TheGreenBow IPSec VPN Client

Konfigurationsbeispiel

Bintec RS232b
Funkwerk Enterprise Communications GmbH

WebSite: http://www.thegreenbow.de/
Kontakt: mailto:support@thegreenbow.de

Configuration Guide written by:

Autor:	Timm Richter
Firma:	www.thegreenbow.de

Inhalt

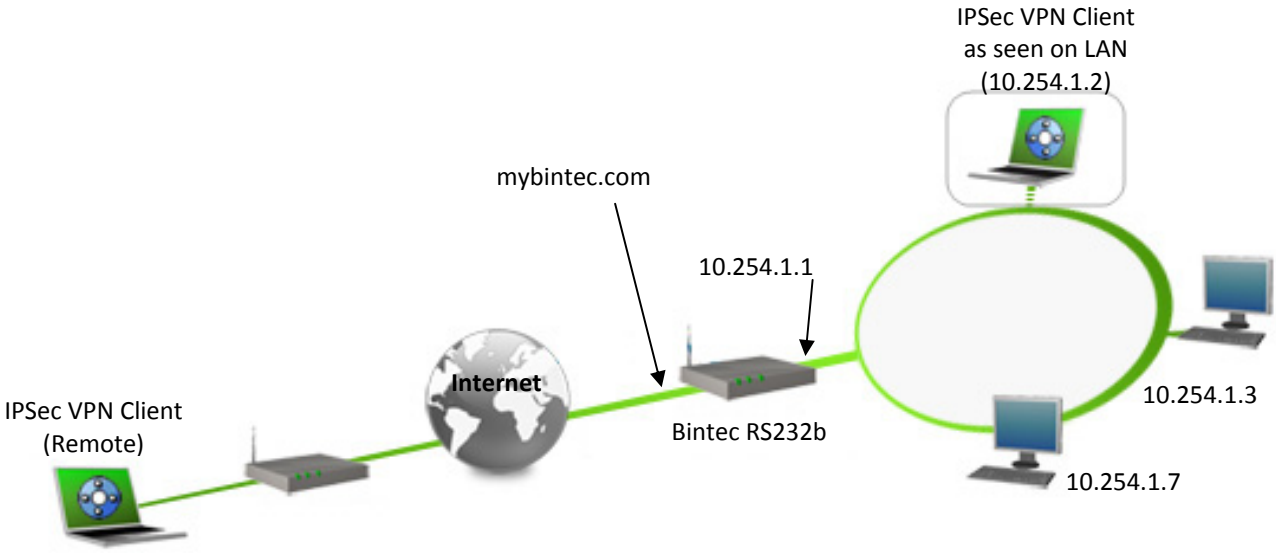
1 Einleitung

1.1 Ziel der Anleitung

Dieses Konfigurationsbeispiel beschreibt eine mögliche Konfiguration des TheGreenBow IPSec VPN Client, um einen IPSec Tunnel zu einem Bintec RS232b und dem dahinter liegenden Firmen- oder Heimnetzwerk aufbauen zu können.

1.2 VPN Netzwerktopologie

Dieses Beispiel zeigt, wie wir den TheGreenBow IPSec Client in das lokale Netzwerk hinter der Bintec RS232b verbinden. Der Rechner mit dem VPN Client ist mit dem Internet über DSL oder einem Firmennetzwerk verbunden. Die hier aufgeführten IP Adressen und Ranges dienen nur als Beispiel.



1.3 Bintec RS232b Einschränkungen

Uns sind keine Einschränkungen bekannt. Mehr Informationen finden Sie unter http://www.funkwerk-ec.com.

1.4 Bintec RS232b VPN Gateway

Unseren Test haben wir mit einem RS232b Gateway mit der Firmware „BOSS-Version V.7.9 Rev. 1 (Patch 6) IPSec“ durchgeführt.

1.5 Bintec RS232b Produktinformationen

Alle Produktinformationen, Handbücher, FAQ und Hilfestellung zu Ihrem Bintec Gateway finden Sie auf den Funkwerk Webseiten: http://www.funkwerk-ec.com.

Bintec Produktseite	http://www.funkwerk-ec.com/prod_bintec_rs232b_main_de,101823,194.html
Bintec Handbuch	http://www.funkwerk-ec.com/dl_bintec_r232b_de,64605,194.html
Bintec FAQ/Hilfe	http://www.funkwerk-ec.com/sup_sup2_1_funkwerk-supportcenter_de,87028,194.html

2 Bintec RS232b Gateway VPN Konfiguration

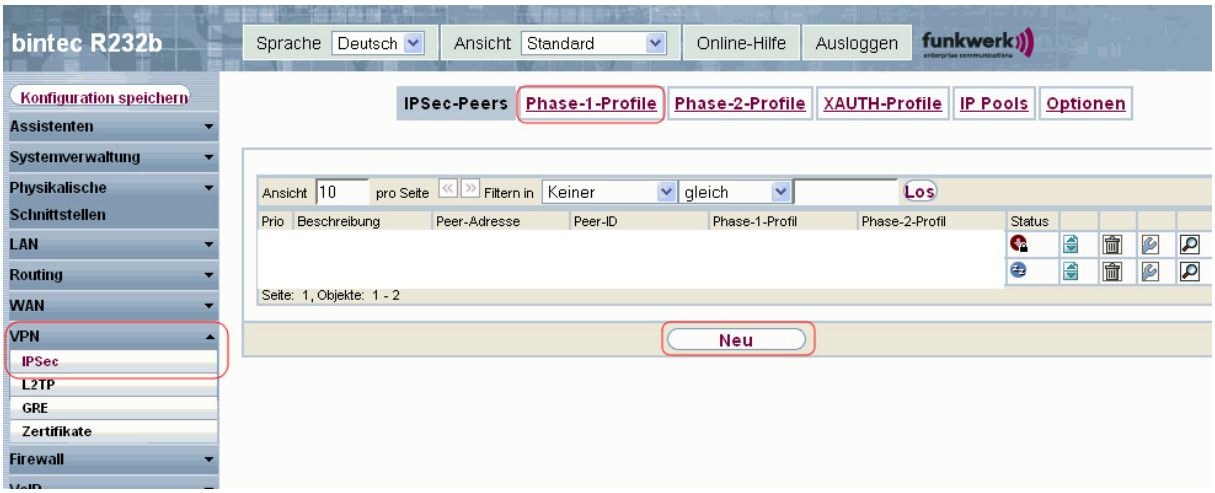
Dieses Kapitel beschreibt die Konfiguration des Bintec RS232b Gateway.

