

KNX IP Interface 731

KNX IP Interface 732 *secure*

KNX IP Router 751

KNX IP Router 752 *secure*

KNX IP LineMaster 762

KNX IP BAOS 773

KNX IP BAOS 774

KNX IP BAOS 777

Fernzugriff mit der ETS

WEINZIERL ENGINEERING GmbH

Achatz 3

84508 Burgkirchen

Tel.: 08677 / 91 636 0

E-Mail: info@weinzierl.de

Web: www.weinzierl.de

Inhaltsverzeichnis

1	Einleitung.....	3
2	Fernzugriff mit NAT.....	4
2.1	Network Address Translation (NAT).....	4
2.2	Beispiel einer Konfiguration.....	5
2.2.1	Aufbau.....	5
2.2.2	Erforderliche Einstellungen im DSL-Router (FRITZ!Box 7490).....	6
2.2.3	IP-Konfiguration des KNX IP Interfaces.....	8
2.2.4	Verbindungsaufbau mit der ETS.....	9
3	Fernzugriff über ein VPN.....	10
3.1	Virtual Private Network (VPN).....	10
3.1.1	Site-To-End.....	10
3.1.2	Site-To-Site.....	10
3.2	VPN - Fernzugriff auf einen KNX/IP-Router am Beispiel der Fritzbox 7490.....	10
3.2.1	VPN-Tunnel einrichten.....	10
3.2.2	VPN-Server (Fritzbox) einrichten (Liegenschaft B).....	16
3.2.3	VPN-Client (PC) (Liegenschaft A).....	18
3.2.4	Zugriff mit der ETS auf das entfernte KNX IP Gerät.....	19
3.2.5	Alternative Möglichkeiten.....	19
4	KNX IP Security.....	20
5	Kombinationen von Zugriffsarten und KNX secure.....	21

1 Einleitung

Dieses Dokument beschreibt die Möglichkeiten eines Fernzugriffes z. B. mit der ETS auf eine KNX-Installation über das Internet.

Für viele KNX Installationen ist der Fernzugriff eine wesentliche Anforderung. Zum einen für den Installateur, der die Anlage aus der Ferne wartet und optimiert, zum anderen aber auch für den Nutzer des Objektes, der Anzeige- und Bedienfunktionen erwartet. Hier bietet das Internet Protokoll IP eine durchgängige Möglichkeit, von beliebigen Standorten weltweit bis in die einzelne Liegenschaft zu kommunizieren.

Gleichzeitig birgt die Nutzung des Internets die Gefahr von unerlaubten Zugriffen. Um diese zu verhindern, sind technische Maßnahmen erforderlich, die nachfolgend aufgeführt sind.

Ein Fernzugriff kann entweder mit der Verwendung von NAT (Network Address Translation) oder auch durch ein VPN (Virtual Private Network) durchgeführt werden. Zusätzlich zur Auswahl der Zugriffsart, ist es möglich, das KNX Netzwerk auch mittels KNX Security abzusichern.

Der Fernzugriff ist mit allen Geräten, die KNXnet/IP Tunnelling unterstützen, möglich. Dies sind das KNX IP Interface 731 / 732 secure , der KNX IP Router 751 / 752 secure, der KNX IP LineMaster 762 sowie das KNX IP BAOS 773, das KNX IP BAOS 774 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 efc – 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

