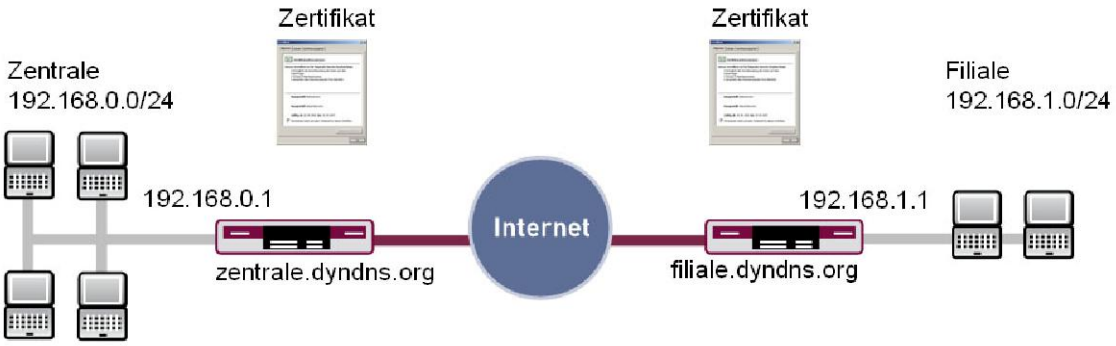
1. IPSec Verbindung zwischen 2 Gateways mit Zertifikaten



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPSec Verbindung mit dynamischen IP-Adressen auf beiden Seiten beschrieben. Zur Authentifizierung verwenden Sie anstelle des Preshared Keys Zertifikate. Außerdem werden Sie einen Eintrag für Ihren DynDNS Namen in dem Gateway konfigurieren. 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.
- Für beide Gateways müssen Sie einen DynDNS Namen registriert haben.
- Sie brauchen eine Zertifizierungsstelle, wo Sie Ihre Zertifikate anfordern können.

1.3 Konfiguration

Die Anleitung konfiguriert ein Beispiel auf Seiten der Zentrale.
Um IPSec zu konfigurieren, müssen Sie im Folgenden Menü Einstellungen vornehmen:

VPN -> IPSec

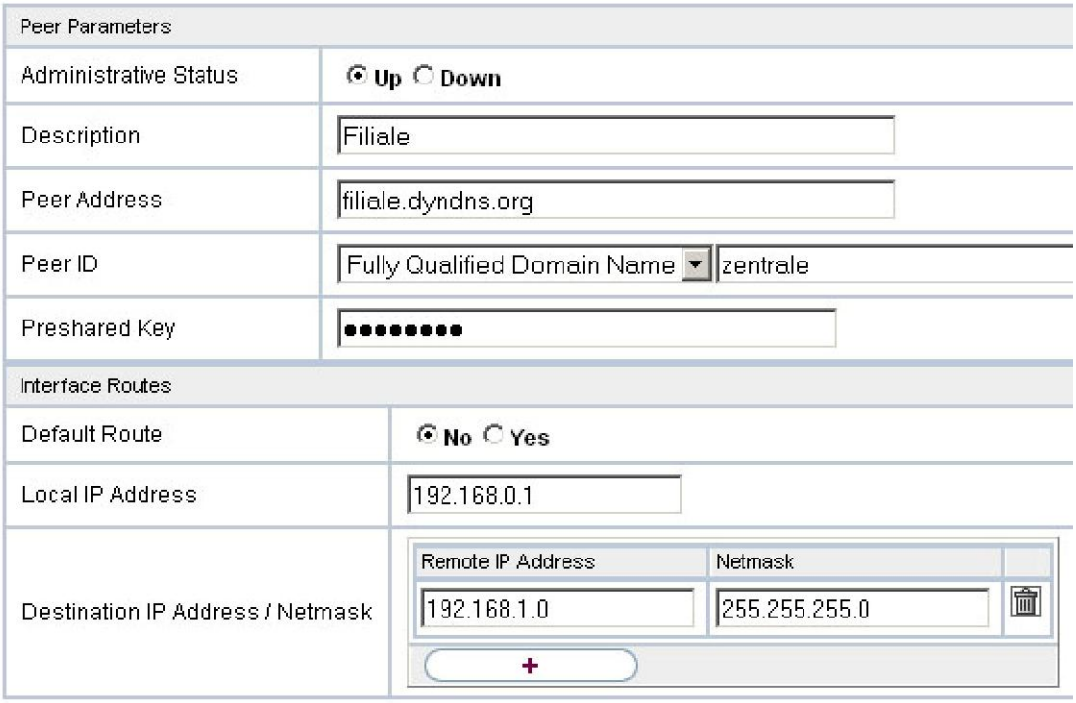
In dem Untermenü "IPSec Peers" haben Sie die Möglichkeit mit **New** Verbindungspartner für IPSec hinzuzufügen.