2.1 Vorbereitungen

Damit Ihr Bintec RS232b Gateway über einen Namen aus dem Internet erreichbar ist, sollten Sie einen dynamischen DNS Dienst konfigurieren. Weitere Hilfe zur Einrichtung finden Sie in Ihrem Bintec RS232b Handbuch oder unter http://www.funkwerk-ec.com.

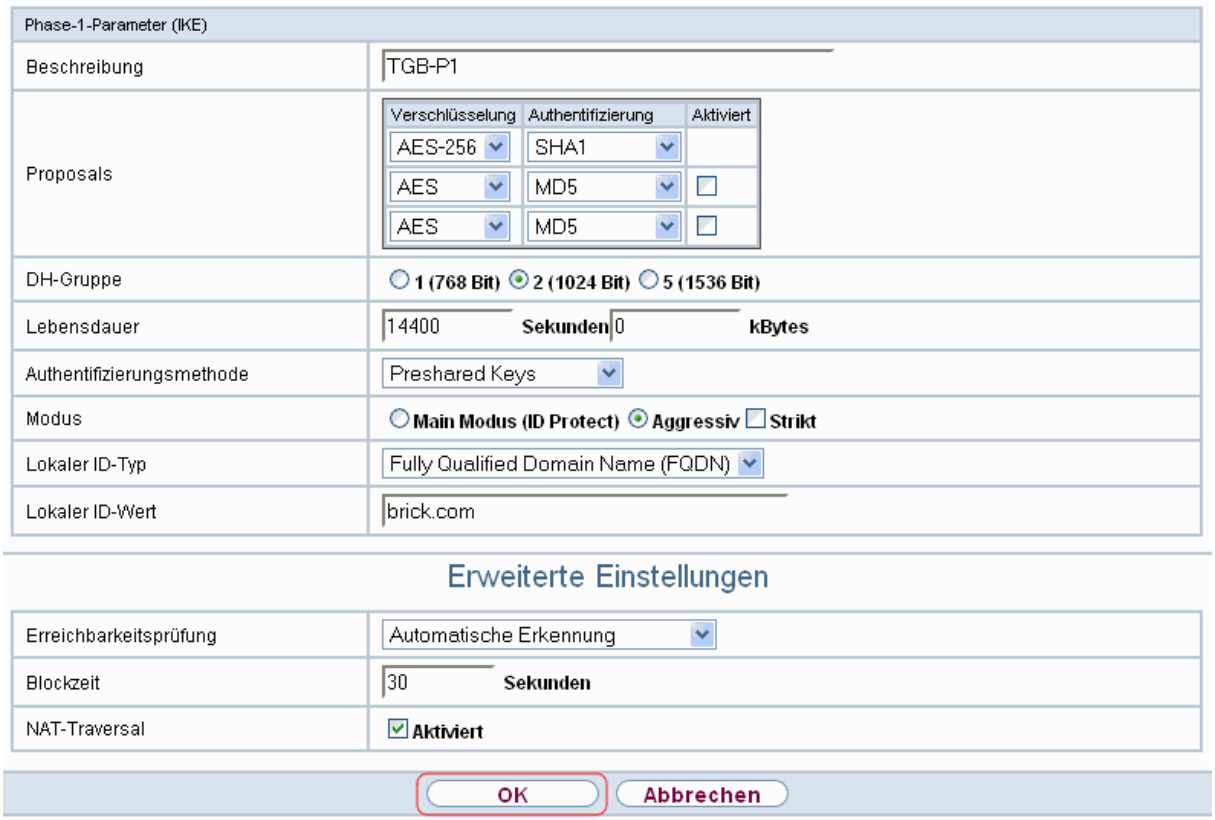
2.2 Einstellungen im Bintec RS232b

Öffnen Sie die Administrationsoberfläche über Ihren Browser.

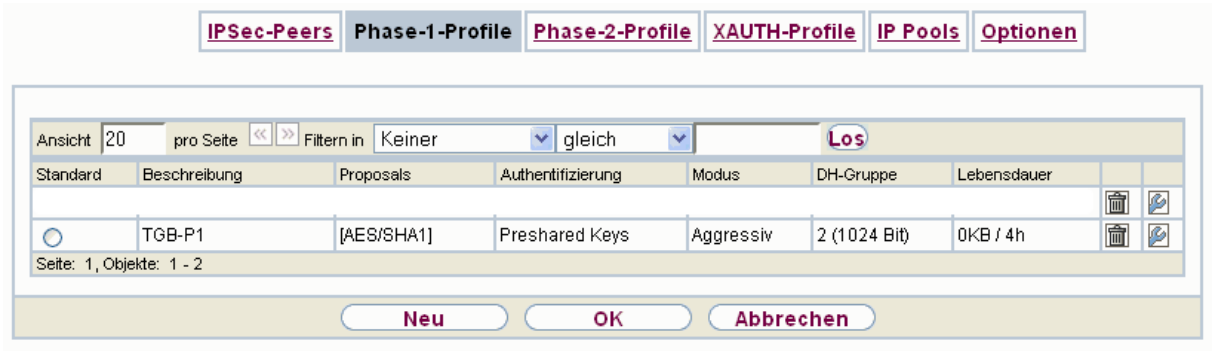


Wählen Sie auf der rechten Seite die Menüpunkte „**VPN**“ – „**IPSec**“ aus.

