

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

Remote access with the ETS

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

Table of contents

1	Introduction.....	3
2	Remote access with NAT.....	3
2.1	Network Address Translation (NAT).....	3
2.2	Example of a configuration	4
2.2.1	Structure	4
2.2.2	Settings in the DSL router.....	5
2.2.3	IP configuration of the KNX IP Interface.....	6
2.2.4	Establishing a connection with the ETS	7
3	Remote access via a VPN	8
3.1	Virtual Private Network (VPN)	8
3.1.1	Introduction.....	8
3.1.2	Site-to-end.....	8
3.1.3	Site-to-site.....	8
3.2	Remote access to a KNX/IP router using the Fritzbox 7490 as an example.....	8
3.2.1	VPN-Tunnel einrichten	8
3.2.2	VPN-Server (Fritzbox) einrichten.....	14
3.2.3	VPN-Client (PC).....	16
3.2.4	Accessing the remote KNX IP device with the ETS.....	17
3.2.5	Alternatives.....	17

Versions

Document version	Date	Editor
Draft	2009-02-18	F. Heiny
Review	2009-03-04	F. Heiny
Added: KNX IP LineMaster 760 Changed: Formatting	2010-06-17	F. Heiny
Added KNX IP BAOS 772	2011-11-08	S. Matsche
Added NAT warning	2014-11-25	St
Updated	2014-12-04	M. Richter
Review and release	2014-12-11	St
Added KNX IP BAOS 777	2015-07-30	St
Error correction	2015-11-16	St

1 Introduction

This document describes how remote access can be established to a KNX installation via the Internet by means of the ETS. Remote access can be achieved using either NAT (Network Address Translation) or VPN (Virtual Private Network).

Any device that supports KNXnet/IP tunnelling can be used for remote access. These devices are the KNX IP Interface 730, KNX IP Router 750, KNX IP LineMaster 760, KNX IP BAOS 771, KNX IP BAOS 772 and the KNX IP BAOS 777. In this document, they will be collectively referred to as "KNX IP devices".

2 Remote access with NAT

2.1 Network Address Translation (NAT)

NAT (Network Address Translation) is a method used to translate IP addresses. It is primarily used in routers (e.g. DSL routers).



Please note that remote access via NAT, without further safety measures, poses significant dangers. Port forwarding provides universal access to your local IP network and your KNX system. Any Internet user can discover the open port on your static public IP address and can, for example, access your KNX network via the ETS software.

We strongly advise using NAT only temporarily for testing or diagnostic purposes. After that, close the port again to prevent abuse.

If remote access is realized through NAT, we strongly advise you not to specify the default port of 3671 towards the Internet. Port 3671 is the official port for efc - eFieldControl(EIBnet) registered by KNX Association. This port can be easily determined by unauthorized persons. Please use a port in the non-reserved range between port 50000 and port 60000.

Permanent remote access should be established only when protected! We recommend remote access through VPN (Virtual Private Network). The VPN feature is already integrated into most DSL routers.