INFO
Da die Zertifikats Implementierung sehr komplex ist, wird empfohlen erst eine funktionsfähige IPSec Verbindung z.B. mit dynamischen IP-Adressen zu konfigurieren und diese dann mit Zertifikaten zu erweitern und anzupassen.

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 Address	Hier geben Sie die Gateway IP Adresse oder Dyndns Namen des Verbindungspartners ein.
Peer ID	Hier tragen Sie eine Identifikation des Partners ein (In der Filiale unter Local ID eingetragen).
Preshared Key	Das gemeinsame Passwort von beiden Gateways.
Local IP Address	Hier steht Ihre lokale IP Adresse vom Ethernet Interface.
Destination IP Address / Netmask	Hier konfigurieren Sie das zu erreichende Partner Netz.

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

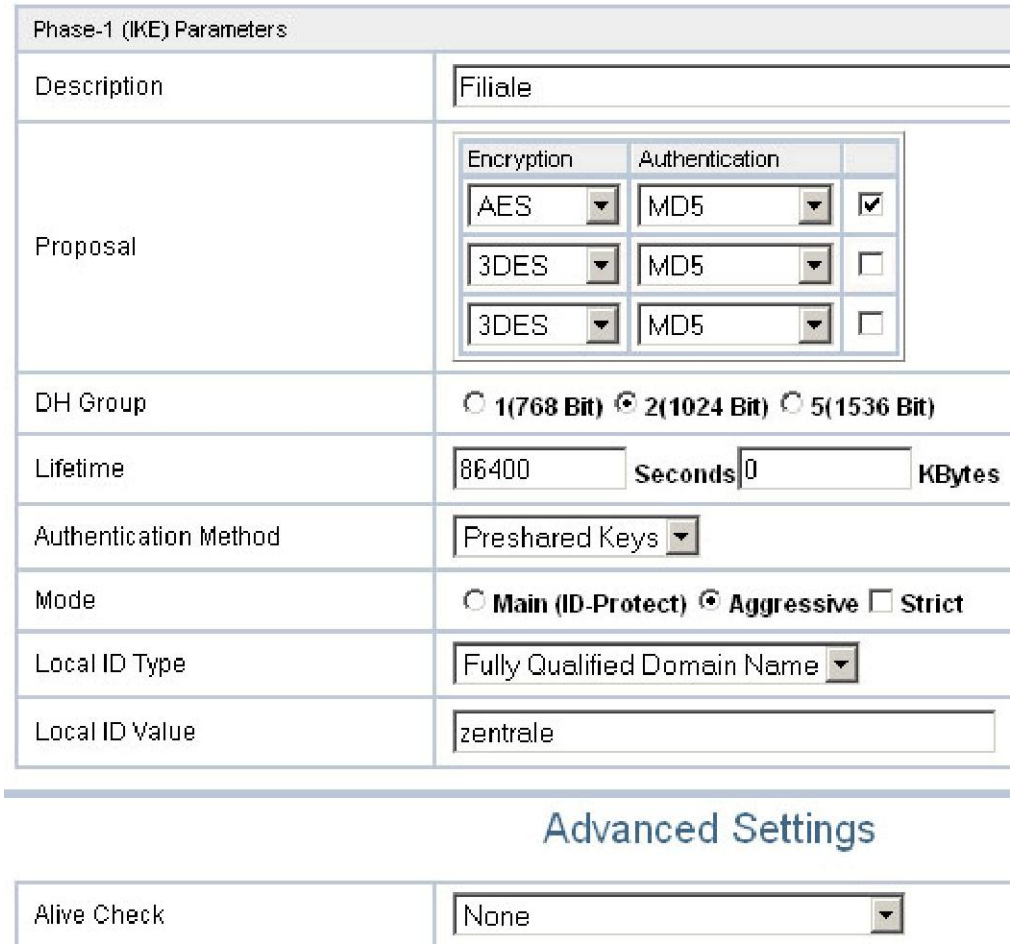
- Benennen Sie den Eintrag unter Description: **z.B. Filiale**.
- Bei Peer Address geben Sie: **filiale.dyndns.org** an.
- Bei Peer ID geben Sie: **Fully Qualified Domain Name / filiale** an.
- Im Preshared Key tragen Sie **z.B. bintec** als Passwort ein.
- Unter Local IP Address tragen Sie **192.168.0.1** ein
- Unter Destination IP Address / Netmask fügen Sie mit **+** einen Eintrag hinzu.
- Tragen Sie in die Felder **192.168.1.0 / 255.255.255.0** ein.
- Bestätigen Sie Ihre Eingaben mit **OK**.