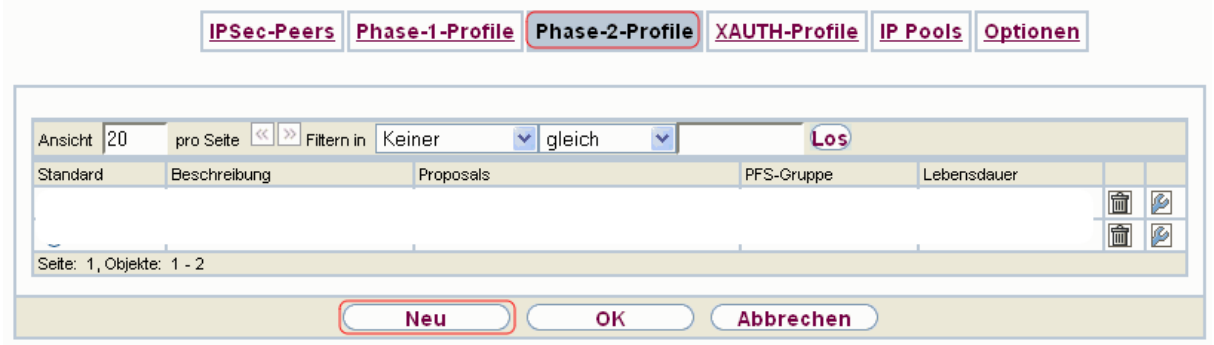
Klicken Sie den Button „**Phase-1-Profile**“ und anschließend „**Neu**“, um eine neue Konfiguration für die Phase 1 zu erstellen.



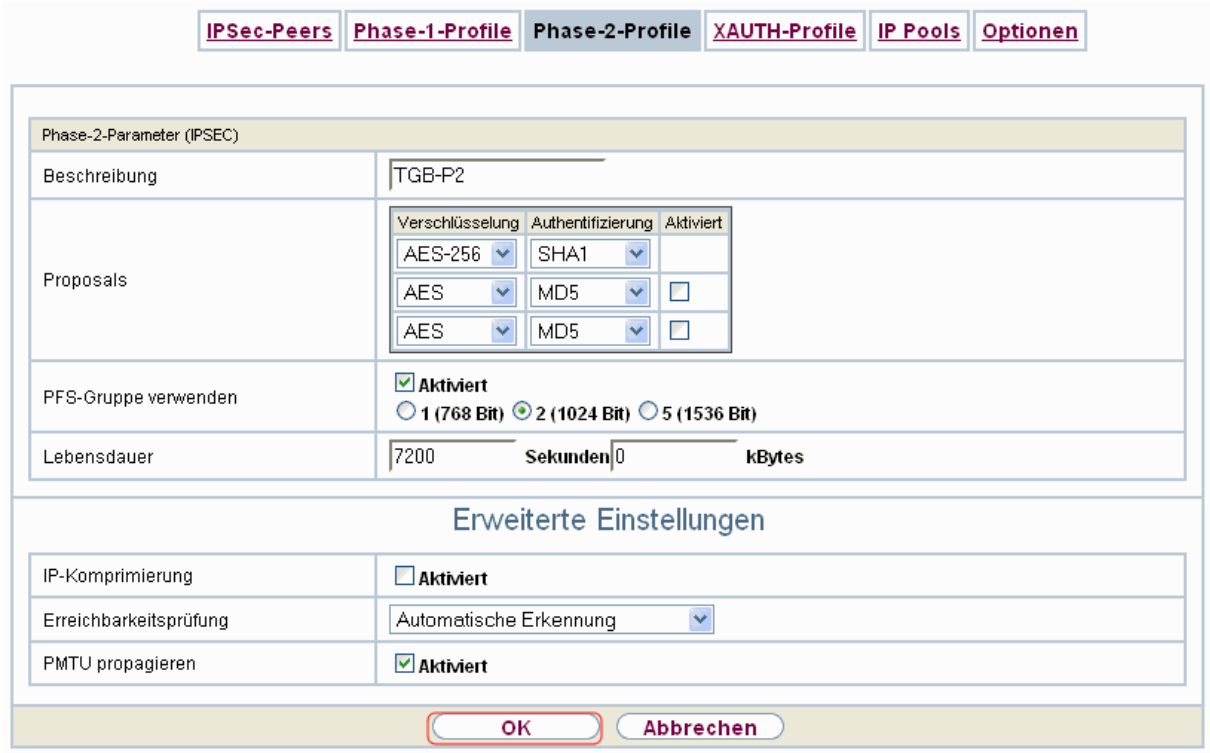
Geben Sie die Konfigurationsdaten wie in o.g. Beispiel ein. Zur Identifizierung des VPN Gateways vergeben wir eine lokale ID – hier „**brick.com**“. Speichern Sie die Eingaben mit „**OK**“.



