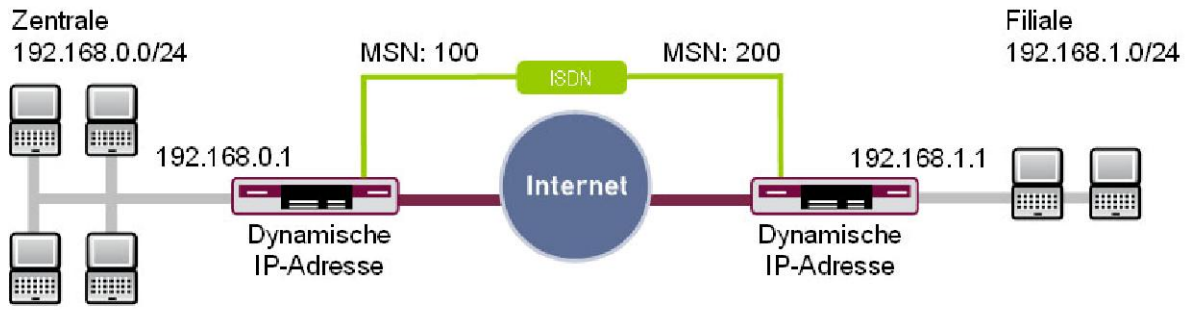
1. IPsec Verbindung mit Übertragung der IP-Adresse im D-/B-Kanal



1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPSec Verbindung mit dynamischen IP Adressen beschrieben. Die IP-Adresse wird vor dem Verbindungsaufbau über ISDN zum VPN Partner übertragen. 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 der Gateways.
- Für das IPSec Gateway ist ein Bootimage ab Version 7.4.4 zu verwenden.
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang zum Provider.
- Beide Geräte müssen am ISDN angeschlossen sein und eine MSN für IPSec zur Verfügung haben.

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

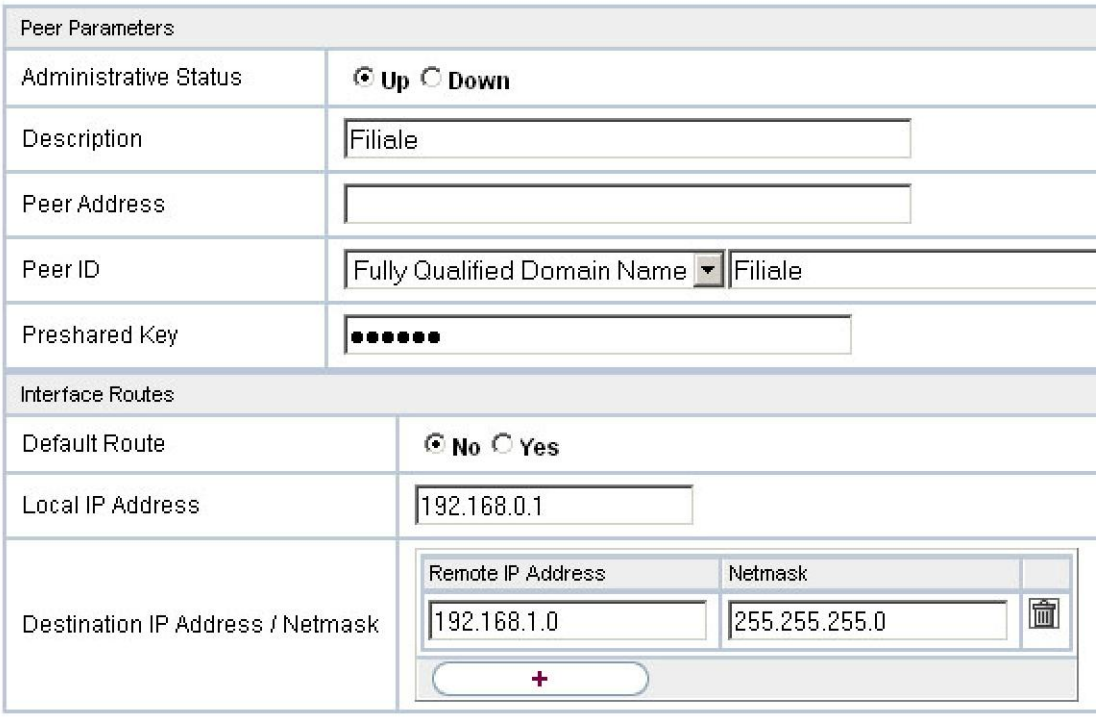
In dem Untermenü "IPSec Peers" haben Sie die Möglichkeit mit **New** Verbindungspartner für IPSec hinzuzufügen.

