WEINZIERL

KNX IP Interface 730
KNX IP Interface 731
KNX IP Router 750
KNX IP Router 751
KNX IP LineMaster 760
KNX IP BAOS 770
KNX IP BAOS 771
KNX IP BAOS 772
KNX IP BAOS 777

Fernzugriff mit der ETS

WEINZIERL ENGINEERING GmbH
Achatz 3
84508 Burgkirchen
Tel.: 08677 / 91 636 0
Fax: 08677 / 91 636 19
E-Mail: info@weinzierl.de
Web: www.weinzierl.de

Inhaltsverzeichnis

Versionen

Stand des Dokumentes	**Datum**	**Bearbeiter**
Entwurf	2009-02-18	F. Heiny
Review	2009-03-04	F. Heiny
LineMaster 760 hinzugefügt Formatierung angepasst	2010-06-17	F. Heiny
KNX IP BAOS 772 hinzugefügt	2011-11-08	S. Matsche
NAT Warnung eingefügt	2014-11-25	St
aktualisiert	2014-12-04	M.Richter
Überarbeitung und Freigabe	2014-12-11	St
KNX IP BAOS 777 hinzugefügt	2015-07-30	St
KNX IP Interface 731, KNX IP Router 751 hinzugefügt	2016-10-11	St

1 Einleitung

Dieses Dokument beschreibt die Möglichkeiten eines Fernzugriffes mit der ETS auf eine KNX-Installation über das Internet. Ein Fernzugriff kann entweder mit der Verwendung von NAT (Network Address Translation) oder auch durch ein VPN (Virtual Private Network) durchgeführt werden.
Der Fernzugriff ist mit allen Geräten, die KNXnet/IP Tunnelling unterstützen, möglich. Dies sind das KNX IP Interface 730/731, der KNX IP Router 750/751, der KNX IP LineMaster 760 sowie das KNX IP BAOS 771, das KNX IP BAOS 772 und das KNX IP BAOS 777. Im Folgenden wird dafür der Begriff KNX IP Geräte verwendet.

2 Fernzugriff mit NAT

2.1 Network Address Translation (NAT)

NAT (Network Address Translation) ist ein Verfahren, um externe IP-Adressen auf interne umzusetzen. Dies wird vor allem in Routern (z.B. DSL-Routern) verwendet.

Bitte beachten Sie, dass der Fernzugriff über NAT ohne weitere Schutzmaßnahmen erhebliche Gefahren birgt. Durch die ungeschützte Portfreigabe wird ein allgemeiner Zugang in Ihr lokales IP Netzwerk und in Ihr KNX System möglich.
Jeder Internetnutzer weltweit kann den freigegebenen Port an Ihrer festen, öffentlichen IP Adresse finden und damit z.B. über die ETS Software auf Ihr KNX Netzwerk zugreifen. Wir raten dringend, den Zugang über NAT nur temporär zu Test- oder Diagnosezwecken zu öffnen und anschließend den Port umgehend wieder zu schließen, um Missbrauch zu verhindern.
Sollte der Fernzugriff über NAT realisiert werden, raten wir Ihnen dringend nicht den Standard-Port 3671 in Richtung Internet anzugeben. Da es sich bei Port 3671 um den offiziellen Port für efcp – eFieldControl(EIBnet) der KNX Association handelt, kann dieser leichter von Unbefugten ermittelt werden. Bitte verwenden Sie einen Port aus dem nicht reservierten Bereich zwischen Port 50000 und Port 60000.

Ein dauerhafter Fernzugriff sollte nur geschützt eingerichtet werden! Dazu empfehlen wir den Fernzugriff über VPN (Virtual Private Network). Die VPN Funktion ist in vielen DSL Routern bereits integriert.

2.2 Beispiel einer Konfiguration

2.2.1 Aufbau

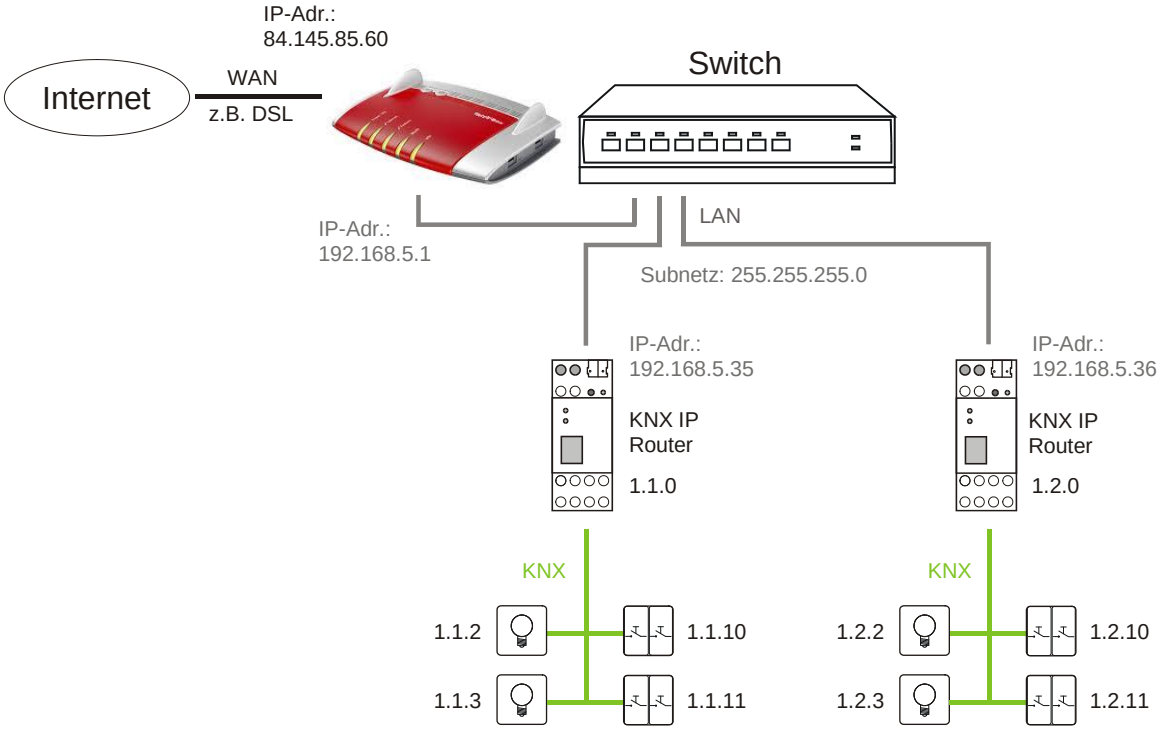

Abbildung 1: KNX-Installation

Obenstehende Abbildung zeigt eine typische KNX-Installation, die über einen DSL-Router an das Internet angebunden ist. Zwei TP-Linien werden hier über zwei KNX IP Router miteinander verbunden. Diesen KNX IP Routern wurden IP-Adressen aus dem lokalen Netz zugewiesen. Der für den Internetzugang erforderliche DSL-Router hat eine lokale IP-Adresse (192.168.5.1) die fest zugewiesen ist, sowie eine öffentliche IP-Adresse (hier 84.145.85.60), welche vom Internet-Provider vergeben wird. Diese öffentliche IP-Adresse ist in der Regel dynamisch, d.h. sie wird bei jedem Aufbau einer Internetverbindung neu vergeben.

