



TheGreenBow IPsec VPN Client

Konfigurationsbeispiel

AVM Fritz!Box Fon WLAN 7270

Diese Anleitung gilt auch für andere VPN unterstützende
Geräte von AVM wie z.B.:
FRITZ!Box WLAN 3270
FRITZ!Box Fon WLAN 7170
FRITZ!Box WLAN 3170
FRITZ!Box Fon WLAN 7390

WebSite: <http://www.thegreenbow.de/>

Kontakt: <mailto:support@thegreenbow.de>

Configuration Guide written by:

Autor: Timm Richter

Firma: www.thegreenbow.de

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x

Inhalt

1	Einleitung	3
1.1	Ziel der Anleitung	3
1.2	VPN Netzwerktopologie	3
1.3	FRITZ!Box Fon WLAN 7270 Einschränkungen.....	3
1.4	FRITZ!Box Fon WLAN 7270 VPN Gateway.....	3
1.5	FRITZ!Box Fon WLAN 7270 VPN Gateway Produktinformationen.....	3
2	FRITZ!Box Fon WLAN 7270 VPN Konfiguration.....	4
2.1	Vorbereitungen.....	4
2.2	Die Fritz Fernzugang Konfigurationsdatei erstellen und einspielen	4
3	TheGreenBow IPSec VPN Client Konfiguration.....	8
3.1	VPN Client Phase 1 (IKE) Konfiguration	8
3.2	Phase 1 – Erweiterte Einstellungen	8
3.3	VPN Client Phase 2 (IPSec) Konfiguration	9
3.4	IPSec VPN Tunnel öffnen	10
4	Fehlerbehebung.....	11
4.1	Eine gute Netzwerkanalyse: Wireshark.....	11
5	VPN IPSec Troubleshooting	12
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA]).....	12
5.2	« INVALID COOKIE » error.....	12
5.3	« no keystate » error	12
5.4	« received remote ID other than expected » error.....	12
5.5	« NO PROPOSAL CHOSEN » error	13
5.6	« INVALID ID INFORMATION » error.....	13
5.7	Ich klicke auf “Tunnel öffnen”, aber nichts passiert.....	13
5.8	Der VPN Tunnel ist aktiv aber ich kann nicht pingeln!	13
6	Kontakt.....	15