INFO
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 Address	Hier geben Sie die Partner IP-Adresse ein (Bleibt in diesem Szenario frei).
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:

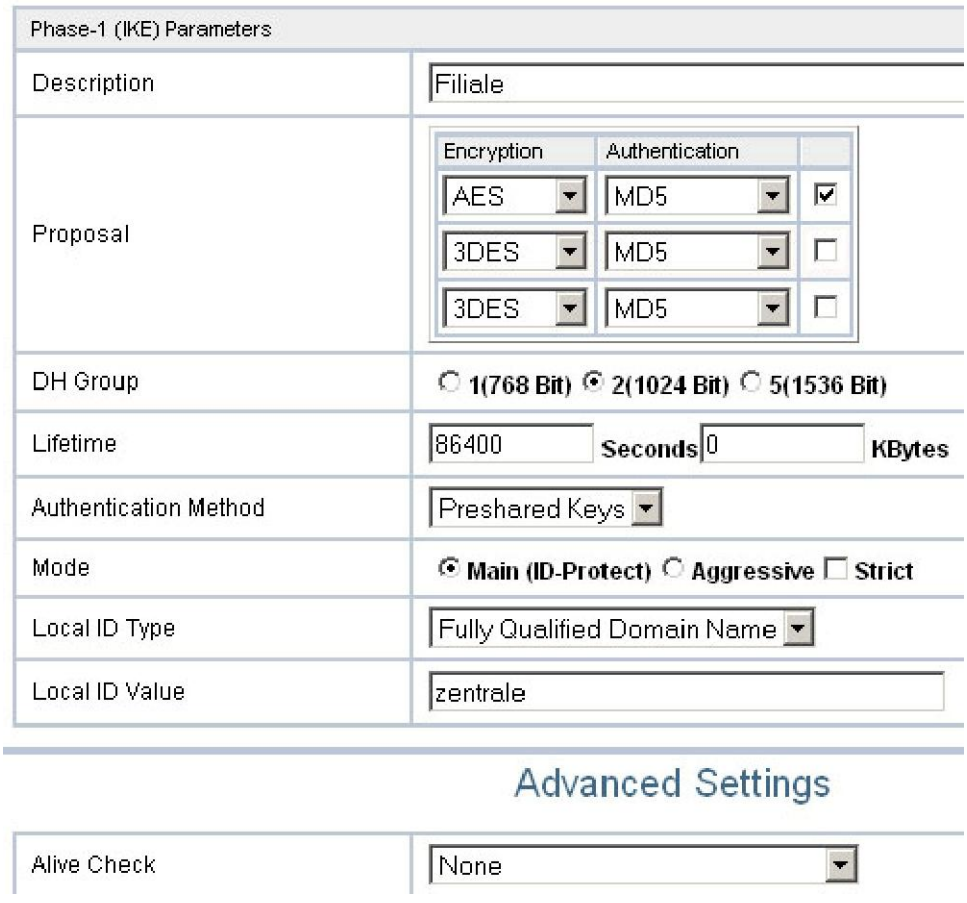
- Benennen Sie den Eintrag unter Description: **z.B. Filiale**.
- Peer Address lassen Sie: **frei**.
- Bei Peer ID geben Sie: **Fully Qualified Domain Name / filiale** an.
- Im Preshared Key tragen Sie **z.B. bintec** als Passwort ein.
- Unter Local IP Address tragen Sie **192.168.0.1** ein.
- Unter 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
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.