2.2.2 Erforderliche Einstellungen im DSL-Router (FRITZ!Box 7490)

Im DSL-Router ist unter dem Punkt „Freigaben“ eine Weiterleitung zu erstellen. Dazu ist ein Port (Standard: 3671) und eine IP-Adresse (lokale IP-Adresse des KNX IP Gerätes, z.B. 192.168.5.30) anzugeben. Nun werden alle Telegramme, die aus dem Internet empfangen werden und an den Port 52011 gerichtet sind, auf das angegebene KNX IP Gerät an Port 3671 weitergeleitet.
Da es sich bei Port 3671 um den offiziellen Port für efcp – eFieldControl(EIBnet) der KNX Association handelt, ist es ratsam in Richtung Internet nicht den Standard-Port zu verwenden! Wie in unserem Beispiel beschrieben, raten wir Ihnen dringend einen Port aus dem nicht reservierten Bereich zwischen Port 50000 und Port 60000 zu verwenden!

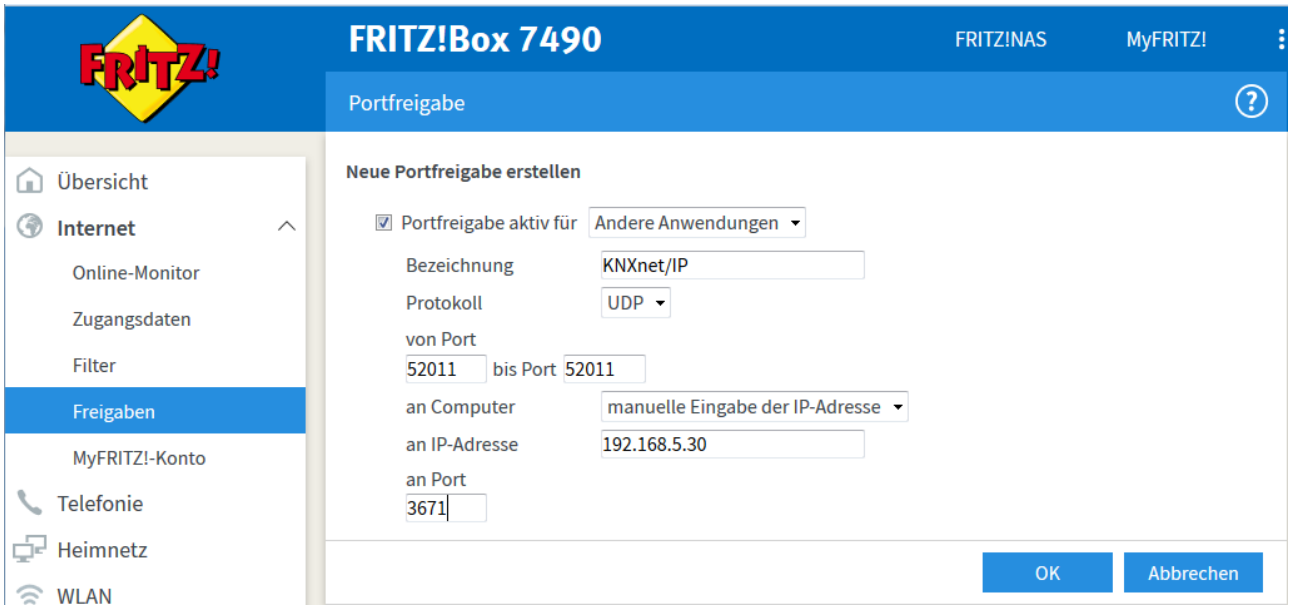

Abbildung 2: Einstellungen im DSL-Router (Portfreigabe für KNXnet/IP)

Abbildung 3: Einstellungen im DSL-Router (Liste der Portfreigaben)

2.2.3 IP-Konfiguration des KNX IP Interfaces

Da die IP-Adresse des KNX IP Gerätes bekannt sein muss, empfiehlt sich eine manuelle Konfiguration. Dazu müssen die IP-Adresse (192.168.5.30), die Subnetzmaske (255.255.255.0) und die Gateway-IP-Adresse (192.168.5.1) angegeben werden.