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x

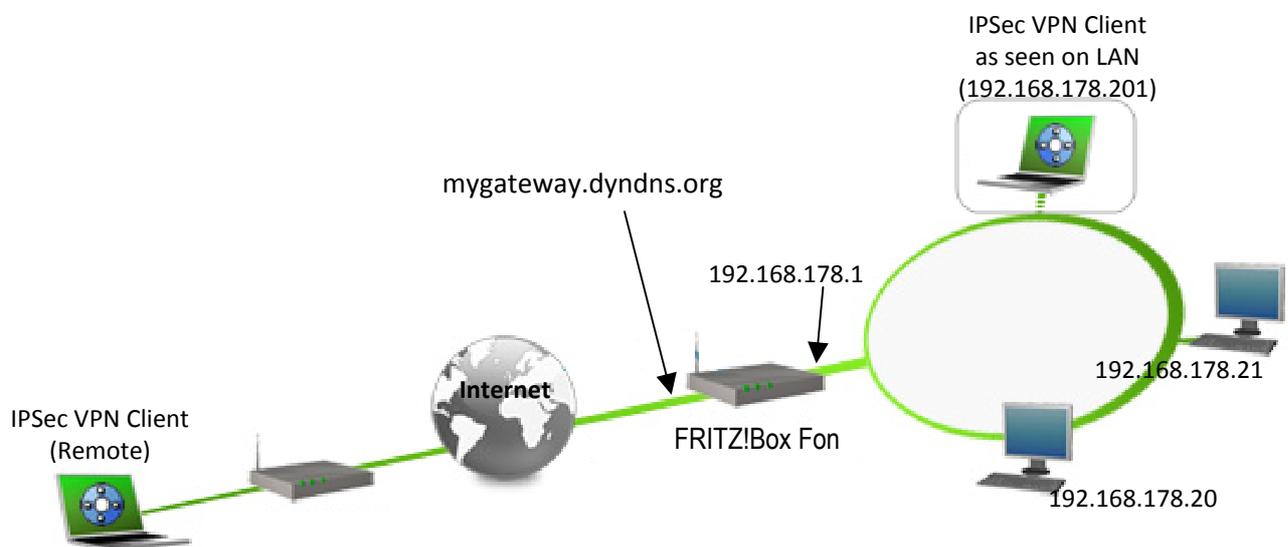
1 Einleitung

1.1 Ziel der Anleitung

Dieses Konfigurationsbeispiel beschreibt eine mögliche Konfiguration des TheGreenBow IPsec VPN Client, um einen IPsec Tunnel zu einer FRITZ!Box Fon WLAN 7270 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 AVM Fritz!Box Fon verbinden. Der Rechner mit dem VPN Client ist mit dem Internet über DSL oder einem Firmennetzwerk verbinden. Die hier aufgeführten IP Adressen und Ranges dienen nur als Beispiel.



1.3 FRITZ!Box Fon WLAN 7270 Einschränkungen

Ältere Firmwareversionen der FRITZ!Box Fon WLAN 7270 beinhalteten noch keine IPsec VPN Unterstützung. Bitte verwenden Sie daher die aktuellste Firmware von AVM, welche volle IPsec VPN Kompatibilität gewährleistet. Die Firmwareversion wird auf der Hauptübersichtsseite der Benutzeroberfläche rechts oben angezeigt. Mehr Informationen finden Sie unter <http://www.avm.de>.

1.4 FRITZ!Box Fon WLAN 7270 VPN Gateway

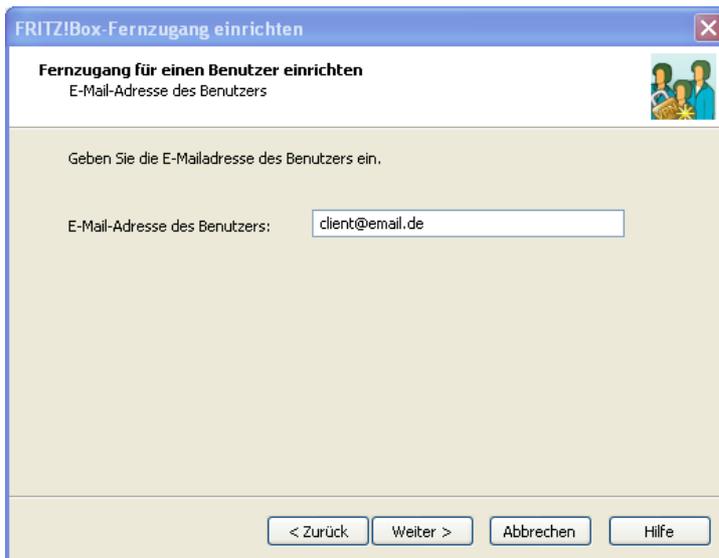
Unseren Test haben wir mit einer FRITZ!Box Fon WLAN 7270 mit der Firmware Version 74.04.76 durchgeführt.