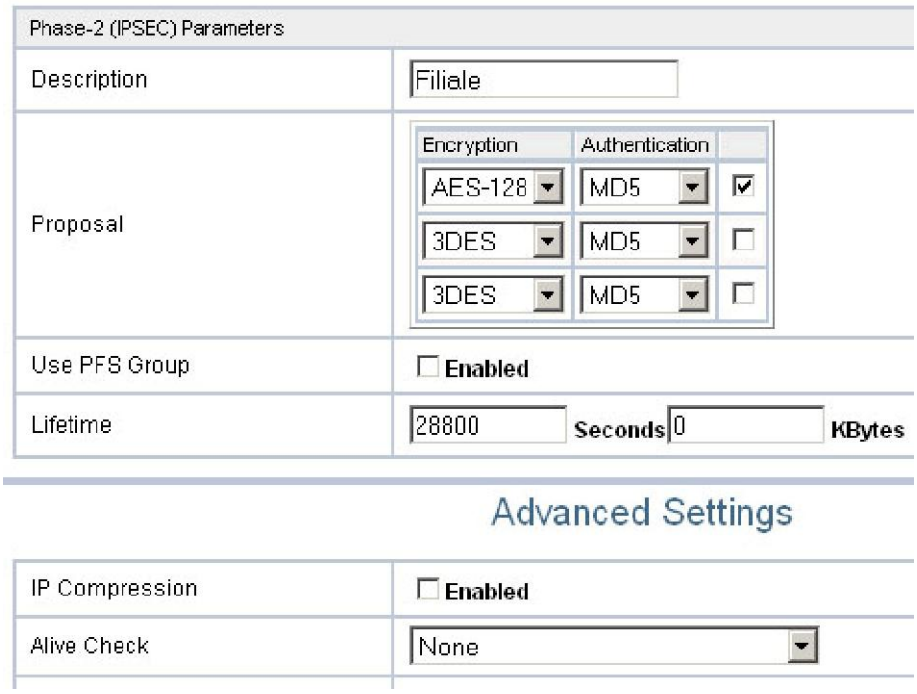
Konfigurieren Sie das Phase 1 Profil mit folgenden Parametern:

- Bei Description geben Sie: **z.B. Filiale** ein.
- Die Proposal markieren Sie mit einem **haken** und stellen Sie auf: **AES/MD5**.
- Den Mode stellen Sie auf **Main (ID-Protect)** 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:

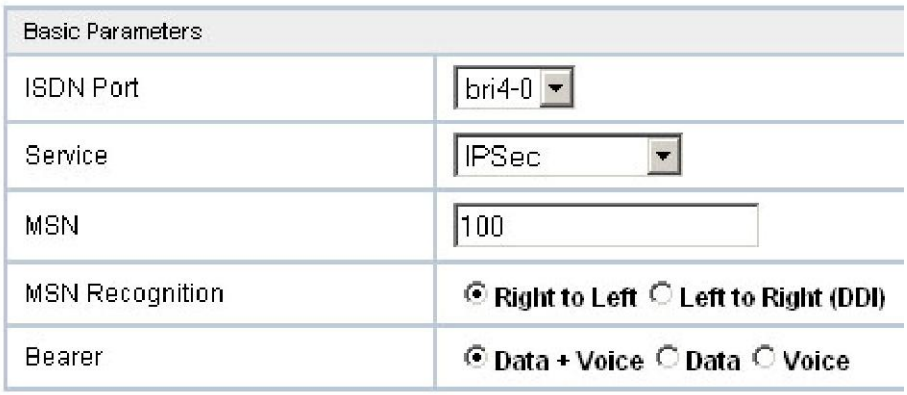
- Bei Description geben Sie: **z.B. Filiale** ein.
- Die Proposal markieren Sie mit einem **haken** und stellen Sie auf: **AES-128/MD5**.
- Alive Check setzen Sie auf: **None**.