INFO
Da Sie später Zertifikate einsetzen werden für Ihre Verbindung, spielt für die temporäre Verbindung die Komplexität der Preshared Keys keine Rolle.

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.

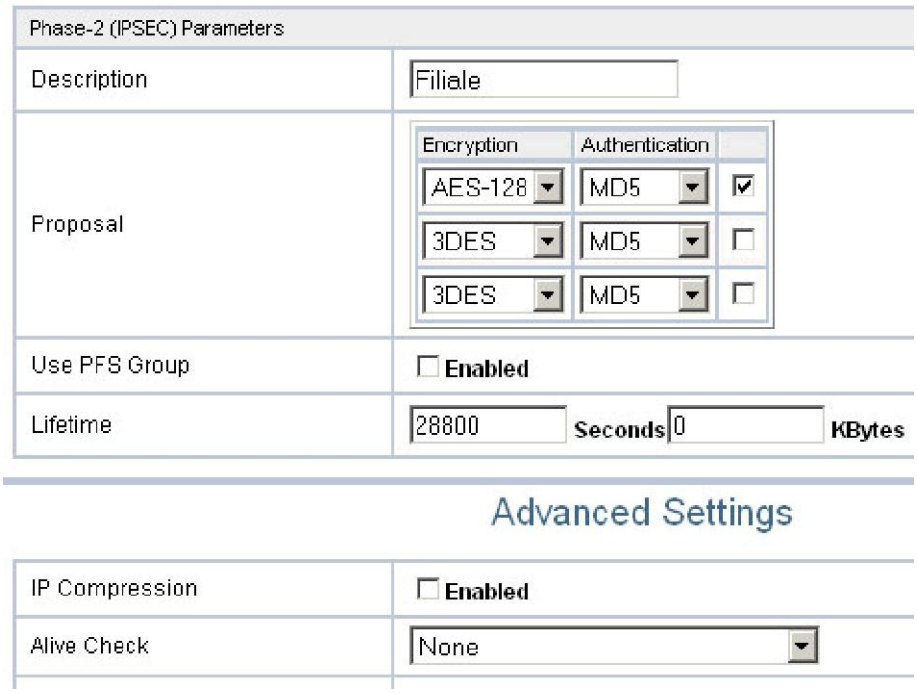
Konfigurieren Sie das Phase-1 Profil mit folgenden Parametern:

- Bei Description geben Sie: **z.B. Filiale** 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.

