



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	3
1.1	Ziel der Anleitung	3
1.2	VPN Netzwerktopologie	3
1.3	Bintec RS232b Einschränkungen	3
1.4	Bintec RS232b VPN Gateway.....	3
1.5	Bintec RS232b Produktinformationen	3
2	Bintec RS232b Gateway VPN Konfiguration	4
2.1	Vorbereitungen	4
2.2	Einstellungen im Bintec RS232b.....	4
3	TheGreenBow IPSec VPN Client Konfiguration.....	9
3.1	VPN Client Phase 1 (IKE) Konfiguration	9
3.2	Phase 1 – Erweiterte Einstellungen	10
3.3	VPN Client Phase 2 (IPSec) Konfiguration	11
3.4	IPSec VPN Tunnel öffnen	11
4	Fehlerbehebung.....	12
4.1	Eine gute Netzwerkanalyse: Wireshark	12
5	VPN IPSec Troubleshooting	13
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	13
5.2	« INVALID COOKIE » error.....	13
5.3	« no keystate » error	13
5.4	« received remote ID other than expected » error.....	13
5.5	« NO PROPOSAL CHOSEN » error	14
5.6	« INVALID ID INFORMATION » error.....	14
5.7	Ich klicke auf “Tunnel öffnen”, aber nichts passiert.	14
5.8	Der VPN Tunnel ist aktiv aber ich kann nicht pingen!	14
6	Kontakt.....	16