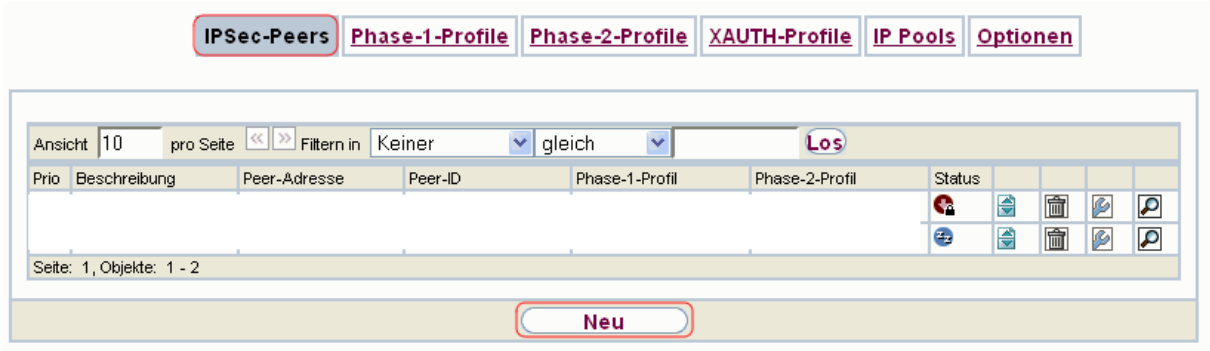
Die Konfiguration für die Phase 1 erscheint nun in der Übersicht.



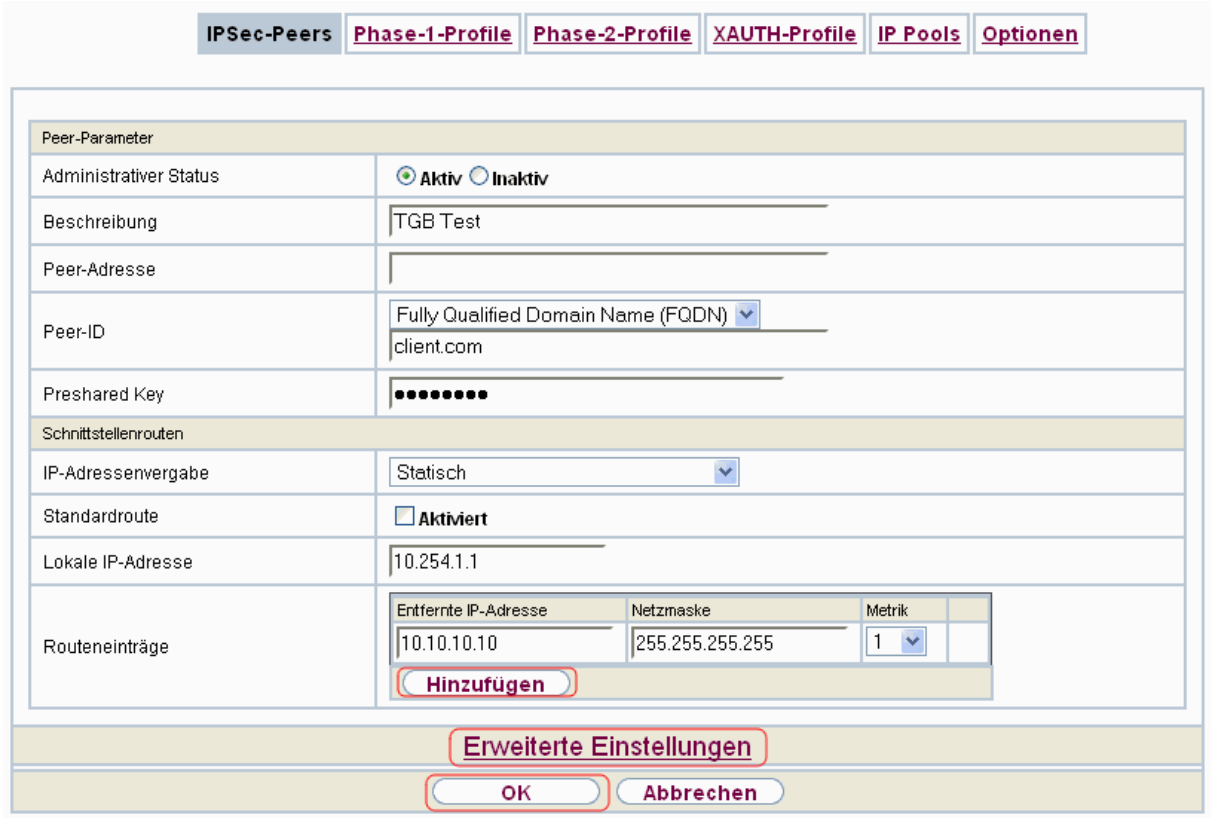
Wechseln Sie zu “**Phase-2-Profile**” und anschließend „**Neu**“, um eine neue Konfiguration für die Phase 2 zu erstellen.



Geben Sie die Konfigurationsdaten wie in o.g. Beispiel ein. Speichern Sie die Eingaben mit „**OK**“.

