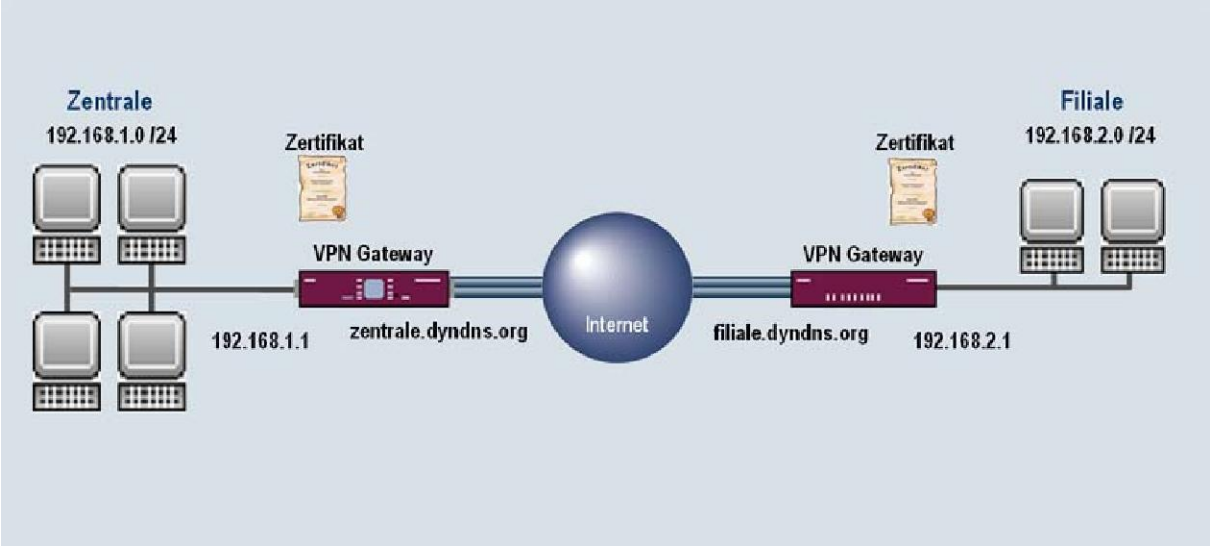
1. IPsec Verbindung zwischen 2 Gateways mit Zertifikaten



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung mit Zertifikaten beschrieben. Die Zertifikate werden zur Authentifizierung genutzt. Die Anleitung zeigt einmal die Konfigurationsschritte für Traffic Lists und den Unterschied zu Interface basierender Konfiguration. Diese Anleitung zeigt die Konfiguration auf Release 7.1.4 auf der Zentralseite.

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 zum Provider
- Auf beiden Gateways müssen Sie Dyndns oder eine statische IP Adresse für den Internet Zugang konfiguriert haben
- Sie brauchen eine Zertifizierungsstelle, wo Sie Zertifikate anfordern können
- Einen TFTP Server im Netzwerk

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. Um Fehler zu vermeiden, konfigurieren Sie als erstes eine Verbindung mit Preshared Key. Erst wenn diese funktioniert, setzen Sie Zertifikate ein.

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:        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)

```
VPN Access 25 Setup Tool                          BinTec Access Networks 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**, bis Sie sich im IPsec Main Menü befinden. 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)

```
VPN Access 25 Setup Tool                          BinTec Access Networks 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 Subnetzmaske, 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

```
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            :  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

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals stellen Sie auf: **19 (Rijndael/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)

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            :  both
   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 Verändern Sie den auf: **23 (ESP(Rijndael/MD5))**
Heartbeats	Baut den Tunnel ab wenn der Partner nicht mehr reagiert Stellen Sie Heartbeats auf **both**

1.3.1e 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&**
- Geben Sie einen Ping von Ihrem Host in der Zentrale zum Host in der Filiale ab

Jetzt sollten Sie folgende Meldungen erhalten:

```
04:30:58 INFO/IPSEC: New Bundle -40 (Peer 1 Traffic 2)
04:30:58 INFO/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): created 192
.168.1.0/192.168.1.0:0 < any > 192.168.2.0/192.168.2.0:0 rekeyed 0
04:30:58 DEBUG/INET: dnsd: qry from 127.0.0.1:1064 id 75 "filiale.dyndns.org." A
 1
04:30:58 DEBUG/INET: dnsd: cache 62.10.10.20 for filiale.dyndns.org.
04:30:58 DEBUG/INET: dnsd: rsp to 127.0.0.1:1064 id 75 "filiale.dyndns.org." A 1
/0/0
04:30:59 DEBUG/INET: NAT: new outgoing session on ifc 300 prot 17 62.10.10.10:50
0/62.10.10.10:1023 -> 62.10.10.20:500
04:30:59 DEBUG/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): identified ip 62.10.10.
10 -> ip 62.10.10.20
04:30:59 INFO/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): Vendor ID: 62.10.10.20:5
00 (fqdn(any:0,[0..6]=filiale)) is 'BINTEC'
04:30:59 INFO/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): Vendor ID: 62.10.10.20:5
00 (fqdn(any:0,[0..6]=filiale)) is 'BINTEC Heartbeats Version 1'
04:30:59 INFO/IPSEC: P1: peer 1 (62.10.10.20) sa 1 (I): done id fqdn(any:0,[0..7
]=zentrale) -> id fqdn(any:0,[0..6]=filiale) AG[cf5ea38f 8aaa6e28 : 4ae27eda 3b7
a0be7]
04:30:59 DEBUG/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): SA 1 estab
lished ESP[2b342411] in[0] Mode tunnel enc blowfish-cbc(16) auth md5(16)
04:30:59 DEBUG/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): SA 2 estab
lished ESP[43bfc201] out[0] Mode tunnel enc blowfish-cbc(16) auth md5(16)
04:30:59 INFO/IPSEC: Activate Bundle -40 (Peer 1 Traffic 2)
04:30:59 DEBUG/INET: NAT: new outgoing session on ifc 300 prot 50 62.10.10.10:0/
62.10.10.10:0 -> 62.10.10.20:0
04:30:59 INFO/IPSEC: P2: peer 1 (62.10.10.20) traf 2 bundle -40 (I): established
  (62.10.10.10<->62.10.10.20) with 2 SAs life 28800 Sec/0 Kb rekey 23040 Sec/0 K
b Hb none
04:30:59 DEBUG/INET: NAT: new incoming session on ifc 300 prot 50 62.10.10.10:0/
62.10.10.10:0 <- 62.10.10.20:0
```

1.3.2 Einstellungen im Menü IPSEC -> Certificate and Key Management

Um einen privaten und einen öffentlichen Schlüssel zu erstellen, den Sie für den Zertifikatsrequest brauchen, müssen Sie in folgendes Untermenü:

IPSEC -> Certificate and Key Management -> Key Management -> CREATE

1.3.2a Schlüssel und Request erstellen

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][CERTMGMT][KEYS][CREATE]: IPsec Configuration - Create Keys     zentrale
------------------------------------------------------------------------------


     Description:           key1
     Algorithm:             rsa
     Key Size (Bits):       1024
     RSA Public Exponent:   65537









                    Create                              Exit
------------------------------------------------------------------------------
Enter string, max length = 255 chars
```

Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Description	Geben Sie dem Schlüssel einen Namen

Gehen Sie wie folgt vor:

- Unter Description geben Sie **key1** ein
- Gehen Sie auf **Create** (Die Erstellung kann einige Sekunden dauern)
- Verlassen Sie das Menü mit **Exit**
- Gehen Sie in das Untermenü **REQUEST CERT**

Zertifikatsanforderungen können Sie in diesem Menü erstellen:

IPSEC -> Certificate and Key Management -> Key Management -> REQUEST CERT

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC]..[ENROLL]: IPsec Configuration - Certificate Enrollment        zentrale
------------------------------------------------------------------------------
     Key to enroll:              1 (key1)

     Method:       Upload


     Subject Name: CN=Zentrale

     Subject Alternative Names (optional):
       Type   Value
       NONE
       NONE
       NONE

     Signing algorithm to use:   md5WithRSAEncryption
     Server:   192.168.1.2
     Filename: Zentrale.req                                      base64

                    Start                                Exit

------------------------------------------------------------------------------
```

Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Key to enroll	Geben Sie dem Schlüssel einen Namen
Method	Hier wählen Sie automatische oder manuelle Anforderung
Subject Name	Geben Sie Ihre Identifikation im X.500 Format an
Subject Alternative Names	Hier können Sie weitere Identifikationen angeben
Signing algorithm	Der Signatur Algorithmus
Server	Die IP Adresse vom TFTP Server
Filename	Der Dateiname des Requests

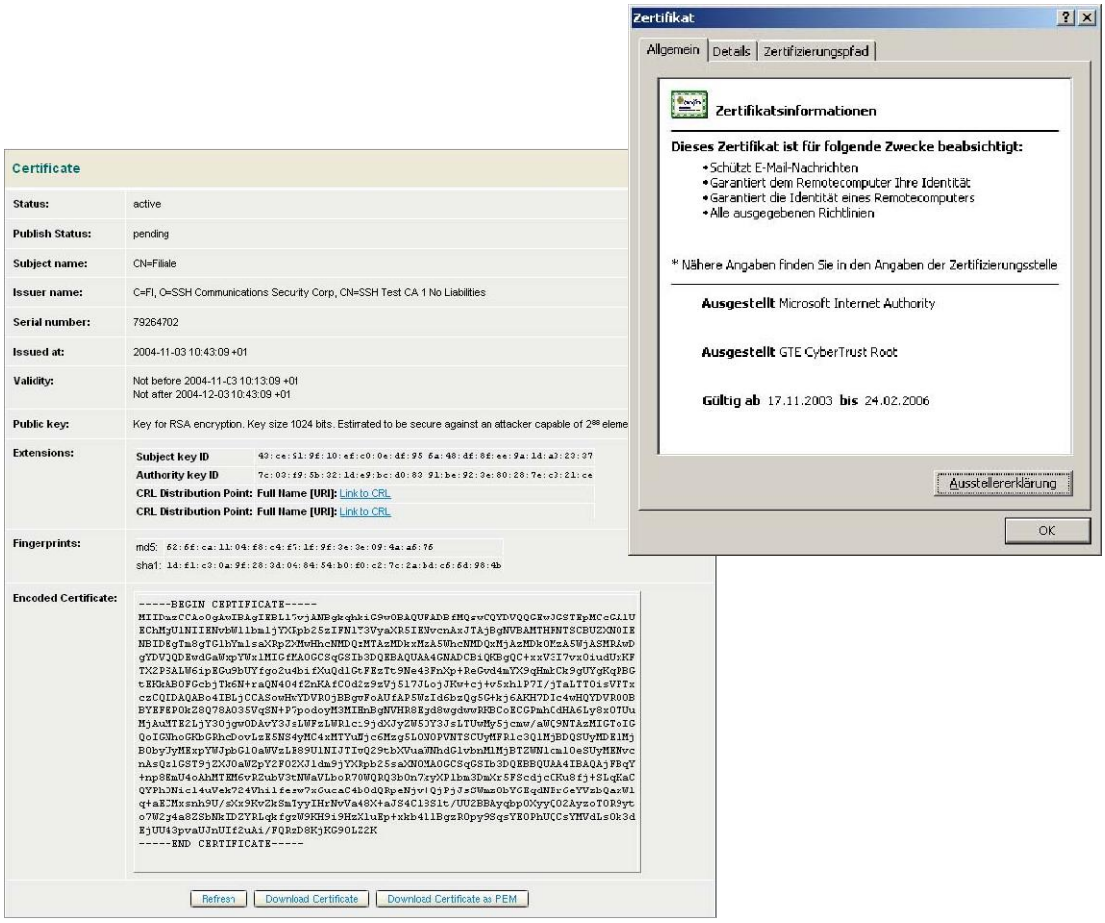
Gehen Sie folgendermassen vor, um Ihren Eintrag zu konfigurieren:

- Geben Sie bei „Key to enroll" Ihren gerade erstellten Schlüssel **key1** an
- Die Methode stellen Sie auf **Upload**
- Als Subject Name schreiben Sie **CN=Zentrale**
- Alle Alternative Subject Names stellen Sie auf **NONE**
- Den Signing algorithm belassen Sie auf: **md5WithRSAEncryption**
- Bei Server geben Sie die IP des TFTP Servers an: **192.168.1.2**
- Unter Filename geben Sie **Zentrale.req** an

Jetzt müssen Sie mit dem Zertifikats Request bei einer Zertifizierungsstelle ein Zertifikat anfordern. Der Request sieht ungefähr so aus:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBUjCBvAIBADATMREwDwYDVQQDEwhaZW50cmFsZTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA6B8S00i9Zcn7AxKcs+a44Vh/Nr10nXQ6XjOiknGmb4M1Vuw/
nqUn6YnCmlGJ1xFHrDTHa6dBa3Q/IVWd3ZL/dsGQcymB77JkKGVutySxu3nl6OHt
u7nUOZWjKfBuoZImJ4L/WaNxUM+/6bLpvMkc5WMnHrv8Ixot5sEVZU3Eu68CAwEA
AaAAMA0GCSqGSIb3DQEBBAUAA4GBAAyXiDjkrOgyWjqZjnGrw/RZHRrGyArkLLjy
GwEn3VFG8iE0i2gclfsor61zyHtFNtuaMKRvHV9845Yp++0p6GnHJVgXBvs9jALL
FCz5j6C2TXyKoVLhv4eYAKOCJX9OOK7+fipt6wP3/LgvEquoqaJh3jwqEcxnjmrr
6Z5hMFtE
-----END CERTIFICATE REQUEST-----
```