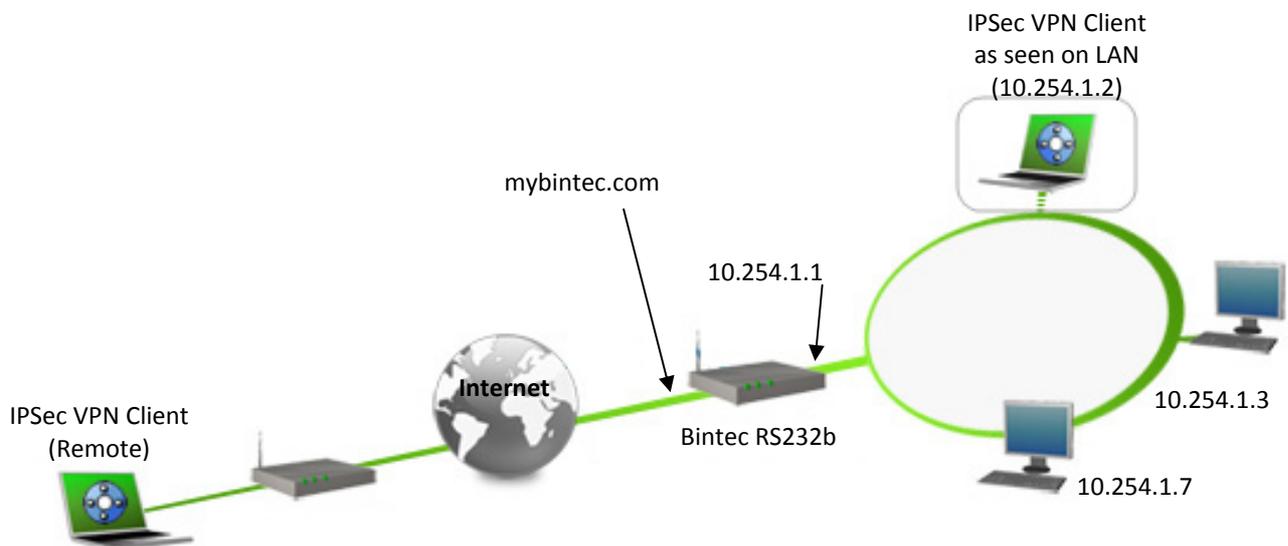
1 Einleitung

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

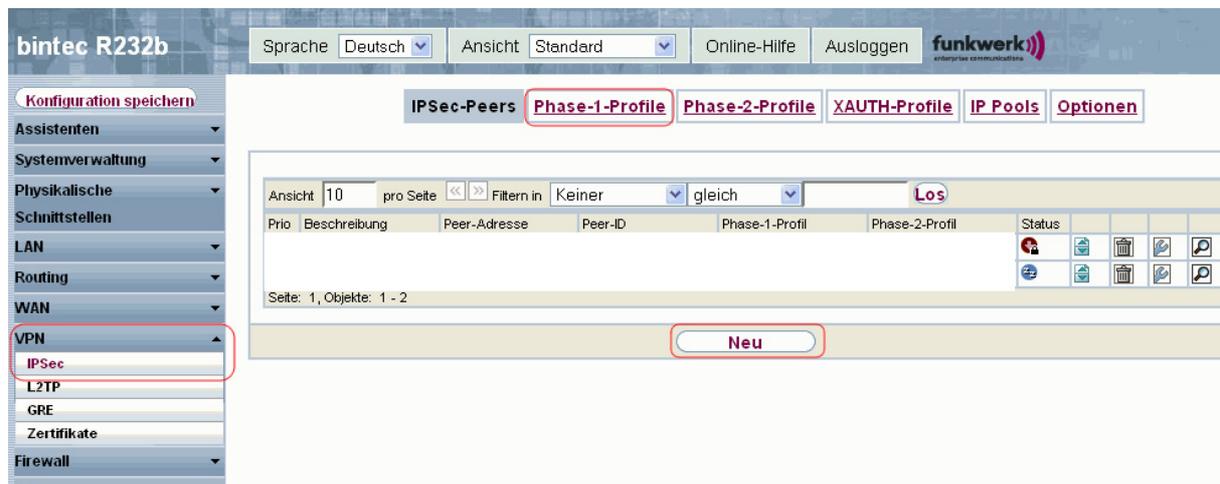
Dieses Kapitel beschreibt die Konfiguration des Bintec RS232b Gateway.

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.

Phase-1-Parameter (IKE)

Beschreibung	TGB-P1		
Proposals	Verschlüsselung	Authentifizierung	Aktiviert
	AES-256	SHA1	<input type="checkbox"/>
	AES	MD5	<input type="checkbox"/>
DH-Gruppe	<input type="radio"/> 1 (768 Bit) <input checked="" type="radio"/> 2 (1024 Bit) <input type="radio"/> 5 (1536 Bit)		
Lebensdauer	14400	Sekunden	0 kBytes
Authentifizierungsmethode	Preshared Keys		
Modus	<input type="radio"/> Main Modus (ID Protect) <input checked="" type="radio"/> Aggressiv <input type="checkbox"/> Strikt		
Lokaler ID-Typ	Fully Qualified Domain Name (FQDN)		
Lokaler ID-Wert	brick.com		

Erweiterte Einstellungen

Erreichbarkeitsprüfung	Automatische Erkennung
Blockzeit	30 Sekunden
NAT-Traversal	<input checked="" type="checkbox"/> Aktiviert

OK

Abbrechen

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**“.

IPSec-Peers Phase-1-Profil **Phase-2-Profil** XAUTH-Profil IP Pools Optionen

Ansicht	20	pro Seite	<<	>>	Filtern in	Keiner	gleich	Los
Standard	Beschreibung	Proposals	Authentifizierung	Modus	DH-Gruppe	Lebensdauer		
<input type="radio"/>	TGB-P1	[AES/SHA1]	Preshared Keys	Aggressiv	2 (1024 Bit)	0KB / 4h		
Seite: 1, Objekte: 1 - 2								
Neu			OK			Abbrechen		

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

IPSec-Peers Phase-1-Profil **Phase-2-Profil** XAUTH-Profil IP Pools Optionen

Ansicht	20	pro Seite	<<	>>	Filtern in	Keiner	gleich	Los
Standard	Beschreibung	Proposals	PFS-Gruppe	Lebensdauer				
<input type="radio"/>	TGB-P1	[AES/SHA1]		0KB / 4h				
Seite: 1, Objekte: 1 - 2								
Neu			OK			Abbrechen		

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

[IPSec-Peers](#) | [Phase-1-Profil](#) | [Phase-2-Profil](#) | [XAUTH-Profil](#) | [IP Pools](#) | [Optionen](#)

Phase-2-Parameter (IPSEC)

Beschreibung: TGB-P2

Verschlüsselung	Authentifizierung	Aktiviert
AES-256	SHA1	<input type="checkbox"/>
AES	MD5	<input type="checkbox"/>
AES	MD5	<input type="checkbox"/>

PFS-Gruppe verwenden: **Aktiviert**
 1 (768 Bit) 2 (1024 Bit) 5 (1536 Bit)

Lebensdauer: 7200 Sekunden 0 kBytes

Erweiterte Einstellungen

IP-Komprimierung: **Aktiviert**

Erreichbarkeitsprüfung: Automatische Erkennung

PMTU propagieren: **Aktiviert**

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

[IPSec-Peers](#) | [Phase-1-Profil](#) | [Phase-2-Profil](#) | [XAUTH-Profil](#) | [IP Pools](#) | [Optionen](#)

