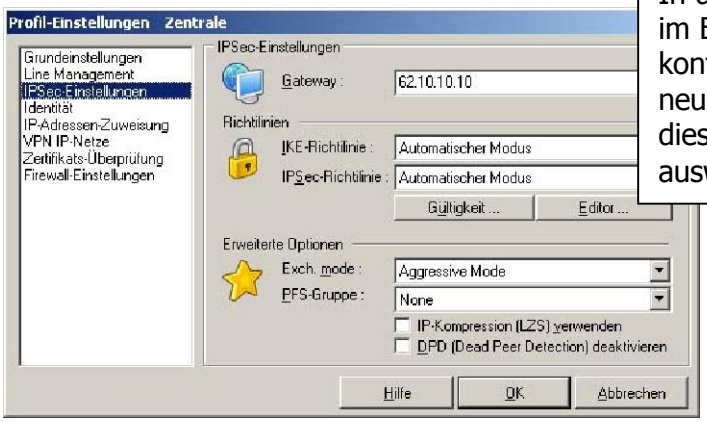



Optional können Sie die Stateful Inspection Firewall aktivieren. Belassen Sie den Eintrag anfangs auf AUS.

Wenn Sie den Wizard ausgeführt haben, müssen Sie die Verbindungs-Parameter noch anpassen. Gehen Sie in folgendes Menü im IPSec Client:

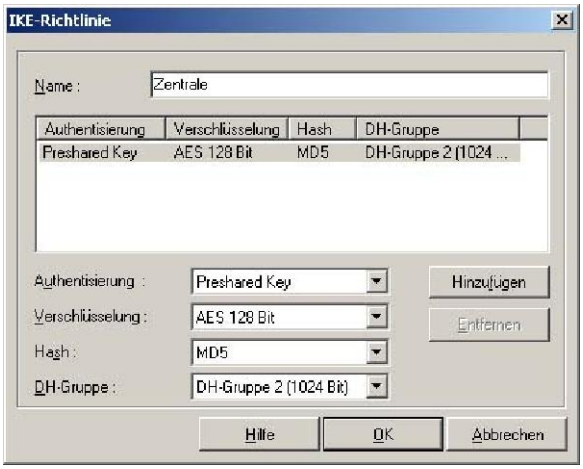
**Konfiguration –> Profil-Einstellungen -> Konfigurieren**

**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.

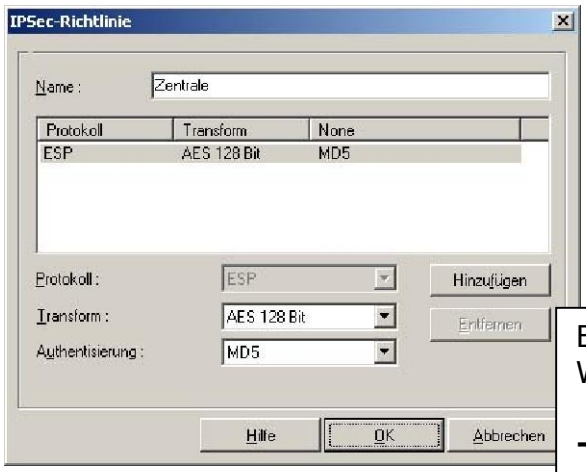
**10.**




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

- **Preshared Key**
- **AES 128 Bit**
- **MD5**
- **DH-Gruppe 2**

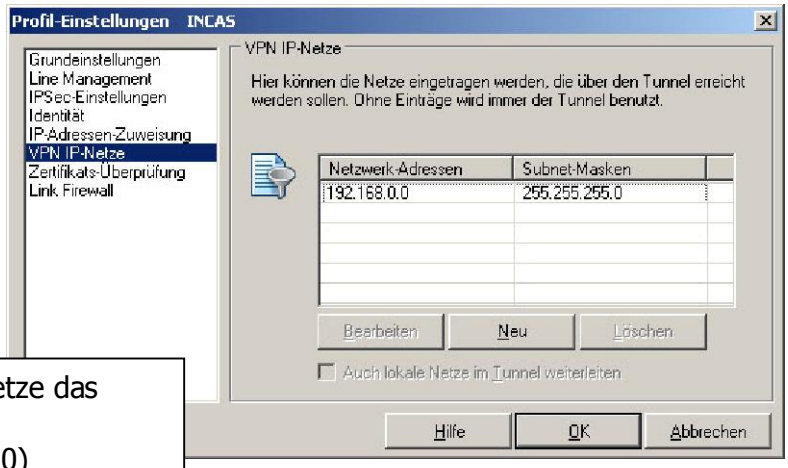
**11.**




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

- **AES 128 Bit**
- **MD5**

**12.**




Geben Sie unter VPN IP-Netze das Netzwerk der Zentrale an. (192.168.0.0/255.255.255.0)

## 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:

- Verbinden Sie sich vom IPSec Client aus zur Zentrale.
- Geben Sie einen Ping von Ihrer Eingabeaufforderung zum Remotenetz der Zentrale ab.

Jetzt sollten Sie folgende Meldungen erhalten:

```
C:\>ping 192.168.0.1

Ping wird ausgeführt für 192.168.0.1 mit 32 Bytes Daten:

Antwort von 192.168.0.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.0.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.0.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.0.1: Bytes=32 Zeit=1ms TTL=62

Ping-Statistik für 192.168.0.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms

C:\>
```

## 1.6 Konfigurationsschritte im Überblick

**IPSec Peer Parameter**

| Feld | Menü | Wert |
|---|---|---|
| Description | VPN -> IPSec -> IPSec Peers -> New | z.B. Client |
| Peer ID | VPN -> IPSec -> IPSec Peers -> New | FQDN / client |
| Preshared Key | VPN -> IPSec -> IPSec Peers -> New | bintec |
| Local IP Address | VPN -> IPSec -> IPSec Peers -> New | 192.168.0.1 |
| Destination IP Address Netmask | VPN -> IPSec -> IPSec Peers -> New | 10.10.10.10/ 255.255.255.255 |

**Phase 1 Profiles**

| Feld | Menü | Wert |
|---|---|---|
| Description | VPN -> IPSec -> Phase-1 Profiles -> New | z.B. Client |
| Proposal | VPN -> IPSec -> Phase-1 Profiles -> New | AES/MD5 |
| Mode | VPN -> IPSec -> Phase-1 Profiles -> New | aggressiv |
| Local ID Type | VPN -> IPSec -> Phase-1 Profiles -> New | Fully Qualified Domain Name |
| Local ID Value | VPN -> IPSec -> Phase-1 Profiles -> New | zentrale |
| Alive Check | VPN -> IPSec -> Phase-1 Profiles -> New | None |

**Phase 2 Profiles**

| Feld | Menü | Wert |
|---|---|---|
| Description | VPN -> IPSec -> Phase-2 Profiles -> New | z.B. Client |
| Proposal | VPN -> IPSec -> Phase-2 Profiles -> New | AES-128/MD5 |
| Alive Check | VPN -> IPSec -> Phase-2 Profiles -> New | None |