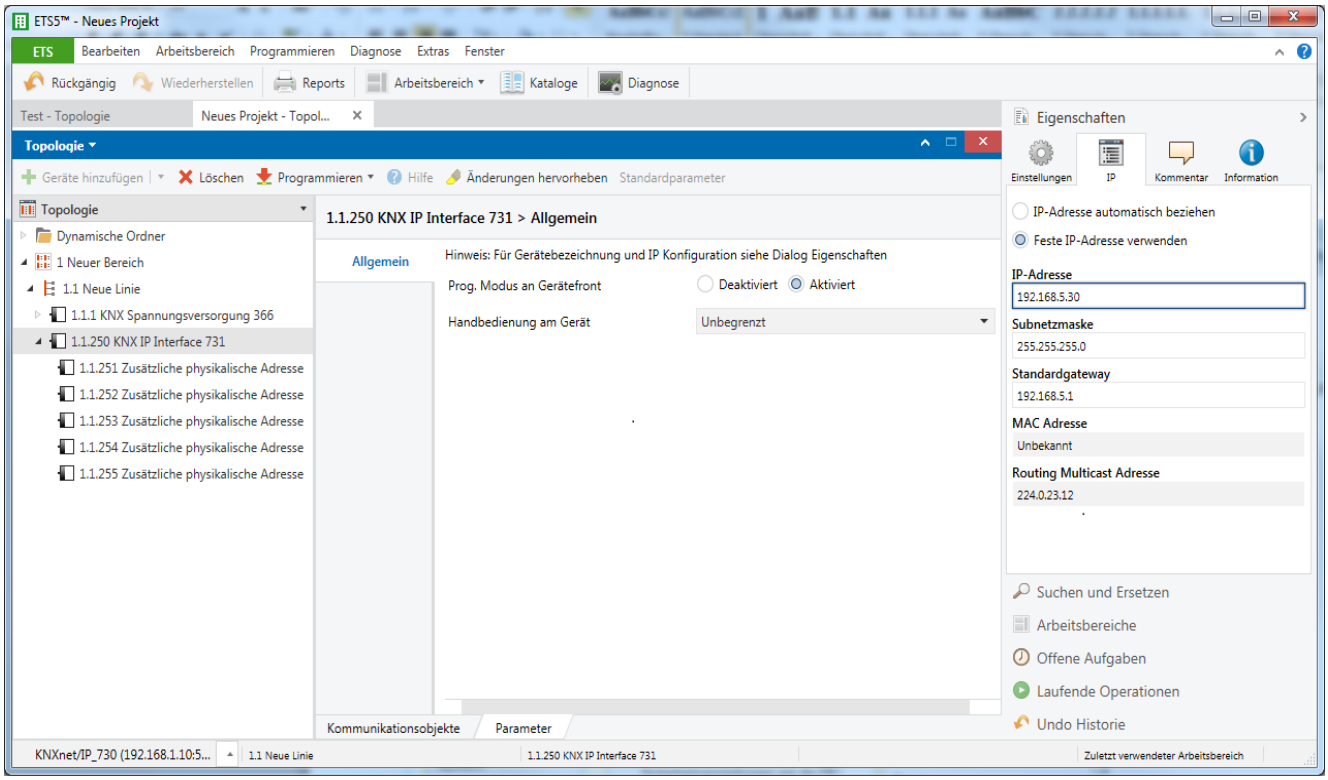

Abbildung 4: IP-Konfiguration exemplarisch an einem KNX IP Interface 731 mit ETS 5

2.2.4 Verbindungsaufbau mit der ETS

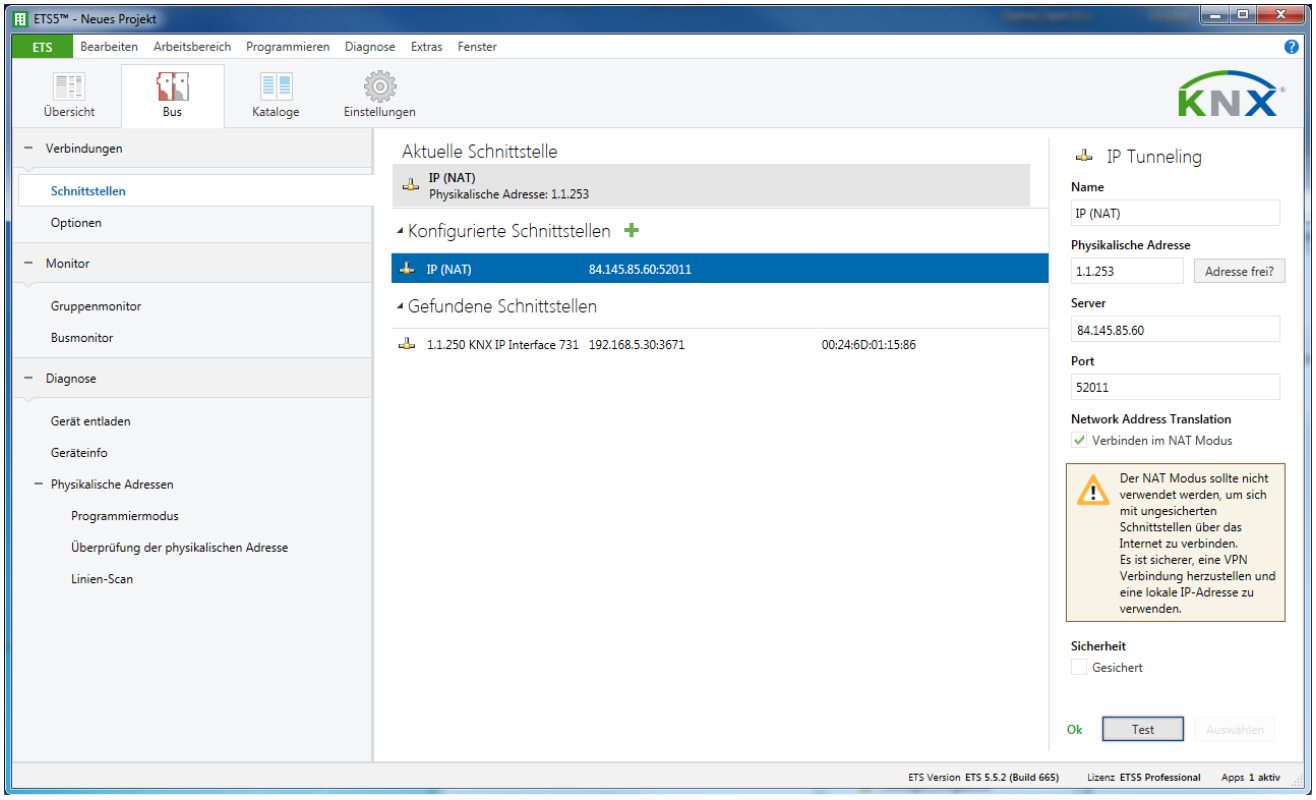

Abbildung 5: ETS Verbindung

Es sollte für den Fernzugriff eine eigene Verbindung angelegt werden, hier im Beispiel „IP (NAT)“. Als Typ ist „IP-Tunneling“ auszuwählen. Im Feld „Server“ muss die öffentliche IP-Adresse der entfernten KNX-Installation eingetragen werden. Der hier angegebene Port (52011) muss der gleiche sein, wie in den Einstellungen des DSL-Routers.
Wichtig: Das Häkchen „Verbinden im NAT-Modus“ muss gesetzt sein.
Anmerkung: Die IP-Adresse muss hier manuell eingetragen werden, da das Scannen von Geräten über das Internet nicht möglich ist.
Für den Fernzugriff mittels NAT ist mindestens die ETS 3.0f erforderlich.

3 Fernzugriff über ein VPN

3.1 Virtual Private Network (VPN)

Ein VPN ist eine Erweiterung privater Netzwerke. Über ein VPN lassen sich Fernzugriff (Site-To-End) und Kopplung privater Netzwerke (Site-To-Site) über das Internet realisieren.