1.5 FRITZ!Box Fon WLAN 7270 VPN Gateway Produktinformationen

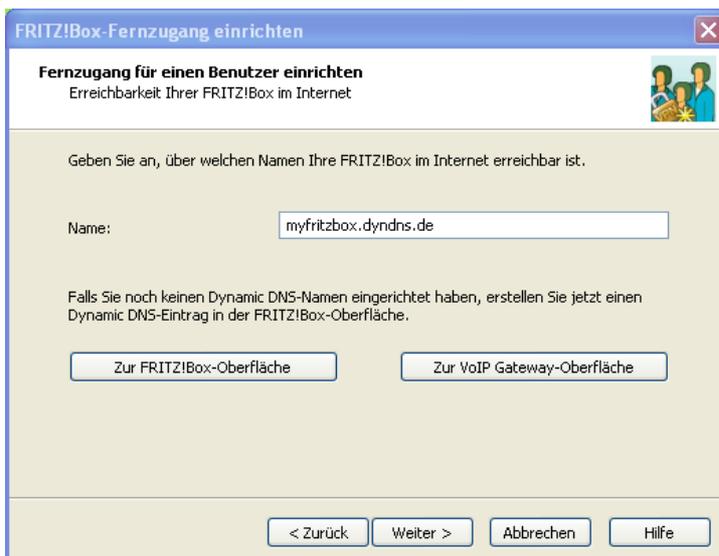
Alle Produktinformationen, Handbücher, FAQ und Hilfestellung zu Ihrer FRITZ!Box Fon WLAN 7270 finden Sie auf den AVM Fritz! Webseiten: <http://www.avm.de/>.

AVM Produktseite	http://www.avm.de/
AVM Handbuch	http://www.avm.de/handbuch
AVM FAQ/Hilfe	http://www.avm.de/serviceportal

	Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
	Doc.version	3.0 – Dec 2009
	VPN version	4.5x

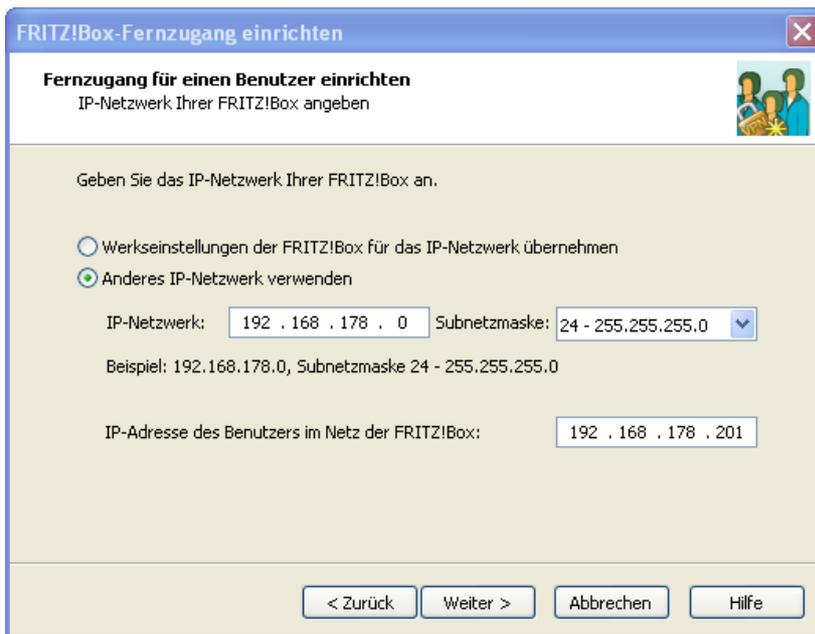


Geben Sie hier eine E-Mail Adresse ein (z.B. client@email.de). Diese E-Mail Adresse dient später als Identifizierungsmerkmal des Tunnel. Klicken Sie nun auf „Weiter“.



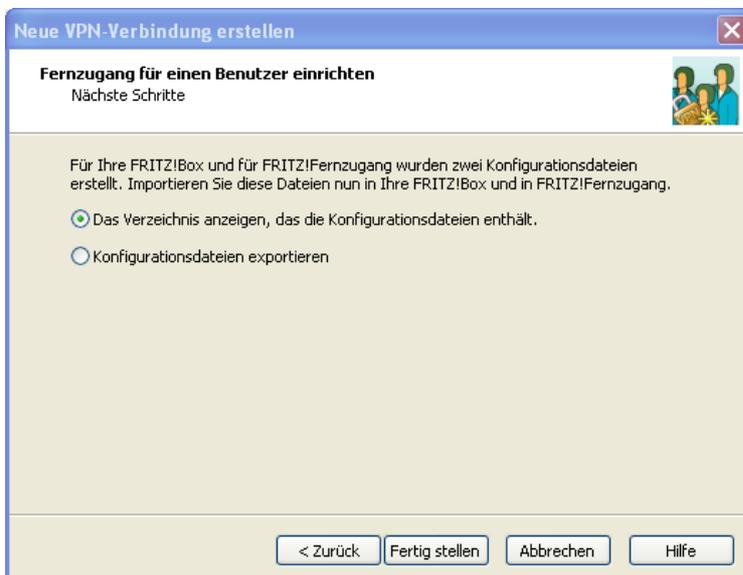
Geben Sie hier bitte den DNS Namen Ihrer Fritz!Box (z.B. myfritzbox.dyndns.de) ein und klicken „Weiter“.