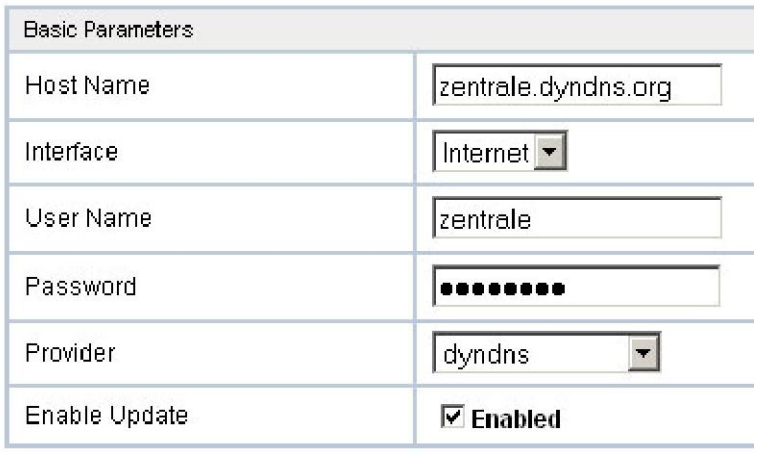
Konfigurieren Sie das Phase-2 Profil mit folgenden Parametern:

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

1.3.4 DynDNS konfigurieren

Erstellen Sie einen neuen Eintrag im Router für Ihren registrierten DynDNS Namen. Gehen Sie dazu in folgendes Menü:

Local Services -> DynDNS Client -> DynDNS Update -> New



Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Hostname	Tragen Sie hier den kompletten Hostnamen ein, den Sie registriert haben.
Interface	Wählen Sie das Internet Interface aus.
Username	Geben Sie Ihren Benutzernamen an.
Password	Geben Sie Ihr Passwort an.

Provider	Hier wählen Sie Ihren DynDNS Provider aus.
Enable Update	Aktivieren oder Deaktivieren Sie den Eintrag.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

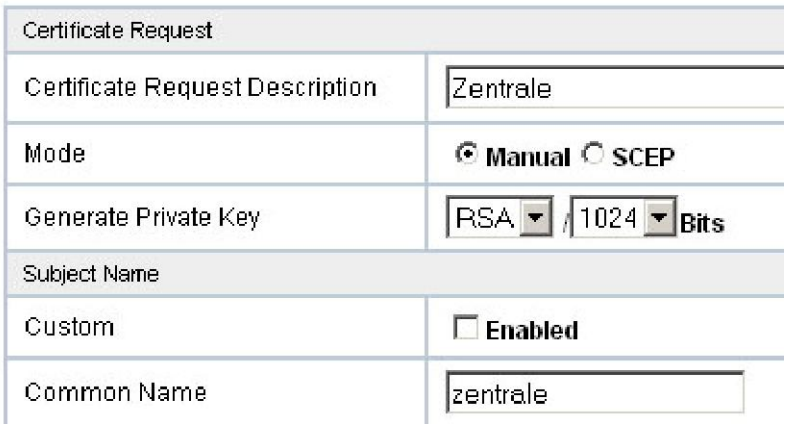
- Unter Hostname tragen Sie: **z.B. zentrale.dyndns.org** ein.
- Wählen Sie bei Interface: **z.B. Internet** aus.
- Tragen Sie unter Username: **z.B. zentrale** ein.
- Bei Password geben Sie: **z.B. passwort** an.
- Der Provider ist: **dyndns**.
- Enable Update: **aktivieren** Sie.

Nach Ihrer Konfiguration und dem Erfolgreichen Test, ob die Verbindung funktioniert, sollten Sie übergehen in das Anfordern und Importieren der Zertifikate.