Ansicht: 10 pro Seite | Filtern in: Keiner | gleich |

Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status
						<input type="button" value="Info"/> <input type="button" value="Aktivieren"/> <input type="button" value="Deaktivieren"/> <input type="button" value="Löschen"/> <input type="button" value="Suchen"/>

Seite: 1, Objekte: 1 - 2

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

[IPSec-Peers](#) | [Phase-1-Profil](#) | [Phase-2-Profil](#) | [XAUTH-Profil](#) | [IP Pools](#) | [Optionen](#)

Peer-Parameter							
Administrativer Status	<input checked="" type="radio"/> Aktiv <input type="radio"/> Inaktiv						
Beschreibung	TGB Test						
Peer-Adresse							
Peer-ID	Fully Qualified Domain Name (FQDN) client.com						
Preshared Key	••••••••						
Schnittstellenrouten							
IP-Adressenvergabe	Statisch						
Standardroute	<input type="checkbox"/> Aktiviert						
Lokale IP-Adresse	10.254.1.1						
Routeneinträge	<table border="1"> <thead> <tr> <th>Entfernte IP-Adresse</th> <th>Netzmaske</th> <th>Metrik</th> </tr> </thead> <tbody> <tr> <td>10.10.10.10</td> <td>255.255.255.255</td> <td>1</td> </tr> </tbody> </table> <input type="button" value="Hinzufügen"/>	Entfernte IP-Adresse	Netzmaske	Metrik	10.10.10.10	255.255.255.255	1
Entfernte IP-Adresse	Netzmaske	Metrik					
10.10.10.10	255.255.255.255	1					
<input type="button" value="Erweiterte Einstellungen"/>							
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>							

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“.

Erweiterte Einstellungen

Erweiterte IPSec-Optionen	
Phase-1-Profil	TGB-P1
Phase-2-Profil	TGB-P2
XAUTH-Profil	Eines auswählen
Anzahl erlaubter Verbindungen	<input checked="" type="radio"/> Ein Benutzer <input type="radio"/> Mehrere Benutzer
Startmodus	<input checked="" type="radio"/> Auf Anforderung <input type="radio"/> Immer aktiv
Erweiterte IP-Optionen	
Überprüfung der Rückroute	<input type="checkbox"/> Aktiviert
Proxy ARP	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv
IPSec-Callback	
Modus	Inaktiv
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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“.

Doc.Ref	tgbvpn_cg_bintec-rs232b_de
Doc.version	2.0 – sep 2010
VPN version	4.7+

[IPSec-Peers](#)
[Phase-1-Profile](#)
[Phase-2-Profile](#)
[XAUTH-Profile](#)
[IP Pools](#)
[Optionen](#)

Ansicht 10 pro Seite << >> Filtern in Keiner gleich Los

Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status			
2	TGB Test		client.com	TGB-P1	TGB-P2				

Seite: 1, Objekte: 1 - 2

[Neu](#)