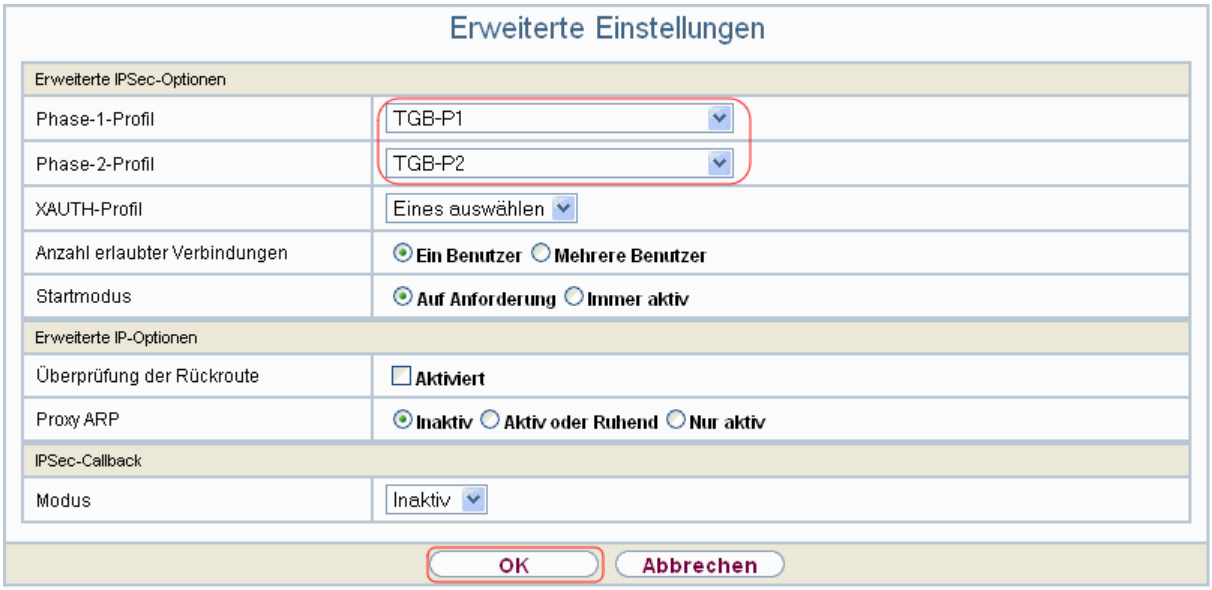


Wechseln Sie zu dem Menüpunkt “**IPSec-Peers**” und klicken anschließend „**Neu**“, um die Tunnelkonfiguration fertig zu stellen.

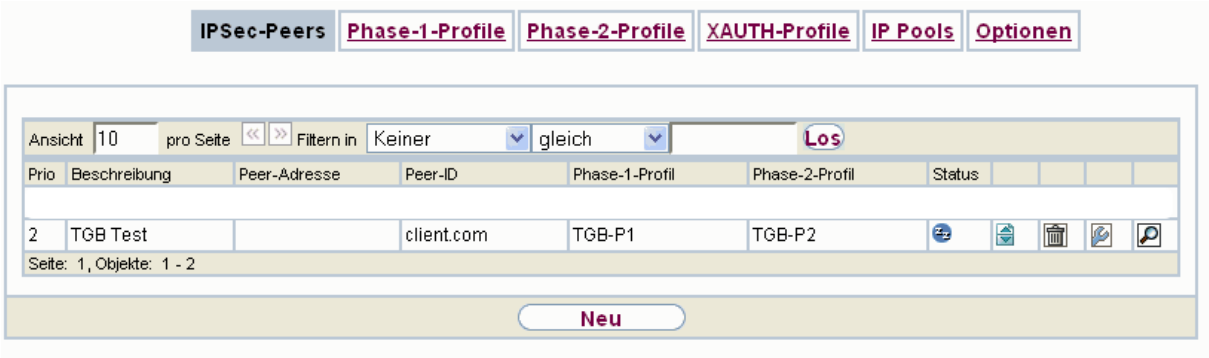


Geben Sie die Konfigurationsdaten wie in o.g. Beispiel ein. Zur Identifizierung des VPN Client vergeben wir eine Peer-ID (entfernte ID) – hier „**client.com**“. Vergeben Sie als „**Preshared Key**“ ein Passwort Ihrer Wahl. Dem VPN Client möchten wir eine dedizierte virtuelle IP zuweisen – hier 10.10.10.10.

Bestätigen Sie die Eingaben mit „**OK**“ und klicken Sie nun auf „**Erweiterte Einstellungen**“.



Wählen Sie nun die eben erstellten Konfigurationen für die Phase 1 und Phase 2 aus und geben Sie die Konfigurationsdaten wie in o.g. Beispiel ein. Speichern Sie die Eingaben mit „**OK**“.



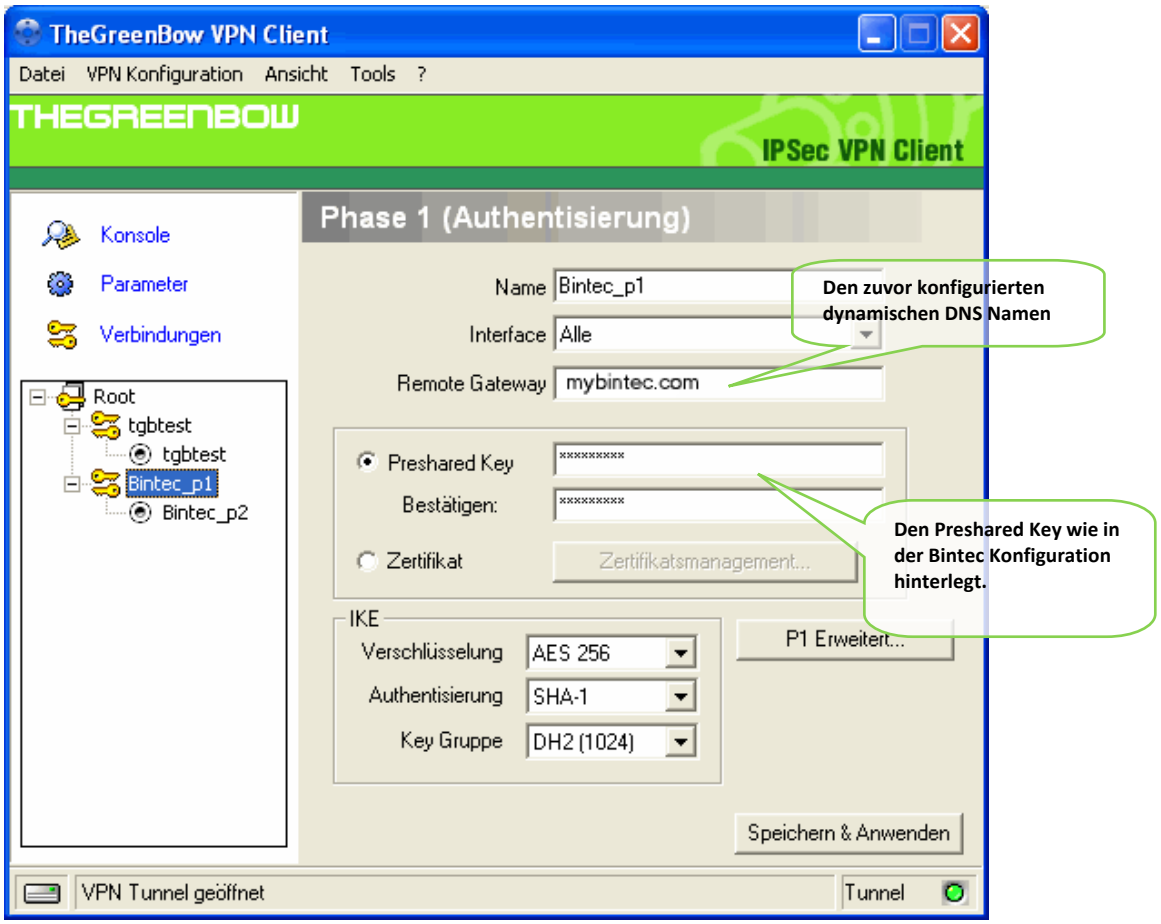
Sie sehen den eingerichteten Tunnel nun in der Übersicht im Menü „**IPSec-Peers**“. Die Einstellungen im Bintec RS 232b Router sind nun abgeschlossen.