3.1.1 Site-To-End

Mit einem Site-To-End VPN kann ein Zugriff auf ein internes Netz aufgebaut werden. Beispielsweise können sich so Mitarbeiter von außerhalb in das Netz ihrer Firma einwählen.

3.1.2 Site-To-Site

Mit einem Site-To-Site VPN können private Netze untereinander gekoppelt werden. Beispielsweise erlaubt ein Site-To-Site VPN die Kopplung zweier entfernter Firmennetze.

3.2 VPN - Fernzugriff auf einen KNX/IP-Router am Beispiel der Fritzbox 7490

Als Beispielaufbau wird hier eine Verbindung über das Internet zwischen einem PC in Liegenschaft A und einer Fritzbox 7490 in Liegenschaft B erklärt. Die KNX-Anlage in Liegenschaft B ist wie in Abbildung 1 konfiguriert.
Über einen VPN-Tunnel kann die ETS in Liegenschaft A mit der KNX-Anlage in Liegenschaft B gesichert kommunizieren. Die KNX-Anlage bleibt dabei nach außen hin gesichert. Nur der PC in Liegenschaft A hat Zugriff über das Internet auf die Anlage.

3.2.1 VPN-Tunnel einrichten

Für die Konfiguration der Fritzbox wird ein Tool von AVM www.avm.de benötigt (FRITZ!Box-Fernzugang_einrichten.exe). Mit diesem Tool werden alle nötigen Daten für den VPN-Tunnel erfasst.

Nach Abschluss stehen zwei Konfigurations-Dateien zur Verfügung. Eine Datei wird in die Fritzbox (Liegenschaft B) importiert und die andere ist für ein weiteres Windows-Tool von AVM vorgesehen, dass den VPN-Tunnel herstellt und verwaltet (siehe Punkt 3.2.3) (VPN-Client für PC mit ETS in Liegenschaft A).

Hinweis:
Ein VPN-Tunnel mit der Fritzbox lässt sich nur mit den Tools von AVM aufbauen. Der Windows-VPN-Client ist nicht mit dem VPN-Server der Fritzbox kompatibel.

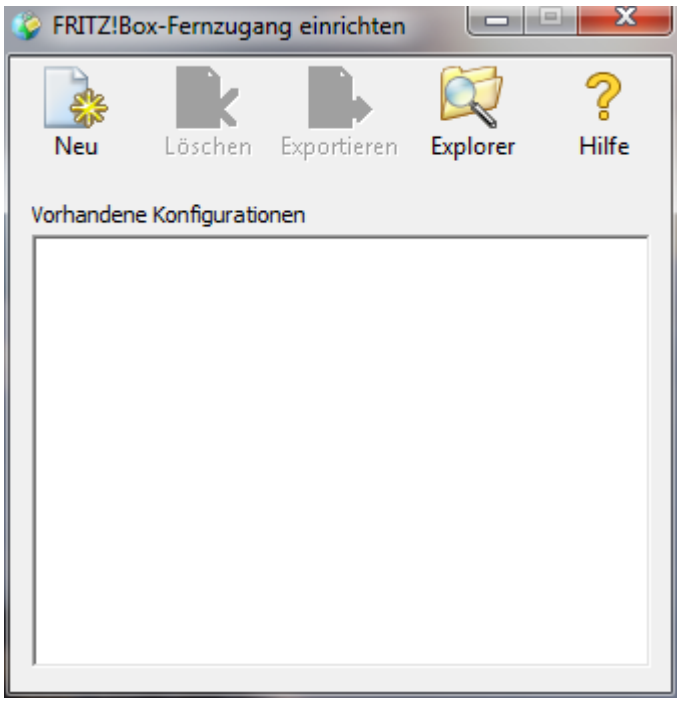

Abbildung 7: AVM Einrichtungstool

Mit diesem Tool werden alle nötigen Daten für einen VPN-Tunnel erfasst. Mit Klick auf „Neu“ erscheint folgendes Fenster:

Abbildung 8: Modus wählen

Für das o.g. Beispiel wird der erste Punkt „Fernzugang für einen Benutzer einrichten“ gewählt.

Abbildung 9: Plattform wählen

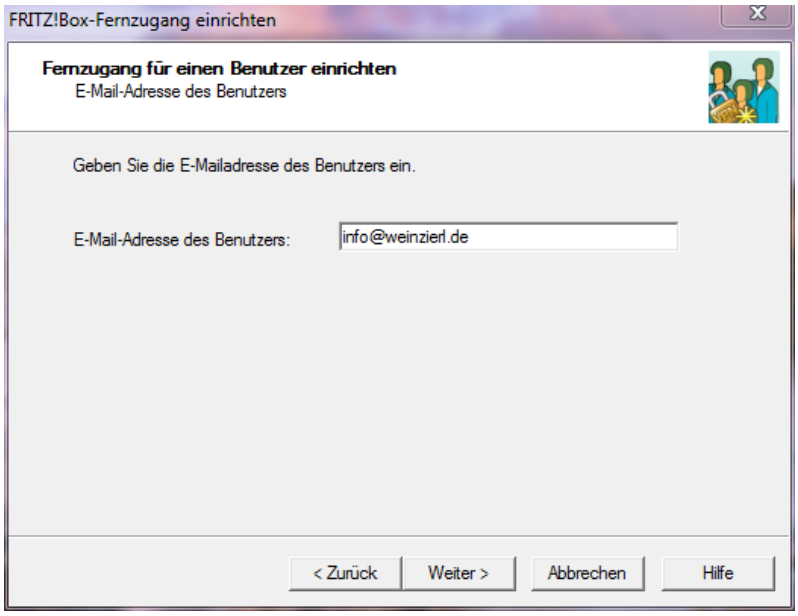

Abbildung 10: Benutzerkonto

Im nächsten Schritt muss das Benutzerkonto mit einem Namen definiert werden. Es ist nicht zwingend notwendig, hier eine E-Mail Adresse anzugeben.