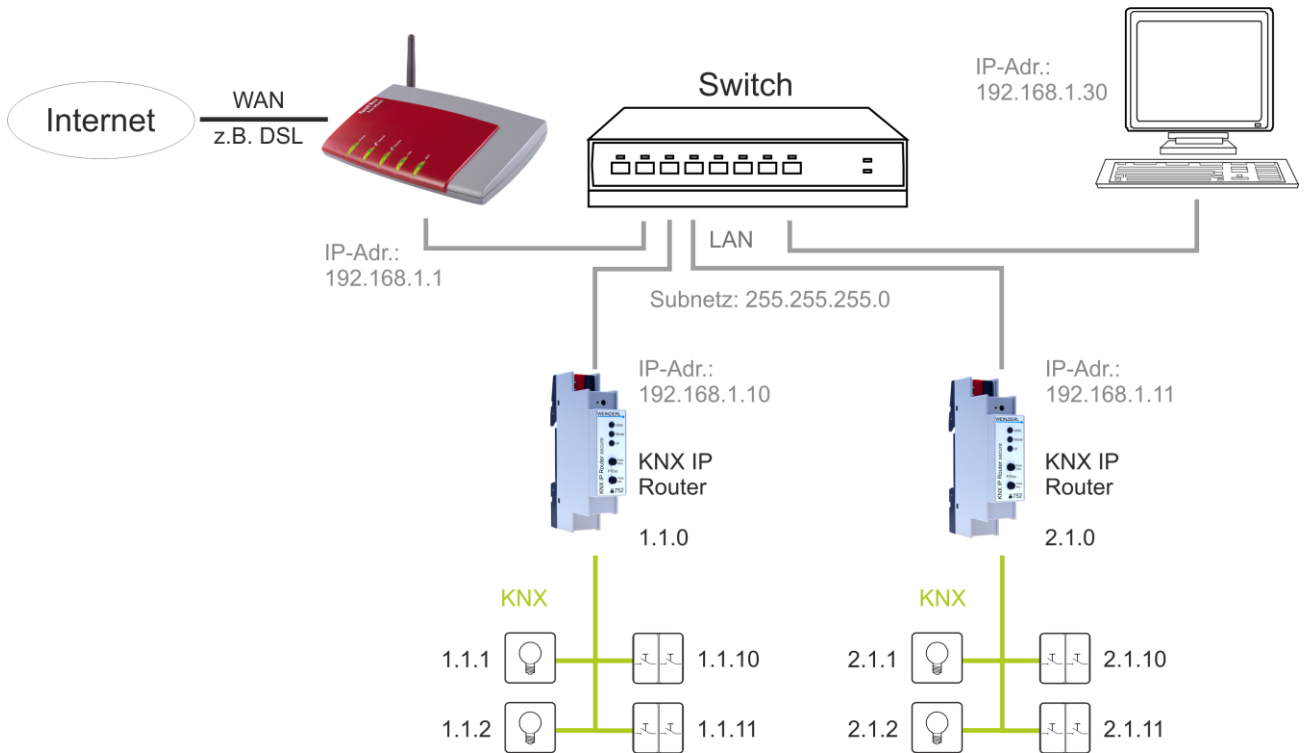


Abbildung 1: KNX-Installation

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 efc – 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)

The screenshot shows the FRITZ!Box 7490 web interface. The top navigation bar includes the FRITZ! logo, the device name 'FRITZ!Box 7490', and links for 'FRITZ!NAS' and 'MyFRITZ!'. The main content area is titled 'Internet > Freigaben' and contains several tabs: 'MyFRITZ!-Freigaben', 'Portfreigaben' (which is selected), 'FRITZ!Box-Dienste', 'Dynamic DNS', and 'VPN'. A left-hand sidebar menu lists various system functions: 'Übersicht', 'Internet', 'Online-Monitor', 'Zugangsdaten', 'Filter', 'Freigaben' (highlighted), 'MyFRITZ!-Konto', 'Telefonie', 'Heimnetz', 'WLAN', 'DECT', and 'Diagnose'. The main content area contains a warning message about internet security and a section titled 'Liste der Portfreigaben'. This section features a table with one entry: 'KNXnet/IP' with protocol 'UDP', port '52011', and 'an Computer' 'PC-192-168-5-30' and 'an Port' '3671'. Below the table is a 'Neue Portfreigabe' button and a checkbox option 'Alle Geräte im Heimnetz dürfen Portfreigaben selbstständig verändern' with explanatory text. At the bottom right of the main area are three buttons: 'Übernehmen', 'Abbrechen', and 'Aktualisieren'.

FRITZ!Box 7490 FRITZ!NAS MyFRITZ!

Internet > Freigaben

MyFRITZ!-Freigaben Portfreigaben FRITZ!Box-Dienste Dynamic DNS VPN

Übersicht Internet Online-Monitor Zugangsdaten Filter Freigaben MyFRITZ!-Konto Telefonie Heimnetz WLAN DECT Diagnose

An FRITZ!Box angeschlossene Computer sind sicher vor unerwünschten Zugriffen aus dem Internet. Für einige Anwendungen wie z.B. Online-Spiele oder das Filesharing-Programm eMule muss Ihr Computer jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Portfreigaben erlauben Sie solche Verbindungen.

Liste der Portfreigaben

Aktiv	Bezeichnung	Protokoll	Port	an Computer	an Port
<input checked="" type="checkbox"/>	KNXnet/IP	UDP	52011	PC-192-168-5-30	3671

Neue Portfreigabe

Alle Geräte im Heimnetz dürfen Portfreigaben selbstständig verändern
Geräte wie Spielekonsolen bzw. Anwendungen mit UPnP- oder PCP-Unterstützung können im Heimnetz Portfreigaberegeln der FRITZ!Box automatisch verändern. Aktivieren Sie diese Option aus Sicherheitsgründen nur, wenn Sie tatsächlich eingehende Verbindungen aus dem Internet gestatten müssen, die von den Geräten selbst verwaltet werden.

Übernehmen Abbrechen Aktualisieren

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, ist eine manuelle Konfiguration nötig. 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.