Das Zertifikat was die Zertifizierungsstelle ausstellt, müssen Sie nun in das Verzeichnis vom TFTP Server kopieren. Benennen Sie das Zertifikat **Zentrale.crt**. Das Zertifikat sieht in etwa so aus:



Sie brauchen noch das Zertifikat der Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Kopieren Sie auch das in das Verzeichnis vom TFTP Server. Benennen Sie das Zertifikat **Ca.crt**. Danach gehen sie in folgendes Menü, um Ihr eigenes Zertifikat in das IPsec Gateway zu importieren.

IPSEC -> Certificate and Key Management -> Own Certificates -> DOWNLOAD

1.3.2b Zertifikate importieren

```
VPN Access 25 Setup Tool                          BinTec Access Networks GmbH
[IPSEC][CERTMGMT][OWN][GETCERT]: IPsec Configuration - Get Certificate zentrale
------------------------------------------------------------------------------

     Import a Certificate/CRL using:  TFTP

      Type of certificate: Own Certificate









     Server:    192.168.1.2
     Name:      Zentrale.crt                              auto

                     START                              EXIT
------------------------------------------------------------------------------
```

Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Server	Hier geben Sie die IP Adresse vom TFTP Server an
Name	Hier kommt der Dateiname vom Zertifikat rein

Gehen Sie folgendermassen vor um Ihren Eintrag zu konfigurieren:

- Geben Sie bei Server **192.168.1.2** an
- Bei Name schreiben Sie **Zentrale.crt** rein
- Gehen Sie auf **START**, um das Zertifikat zu importieren
- Verlassen Sie die nächsten beiden Menüs mit **EXIT**

Gehen sie in folgendes Menü, um das Zertifikat der Zertifizierungsstelle in das IPsec Gateway zu importieren.