1.3.4 Rufnummern konfigurieren

1.3.4a Eigene MSN

Gehen Sie in folgendes Menü, um eine Ihrer Rufnummern einer IPSec Verbindung zuzuordnen:

Physical Interfaces -> ISDN Ports -> MSN Configuration -> New



Folgende Felder sind hierbei relevant:

Feld	Bedeutung
ISDN Port	Wählen Sie hier das ISDN Interface aus.
Service	Bestimmen Sie den Dienst für die Rufnummer.
MSN	Tragen Sie hier Ihre eigene Rufnummer ein, die für eingehende IPSec Verbindungen gedacht ist.

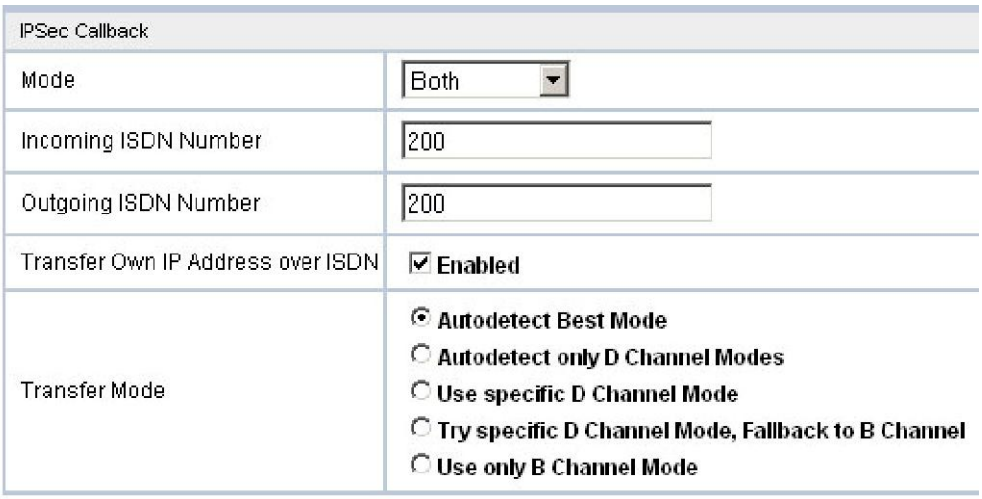
Konfigurieren Sie den Eintrag mit folgenden Parametern:

- Bei ISDN Port wählen Sie: **bri4-0** aus.
- Den Service stellen Sie auf: **IPSec**.
- Bei MSN tragen Sie die Rufnummer ein: **z.B. 100**.

1.3.4b Partner MSN

Damit Sie IPSec Verbindungen vom Partner entgegennehmen und die IP-Adresse über den D/B-Kanal übermitteln können, müssen in folgendes Menü gehen und Veränderungen vornehmen:

VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings



Folgende Felder sind hierbei relevant:

Feld	**Bedeutung**
Mode	Wählen Sie die Richtung des IPSec Callbacks aus.
Incoming ISDN Number	Dies ist die Partner MSN, die bei einem eingehenden Ruf übermittelt wird.
Outgoing ISDN Number	Dies ist die Partner MSN, die bei einem ausgehenden Ruf angewählt wird.
Transfer Own IP-Address over ISDN	Bestimmen Sie, ob die IP-Adresse über ISDN übermittelt wird.
Transfer Mode	Wählen Sie die Art der Übermittlung aus.