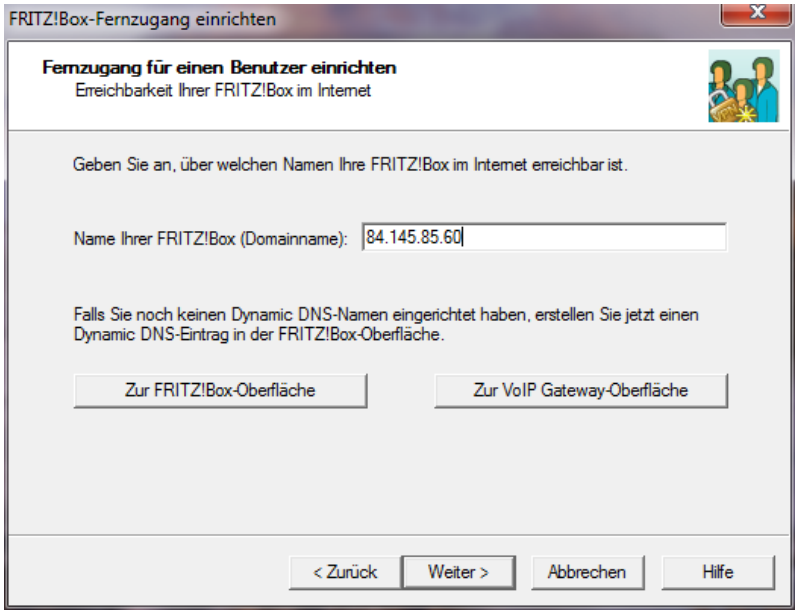

Abbildung 11: VPN-Server definieren

In diesem Fenster wird die zu erreichende Fritzbox in Liegenschaft B definiert. Man kann eine feste IP-Adresse eingeben, oder man benutzt eine dynamische Adresse (DynDNS), wie sie z.B. von www.dyn.com, oder www.Selfhost.de angeboten werden.

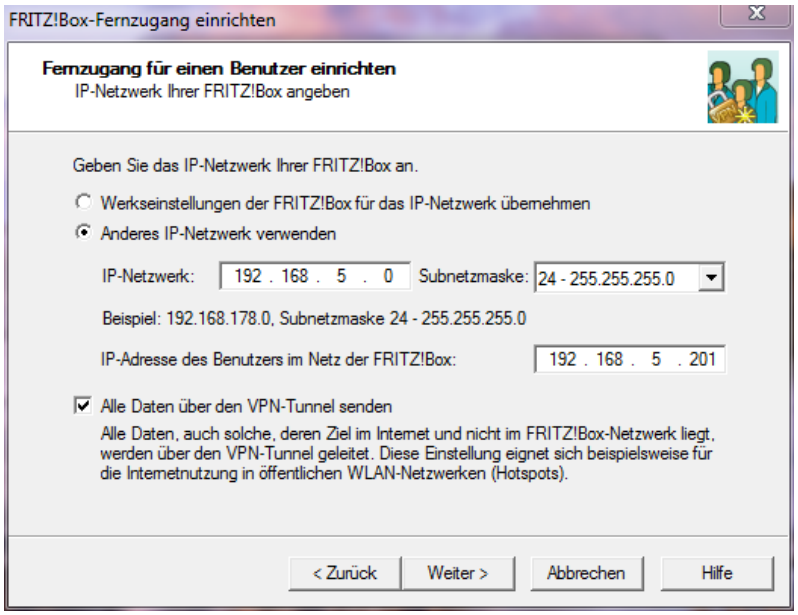

Abbildung 12: IP-Subnetz der Liegenschaft B einrichten

Hinweis:
Die „IP-Adresse des Benutzers im Netz der FRITZ!Box:“ darf nicht bereits von einem andern IP Gerät im Subnetz verwendet werden

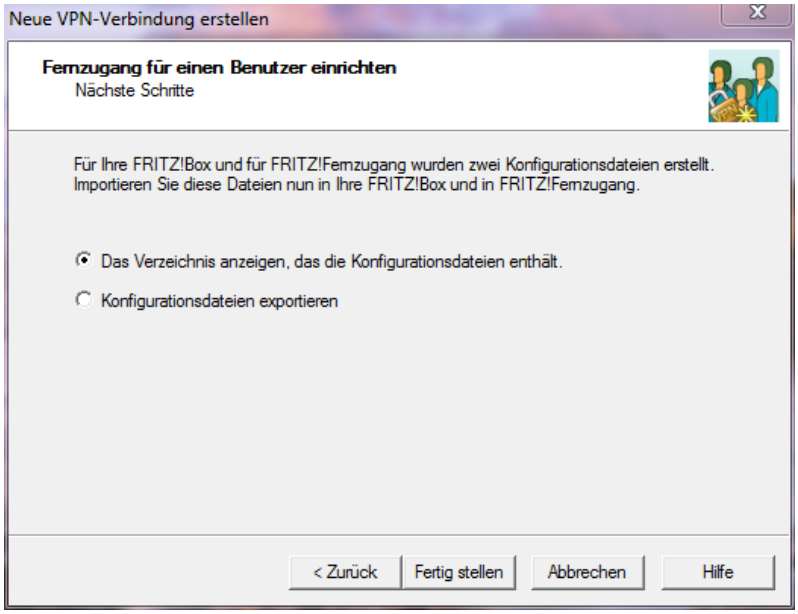

Abbildung 13: Konfiguration beenden

Zum Schluss wählt man die erste Position in diesem Fenster, um direkt auf die vom Tool erzeugten Dateien zugreifen zu können.

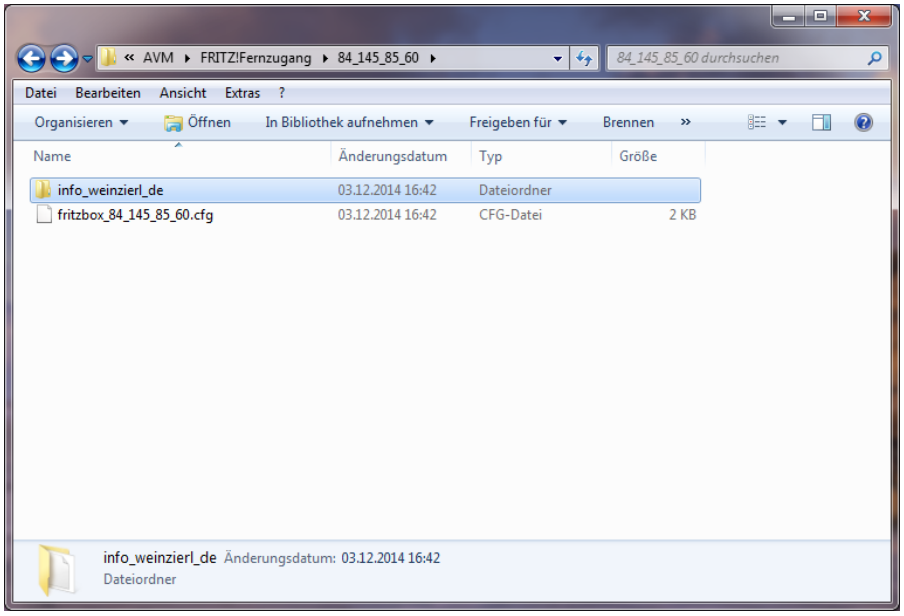

Abbildung 14: Konfigurationsdateien

Im Verzeichnis
…\User\AppData\Roaming\AVM\FRITZ!Fernzugang
wird ein Verzeichnis mit dem Namen der Fritzbox in Liegenschaft B erzeugt.
In diesem Verzeichnis befindet sich eine Konfigurationsdatei für die Fritzbox in Liegenschaft B und ein weiteres Verzeichnis für den Benutzer des VPN-Tunnels in Liegenschaft A.