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x



Wählen Sie hier die Option „Anderes IP-Netzwerk verwenden“ und geben Sie die Range des entfernten Netzwerks (das lokale Netzwerk hinter der Fritz!Box) an. In unserem Beispiel die 192.168.178.0 mit der Subnetzmaske 255.255.255.0. Als IP Adresse des Benutzers im Netz der Fritz!Box wählen Sie bitte eine IP, aus der Range des entfernten Netzwerks, hier z.B. die 192.168.178.201 und klicken Sie „Weiter“.

Wichtig: Bitte beachten Sie, dass diese IP **nicht** vom integrierten DHCP Server der Fritz!Box verwaltet werden sollte. Per Werkseinstellung verwaltet der DHCP Server der Fritz!Box die Adressen 192.168.178.20 bis 192.168.178.200.



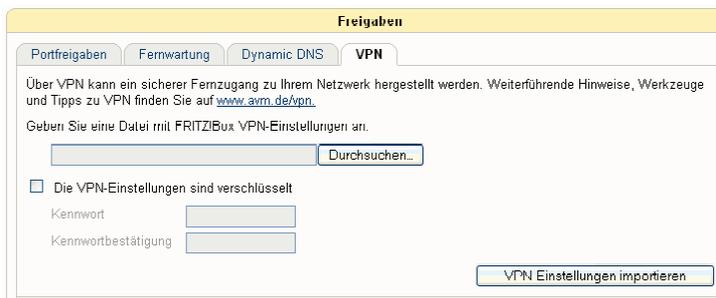
Wählen Sie die Option „Das Verzeichnis anzeigen, das die Konfigurationsdateien enthält“ und klicken Sie „Fertig stellen“.

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x



Sie sehen nun, dass die FRITZ!Box-Fernzugang Software eine VPN Konfigurationsdatei für Ihren Router erstellt hat, hier z.B. fritzbox_myfritzbox_dyndns_de.cfg. Diese Datei muss nun in Ihre Fritz!Box eingespielt werden.

Klicken Sie hierzu in Ihrer Fritz!Box Benutzeroberfläche „Einstellungen“ – „Erweiterte Einstellungen“ – „Internet“ – „Freigaben“ und wählen den Tab „VPN“.



Klicken Sie hier „Durchsuchen“ und wählen Sie im anschließenden Dialog die VPN Konfigurationsdatei (z.B. fritzbox_myfritzbox_dyndns_de.cfg) aus und bestätigen Sie mit „Öffnen“. Klicken Sie nun „VPN-Einstellungen importieren“, die Konfigurationsdatei wird nun eingespielt. Nach erfolgreicher Einspielung sehen Sie unter „VPN Verbindungen“ den konfigurierten und betriebsbereiten Tunnel.