3 TheGreenBow IPSec VPN Client Konfiguration

Dieses Kapitel beschreibt die Konfigurationseinstellungen des TheGreenBow IPSec VPN Client.

Die aktuellste Version des TheGreenBow IPSec VPN Client finden Sie auf der TheGreenBow Webseite: http://www.thegreenbow.de/vpn_down.html.

3.1 VPN Client Phase 1 (IKE) Konfiguration



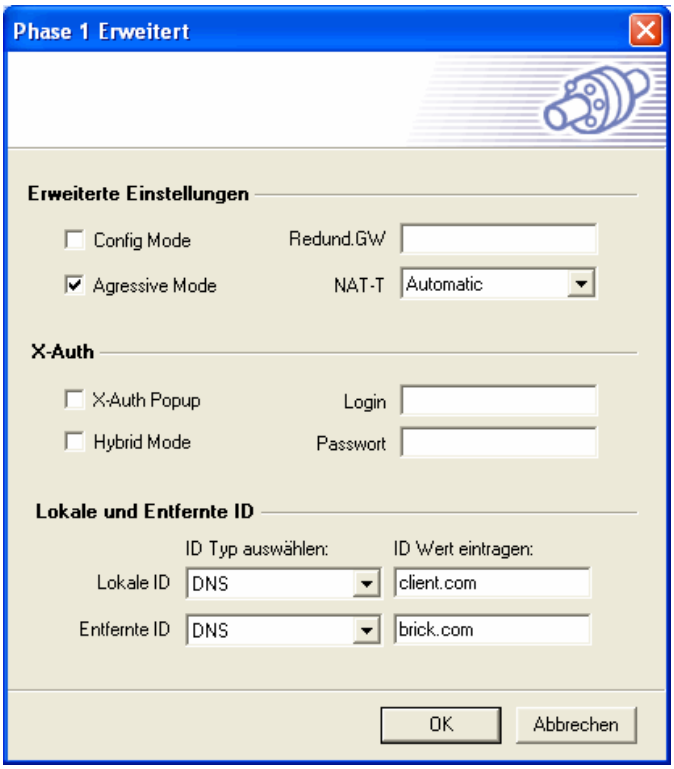
Phase 1 Konfiguration

Zur Benutzerauthentisierung verwenden wir in diesem Beispiel die Methode per **Preshared Key** .
Weitere Möglichkeiten der Authentisierung wie z.B. durch X-Auth, Token, Zertifikate usw. entnehmen Sie bitte Ihrer Bintec Dokumentation.

Geben Sie einen eindeutigen Namen für die VPN Verbindung (in unserem Beispiel „**Bintec_p1**). „**Interface**“ kann auf „**Alle**“ bleiben. Im Feld „**Remote Gateway**“ den dynamischen DNS Namen (in unserem Beispiel „**mybintec.com**“) oder die externe IP Adresse des RS232b eingeben. Setzen Sie nun unter „**IKE**“ die im Bintec Gateway definierten Werte ein.

