PPTP

Bintec Benutzerhandbuch - VPN Access Reihe
Version 1.0

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.bintec.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für Bintec-Gateways finden Sie unter www.bintec.de.

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

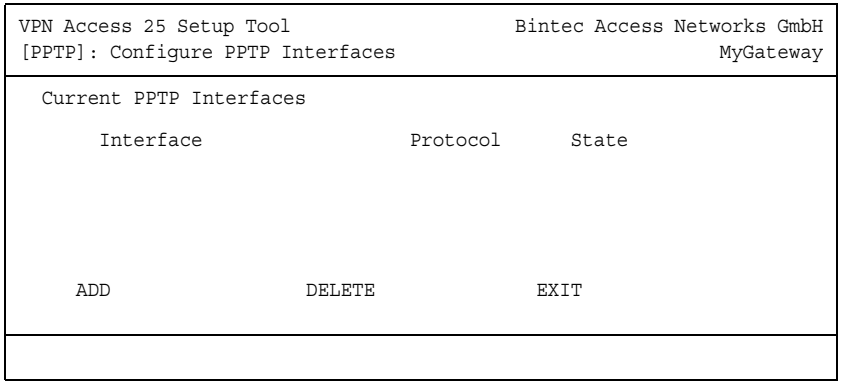
Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Menü PPTP

Im Folgenden werden die Felder des Menüs *PPTP* beschrieben.



Zur Absicherung des Datenverkehrs über eine vorhandene IP-Verbindung kann mittels Point-to-Point-Tunneling-Protokoll (=PPTP) ein verschlüsselter PPTP-Tunnel aufgebaut werden.

Der Aufbau eines Tunnels

Zunächst wird an beiden Standorten eine Verbindung zu einem ISP (=Internet Service Provider) aufgebaut. Wenn diese Verbindungen stehen, wird über das Internet ein Tunnel zum PPTP Partner, hier dann mit PPTP, aufgebaut.

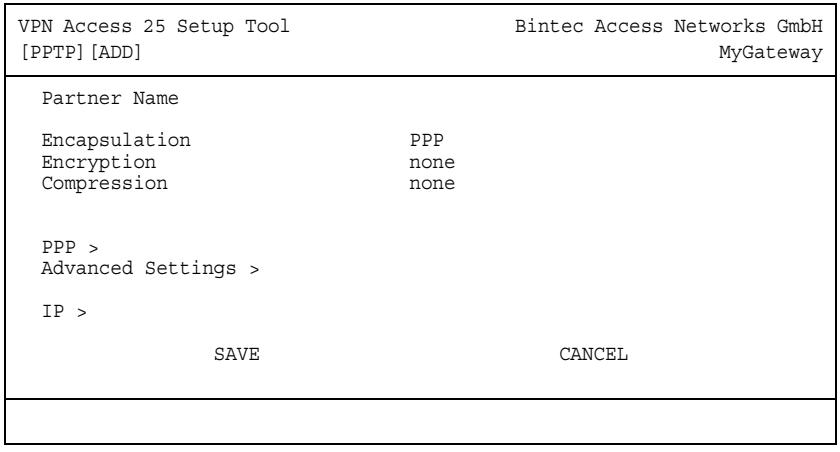
Kontrollverbindung

Für diesen Vorgang baut das PPTP-Subsystem eine Kontrollverbindung zwischen den Tunnelendpunkten auf. Diese übermittelt Steuerungsdaten, die die Verbindung zwischen den zwei PPTP-Tunnelendpunkten aufbauen, aufrechterhalten und beenden.

Datenstrom

Sobald diese Kontrollverbindung aufgebaut ist, überträgt das PPTP die in GRE-Pakete (GRE = Generic Routing Encapsulation) eingepackten Nutzdaten.

Die Konfiguration der PPTP-Interfaces erfolgt im Menü ***PPTP ➜ ADD/EDIT.***



Das Menü besteht aus folgenden Feldern:

Feld	Wert
Partner Name	Geben Sie einen beliebigen Namen ein, um den PPTP Partner eindeutig zu benennen. In diesem Feld darf die erste Ziffer keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden. Die Länge ist auf maximal 25 Zeichen beschränkt.
Encapsulation	Die Enkapsulierungsmethode, die angewendet werden soll. Derzeit ist nur PPP möglich.
Encryption	Definiert die Datenverschlüsselung, die angewendet werden soll. Mögliche Werte: siehe “Auswahlmöglichkeiten von ENCRYPTION” auf Seite 6

Feld	Wert
Compression	Legt die Komprimierung fest, die angewendet werden soll und ist nur aktiv bei analoger Konfiguration auf der Gegenstelle. Mögliche Werte: ■ *none* (Defaultwert): keine Komprimierung ■ *STAC*: STAC-Datenkomprimierung (nach RFC 1974, 1967) ■ *MS-STAC*: Microsoft-Variante der STAC-Datenkomprimierung ■ *MPPC*: Microsoft Point-to-Point Compression Eine Kombination von Verschlüsselung und Kompression ist nur mit einer (beliebigen) MPPE-Verschlüsselung und MPPC möglich. Für die Verwendung von STAC und MPPC ist eine kostenlose Lizenz erforderlich, Sie erhalten diese im Service-Bereich von www.bintec.de.