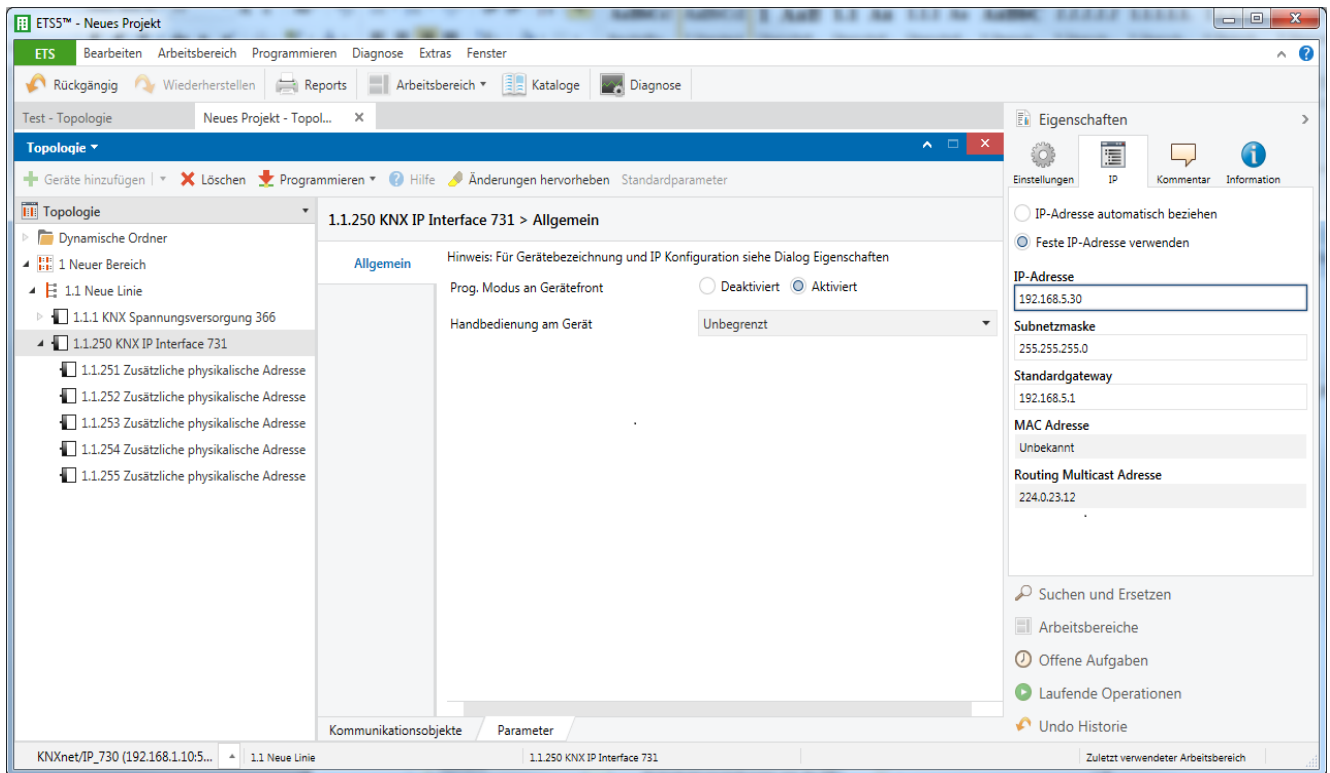


Abbildung 4: IP-Konfiguration exemplarisch an einem KNX IP Interface 731 mit ETS 5

2.2.4 Verbindungsaufbau mit der ETS

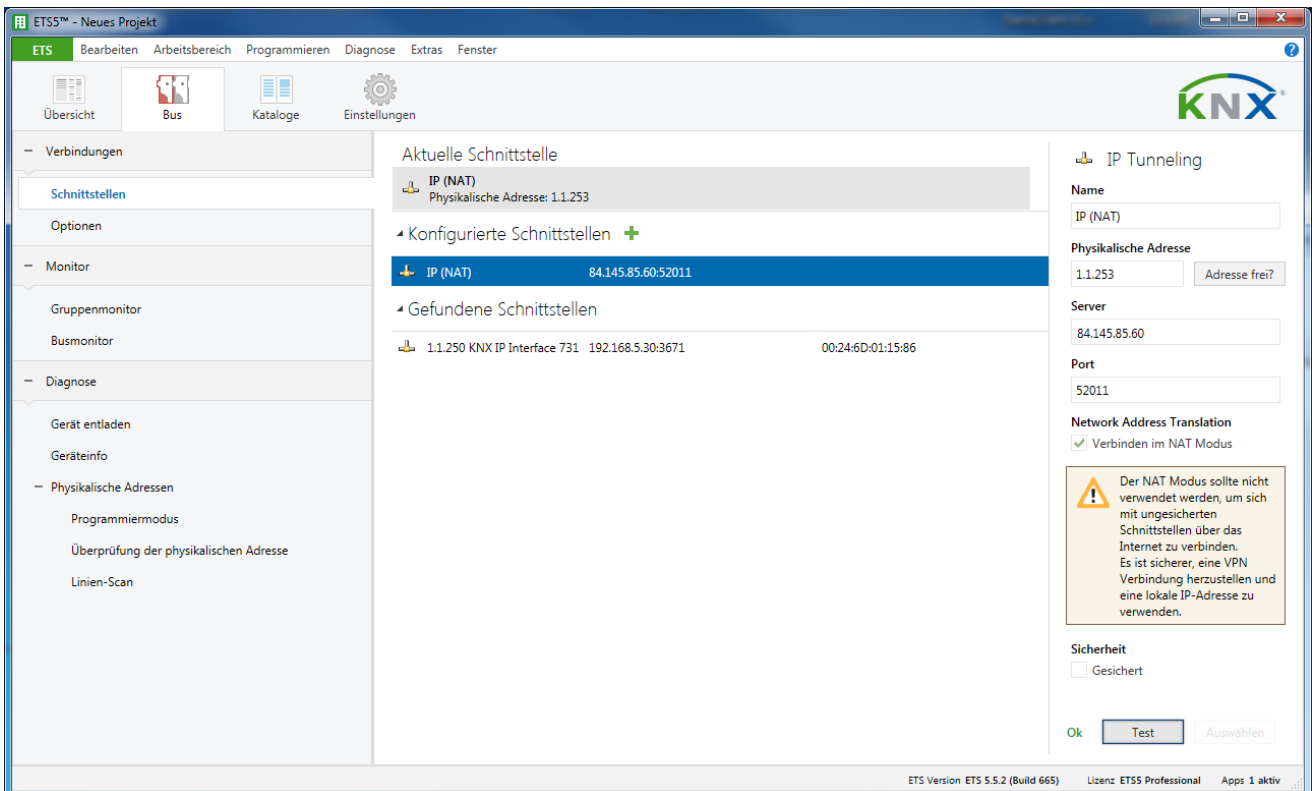


Abbildung 5: ETS Verbindung

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.

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.