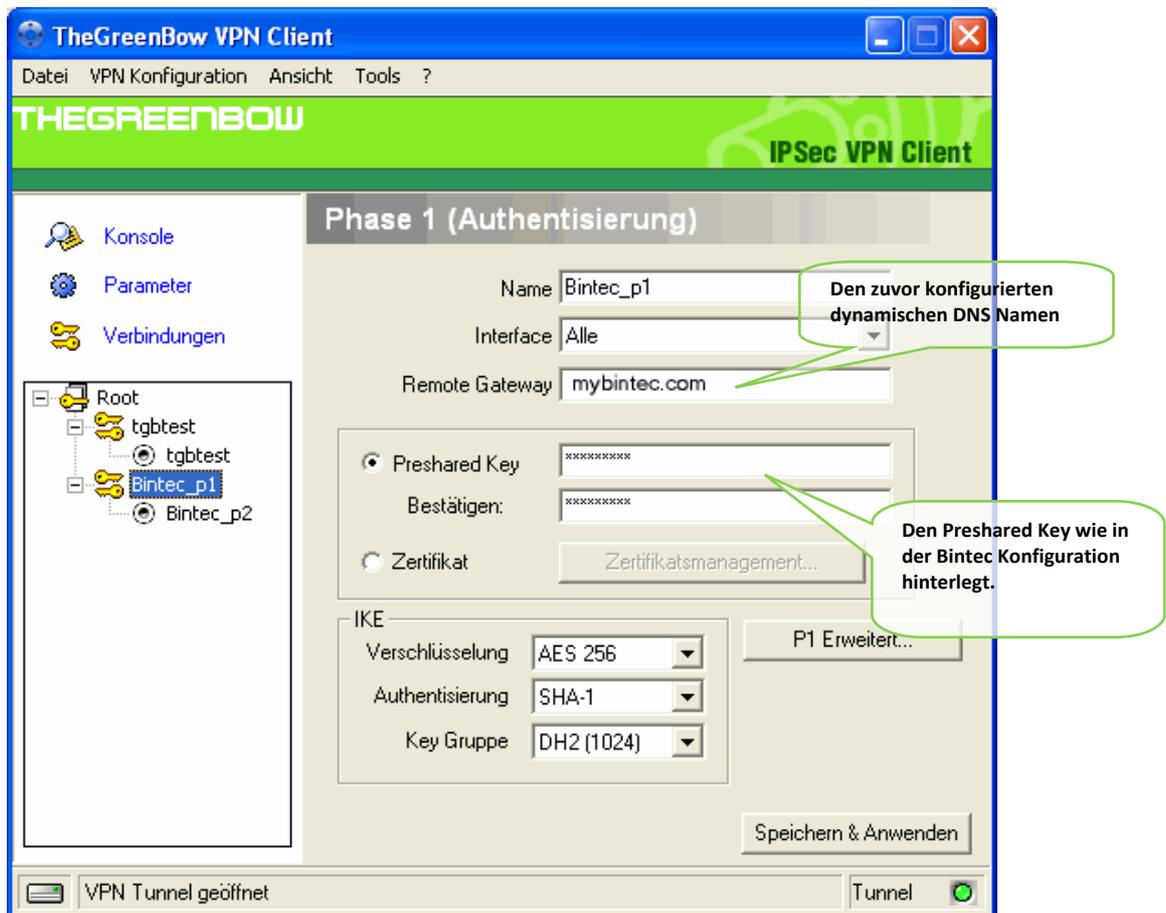
Sie sehen den eingerichteten Tunnel nun in der Übersicht im Menü „IPSec-Peers“. Die Einstellungen im Bintec RS 232b Router sind nun abgeschlossen.

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.

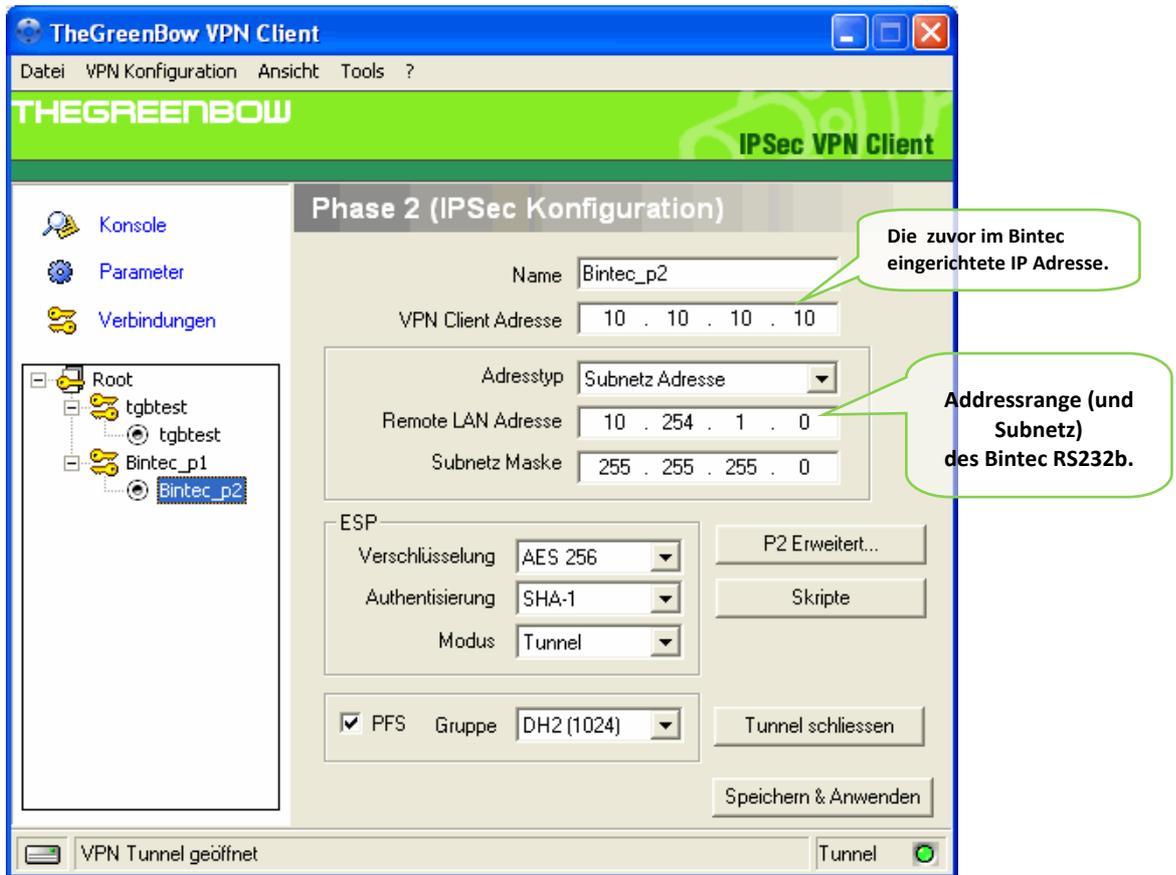
Geben Sie einen eindeutigen Namen für die VPN Verbindung (in unserem Beispiel „**Bintec_p1**“). „**Interface**“ kann auf „**Alle**“ bleiben. Im Feld „**Remote Gateway**“ den dynamischen DNS Namen (in unserem Beispiel „**mybintec.com**“) oder die externe IP Adresse des RS232b eingeben. Setzen Sie nun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