Tabelle 1-1: Felder im Menü ***PPTP***

ENCRYPTION enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
none (Defaultwert)	keine Verschlüsselung
MPPE 40	MPPE Version 1 und 2 mit 40-Bit-Schlüssel
MPPE V2 40	MPPE Version 2 mit 40-Bit-Schlüssel
MPPE V2 40 (RFC 3078)	MPPE Version 2 mit 40-Bit-Schlüssel gemäß RFC 3078: für Microsoft Clients ab Windows 2000 (ggf. mit Service Packs)
MPPE V1 40 only	MPPE Version 1 mit 40-Bit-Schlüssel
MPPE 56	MPPE Version 1 und 2 mit 56-Bit-Schlüssel

Wert	Bedeutung
MPPE V2 56	MPPE Version 2 mit 56-Bit-Schlüssel
MPPE V2 56 (RFC 3078)	MPPE Version 2 mit 56-Bit-Schlüssel gemäß RFC 3078: für Microsoft Clients ab Windows 2000 (ggf. mit Service Packs)
MPPE V1 56 only	MPPE Version 1 mit 56-Bit-Schlüssel
DES 56	DES mit 56-Bit-Schlüssel
Blowfish 56	Blowfish mit 56-Bit-Schlüssel
MPPE 128	MPPE Version 1 und 2 mit 128-Bit-Schlüssel
MPPE V2 128	MPPE Version 2 mit 128-Bit-Schlüssel
MPPE V2 128 (RFC 3078)	MPPE Version 2 mit 128-Bit-Schlüssel gemäß RFC 3078: für Microsoft Clients ab Windows 2000 (ggf. mit Service Packs)
MPPE V1 128 only	MPPE Version 1 mit 128-Bit-Schlüssel
MPPE V1 128 (MS compatible mode)	Microsoft-kompatible MPPE Version 1 mit 128-Bit-Schlüssel für Authentifizierung MS-CHAP V1 (nicht konform zu RFC 3079)
MPPE V2 128 (MS compatible mode)	Microsoft-kompatible MPPE Version 2 mit 128-Bit-Schlüssel für Authentifizierung MS-CHAP V1 (nicht konform zu RFC 3079)
DES3 168	Triple DES mit 168-Bit-Schlüssel
Blowfish 168	Blowfish mit 168-Bit-Schlüssel

Tabelle 1-2: Auswahlmöglichkeiten von ***ENCRYPTION***

Das Menü führt weiterhin in die folgenden Untermenüs:

- ***PPP***
- ***ADVANCED SETTINGS***
- ***IP***
- ***WAN NUMBERS***: nur bei ***CALLBACK*** = *yes (callback via PPTP VPN)*.

2 Untermenü PPP

Im Folgenden wird das Untermenü *PPP* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][ADD][PPP]: PPP Settings (Zentrale)                    MyGateway

    Authentication              CHAP + PAP
    Partner PPP ID
    Local PPP ID                VPN Access 25
    PPP Password

    Keepalives                  off
    Link Quality Monitoring     off


            OK                              CANCEL
```

Im Untermenü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***PPP*** werden spezifische ➤➤ **PPP**-Einstellungen für das jeweilige PPTP-Partner-Interface vorgenommen. Mit diesen Einstellungen führt das Gateway die Authentifizierungsverhandlung mit der Gegenstelle aus.

Das Menü ***PPP*** besteht aus folgenden Feldern:

Feld	Wert
Authentication	Authentifizierungsprotokoll Mögliche Werte: siehe “Auswahlmöglichkeiten im Feld AUTHENTICATION” auf Seite 9
Partner PPP ID	Kennung des PPTP Partners
Local PPP ID	Kennung Ihres Gateways Defaultwert ist der Eintrag aus ***LOCAL PPP ID*** im Menü ***SYSTEM***.
PPP Password	Passwort

Feld	Wert
Keepalives	Einstellung der Funktion PPP-Keepalive zur Überprüfung der Erreichbarkeit der PPP-Gegenstelle. Mögliche Werte: ■ *off* (Defaultwert) - Deaktiviert Keepalive. ■ *on* - Aktiviert Keepalive. Die PPP-Keepalive-Funktion schickt alle drei Sekunden ein Paket zur Gegenstelle. Wenn das Paket fünf mal unbeantwortet bleibt, wird das Interface auf *dormant* gesetzt.
Link Quality Monitoring	Aktiviert PPP Link Quality Monitoring nach RFC 1989. Mögliche Werte: ■ *off* (Defaultwert) ■ *on:* Nur notwendig in Ausnahmefällen

Tabelle 2-1: Felder im Menü ***PPP***

Das Feld ***AUTHENTICATION*** enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
PAP	Nur ➤➤ **PAP** (Password Authentication Protocol) ausführen, Paßwort wird unverschlüsselt übertragen.
CHAP	Nur ➤➤ **CHAP** (Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Paßwort wird verschlüsselt übertragen.
CHAP + PAP (Defaultwert)	Vorrangig CHAP, sonst PAP ausführen.
MS-CHAP	Nur MS-CHAP Version 1 (Microsoft Challenge Handshake Authentication Protocol) ausführen.
CHAP + PAP + MS-CHAP	Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom WAN Partner geforderte Authentifizierungsprotokoll ausführen (MS-CHAP Version 1 oder 2 möglich).
MS-CHAP V2	Nur MS-CHAP Version 2 ausführen.
none	Kein PPP-Authentifizierungsprotokoll ausführen.

Tabelle 2-2: Auswahlmöglichkeiten im Feld ***AUTHENTICATION***

3 Untermenü Advanced Settings

Im Folgenden wird das Untermenü *ADVANCED SETTINGS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][EDIT][ADVANCED]: Advanced Settings (Zentrale)          MyGateway


  Callback                                  no
  Static Short Hold (sec)                   20

  Delay after Connection Failure (sec)      300
  PPTP Mode                                 PPTP PNS


  Extended Interface Settings (optional) >

  Special Interface Types                   none

            OK                                        CANCEL
```

Die Einstellungen im Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ermöglichen die Festlegung weiterer individueller Eigenschaften des PPTP Partners.