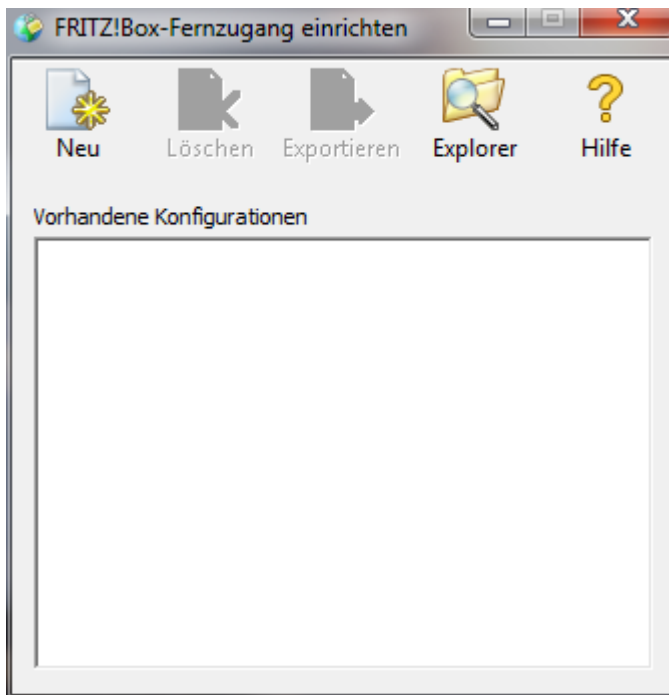


Abbildung 7: AVM Einrichtungstool

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

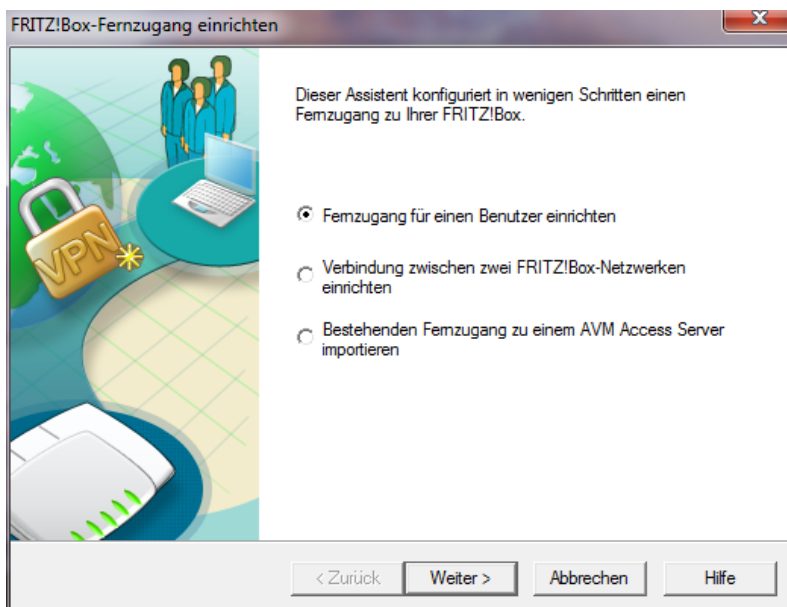


Abbildung 8: Modus wählen

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



Abbildung 9: Plattform wählen

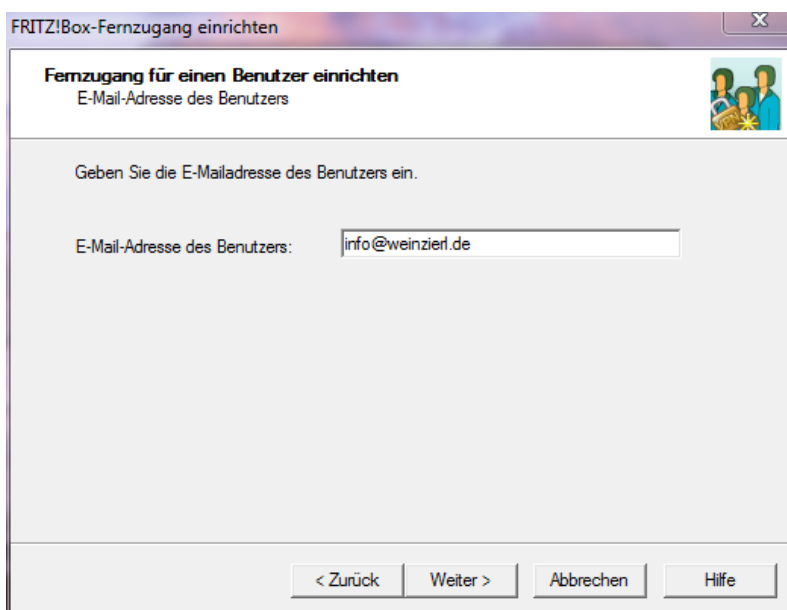


Abbildung 10: Benutzerkonto

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.

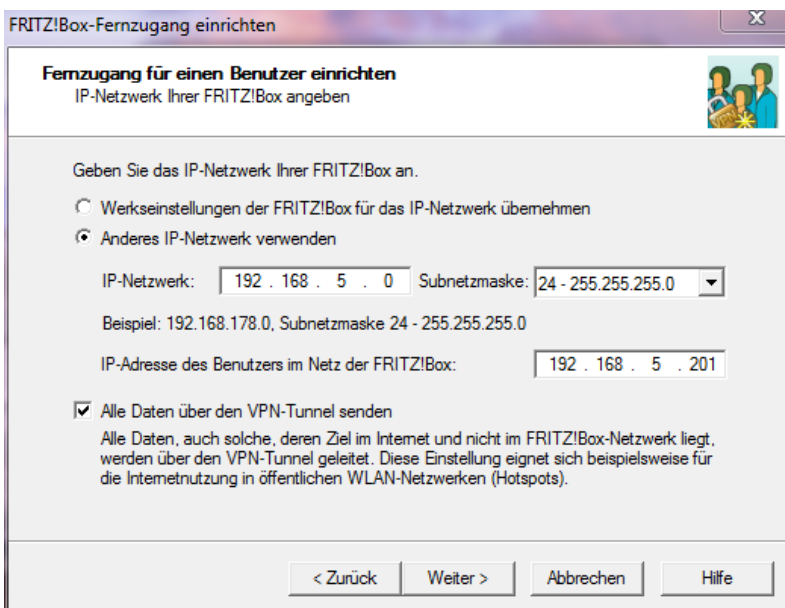


Abbildung 12: IP-Subnetz der Liegenschaft B einrichten

Hinweis:

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

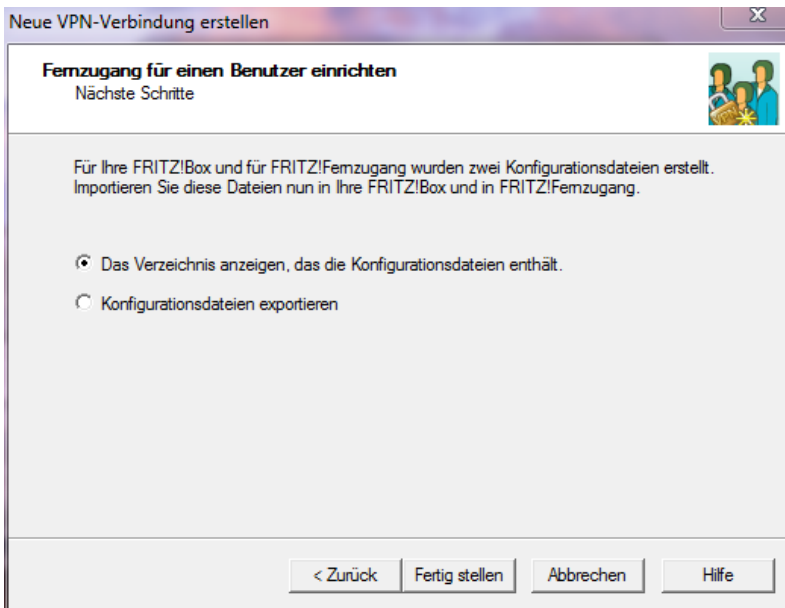


Abbildung 13: Konfiguration beenden

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

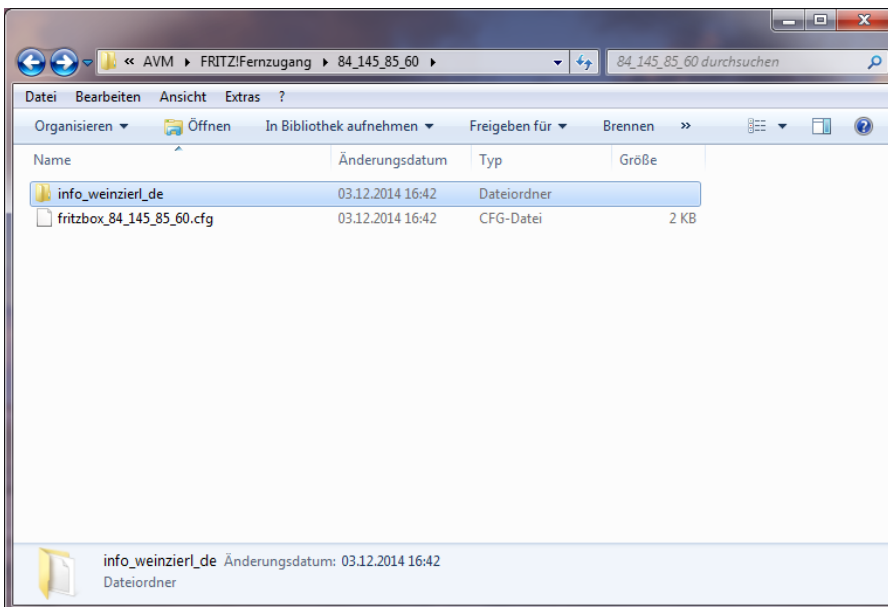


Abbildung 14: Konfigurationsdateien

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.