1.3.4a Zertifikate anfordern und importieren

Gehen Sie in folgendes Menü, um Zertifikat-Requests zu erstellen:

VPN -> Certificates -> Requests



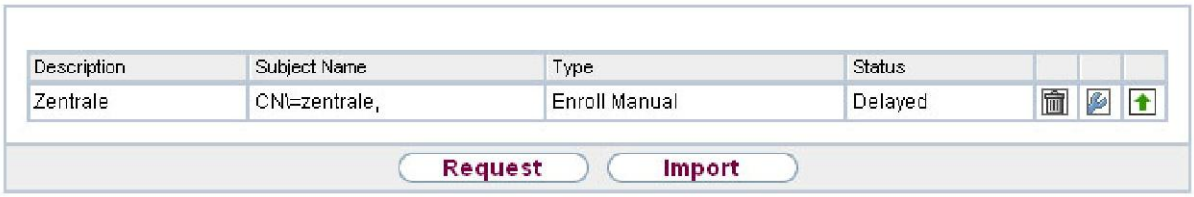
Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Certificate Request Description	Geben Sie der Zertifikatsanforderung einen Namen.
Mode	Bestimmen Sie manuell oder automatisch Zertifikate anfordern.
Common Name	Tragen Sie die Identifikation der Zentrale ein.

INFO
Unter Subject Name können Sie wesentlich mehr Identifikationsmerkmale nach dem X.500 Standard für die Zentrale angeben. Der Einfachheit halber wird hier nur einer verwendet.

Gehen Sie folgendermaßen vor, um den Eintrag zu konfigurieren:

- Unter Certificate Request Description geben Sie: **z.B. Zentrale** ein.
- Den Mode setzen Sie auf: **Manual**.
- Bei Common Name tragen Sie: **z.B. zentrale** ein.
- Bestätigen Sie Ihre Eingaben mit: **OK**.



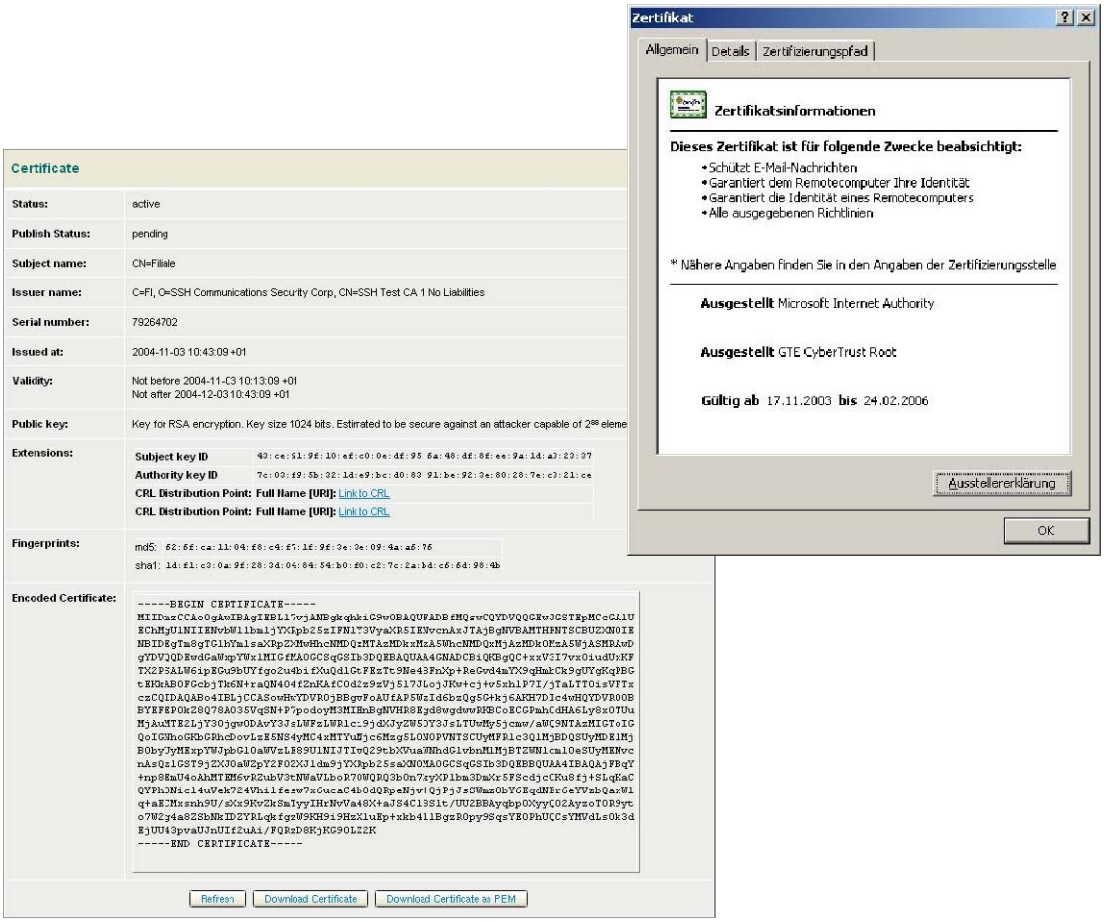
Im Hintergrund generiert das IPSec Gateway den privaten und den öffentlichen Schlüssel. Jetzt sollte sich ein Fenster öffnen, wo Sie den Zertifikat-Request auf Ihrem Computer unter dem Namen **Zentrale.req** speichern. Optional besteht die Möglichkeit über den rechten grünen Pfeil die Datei zu sichern.