Das Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
Callback	Ermöglicht den Aufbau eines PPTP Tunnels über das Internet mit einem PPTP Partner, selbst wenn dieser augenblicklich nicht online ist. In der Regel wird mittels ISDN-Ruf der PPTP Partner aufgefordert, online zu gehen und eine PPTP-Verbindung aufzubauen. Mögliche Werte: ■ *yes (callback via PPTP VPN)*: aktiviert die Funktion Callback ■ *no* (Defaultwert): deaktiviert die Funktion Callback Beachten Sie, dass Sie die entsprechende Option auf den Gateways beider Partner aktivieren müssen. Für diese Funktion wird in der Regel ein ISDN-Anschluss benötigt. Die Geräte der **VPN Access** Serie sind mit unterschiedlichen Schnittstellen ausgestattet. Ob Ihr Gateway über ein ISDN-Interface verfügt, lesen Sie bitte auf dem Datenblatt oder im Handbuch-Kapitel **Technische Daten** nach. Ohne ISDN ist Callback nur in Spezialanwendungen zu aktivieren.
Static Short Hold (sec)	Mit statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten ➤➤ Nutz-**Datenpakets** und Abbau der Verbindung vergehen soll. Zur Verfügung stehen Werte von *-1* bis *3600* (Sekunden). Ein Wert von *-1* bedeutet, dass die Verbindung nach einem Abbruch sofort wieder aufgebaut wird, *0* deaktiviert den Shorthold. Defaultwert ist *20*.

Feld	Wert
Delay after Connection Failure (sec)	Gibt an, für wie viele Sekunden nach einem fehlgeschlagenen Verbindungsaufbau kein erneuter Versuch durch das **VPN Access** Gateway unternommen wird (=Blocktimer). Defaultwert ist *300*.
PPTP Mode	Hier geben Sie die Rollenverteilung des PPTP-Interface an. Mögliche Werte: ■ *PPTP PNS* (Defaultwert): PPTP network server; hiermit weisen Sie dem PPTP-Interface die Rolle des PPTP-Servers zu. ■ W*indows PPTP client mode*: Hiermit weisen Sie dem PPTP-Interface die Rolle des PPTP-Clients zu.
Special Interfaces Types	Diese Option erlaubt eine spezielle Nutzung des Interfaces. Mögliche Werte: ■ *none* (Defaultwert): Kein spezieller Typ ausgewählt. ■ *dialin only*: Das Interface ist nur für eingehende Verbindungen und für von der Gegenstelle initiierten Callback zugelassen. ■ *Call-by-Call (dialin only)*: Das Interface wird als Multi-User PPTP Partner definiert, wodurch sich mehrere Clients sich mit gleichem Username und Passwort anmelden können. Nur sinnvoll bei ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***BASIC IP SETTINGS*** ➜ ***IP ADDRESS NEGOTIATION*** = *dynamic server*.

Tabelle 3-1: Felder im Menü ***ADVANCED SETTINGS***

3.1 Untermenü Extended Interface Settings (optional)

Im Folgenden wird das Untermenü *EXTENDED INTERFACE SETTINGS (OPTIONAL)* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[WAN][EDIT][ADVANCED][EXTIF]: Extended Interface              MyGateway
                              Settings (Zentrale)

   Optional Extended Interface Settings not configured yet!


   Encryption Key Negotiation           static
   Encryption Key (TX)
   Encryption Key (RX)

          SAVE                                          CANCEL
```

In dem Untermenü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** ➜ ***EXTENDED INTERFACE SETTINGS*** können zusätzliche Einstellungen zur Funktion ***ENCRYPTION KEY NEGOTIATION*** vorgenommen werden.

Nach erstmaligem Sichern der Konfiguration in diesem Menü wird die Meldung *Optional Extended Interface Settings not configured yet!* ausgeblendet und die Option **Delete Configuration** angezeigt.

Das Menü ***EXTENDED INTERFACE SETTINGS (OPTIONAL)*** besteht aus folgenden Feldern:

Feld	Wert
Encryption Key Negotiation	Definiert, ob der Schlüssel für eine ggf. in ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ENCRYPTION*** aktivierte Verschlüsselung automatisch generiert oder statisch definiert wird. Mögliche Werte: ■ *authentication* (Defaultwert): Schlüssel wird vom **VPN Access** Gateway automatisch generiert. ■ *static*: Schlüssel wird statisch definiert und muss unter ***ENCRYPTION KEY (TX)*** und ***ENCRYPTION KEY (RX)*** eingetragen werden.
Encryption Key (TX)	(nur bei ***ENCRYPTION KEY NEGOTIATION*** = *static*) Schlüssel im hexadezimalen Format zur Verschlüsselung ausgehender Daten (muss mit dem Eintrag unter ***ENCRYPTION KEY (RX)*** beim Verbindungspartner übereinstimmen).
Encryption Key (RX)	(nur bei ***ENCRYPTION KEY NEGOTIATION*** = *static*) Schlüssel im hexadezimalen Format zur Entschlüsselung eingehender Daten (muss mit dem Eintrag unter ***ENCRYPTION KEY (TX)*** beim Verbindungspartner übereinstimmen).

Tabelle 3-2: Felder im Menü ***EXTENDED INTERFACE SETTINGS (OPTIONAL)***

4 Untermenü WAN Numbers

Im Folgenden werden die Felder des Untermenüs *WAN NUMBERS* beschrieben.

Das Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***WAN NUMBERS*** erscheint nur, wenn in ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***ADVANCED SETTINGS*** Callback aktiviert wurde (siehe “Callback” auf Seite 12).

Hier sind die aktuell eingetragenen Rufnummern des PPTP-Partners für die Funktion Callback aufgelistet. Weitere Nummern werden über die Schaltfläche ***ADD*** hinzugefügt. Bestehende Einträge werden durch Auswahl des jeweiligen Listeneintrags bearbeitet.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][ADD][WAN NUMBERS][ADD]: Add or Change                  MyGateway
                                WAN Numbers (Zentrale)

 Number
 Direction                          outgoing

 Advanced Settings >

 ISDN Ports to use  <X> Slot 0 Auxiliary        <X> Slot 0 ISDN S0


            SAVE                                      CANCEL
```