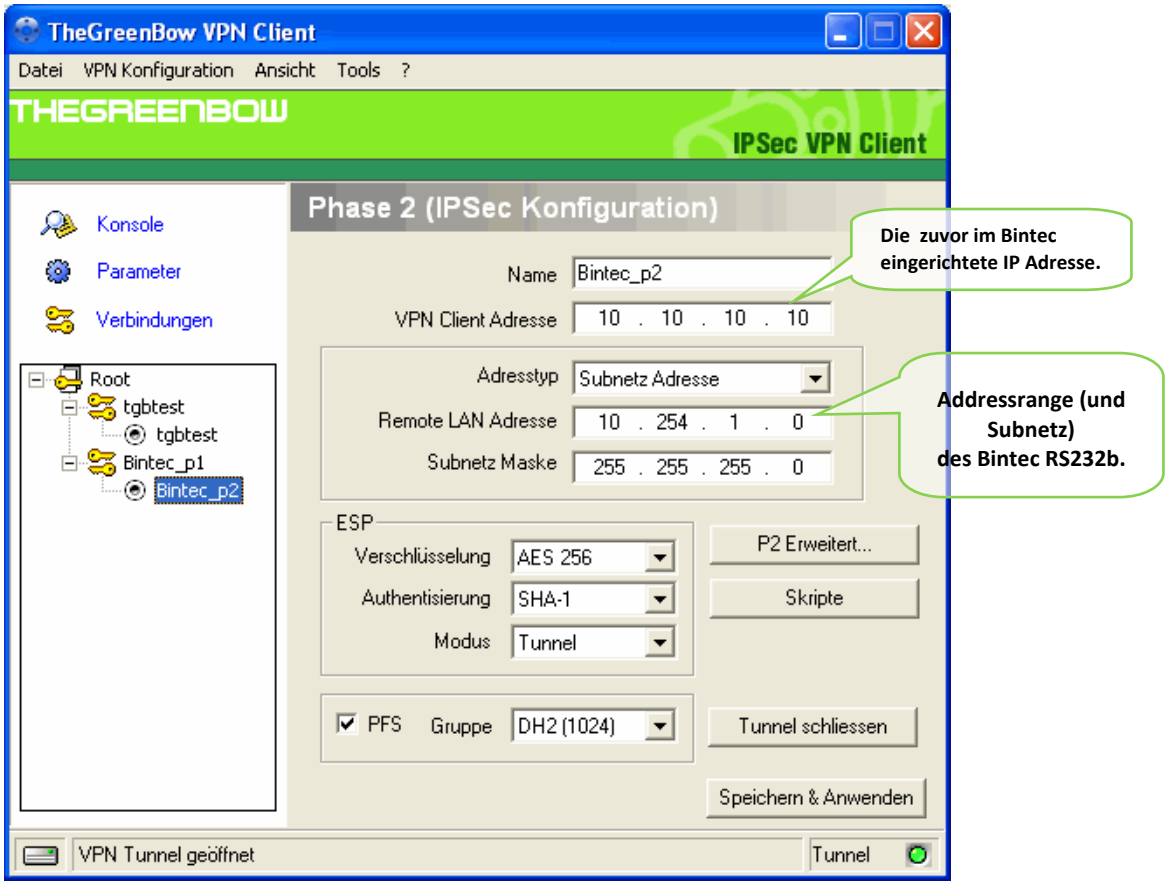
3.2 Phase 1 – Erweiterte Einstellungen

Klicken Sie „**P1 Erweitert**“ um in die erweiterten Konfigurationseinstellungen der Phase 1 zu gelangen.



Setzen Sie nun die lokale und entfernte ID für den VPN Client. Als ID Typ für beide (lokal und entfernt) „**DNS**“ auswählen. Tragen Sie hier die jeweils im RS232b hinterlegten **ID-Werte** ein. Aktivieren Sie den „**Aggressive Mode**“. Bestätigen Sie die Einstellungen mit Klick auf „**OK**“.

3.3 VPN Client Phase 2 (IPSec) Konfiguration



Phase 2 Konfiguration

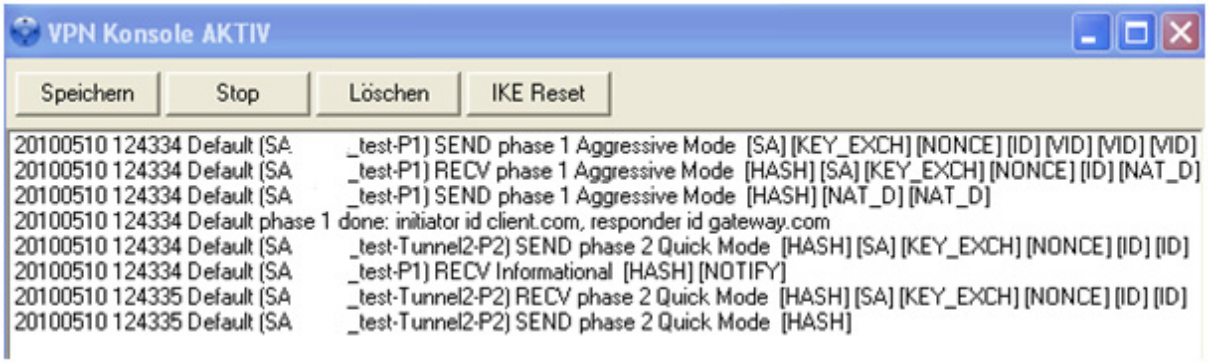
Tragen Sie die fehlenden Konfigurationsdaten gemäss Ihrer Gateway-Konfiguration ein. Klicken Sie "**Speichern & Anwenden**" um alle Konfigurationseinstellungen zu sichern. Der VPN Client ist nun betriebsbereit.

3.4 IPSec VPN Tunnel öffnen

1. Klicken Sie auf "**Tunnel öffnen**", das VPN Icon im Systemtray färbt sich grün, sobald der Tunnel etabliert ist.

2. Über den Menüpunkt "**Verbindungen**" können Sie den Status der konfigurierten VPN Tunnel einsehen.

3. Über den Menüpunkt "**Konsole**" haben Sie Einsicht in die Logdatei. Hier wird alle Kommunikation über das IPSec Protokoll zwischen Client und Gateway angezeigt.