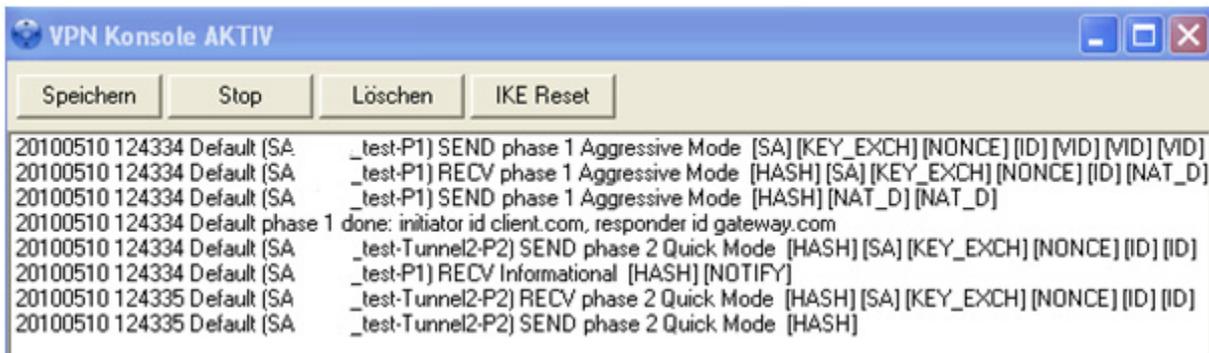


Phase 2 Konfiguration

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/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
2	0.153567	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
3	0.205363	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
4	0.257505	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
5	0.300882	192.168.1.3	192.168.1.2	ISAKMP	Identity Protection (Main Mode)
6	0.310186	192.168.1.2	192.168.1.3	ISAKMP	Identity Protection (Main Mode)
7	0.313742	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
8	0.321913	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
9	0.323741	192.168.1.3	192.168.1.2	ISAKMP	Quick Mode
10	0.334980	192.168.1.2	192.168.1.3	ISAKMP	Quick Mode
11	0.691160	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
12	1.692568	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
13	1.693164	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)
14	2.693600	192.168.1.3	192.168.1.2	ESP	ESP (SPI=0x919bfabc)
15	2.694026	192.168.1.2	192.168.1.3	ESP	ESP (SPI=0x53a5925e)

Frame 1 (142 bytes on wire, 142 bytes captured)
 Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff

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 Firewall-Einstellungen die Kommunikation blockieren.

Doc.Ref	tgbvpn_cg_bintec-rs232b_de
Doc.version	2.0 – sep 2010
VPN version	4.7+

- 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.

THEGREENBOW	Doc.Ref	tgbvpn_cg_bintec-rs232b_de
	Doc.version	2.0 – sep 2010
	VPN version	4.7+

6 Kontakt

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

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

Vertrieb: sales@thegreenbow.de

Secure, Strong, Simple.

TheGreenBow Security Software