Das Menü ***WAN NUMBERS*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Number	Rufnummer des PPTP Partners

Feld	Wert
Direction	Definiert, ob ***NUMBER*** für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte: ■ *outgoing* (Defaultwert): Für ausgehende initiale Rufe zum PPTP-Partner, um von diesem den PPTP-Tunnel aufbauen zu lassen. ■ *both (CLID)*: Für eingehende und ausgehende Rufe. ■ *incoming (CLID):* Zur Identifizierung eines eingehenden initialen Rufes des PPTP Partners, um vom eigenen Gateway einen PPTP-Tunnel aufbauen zu lassen. Die Calling Party Number des eingehenden Rufes wird mit der unter ***NUMBER*** eingetragenen Nummer verglichen. Die Calling Party Number eines Anrufers wird u.a. in ***MONITORING & DEBUGGING ➜ ISDN MONITOR*** als ***REMOTE NUMBER*** angezeigt.

Feld	Wert
ISDN Ports to use	Nur bei Geräten mit ISDN S0-Anschluss. Über welche Schnittstellen Ihr Gateway verfügt, entnehmen Sie bitte dem Datenblatt zu der **VPN Access** Gerätereihe auf www.bintec.de. Definiert die Verbindungsart für den Callback: ■ Slot 0 Auxiliary ■ Slot 0 ISDN S0 Mit *X* (Defaultwert) wird der jeweilige Eintrag aktiviert, kein Eintrag deaktiviert die Option. Beachte: Wenn ein Modem an der AUX-Schnittstelle des Gateways angeschlossen ist, aktivieren Sie hier nur die für Callback gewünschte Verbindungsart. Im Standardfall wird hierbei ISDN gewählt. AUX sollte nur in Spezialanwendungen aktiviert sein.

Tabelle 4-1: Felder im Menü ***WAN NUMBERS***

Hinweis

Wenn das Gateway an eine TK-Anlage angeschlossen ist, bei der für eine Amtsholung eine führende "0" gewählt wird, müssen Sie diese führende "0" bei der Einwahlnummer berücksichtigen.

Wildcards

Beim Eintragen von ***NUMBER*** können Sie entweder die Rufnummer Ziffer für Ziffer eintragen oder einzelne Ziffern oder Gruppen von Ziffern durch Wildcards ersetzen. Damit kann ***NUMBER*** für verschiedene Rufnummern zutreffen.

Die Benutzung der in der folgenden Tabelle dargestellten Wildcards wirkt sich unterschiedlich für eingehende und ausgehende Rufe aus:

Wildcard	Bedeutung		Beispiel		
	Eingehende Rufe	Ausgehende Rufe	Number	Das Gateway akzeptiert eingehende Rufe z.B. mit:	Ausgehende Rufe
*	Entspricht einer Gruppe von keiner bis mehreren Ziffern.	Wird ignoriert.	123*	123, 1234, 123789	123
?	Entspricht genau einer Ziffer.	Wird durch 0 ersetzt.	123?	1234, 1238, 1231	1230
[a-b]	Definiert einen Bereich von passenden Ziffern.	Die erste Ziffer des definierten Bereiches wird verwendet.	123[5-9]	1235, 1237, 1239	1235
[^a-b]	Definiert einen Bereich von verbotenen Ziffern.	Die erste Ziffer nach dem definierten Bereich wird verwendet.	123[^0-5]	1236, 1238, 1239	1236
{ab}	Entspricht einer Gruppe von optionalen Ziffern.	Wird verwendet.	{00}1234	001234 und 1234	001234

Tabelle 4-2: Wildcards für ein- und ausgehende Rufe

Hinweis

Wenn die Calling Party Number eines eingehenden Rufes sowohl mit ***NUMBER*** eines PPTP-Partners mit Wildcards als auch mit ***NUMBER*** eines PPTP-Partners ohne Wildcards übereinstimmt, dann wird immer der Eintrag ohne Wildcards genutzt.

4.1 Untermenü Advanced Settings

Im Folgenden wird das Untermenü PPTP ➜ ADD/EDIT ➜ WAN Numbers ➜ ADD/EDIT ➜ *ADVANCED SETTINGS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][EDIT][WAN NUMBERS][ADD][ADVANCED]: Advanced Settings  MyGateway

Closed User Group                 none

            OK                                      CANCEL
```

Das **VPN Access** Gateway unterstützt die Nutzung des Dienstemerkmals "Geschlossene Benutzergruppe", das Sie bei Ihrer Telefongesellschaft für Ihren ISDN-Anschluss beantragen können. Damit wird die externe/interne Erreichbarkeit durch die Vermittlungsstellen überwacht und geregelt.

Wenn keine "Geschlossene Benutzergruppe" definiert ist, steht im Feld ***CLOSED USER GROUP*** (=CUG) der Wert *none* (Defaultwert). Um eine Geschlossene Benutzergruppe zu aktivieren, wählen Sie *specify*. In das sich öffnende Feld wird der CUG-Index eingetragen. Informationen zu CUG erhalten Sie von Ihrer Telefongesellschaft.

5 Untermenü IP

Im Folgenden wird das Untermenü *IP* beschrieben.

In dem Untermenü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** werden u.a. Routing-Einstellungen spezifisch für einen PPTP-Partner vorgenommen.

Das Menü bietet Zugang zu den Untermenüs:

- ***BASIC IP-SETTINGS***
- ***MORE ROUTING***
- ***ADVANCED SETTINGS.***

5.1 Untermenü Basic IP-Settings

Im Folgenden werden die Felder des Untermenüs *BASIC IP-SETTINGS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][EDIT][IP][BASIC]: IP-Settings (Zentrale)              MyGateway

Dynamic PPTP VPN                        no
Identification by IP Address            no
PPTP VPN Partner's IP Address           193.127.100.1
    via IP Interface                    AUTO


Local IP Address                        192.168.100.1

IP Address Negotiation                  static

Default Route                           no

Remote IP Address                       192.168.200.0
Remote Netmask                          255.255.255.0


          SAVE                                  CANCEL
```