Jetzt müssen Sie mit dem Zertifikat-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-----
```

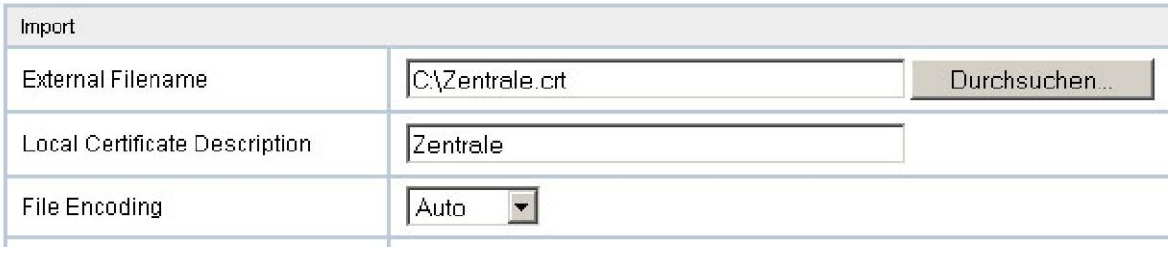
Das Zertifikat was die Zertifizierungsstelle ausstellt, müssen Sie nun auf den Computer kopieren. Benennen Sie das Zertifikat **Zentrale.crt**.
Sie brauchen noch das Zertifikat der Zertifizierungsstelle, die das Zertifikat ausgestellt hat. Kopieren Sie auch das auf den Computer. Benennen Sie das Zertifikat **Ca.crt**.

Das Zertifikat sieht in etwa so aus:



Danach gehen sie in folgendes Menü, um Ihr eigenes Zertifikat und das Zertifizierungsstellen Zertifikat in das IPSec Gateway zu importieren:

VPN -> Certificates -> Import



Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
External Filename	Das ist der Pfad und Dateiname des Zertifikats.
Local Certificate Description	Geben Sie dem Zertifikat einen Namen für den internen gebrauch.

Gehen Sie folgendermaßen vor, um das eigene Zertifikat zu importieren:

- Unter External Filename geben Sie: **z.B. C:\Zentrale.crt** ein.
- Bei Local Certificate Description geben Sie **z.B. Zentrale** an.
- Bestätigen Sie Ihre Eingaben mit: **OK**.

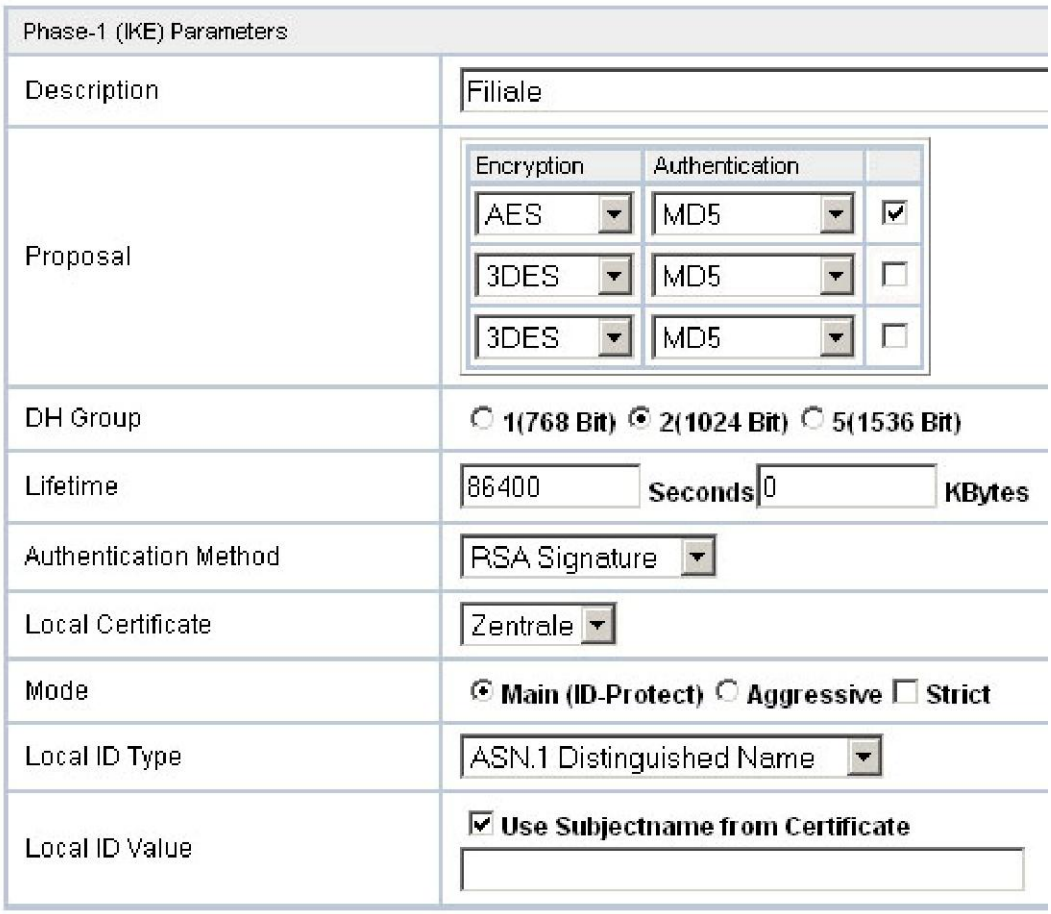
Gehen Sie folgendermaßen vor, um das Zertifikat der Zertifizierungsstelle zu importieren:

- Unter External Filename geben Sie: **z.B. C:\Ca.crt** ein.
- Bei Local Certificate Description geben Sie **z.B. CA** an.
- Bestätigen Sie Ihre Eingaben mit: **OK**.

1.3.4b IPSec Verbindung anpassen