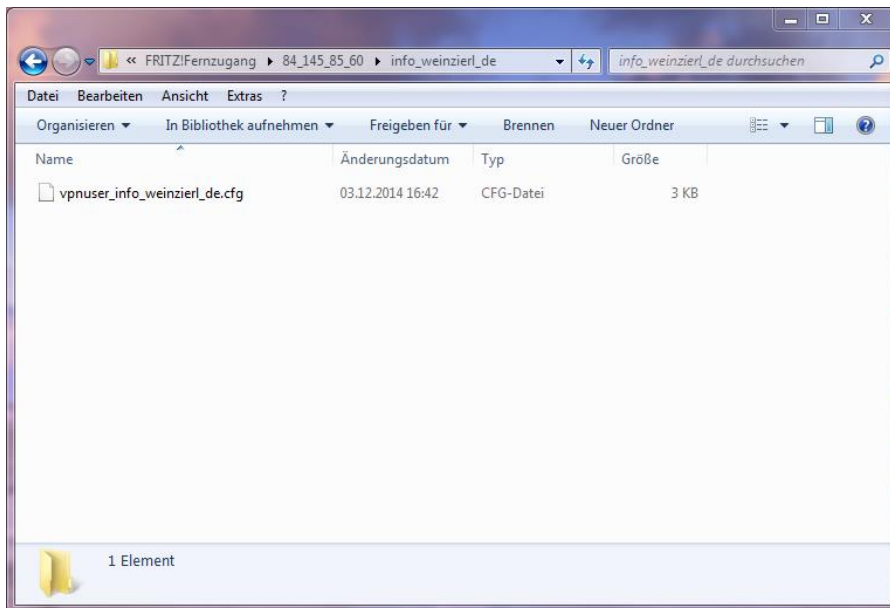


Abbildung 15: Konfigurationsdatei(en) Benutzer

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

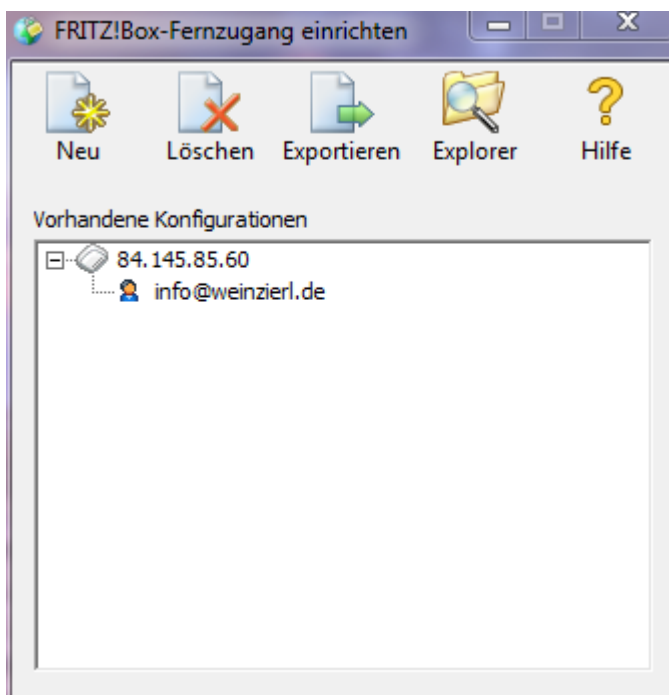


Abbildung 16: vollständige Konfiguration

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“.