Damit IP-Pakete zwischen zwei PPTP-Tunnelendpunkten übertragen werden können, muss das Gateway die Route zu dem jeweiligen PPTP-Partner ken-

nen. In diesem Menü können Sie die grundlegende Route festlegen oder eine Default Route zum PPTP-Partner generieren.

Das Menü ***BASIC IP-SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
Dynamic PPTP VPN	Ihr Gateway unterstützt PPTP-Tunnel auch zu Gegenstellen mit dynamischen IP-Adressen. Dazu muss der jeweilige PPTP-Partner über einen z. B. via DynDNS-Provider auflösbaren Hostnamen verfügen. Mögliche Werte: ■ *yes*: Aktiviert die Funktion. In ***PPTP VPN PARTNER'S IP ADDRESS*** kann ein DynDNS-Name eingegeben werden. ■ *no* (Defaultwert): Deaktiviert die Funktion. In ***PPTP VPN PARTNER'S IP ADDRESS*** wird eine IP-Adresse eingegeben.
Identification by IP Address	Nur für ***DYNAMIC PPTP VPN*** = *no*. ■ *yes*: Der VPN-Partner soll anhand seiner IP-Adresse identifiziert werden. ■ *no* (Defaultwert)
PPTP VPN Partner's IP Address	Die IP Adresse des PPTP-Partners. Bei einem PPTP-Tunnel über das Internet muss dies eine feste offizielle IP-Adresse sein. Wenn Sie für ***DYNAMIC PPTP VPN*** *yes* gewählt haben, müssen Sie hier einen auflösbaren Hostnamen eingeben. Geben Sie dennoch eine IP-Adresse ein, wird ***DYNAMIC PPTP VPN*** auf *no* zurückgesetzt und der PPTP-Partner anhand der eingegebenen IP-Adresse gesucht.

Feld	Wert
via IP Interface	Dieses Feld wird angezeigt, wenn in ***PPTP VPN PARTNER'S IP ADDRESS*** eine IP Adresse eingetragen wurde. Hier wählen Sie das IP Interface aus, über das Pakete zur PPTP-Gegenstelle transportiert werden. Defaultwert ist *AUTO*.
Use Gateway	Dieses Feld wird angezeigt, wenn in ***VIA IP INTERFACE*** ein ETH-Interface ausgewählt wird. Definiert, ob der PPTP-Tunnel über ein Gateway realisiert wird. Standardmässig ist hier *no* eingestellt und sollte nur in Spezialfällen geändert werden.
Gateway IP Address	Nur für ***USE GATEWAY*** = *yes* IP Adresse des zwischengeschalteteten Gateways.
Local PPTP VPN IP Address	Dieses Feld wird angezeigt, wenn in ***VIA IP INTERFACE*** ein ETH-Interface ausgewählt wird und ***USE GATEWAY*** = *no* gesetzt ist. IP-Adresse Ihres Gateways für die PPTP-Anbindung. Bei einem PPTP-Tunnel ist dieses eine offizielle IP-Adresse.
Local IP Address	Nur für ***IP ADDRESS NEGOTIATION*** = *static.* Hier weisen Sie dem PPTP-Interface eine IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse des Gateways verwendet wird.

Feld	Wert
IP Address Negotiation	Hier wählen Sie aus, wie die interne Quelladresse des Gateways bestimmt wird. Mögliche Werte: ■ *static* - (Defaultwert) Feste Vergabe der IP-Adresse in ***LOCAL IP ADDRESS***. ■ *dynamic client* - Ihr Gateway erhält dynamisch eine IP-Adresse von der PPTP Gegenstelle. ■ *dynamic server* - Das Gateway vergibt der PPTP-Gegenstelle dynamisch eine IP-Adresse.
Enable NAT	Nur für ***IP ADDRESS NEGOTIATION*** = *dynamic client.* Definiert, ob Network Address Translation (=NAT) für diese Verbindung aktiviert wird. Mögliche Werte: ■ *yes*: NAT ist aktiviert. ■ *no* (Defaultwert): NAT ist deaktiviert.
Default Route	Nur für ***IP ADDRESS NEGOTIATION*** = *static* oder *dynamic client.* Definiert, ob die Route zum PPTP Partner als Default-Route festgelegt wird. Mögliche Werte: ■ *yes*: Die Route zu diesem PPTP-Partner wird als Default-Route festgelegt. ■ *no* (Defaultwert): Die Route zu diesem PPTP-Partner wird nicht als Default-Route festgelegt.

Feld	Wert
Remote IP Address	Nur für ***IP ADDRESS NEGOTIATION*** = *static* und ***DEFAULT ROUTE*** = *no.* Hier geben Sie die IP-Adresse des LANs des PPTP-Partners ein.
Remote Netmask	Nur für ***IP ADDRESS NEGOTIATION*** = *static* und ***DEFAULT ROUTE*** = *no.* Netzmaske zu ***REMOTE IP ADDRESS***.