Um Zertifikate nutzen zu können, müssen Sie in folgendem Menü Anpassungen vornehmen:

VPN -> IPSec -> Phase-1 Profiles



Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Authentication Method	Hier wählen Sie die Authentifizierungsmethode aus.
Local Certificate	Wählen Sie das eigene Zertifikat aus.
Mode	Wählen Sie den Verbindungsmodus aus.
Local ID Type	Bestimmen Sie die Art der Identifikation.
Local ID Value	Tragen Sie die eigene Identifikation ein.

Gehen Sie folgendermaßen vor, um den Eintrag zu verändern:

- Unter Authentication Method wählen Sie: **DAS Signature**.
- Als Local Certificate wählen Sie: **Zentrale**.
- Den Mode stellen Sie auf: **Main (ID-Protect)**.
- Stellen Sie Local ID Type auf: **ASN.1 Distinguished Name**.
- Unter Local ID Value setzen Sie den Haken: **Use Subjectname from Certificate**.

Ein weiteres Menü erfordert Anpassungen für Zertifikate:

VPN -> IPSec -> IPSec Peers -> Edit

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Peer ID	Hier tragen Sie die Identifikation des Partners ein (In der Filiale unter Local ID eingetragen).

Gehen Sie folgendermaßen vor, um den Eintrag zu ändern:

- Unter Peer ID geben Sie **z.B. ASN.1 Distinguished Name / CN=filiale** ein.

1.4 Ergebnis

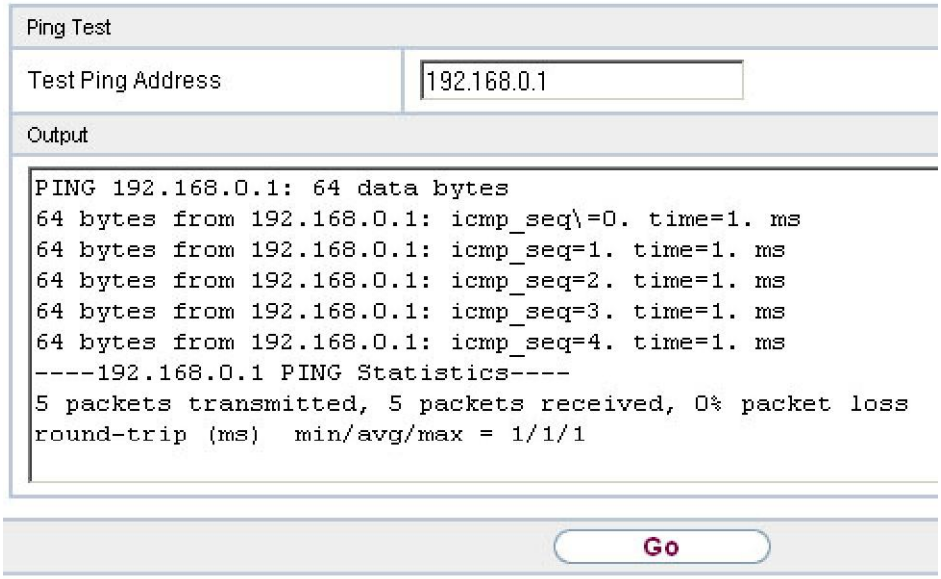
Sie haben eine IPsec Verbindung mit Zertifikaten zwischen 2 Gateways konfiguriert. Dazu haben Sie dynamische IP Adressen in Kombination mit DynDNS auf Seiten des Providers verwendet. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter auf der Filialseite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