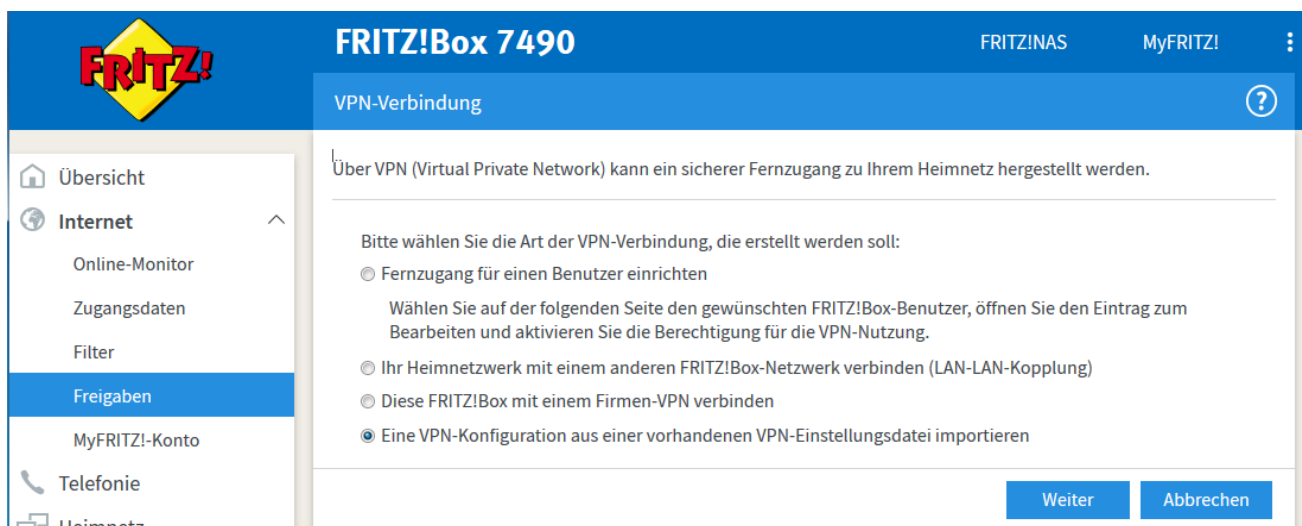


Abbildung 18: VPN-Fritzbox – Konfigurationsart wählen

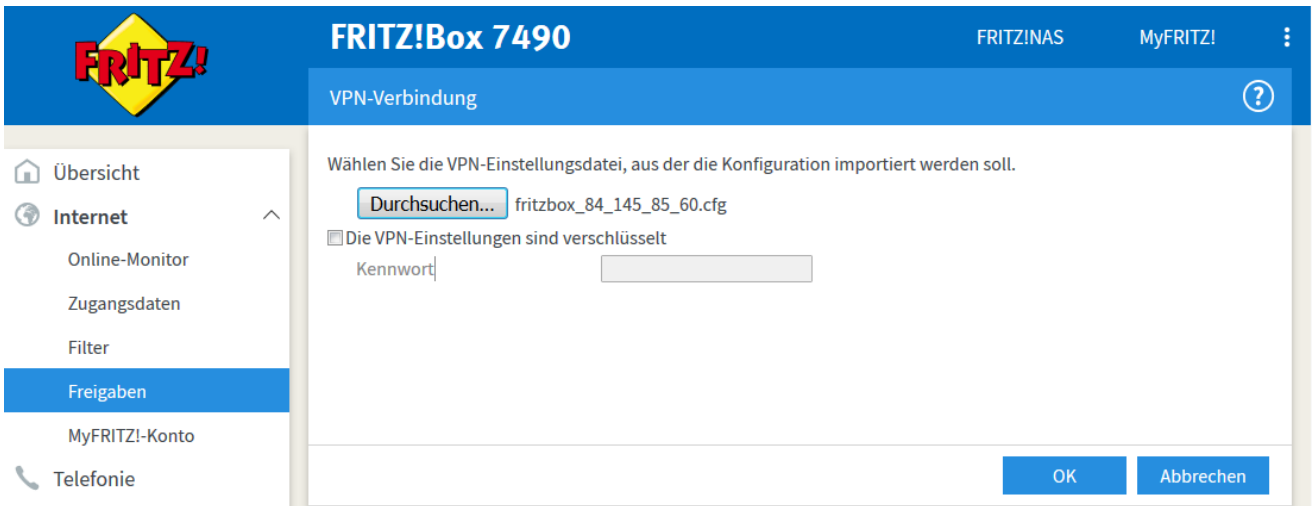


Abbildung 19: VPN-Fritzbox – Konfigurationsdatei wählen

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/fritzbox/tools/vpn/>

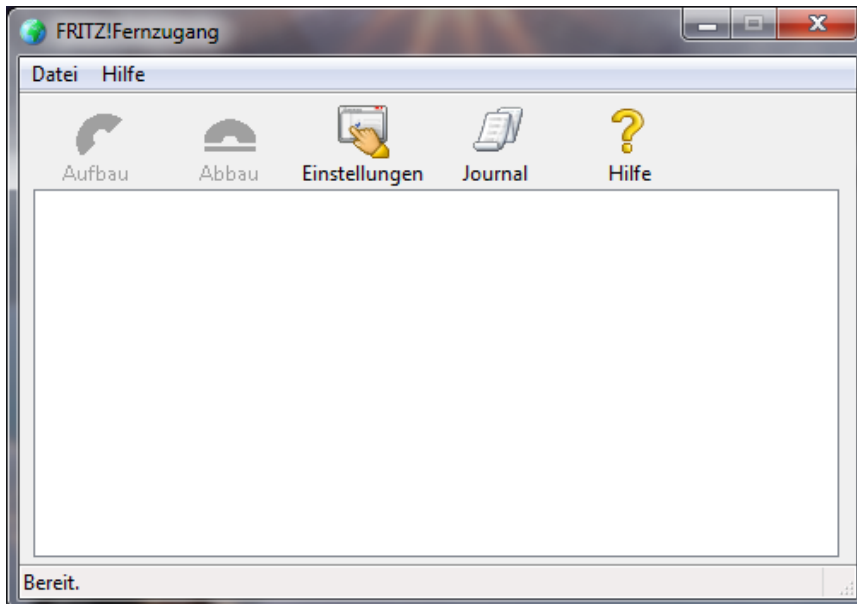


Abbildung 21: VPN-Client

Dieser Client kann auch automatisch mit Windows gestartet werden.