Konfigurieren Sie den Eintrag mit folgenden Parametern:

- Den Mode setzen Sie auf: **Both**.
- Bei Incoming ISDN Number tragen Sie: **z.B. 200** ein.
- Unter Outgoing ISDN Number tragen Sie: **z.B. 200** ein.
- Den Transfer Own IP Address over ISDN setzen Sie auf: **Enabled**.
- Unter Transfer Mode wählen Sie die Option: **Autodetect Best Mode**.

1.4 Ergebnis

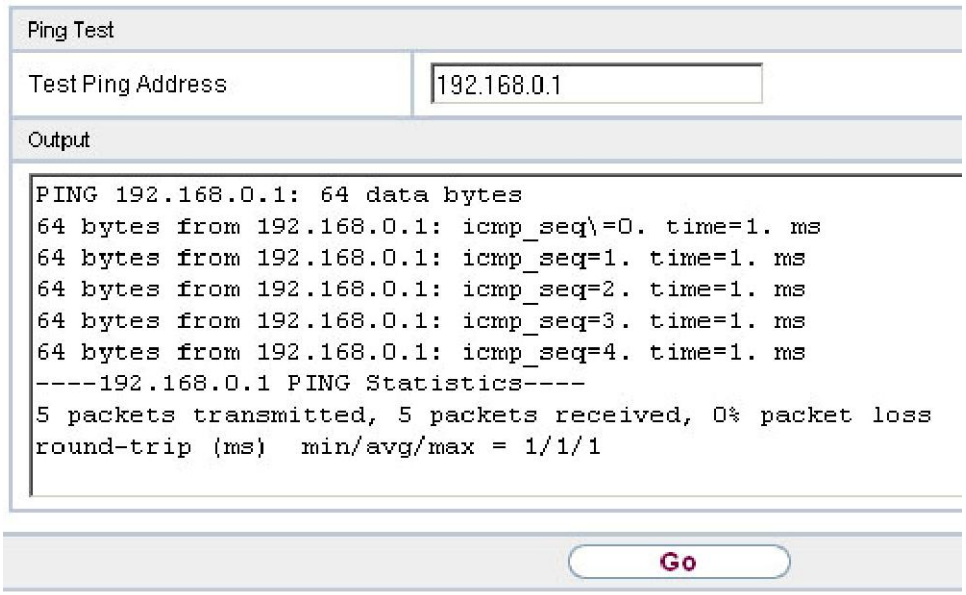
Sie haben eine IPsec Verbindung mit dynamischen IP-Adressen zwischen 2 Gateways konfiguriert. Die IP-Adresse der Zentrale wurde vor dem Verbindungsaufbau über ISDN zum VPN Partner übertragen. Da die Anleitung nur das Beispiel auf der Seite der Zentrale zeigt, müssen Sie auch die Verbindungsparameter 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:



1.6 Konfigurationsschritte im Überblick

IPSec Peer Parameter

Feld	Menü	Wert
Description	VPN -> IPSec -> IPSec Peers -> New	z.B. Filiale
Peer ID	VPN -> IPSec -> IPSec Peers -> New	FQDN / 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
Mode	VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings	Both
Incoming ISDN Number	VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings	z.B. 200
Outgoing ISDN Number	VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings	z.B. 200
Transfer Own IP Address over ISDN	VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings	Enabled
Transfer Mode	VPN -> IPSec -> IPSec Peers -> New -> Advanced Settings	Autodetect Best Mode

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
Mode	VPN -> IPSec -> Phase-1 Profiles -> New	Main (ID-Protect)
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. Filiale
Proposal	VPN -> IPSec -> Phase-2 Profiles -> New	AES-128/MD5
Alive Check	VPN -> IPSec -> Phase-2 Profiles -> New	None

MSN Configuration

Feld	Menü	Wert
ISDN Port	Physical Interfaces -> ISDN Ports -> MSN Configuration -> New	bri4-0
Service	Physical Interfaces -> ISDN Ports -> MSN Configuration -> New	IPSec
MSN	Physical Interfaces -> ISDN Ports -> MSN Configuration -> New	z.B. 100