1.5 Kontrolle

Um die IPSec Verbindung zu testen, gehen Sie in folgendes Menü:

Maintenance -> Diagnostics -> Ping Test

Wenn Sie eine IP-Adresse der Remote Seite angeben, sollten Sie eine ähnliche Meldung erhalten:



INFO
Sollte die Verbindung nicht Ordnungsgemäß aufgebaut werden, könnte das mit dem lokalen Datum oder Uhrzeit des Routers zusammenhängen. Überprüfen Sie das aktuelle Datum damit die Zertifikate gültig sind.

1.6 Konfigurationsschritte im Überblick

IPSec Peer Parameter

Feld	Menü	Wert
Description	VPN -> IPSec -> IPSec Peers -> New	z.B. Filiale
Peer Address	VPN -> IPSec -> IPSec Peers -> New	filiale.dyndns.org
Peer ID	VPN -> IPSec -> IPSec Peers -> New	ASN.1 / <CN=filiale>
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	192.168.1.0/ 255.255.255.0

Phase 1 Profiles

Feld	Menü	Wert
Description	VPN -> IPSec -> Phase-1 Profiles -> New	z.B. Filiale
Proposal	VPN -> IPSec -> Phase-1 Profiles -> New	AES/MD5
Authentication Method	VPN -> IPSec -> Phase-1 Profiles -> New	RSA Signature
Mode	VPN -> IPSec -> Phase-1 Profiles -> New	Main (ID-Protect)
Local ID Type	VPN -> IPSec -> Phase-1 Profiles -> New	ASN.1 Distinguished Name
Local ID Value	VPN -> IPSec -> Phase-1 Profiles -> New	Use Subjectname from Certificate
Alive Check	VPN -> IPSec -> Phase-1 Profiles -> New	None

Phase 2 Profiles

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