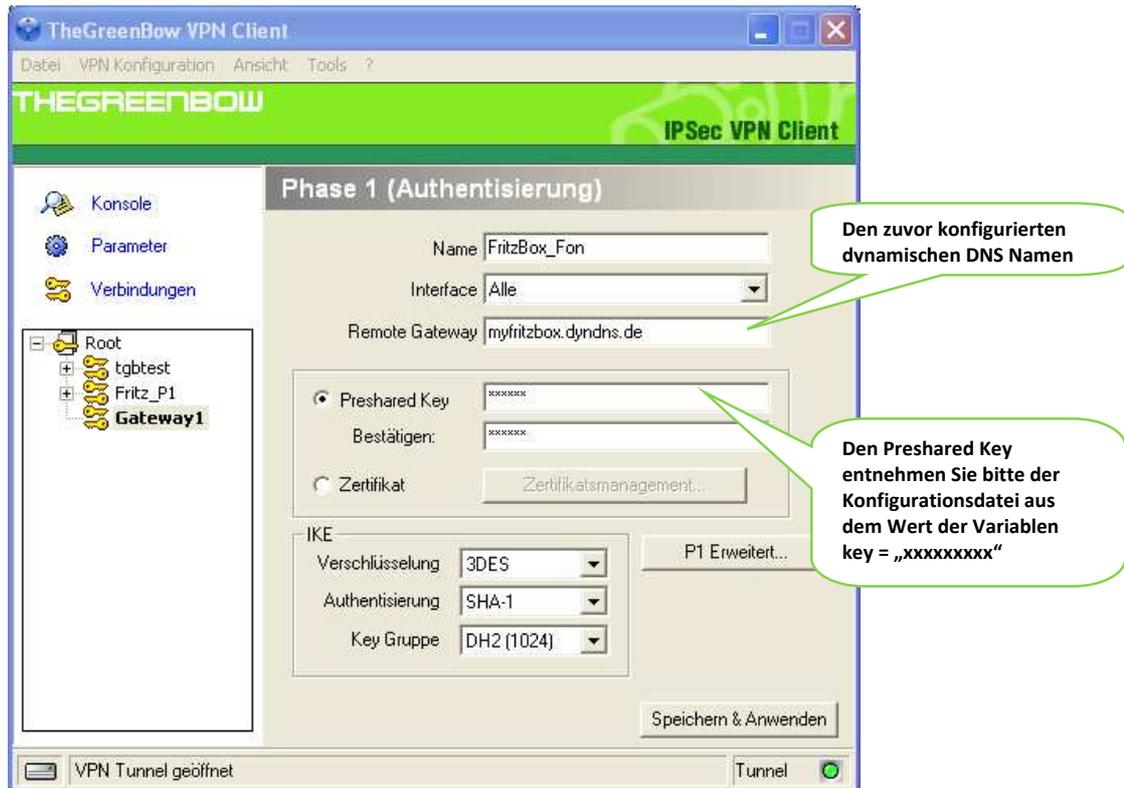
Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x

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 Fritz!Box Fon Dokumentation.

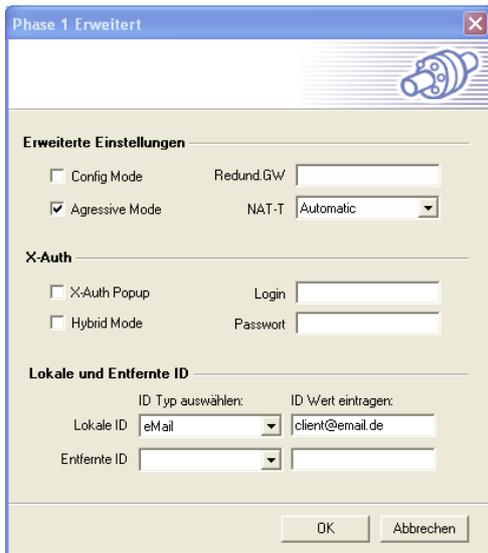
```
keytype = keytype_pre_shared;
key = "fcL2296bc vd3ad8ebb91d%1e] 07#db97";
cert_do_server_auth = no;
```

Öffnen Sie die Konfigurationsdatei, hier z.B. fritzbox_myfritzbox_dyndns_de.cfg mit einem Texteditor. Suchen Sie die Zeile mit der Variable key = "" und verwenden Sie den Wert als Preshared Key im VPN Client.