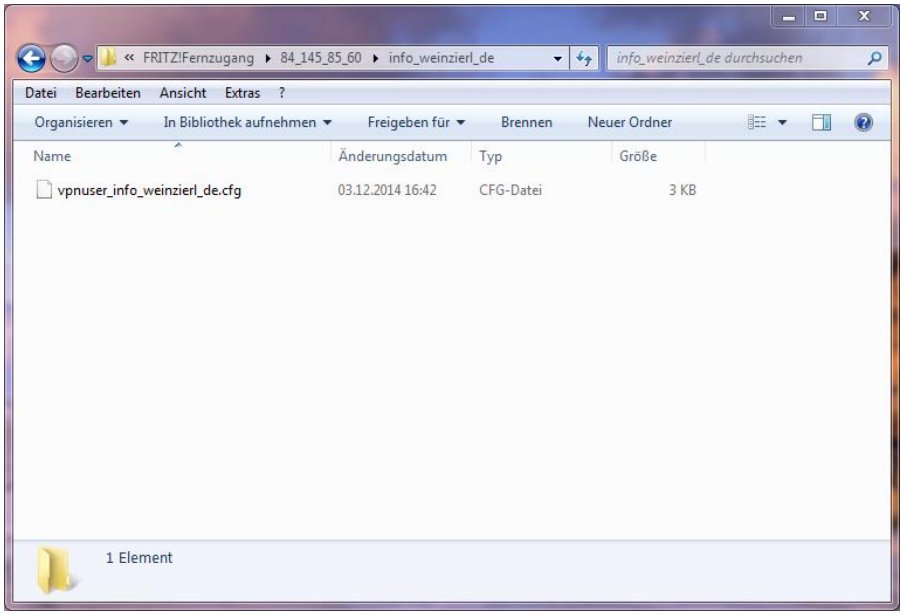

Abbildung 15: Konfigurationsdatei(en) Benutzer

Wenn man mehrere VPN-Tunnel für die Fritzbox in Liegenschaft B benötigt, erscheinen hier die Konfigurationsdateien aller angelegten Benutzer.

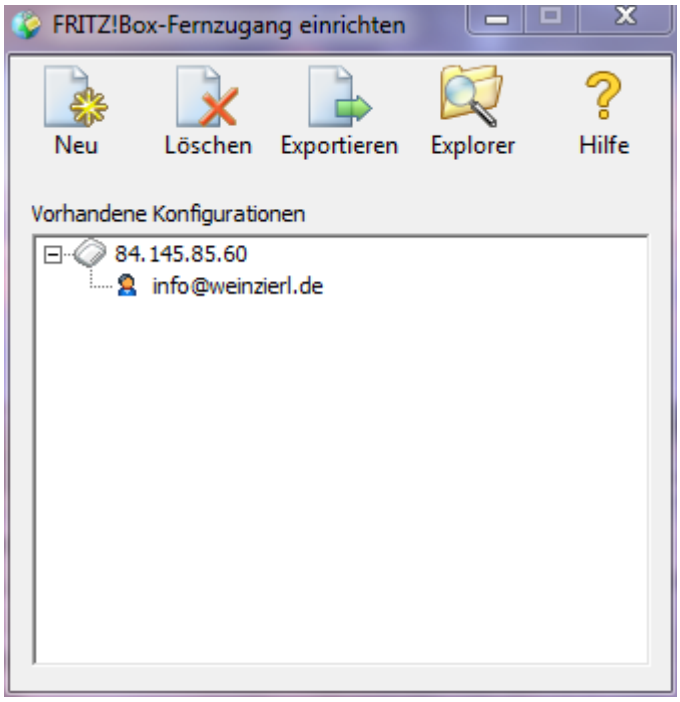

Abbildung 16: vollständige Konfiguration

Damit ist die Konfiguration des VPN-Tunnels abgeschlossen. Alle nötigen Daten für die Fritzbox und den VPN-Client befinden sich in den beiden Konfigurationsdateien.

Das Einrichtungstool definiert selbstständig ein Passwort (shared key) für den VPN-Tunnel.

3.2.2 VPN-Server (Fritzbox) einrichten (Liegenschaft B)

Abbildung 17: VPN-Fritzbox – Verbindung hinzufügen

In Menüpunkt „Freigaben“ findet man unter anderem auch den Reiter „Dynamic DNS“ zur Definierung einer DynDNS.
Für den VPN-Tunnel wählt man den Reiter „VPN“ und die Schaltfläche „VPN-Verbindung hinzufügen“.