Tabelle 5-1: Felder im Menü ***BASIC IP-SETTINGS***

5.2 Untermenü More Routing

Im Folgenden werden die Felder des Untermenüs *MORE ROUTING* beschrieben.

Wenn für einen spezifischen PPTP Partner eine Route in ***BASIC IP-SETTINGS*** eingegeben wurde, wird automatisch ein Routing-Eintrag in der Routing-Tabelle Ihres Gateways erzeugt. Im Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** erscheint das Untermenü ***MORE ROUTING***. In diesem Menü können Sie die Routing-Einträge eines spezifischen PPTP-Partners ändern und weitere hinzufügen.

Im Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***MORE ROUTING*** sind die IP-Routen des spezifischen PPTP Partners aufgelistet:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][EDIT][IP][ROUTING]: IP Routing (Zentrale)              MyGateway

 The flags are:  U (Up), D (Dormant), B (Blocked),
                 G (Gateway Route), I (Interface Route),
                 S (Subnet Route), H (Host Route), E (Extended Route)

 Destination   Gateway       Mask           Flags Met.  Interface  Pro
 192.168.200.1 192.168.100.1 255.255.255.0   DG    0     Zentrale   loc




   ADD              ADDEXT            DELETE             EXIT
```

Unter ***FLAGS*** wird der aktuelle Status (*Up* – Aktiv, *Dormant* – Ruhend, *Blocked* – Gesperrt) und die Art der Route (*Gateway Route*, *Interface Route*, *Subnet Route*, *Host Route*, *Extended Route*) angezeigt. Unter ***PRO*** wird angezeigt, mit welchem Protokoll Ihr Gateway den Routing-Eintrag "gelernt" hat, z.B. *loc* = local, d.h. manuell konfiguriert.

Weitere Routen werden im Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***MORE ROUTING*** ➜ ***ADD*** hinzugefügt. Bestehende Einträge können bearbeitet werden, indem der gewünschte Listeneintrag ausgewählt und mit der Eingabetaste bestätigt wird.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][EDIT][IP][ROUTING][ADD]                                MyGateway

 Route Type                  Host route
 Network                     WAN without transit network

 Destination IP-Address



 Metric                      1



           SAVE                                    CANCEL
```

Das Menü ***MORE ROUTING*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route* (Defaultwert): Route zu einem einzelnen Host ■ *Network route*: Route zu einem Netzwerk ■ *Default route*: Die Route gilt für alle IP-Adressen und wird nur benutzt, wenn keine andere passende Route verfügbar ist.
Network	Definiert die Art der Verbindung. Für einen PPTP Partner wird hier *WAN without transit network* angezeigt. Der angezeigte Wert kann hier nicht verändert werden.
Destination IP-Address	Nur für ***ROUTE TYPE*** *Host route* oder *Network route*. IP-Adresse des Ziel-Hosts oder -Netzwerkes.
Netmask	Nur für ***ROUTE TYPE*** = *Network route*. Netzmaske zu ***DESTINATION IP-ADDRESS***. Wenn kein Eintrag erfolgt, benutzt das Gateway eine Standardnetzmaske.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0...15*). Defaultwert ist *1*.

Tabelle 5-2: Felder im Menü ***MORE ROUTING***

Zusätzlich zu der normalen Routing-Tabelle kann das **VPN Access** Gateway auch Routing-Entscheidungen aufgrund einer erweiterten Routing-Tabelle, der Extended Routing Table, treffen. Dabei kann das **VPN Access** Gateway neben der Quell- und Zieladresse u. a. auch das Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und den Status der Ziel-Schnittstelle in die Entscheidung mit einbeziehen.

Hinweis

Die Einträge in der Extended Routing Table werden gegenüber den Einträgen in der normalen Routing-Tabelle stets bevorzugt behandelt.

Die Konfiguration erfolgt im Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***MORE ROUTING*** ➜ ***ADDEXT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][ADD][IP][ROUTING][ADD]: IP Routing - Extended Route   MyGateway

 Route Type                  Host route
 Network                     WAN without transit network

 Destination IP-Address
                                                  Mode  always

 Metric                      1
 Source Interface            don't verify
 Source IP-Address
 Source Mask
 Type of Service (TOS)       00000000              TOS Mask  00000000
 Protocol                    don't verify


             SAVE                                  CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Route Type	Art der Route. Mögliche Werte: ■ *Host route* (Defaultwert): Route zu einem einzelnen Host ■ *Network route*: Route zu einem Netzwerk ■ *Default route*: Die Route gilt für alle IP-Adressen und wird nur benutzt, wenn keine andere passende Route verfügbar ist

Feld	Wert
Network	Definiert die Art der Verbindung. Für einen PPTP Partner wird hier *WAN without transit network* angezeigt. Der angezeigte Wert kann hier nicht verändert werden.
Destination IP-Address	Nur für ***ROUTE TYPE*** = *Host route* oder *Network route* IP-Adresse des Ziel-Hosts oder -Netzwerkes.
Netmask	Nur für ***ROUTE TYPE*** = *Network route* Netzmaske zu ***DESTINATION IP-ADDRESS***.
Partner / Interface	Anzeige des PPTP Partners. Feld kann nicht verändert werden.
Mode	Definiert, wann der PPTP Partner benutzt werden soll. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von MODE” auf Seite 32.
Metric	Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*...*15*, Defaultwert ist *1*).
Source Interface	Schnittstelle, über die die Datenpakete das Gateway erreichen. Defaultwert ist *don’t verify*.
Source IP-Address	IP-Adresse des Quell-Hosts bzw. -Netzwerkes.
Source Mask	Netzmaske zu ***SOURCE IP-ADDRESS***
Type of Service (TOS)	Mögliche Werte: *0*..*255* in binärem Format.
TOS Mask	Bitmaske zu ***TYPE OF SERVICE***.