3.2 Phase 1 – Erweiterte Einstellungen

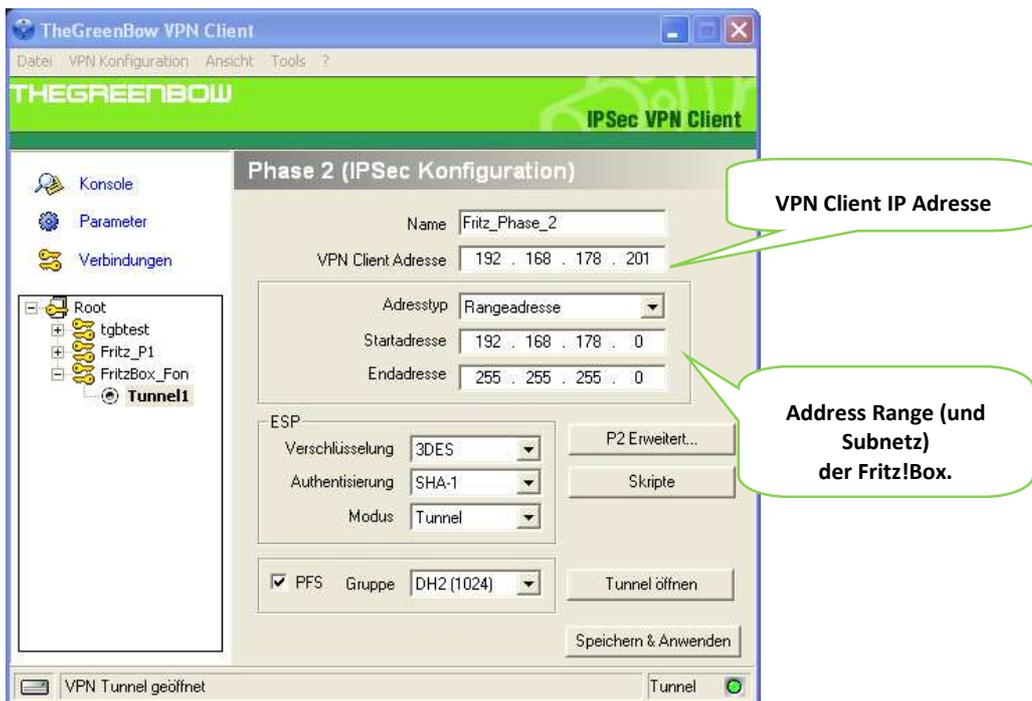
Klicken Sie „P1 Erweitert“ um in die erweiterten Konfigurationseinstellungen der Phase 1 zu gelangen.

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x



Aktivieren Sie die Option "Aggressive Mode". Setzen Sie nun eine lokale ID für den Client. Wählen Sie hier als ID Typ „eMail“ und tragen Sie unter ID Wert die zuvor definierte E-Mailadresse, hier z.B. client@email.de ein. Bestätigen Sie die Einstellungen mit Klick auf „OK“.

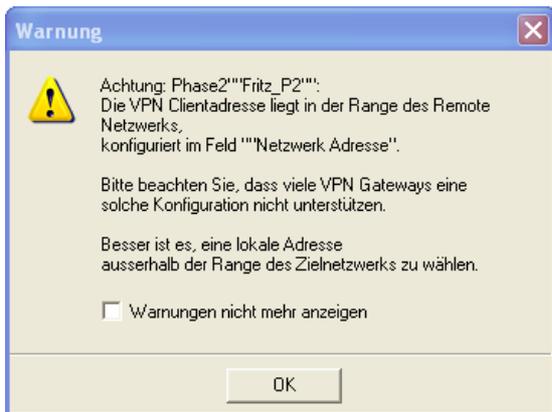
3.3 VPN Client Phase 2 (IPSec) Konfiguration



Phase 2 Konfiguration

Klicken Sie "Speichern & Anwenden" um alle Konfigurationseinstellungen zu sichern. Da die VPN Client Adresse in der Range des Remote Netzwerk liegt, erscheint eine Warnmeldung:

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x



Überspringen Sie diese Warnung mit „OK“, Ihre Fritz!Box unterstützt dieses Feature in vollem Umfang. Der VPN Client wird nun reinitialisiert und 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.

```

20090630 104525 Default (SA Gateway2-P1) SEND phase 1 Main Mode [SA][VID][VID][VID][VID][VID]
20090630 104525 Default (SA Gateway2-P1) RECV phase 1 Main Mode [SA][VID][VID]
20090630 104526 Default (SA Gateway2-P1) SEND phase 1 Main Mode [KEY_EXCH][NONCE][NAT_D][NAT_D]
20090630 104526 Default (SA Gateway2-P1) RECV phase 1 Main Mode [KEY_EXCH][NONCE][NAT_D][NAT_D]
20090630 104526 Default (SA Gateway2-P1) SEND phase 1 Main Mode [HASH][ID][NOTIFY]
20090630 104526 Default (SA Gateway2-P1) RECV phase 1 Main Mode [HASH][ID]
20090630 104526 Default phase 1 done: initiator id 192.168.205.151, responder id mygateway.dyndns.org
20090630 104526 Default (SA Gateway2-Tunnel3-P2) SEND phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20090630 104527 Default (SA Gateway2-Tunnel3-P2) RECV phase 2 Quick Mode [HASH][SA][KEY_EXCH][NONCE][ID][ID]
20090630 104527 Default (SA Gateway2-Tunnel3-P2) SEND phase 2 Quick Mode [HASH]
20090630 104555 Default (SA Gateway2-P1) SEND Informational [HASH][NOTIFY] type DPD_R_U_THERE
20090630 104555 Default (SA Gateway2-P1) RECV Informational [HASH][NOTIFY] type DPD_R_U_THERE_ACK
    
```

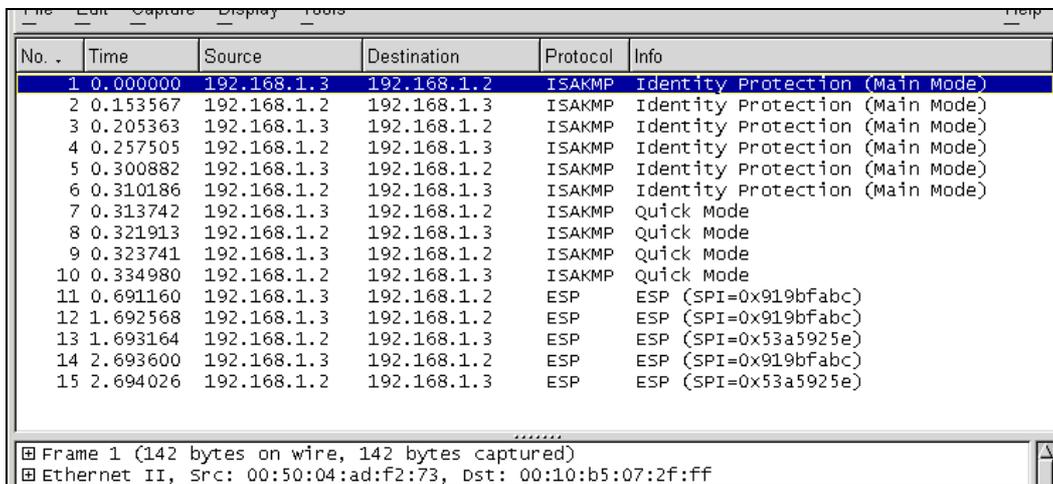
Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x

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

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x

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.

Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x

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 pinggen!

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.

Doc.Ref	tgvpn_cg-avm-fritzbox-fon-WLAN-7270-de
Doc.version	3.0 – Dec 2009
VPN version	4.5x

- Prüfen Sie die Logdateien des VPN Gateway. Auch hier können Firewall-Einstellungen 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.

	Doc.Ref	tgbvpn_cg-avm-fritzbox-fon-WLAN-7270-de
	Doc.version	3.0 – Dec 2009
	VPN version	4.5x

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