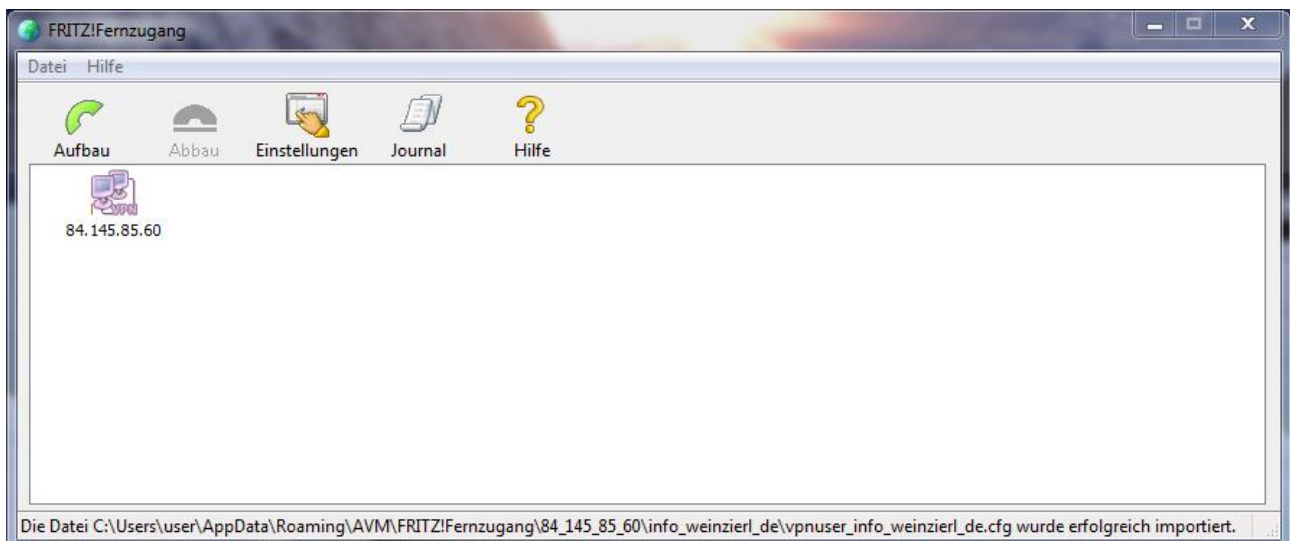


Abbildung 22: Importierte Verbindung

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

3.2.4 Zugriff mit der ETS auf das entfernte KNX IP Gerät

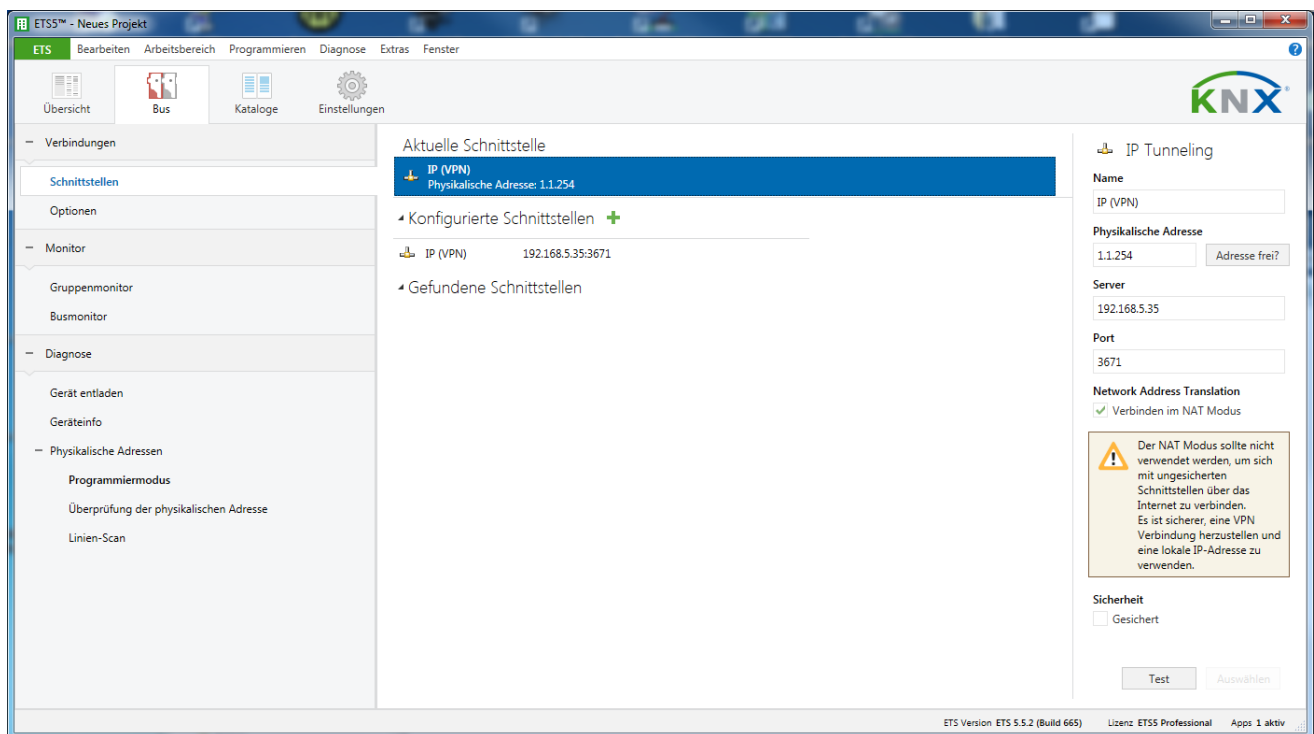


Abbildung 23: VPN-Schnittstelle in der ETS

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.

4 KNX IP Security

KNX IP Security ist ein pragmatischer Ansatz, der davon ausgeht, dass der wesentliche Angriffspunkt auf der IP Ebene besteht. KNX Twisted Pair wird als lokales Medium, das in der Wand liegt, als relativ sicher angenommen. Hingegen ist IP Kommunikation oft mit dem Internet verbunden und somit auch aus der Ferne angreifbar.

KNX IP Security sichert die KNX IP Kommunikation, während die Kommunikation auf KNX TP unverschlüsselt bleibt. Der wesentliche Vorteil dieses Ansatzes ist, dass die vorhandenen KNX TP Geräte und Installationen unverändert weiter verwendet werden können. Nur die KNX IP Geräte, also im Wesentlichen KNX IP Interfaces und KNX IP Router, müssen ersetzt werden.

KNX IP beinhaltet zum einen das Routing Protokoll, das für IP Backbones dient aber auch das Medium KNX IP repräsentiert. Zum anderen wird das Tunneling Protokoll verwendet, um einem Client (zum Beispiel ETS) über IP Zugriff auf eine TP Linie zu ermöglichen. Während KNX IP Router in der Regel beide Protokolle implementieren, unterstützen KNX IP Interfaces nur die Tunneling Funktion.

So unterschiedlich wie die beiden Anwendungen von KNX IP sind, so unterschiedlich sind die jeweiligen Erweiterungen für Security. Beim Secure Routing Protokoll, das auf UDP Multicast basiert, dient ein gemeinsamer Schlüssel, um die gesamte KNX IP Routing Kommunikation zu verschlüsseln. Eine Besonderheit ist der Telegrammzähler beim Routing. Dieser ist zeitbasiert und stellt somit einen Zeitstempel dar, der veraltete Telegramme erkennen lässt. Die gemeinsame Systemzeit wird laufend zwischen den Geräten synchronisiert.

Beim Tunneling Protokoll bauen Client und KNX IP Gerät (KNXnet/IP Server) erst einen sicheren Kanal mithilfe des sogenannte Diffie-Hellmann-Verfahren auf. Erst dann werden Benutzer ID und Passwort übertragen. Neu bei KNX Secure Tunneling ist die Möglichkeit, die Verbindung mit TCP aufzubauen.

5 Kombinationen von Zugriffsarten und KNX Security

Aus den verschiedenen Arten auf das Gerät zuzugreifen und der Möglichkeit KNX secure oder KNX unsecure zu benutzen, ergeben sich folgende Möglichkeiten.

	NAT	VPN
KNX unsecure	Warnung! ungeschützt	OK
KNX secure	OK	optimaler Schutz

Ein Fernzugriff über NAT und KNX unsecure ist vollkommen ungeschützt und sollte auf keinen Fall verwendet werden. Ein optimaler Schutz ergibt sich aus der gleichzeitigen Verwendung von KNX Security und VPN.