IPSEC -> Certificate and Key Management -> Certificate Authority Certificates -> DOWNLOAD

Das Importieren erfolgt genauso wie bei Ihrem eigenen Zertifikat. Nach dem Sie das Zertifikat der CA (**Ca.crt**) in das Gateway geladen haben bearbeiten Sie es und stellen Sie den Punkt **Type of certificate** auf: Certificate Authority **no CRLs**.

INFO
Sollten Sie CRL's verwenden wollen, müssen Sie noch die CRL Datei von der Zertifizierungsstelle in das VPN Gateway importieren.

1.3.2c Zertifikats Anpassungen

Um die zuvor mit Preshared Key konfigurierte Verbindung an Zertifikate anzupassen, müssen Sie in folgendes Menü gehen:

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 :  RSA Signatures
   Mode                 :   id_protect
   Heartbeats           :   both
   Block Time           :   0
   Local ID             :   <CN=Zentrale>
   Local Certificate    :   1 (Zentrale.crt)
   CA Certificates      :
   Nat-Traversal        :   enabled

   View Proposals >
   Edit Lifetimes >

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

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
Authentication Method	Hier wählen Sie die Authentifizierungs-Methode
Mode	Der Mode bestimmt die Methode des IKE Aufbaus
Heartbeats	Überprüft den VPN Partner auf Erreichbarkeit
Local ID	Hier tragen Sie die eigene Identifikation für das Gateway ein
Local Certificate	Hier wählen Sie das eigene Zertifikat aus

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals stellen Sie auf: **19 (Rijndael/MD5)**
- Authentication Method stellen Sie auf **RSA Signatures**
- Den Mode stellen Sie zurück auf **id_protect** da Sie Zertifikate einsetzen
- Heartbeats schalten Sie auf **both**
- Unter Local ID geben Sie **<CN=Zentrale>** ein. Das ist Ihr Subject Name vom Zertifikat
- Bei Local Certificate wählen Sie Ihr eigenes Zertifikat aus **1 (Zentrale.crt)**
- Nat-Traversal stellen Sie auf: **disabled**

Jetzt müssen Sie noch eine Anpassung in folgendem Menü machen:

IPSEC -> Configure Peers -> Edit

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

     Description:       filiale
     Admin Status:      up        Oper Status:    up

     Peer Address:      filiale.dyndns.org
     Peer IDs:          <CN=Filiale>


     IPSec Callback >
     Peer specific Settings >

     Virtual Interface: no
     Traffic List Settings >



                          SAVE                          CANCEL

------------------------------------------------------------------------------
Enter string, max length = 255 chars
```

Verändern Sie folgende Felder mit den angegebenen Werten:

Feld	**Wert**
Peer IDs	Hier tragen Sie den Subject Name des IPsec Partners ein, der im Zertifikat steht **<CN=Filiale>**

1.4 Ergebnis

Sie haben eine IPsec Verbindung mit Zertifikaten zwischen 2 Gateways konfiguriert. Dazu haben Sie dynamische IP Adressen in Kombination mit Dyndns auf Seiten des Providers verwendet. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite konfigurieren.

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&**
- Geben Sie einen Ping von Ihrem Host in der Zentrale zum Host in der Filiale ab

Jetzt sollten Sie folgende Meldungen erhalten:

```
14:24:39 INFO/IPSEC: New Bundle -253 (Peer 1 Traffic 2)
14:24:39 INFO/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): created 192.16
8.1.0/192.168.1.0:0 < any > 192.168.2.0/192.168.2.0:0 rekeyed 0
14:24:39 DEBUG/IPSEC: P1: peer 1 (filiale) sa 1 (I): identified ip 62.10.10.10 -
> ip 62.10.10.20
14:24:39 INFO/IPSEC: P1: peer 1 (filiale) sa 1 (I): Vendor ID: 62.10.10.20:500 (
No Id) is 'BINTEC'
14:24:39 INFO/IPSEC: P1: peer 1 (filiale) sa 1 (I): Vendor ID: 62.10.10.20:500 (
No Id) is 'BINTEC Heartbeats Version 1'
14:24:40 INFO/IPSEC: P1: peer 1 (filiale) sa 1 (I): done id der_asn1_dn(any:0,[0
..20]=CN=Zentrale) -> id der_asn1_dn(any:0,[0..19]=CN=Filiale) IP[828c005d ecf69
620 : cbffd735 3a37ec50]
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 1 establis
hed IPComP[00000002] in[1] Mode tunnel comp deflate
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 2 establis
hed IPComP[00000002] out[1] Mode tunnel comp deflate
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 3 establis
hed ESP[153b2914] in[0] Mode transport enc rijndael-cbc(16) auth md5(16)
14:24:40 DEBUG/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): SA 4 establis
hed ESP[5b3e75c2] out[0] Mode transport enc rijndael-cbc(16) auth md5(16)
14:24:40 INFO/IPSEC: Activate Bundle -253 (Peer 1 Traffic 2)
14:24:40 DEBUG/INET: NAT: new outgoing session on ifc 300 prot 50 62.10.10.10:0/
62.10.10.10:0 -> 62.10.10.20:0
14:24:40 INFO/IPSEC: P2: peer 1 (filiale) traf 2 bundle -253 (I): established  (
62.10.10.10<->62.10.10.20) with 4 SAs life 28800 Sec/0 Kb rekey 23040 Sec/0 Kb H
b both
14:24:40 DEBUG/INET: NAT: new incoming session on ifc 300 prot 50 62.10.10.10:0/
62.10.10.10:0 <- 62.10.10.20:0
```

INFO
Beachten Sie bitte, dass IPsec Verbindungen mit Zertifikaten nicht zustande kommen, wenn das Datum und die Zeit nicht richtig sind. Daher überprüfen Sie vor jeder Konfiguration das eingestellte Datum auf beiden IPsec Gateways.

1.6 Die wichtigsten Konfigurationsschritte im IPSEC Menü im Überblick

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

Feld	Menü	Wert
Description	Configure Peers > APPEND	Filiale
Peer Address	Configure Peers > APPEND	filiale.dyndns.org
Peer IDs	Configure Peers > APPEND	<CN=Filiale>

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

Feld	Menü	Wert
Description	Configure Peers > Traffic List Settings > APPEND	Filiale
Local IP	Configure Peers > Traffic List Settings > APPEND	192.168.1.0 /24
Remote IP	Configure Peers > Traffic List Settings > APPEND	192.168.2.0 /24

---------- IP Routing ----------

Feld	Menü	Wert
IP Transit Network	Configure Peers > Interface IP Settings > Basic IP	no
Local IP Address	Configure Peers > Interface IP Settings > Basic IP	192.168.1.1
Remote IP Address	Configure Peers > Interface IP Settings > Basic IP	192.168.2.0
Remote Netmask	Configure Peers > Interface IP Settings > Basic IP	255.255.255.0

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

Feld	Menü	Wert
Proposal	IKE (Phase 1) Defaults > edit > ADD	19 (Rijndael/MD5)
Authentication Method	IKE (Phase 1) Defaults > edit > ADD	RSA Signatures
Mode	IKE (Phase 1) Defaults > edit > ADD	id_protect
Local ID	IKE (Phase 1) Defaults > edit > ADD	<CN=Zentrale>
Local Certificate	IKE (Phase 1) Defaults > edit > ADD	1 (Zentrale.crt)

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

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