Feld	Wert
Protocol	Legt ein Protokoll fest. Mögliche Werte: *don't verify, icmp, ggp, tcp, egp, pup, udp, hmp, xns, rdp, rsvp, gre, esp, ah, igrp, ospf, l2tp.* Defaultwert ist *don't verify*.
Source Port	Nur für ***PROTOCOL*** = *tcp* oder *udp* Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern.
Destination Port	Nur für ***PROTOCOL*** = *tcp* oder *udp* Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern.

Tabelle 5-3: Felder im Menü ***ADDEXT***

MODE enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
always (Defaultwert)	Route immer benutzen.
dialup-wait	Route benutzen, wenn das Interface "up" ist. Ist das Interface "dormant", dann wählen und warten, bis das Interface "up" ist. Sonst rerouten.
dialup-continue	Route benutzen, wenn das Interface "up" ist. Ist das Interface "dormant", dann wählen, aber rerouten, bis das Interface "up" ist. Sonst rerouten.
up-only	Route benutzen, wenn das Interface "up" ist. Sonst rerouten.

Tabelle 5-4: Auswahlmöglichkeiten von ***MODE***

Die Felder ***SOURCE PORT*** bzw. ***DESTINATION PORT*** enthalten folgende Auswahlmöglichkeiten:

Wert	Bedeutung
any (Defaultwert)	Die Route gilt für alle ➤➤ **Port**-Nummern.
specify	Ermöglicht Eingabe einer Port-Nummer.
specify range	Ermöglicht Eingabe eines Bereiches von Port-Nummern.
priv (0..1023)	Port-Nummern: 0 ... 1023
server (5000..32767)	Port-Nummern: 5000 ... 32767
clients 1 (1024..4999)	Port-Nummern: 1024 ... 4999
clients 2 (32768..65535)	Port-Nummern: 32768 ... 65535
unpriv (1024..65535)	Port-Nummern: 1024 ... 65535

Tabelle 5-5: Auswahlmöglichkeiten von ***SOURCE PORT*** bzw. ***DESTINATION PORT***

5.3 Untermenü Advanced Settings

Im Folgenden werden die Felder des Untermenüs *ADVANCED SETTINGS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[PPTP][EDIT][IP][ADVANCED]: Advanced Settings (Zentrale)      MyGateway


 RIP Send                              none
 RIP Receive                           none

 IP Accounting                         off
 Back Route Verify                     off
 Route Announce                        up or dormant
 Proxy Arp                             off