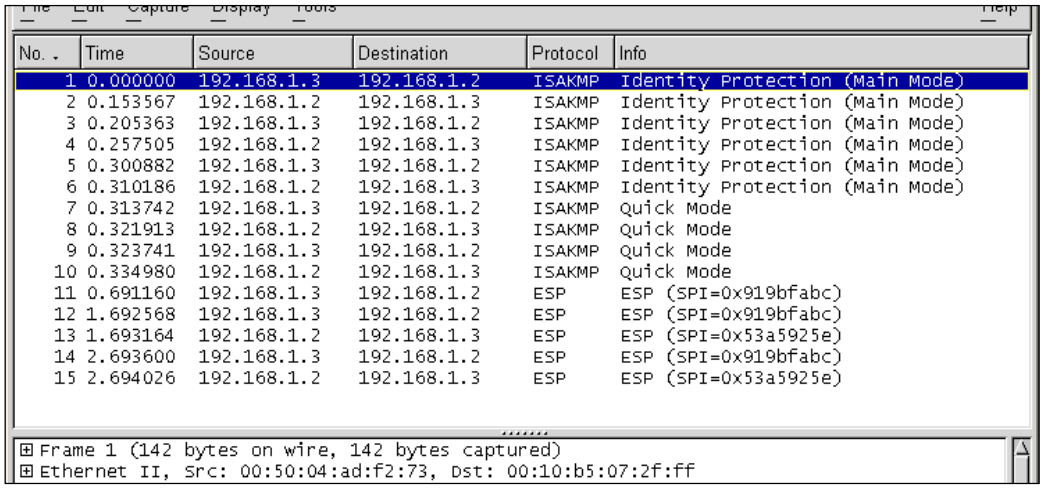


4 Fehlerbehebung

IPSec VPN Tunnel reagieren äußerst sensibel. Ein falscher oder fehlender Parameter kann einen erfolgreichen Tunnelaufbau verhindern. Hier einige Werkzeuge und Informationen zur Fehlerbehebung.

4.1 Eine gute Netzwerkanalyse: Wireshark

Wireshark ist eine freie Software (Freeware), mit der Sie Netzwerkpakete und Netzwerkverkehr analysieren können. Sie zeigt und protokolliert alle IP oder TCP Pakete an, die von der Netzwerkkarte empfangen werden. Die Software erhalten sie auf der Webseite http://www.wireshark.org. Sie kann zur Analyse der Protokollkommunikation zwischen 2 Geräten verwendet werden. Hilfe zur Installation und Verwendung vom Wireshark finden Sie hier: http://www.wireshark.org/docs/



5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

Der Fehler « PAYLOAD MALFORMED » indiziert, dass die Einstellungen der Phase 1 im Client und Gateway nicht übereinstimmen. Prüfen Sie bitte die Verschlüsselungsalgorithmen auf beiden Seiten.

5.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
```

Der Fehler « INVALID COOKIE » bedeutet, dass einer der Endpunkte (Client oder Gateway) eine Security Association (SA) verwendet, die nicht mehr aktiv oder gültig ist. Setzen Sie in diesem Fall bitte die VPN Verbindung auf beiden Seiten zurück.

5.3 « no keystate » error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Prüfen Sie bitte, dass der PreShared Key korrekt ist und mit dem im VPN Gateway hinterlegtem Schlüssel übereinstimmt. Prüfen Sie auch die erweiterten Einstellungen in der Phase 1. Achten Sie hier bitte genau auf die korrekte Konfiguration der lokalen und entfernten ID's. In den Logdateien des VPN Gateways finden Sie in der Regel detailliertere Informationen, welcher Wert hier konkret als fehlerhaft angemahnt wird.

5.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

Die Remote ID (Typ und/oder Wert) in den erweiterten Einstellungen der Phase 1 stimmen nicht mit den Einstellungen des VPN Gateway überein.

5.5 « NO PROPOSAL CHOSEN » error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

In diesem Fall stimmen die Verschlüsselungseinstellungen in der Phase 2 nicht mit denen des VPN Gateway überein. Prüfen Sie die Verschlüsselungseinstellungen in der Phase 1, wenn sich der Fehler so darstellt:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626   Default   (SA   CNXVPN1-CNXVPN1-P2)   SEND   phase   2   Quick   Mode
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

Prüfen Sie bei diesem Fehler die Netzwerkeinstellungen der Phase 2. Diese müssen explizit mit der Konfiguration des VPN Gateways übereinstimmen. Beachten Sie hier besonders die Werte der VPN Client IP und der Netzwerkadresse. Prüfen Sie auch den Typ (Subnetz oder Einzeladresse).

5.7 Ich klicke auf “Tunnel öffnen”, aber nichts passiert.

Prüfen Sie die Logdateien auf beiden Seiten (Client und Gateway). Die IKE Anfragen könnten hier durch eine Firewall blockiert werden. IPSec VPNs verwenden das UDP Ports 500 und 4500, sowie das Protokoll ESP (Protokoll 50).

5.8 Der VPN Tunnel ist aktiv aber ich kann nicht pingen!

Ist der VPN Tunnel etabliert, aber das entfernte Netzwerk lässt sich nicht anpingen, prüfen Sie bitte folgende Optionen und Einstellungen:

- Phase 2 Einstellungen: VPN Client Adresse and Remote LAN Adresse. Üblicherweise darf die VPN Client IP Adresse nicht innerhalb der Range des Subnet hinter dem VPN Gateway liegen.
- Ist der Tunnel geöffnet, werden Pakete mittels des ESP Protokoll übertragen. Dies könnte durch eine Firewall blockiert werden. Prüfen Sie jedes Gerät zwischen VPN Client und VPN Gateway, ob dies der Fall ist.
- Prüfen Sie die Logdateien des VPN Gateway. Auch hier können Firewalleinstellungen die Kommunikation blockieren.

- Prüfen Sie bitte, ob Ihr Zugangsprovider ESP Paketübertragungen unterstützt.

- Prüfen Sie die “Standardgateway” Einstellungen im entfernten Netzwerk. Ein Zielhost im entfernten Netzwerk könnte wohlmöglich die Pings empfangen, jedoch an ein falsches Gateway antworten.
- Möglicherweise können Sie den Zielhost nicht über seinen Namen erreichen. Probieren Sie stattdessen die interne IP Adresse.
- Zur weiteren Analyse empfehlen wir Wireshark (http://www.wireshark.org) um zu prüfen, ob die Pings im entfernten Netzwerk ankommen.

6 Kontakt

News und Updates auf der TheGreenBow Website: http://www.thegreenbow.de

Technischer Suppoert per E-Mail: support@thegreenbow.de

Vertrieb: sales@thegreenbow.de

Secure, Strong, Simple.

TheGreenBow Security Software