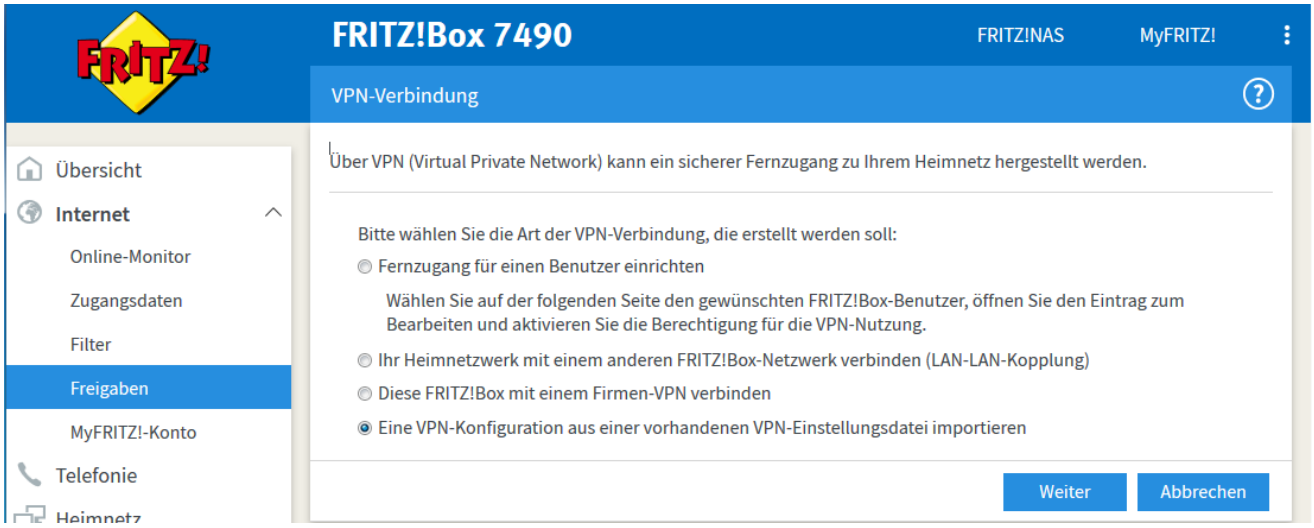

Abbildung 18: VPN-Fritzbox – Konfigurationsart wählen

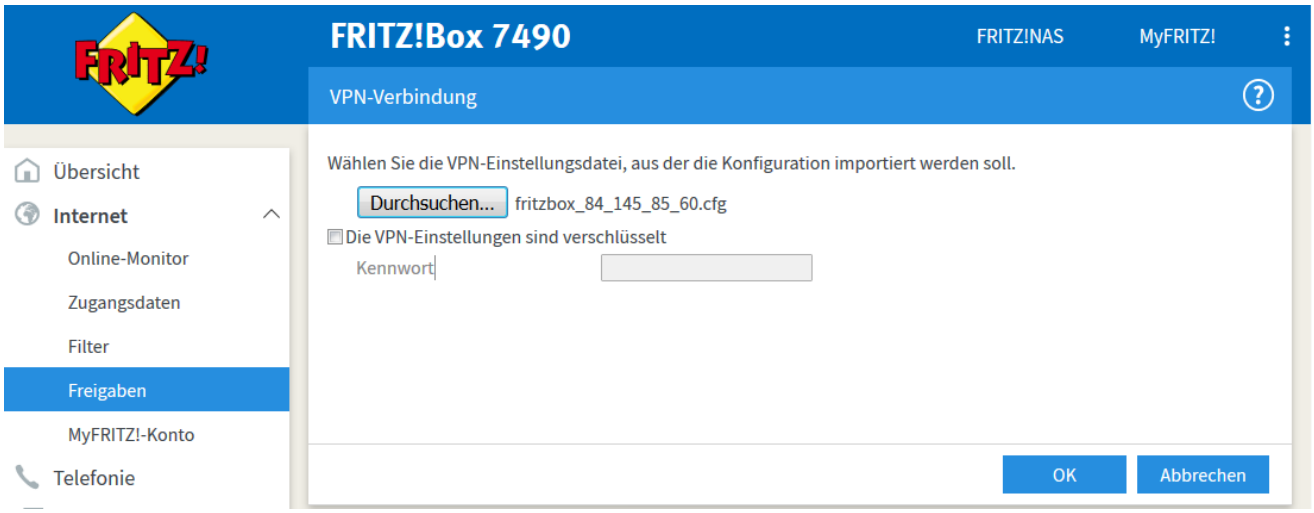

Abbildung 19: VPN-Fritzbox – Konfigurationsdatei wählen

Die Datei fritzbox_84_145_85_60.cfg wurde zuvor mit dem Einrichtungstool „FRITZ!Fernzugang einrichten“ erstellt.

Abbildung 20: VPN-Fritzbox – VPN-Freigaben

3.2.3 VPN-Client (PC) (Liegenschaft A)

Für den Client wird ein Tool von AVM benötigt. Auf dem Datei-Server von AVM findet man für jedes System die entsprechende Variante:

http://download.avm.de/fritz.box/tools/vpn/fritz_fernzugang/

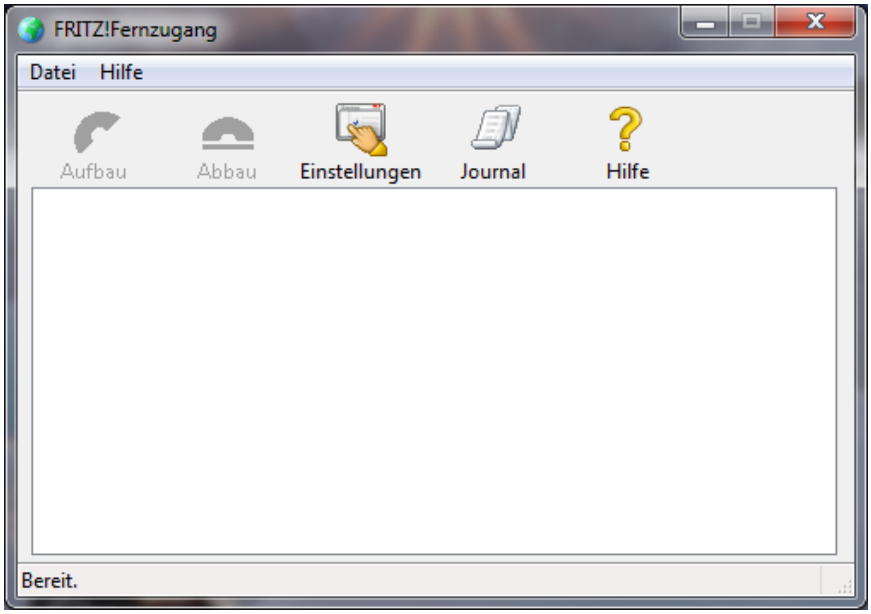

Abbildung 21: VPN-Client

Dieser Client kann auch automatisch mit Windows gestartet werden.