 Dynamic Name Server Negotiation       yes


            OK                                        CANCEL
```

Im Menü ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** ➜ ***ADVANCED SETTINGS*** können u.a. erweiterte Routing-Einstellungen für den jeweiligen PPTP Partner vorgenommen werden.

RIP Die Eintragungen der Routing-Tabelle können entweder statisch festgelegt werden, oder es erfolgt eine laufende Aktualisierung der Routing-Tabelle durch dynamischen Austausch der Routing-Informationen zwischen mehreren Gateways. Diesen Austausch regelt ein sogenanntes Routing-Protokoll, z. B. RIP (Routing Information Protocol).

Mit ➤➤ **RIP** tauschen Gateways ihre in Routing-Tabellen gespeicherten Informationen aus, indem sie in regelmäßigen Abständen miteinander kommunizieren. Das **VPN Access** Gateway unterstützt sowohl Version 1 als auch Version 2 von RIP, wahlweise einzeln oder gemeinsam.

RIP wird für LAN und WAN separat konfiguriert.

Aktiv und Passiv

Man kann dabei aktive und passive Gateways unterscheiden: Aktive Gateways bieten Ihre Routing-Einträge per ➤➤ **Broadcasts** anderen Gateways an. Passive Gateways nehmen die Informationen der aktiven Gateways an und speichern sie, geben aber ihre eigenen Routing-Einträge nicht weiter. Das **VPN Access** Gateway kann beides.

PPTP Partner

Wenn Sie mit einem PPTP Partner Empfangen und/oder Senden von RIP-Paketen vereinbaren, kann Ihr Gateway mit den Gateways im LAN der Gegenstelle dynamisch Routing-Informationen austauschen.

Hinweis

Der Empfang von Routing-Tabellen über RIP kann eine Sicherheitslücke sein, da fremde Rechner bzw. Gateways die Routing-Funktionalität des **VPN Access** Gateways verändern können.

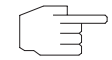
PPTP-Verbindungen werden durch RIP-Pakete nicht aufgebaut oder gehalten.

IP Accounting Diese Option ermöglicht die Aktivierung bzw. Deaktivierung der Erstellung von IP Accounting Meldungen für diesen PPTP Partner. Wenn IP Accounting aktiviert ist, wird eine Statistikmeldung generiert (und in die **biboAdmSyslogTable** eingeschrieben), welche detaillierte Informationen über die Verbindungen mit diesem PPTP Partner enthält. (Einstellungen zum Speichern der Accounting Messages in eine Datei finden Sie in ***System*** ➜ ***External System Logging***.)

Back Route Verify Hinter diesem Begriff versteckt sich eine einfache, aber sehr leistungsfähige Funktion des **VPN Access** Gateways. Wenn Backroute Verification bei einem Interface aktiviert ist, werden über dieses eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über das gleiche Interface geroutet würden. Dadurch können Sie – auch ohne Filter – die Akzeptanz von Paketen mit gefälschten IP-Adressen verhindern.

Route Announce Diese Option ermöglicht die Einstellung, wann ggf. aktivierte Routing Protokolle (z.B. RIP) die für dieses Interface definierten IP Routen propagieren sollen.

Proxy Arp Mit Hilfe von ➤➤ **Proxy ARP** kann das Gateway ➤➤ **ARP**-Requests aus dem eigenen LAN stellvertretend für diesen spezifischen PPTP Partner beantworten. Wenn ein Host im LAN eine Verbindung zu einem anderen Host im LAN oder zu einem PPTP Partner aufbauen will, aber dessen Hardware-Adresse (MAC Adresse) nicht kennt, sendet er einen sogenannten ARP-Request als ➤➤ **Broadcast** ins Netz. Wenn auf dem Gateway Proxy ARP aktiviert ist und der gewünschte Ziel-Host z.B. über eine Host-Route erreichbar ist, beantwortet das Gateway den ARP-Request mit seiner eigenen Hardware-Adresse. Die ➤➤ **Datenpakete** werden an das Gateway geschickt, das sie dann an den gewünschten Host weiterleitet.



Hinweis

Achten Sie darauf, dass auch LAN-seitig Proxy ARP aktiviert ist.

Das Menü ***ADVANCED SETTINGS*** besteht aus folgenden Feldern:

Feld	Wert
RIP Send	Ermöglicht Senden von RIP-Paketen über die Schnittstelle zum PPTP Partner. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von RIP SEND und RIP RECEIVE” auf Seite 38
RIP Receive	Ermöglicht Empfangen von RIP-Paketen über die Schnittstelle zum PPTP Partner. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von RIP SEND und RIP RECEIVE” auf Seite 38
IP Accounting	Ermöglicht Erzeugen von Accounting-Messages für z.B. ➤➤ **TCP-**, ➤➤ **UDP-** und ICMP-Sitzungen. Mögliche Werte: *on*, *off* (Defaultwert).
Back Route Verify	Aktiviert Backroute Verification für die Schnittstelle zum PPTP Partner. Mögliche Werte: *on, off* (Defaultwert).
Route Announce	Mögliche Werte: ■ *up or dormant* (Defaultwert): Routen werden propagiert, wenn der Status des Interfaces *up* oder *dormant* ist. ■ *always*: Routen werden immer propagiert unabhängig vom Betriebsstatus. ■ *up only*: Routen werden nur propagiert, wenn der Status der Schnittstelle auf *up* steht.

Feld	Wert
Proxy Arp	Ermöglicht dem Gateway, ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen PPTP Partner zu beantworten. Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von PROXY ARP” auf Seite 39
Dynamic Name Server Negotiation	Definiert, ob das **VPN Access** Gateway IP-Adressen für ***PRIMARY DOMAIN NAME SERVER, SECONDARY DOMAIN NAME SERVER, PRIMARY WINS*** und ***SECONDARY WINS*** vom PPTP Partner erhält oder diese zum PPTP Partner schickt. Mögliche Werte siehe Tabelle “Auswahlmöglichkeiten von DYNAMIC NAME SERVER NEGOTIATION” auf Seite 40.

Tabelle 5-6: Felder im Menü ***ADVANCED SETTINGS***

RIP SEND bzw. ***RIP RECEIVE*** enthalten folgende Auswahlmöglichkeiten:

Wert	Bedeutung
none (Defaultwert)	Nicht aktiviert.
RIP V2 multicast	Nur für ***RIP SEND*** Ermöglicht das Senden von RIP-V2-Nachrichten über die Multicast-Adresse 224.0.0.9.
RIP V1 triggered	RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered ➤➤ **RIP**).
RIP V2 triggered	RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered ➤➤ **RIP**).
RIP V1	Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1.

Wert	Bedeutung
RIP V2	Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2.
RIP V1 + V2	Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2.

Tabelle 5-7: Auswahlmöglichkeiten von ***RIP SEND*** und ***RIP RECEIVE***

PROXY ARP enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
off (Defaultwert)	Deaktiviert Proxy ARP für diesen PPTP Partner.
on (up or dormant)	Das **VPN Access** Gateway beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP Partner *up* (aktiv) oder *dormant* (ruhend) ist. Bei *dormant* beantwortet das **VPN Access** Gateway lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.

Wert	Bedeutung
on (up only)	Das **VPN Access** Gateway beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP Partner *up* (aktiv) ist, wenn also bereits eine Verbindung zum PPTP Partner besteht.

Tabelle 5-8: Auswahlmöglichkeiten von ***PROXY ARP***

DYNAMIC NAME SERVER NEGOTIATION enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
off	Das **VPN Access** Gateway sendet oder beantwortet keine Anfragen für Name Server Adressen.
yes (Defaultwert)	Die Bedeutung ist abhängig von der Einstellung in ***PPTP*** ➜ ***ADD/EDIT*** ➜ ***IP*** unter ***IP ADDRESS NEGOTIATION***: ■ Wenn *dynamic client* ausgewählt wurde, sendet das **VPN Access** Gateway Name Server Adress-Anfragen zum PPTP Partner. ■ Wenn *dynamic server* ausgewählt wurde, beantwortet das **VPN Access** Gateway Name Server Adress-Anfragen vom PPTP Partner. ■ Wenn *yes* oder *no* ausgewählt wurde, antwortet das **VPN Access** Gateway, schickt aber keine Name Server Adress-Anfragen.
client (receive)	Das **VPN Access** Gateway sendet Name Server Adress-Anfragen zum PPTP Partner.

Wert	Bedeutung
server (send)	Das **VPN Access** Gateway beantwortet Name Server Adress-Anfragen vom PPTP Partner.

Tabelle 5-9: Auswahlmöglichkeiten von ***Dynamic Name Server Negotiation***

Index: PPTP