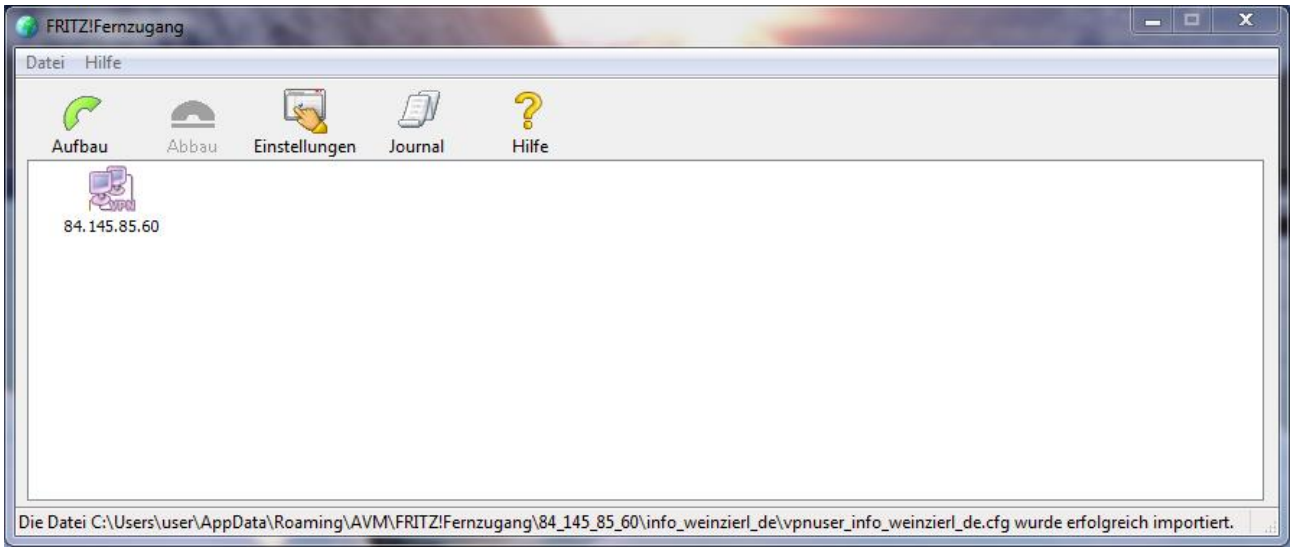

Abbildung 22: Importierte Verbindung

Verbindung auswählen (selektieren) und auf „Aufbau“ klicken.

3.2.4 Zugriff mit der ETS auf das entfernte KNX IP Gerät

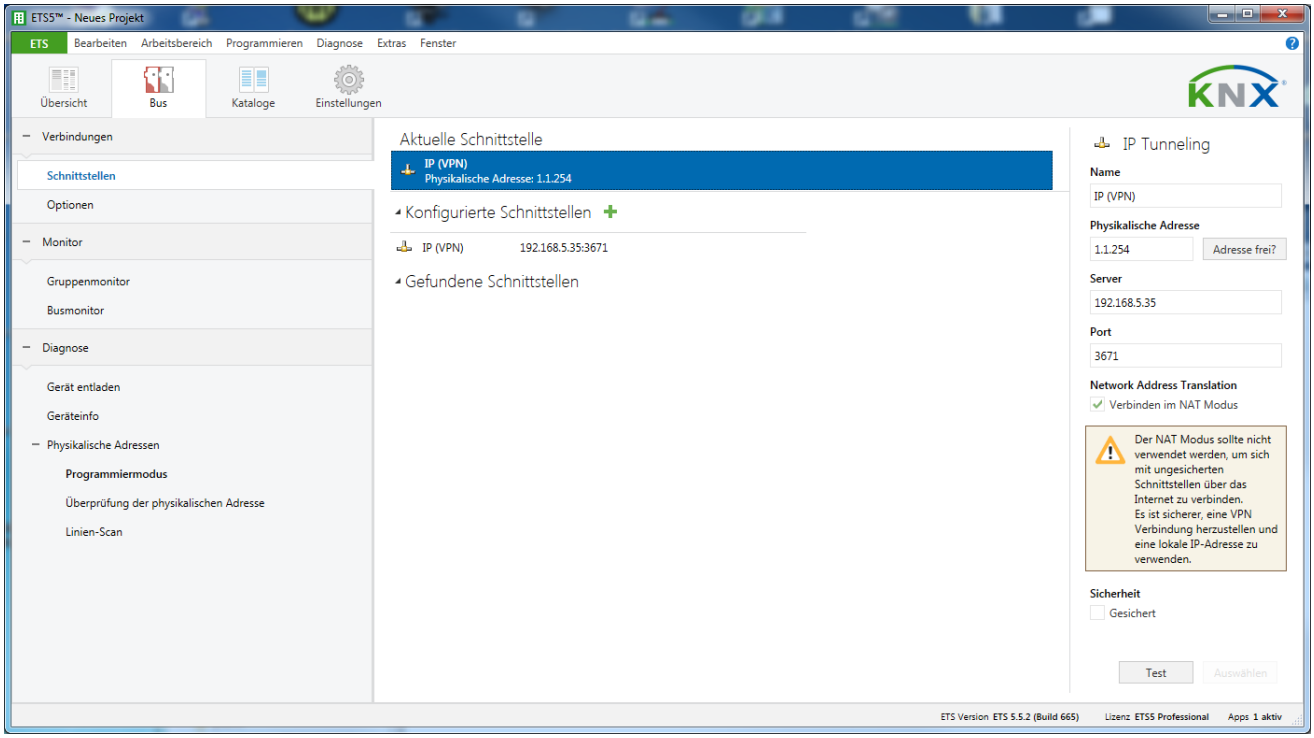

Abbildung 23: VPN-Schnittstelle in der ETS

Die IP-Schnittstelle wird nicht automatisch gefunden. Sie muss manuell konfiguriert werden. Als Server wird die IP Adresse des KNX IP Routers im Netzwerk der Liegenschaft B angegeben (hier 192.168.5.35).

Hinweis: Der Haken „Verbinden im NAT-Modus“ ist zwingend zu setzen. Die Verbindung wird dennoch nicht im NAT-Modus aufgebaut. Durch diese Aktivierung wird eine wichtige Initialisierung durchgeführt, die bedingt durch den IP-Aufsatz nötig ist.

3.2.5 Alternative Möglichkeiten

Neben der verwendeten Fritzbox 7490 gibt es noch weitere Geräte mit denen ein VPN aufgebaut werden kann. Es sind beispielsweise von Linksys, Netgear und DrayTek entsprechende Geräte erhältlich.

Neben einer Embedded-Lösung kann auch ein PC mit „OpenVPN“ verwendet werden.

Copyright Weinzierl Engineering GmbH 2016

Marken: Kennzeichen wie AVM, FRITZ! Und FRITZ!Box (Produktnamen und Logos) sind geschützte Marken der AVM GmbH. Microsoft, Windows und das Windows Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.