2.2 Example of a configuration

2.2.1 Structure

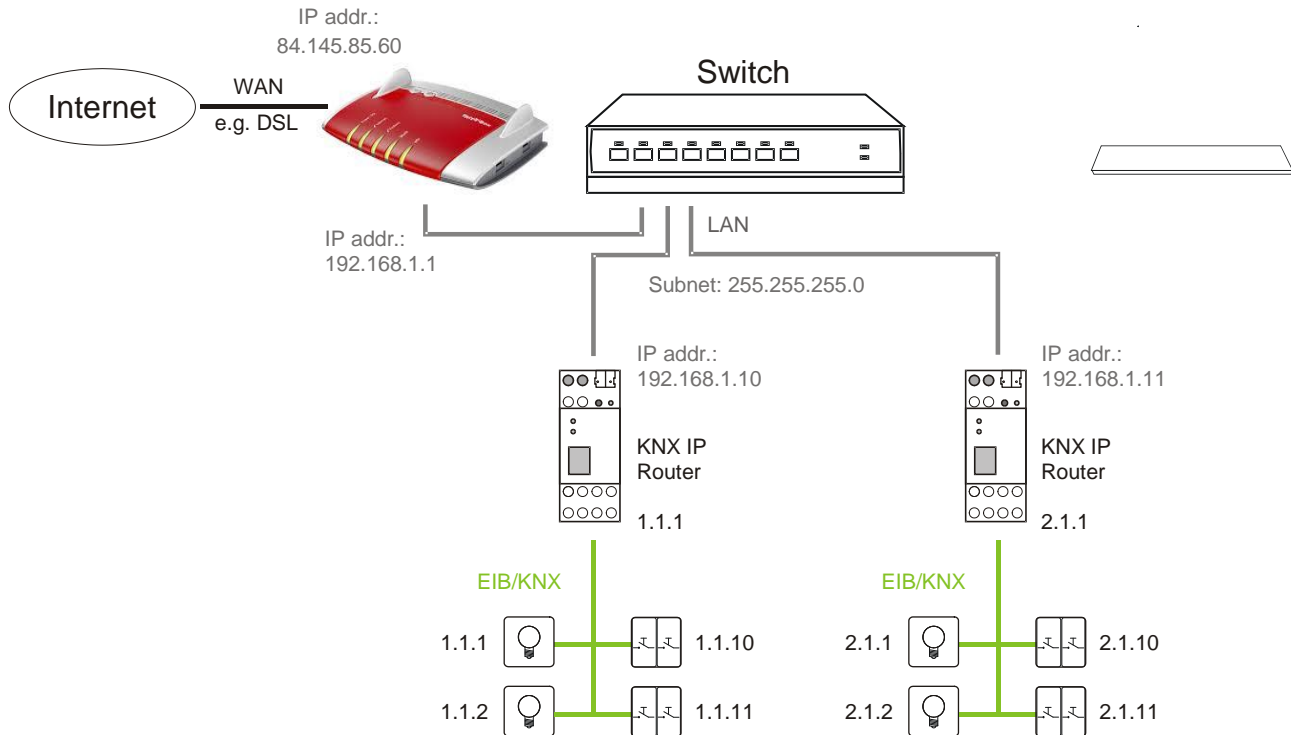


Figure 1: KNX installation

The diagram above shows a typical KNX installation that is connected to the Internet via a DSL router. Two TP lines are connected to each other via two KNX IP routers. These KNX IP routers were assigned static IP addresses from the local network. The DSL router needed for Internet access has a fixed local IP address (192.168.1.1) and a public IP address (here, 84.145.85.60), which is assigned by the Internet service provider. Generally, the public IP address is dynamic, meaning that it is reassigned every time an Internet connection is re-established.

2.2.2 Settings in the DSL router

In the DSL router, forwarding must be set up under the "Permit Access" item. For this, a port (standard: 3671) and an IP address (local IP address of the KNX IP device, e.g. 192.168.1.10) must be specified. Afterwards, all telegrams that are received from the Internet and are directed to port 52011 will be forwarded to the specified KNX IP device to Port 3671.

Port 3671 is the official port for efc - eFieldControl(EIBnet) registered by KNX Association. This port can be easily determined by unauthorized persons. We strongly advise you to use a port in the non-reserved range between port 50000 and port 60000 as described in our example.

The screenshot shows the FRITZ!Box 7490 web interface. The left sidebar contains navigation links: Overview, Internet, Online Monitor, Account Information, Filters, Permit Access (selected), MyFRITZ!, Telephony, Home Network, WLAN, DECT, Diagnostics, and System. The main content area is titled 'Port Forwarding' and shows a 'Create New Port Forwarding Setting' form. The form has the following fields: 'Port forwarding enabled for' (checked), 'Name' (KNXnet/IP), 'Protocol' (UDP), 'From port' (52011) through port (52011), 'to computer' (Enter the IP address manually), 'to IP address' (192.168.1.10), and 'to Port' (3671). There are 'OK' and 'Cancel' buttons at the bottom right.

Figure 2: Settings in the DSL router (port forwarding for KNXnet/IP)

The screenshot shows the FRITZ!Box 7490 web interface. The left sidebar is the same as in Figure 2. The main content area is titled 'Permit Access' and has tabs for 'Port Forwarding' (selected), 'Storage', 'FRITZ!Box Services', 'Dynamic DNS', and 'VPN'. Below the tabs, there is a warning message: 'Computers connected to FRITZ!Box are safe from unauthorized access from the Internet. However, for certain applications such as online games or the eMule file sharing program, it must be possible for other users in the Internet to access your computer. Such connections are made possible by enabling port forwarding.' Below this is a 'List of Ports with Port Forwarding Enabled' table:

Enabled	Name	Protocol	Port	to Computer	to Port	
<input checked="" type="checkbox"/>	KNXnet/IP	UDP	52011	Mathias-PC	3671	

Below the table is a 'New Port Forwarding' button. At the bottom, there is a checkbox 'Allow changes to security settings over UPnP' with a warning message: 'Devices like Smart TV and smartphones, and applications that support UPnP, can be used to change security settings in the home network automatically, such as the FRITZ!Box port forwarding rules. For reasons of security, only enable this option if you really want to allow incoming connections from the Internet.' There are 'Apply', 'Cancel', and 'Refresh' buttons at the bottom right.

Figure 3: Settings in the DSL router (list of port forwarding's)

2.2.3 IP configuration of the KNX IP Interface

Since the IP address of the KNX IP device has to be known, manual configuration is recommended. The IP address (192.168.1.10), subnet mask (255.255.255.0) and gateway IP address (192.168.1.1) must be specified.

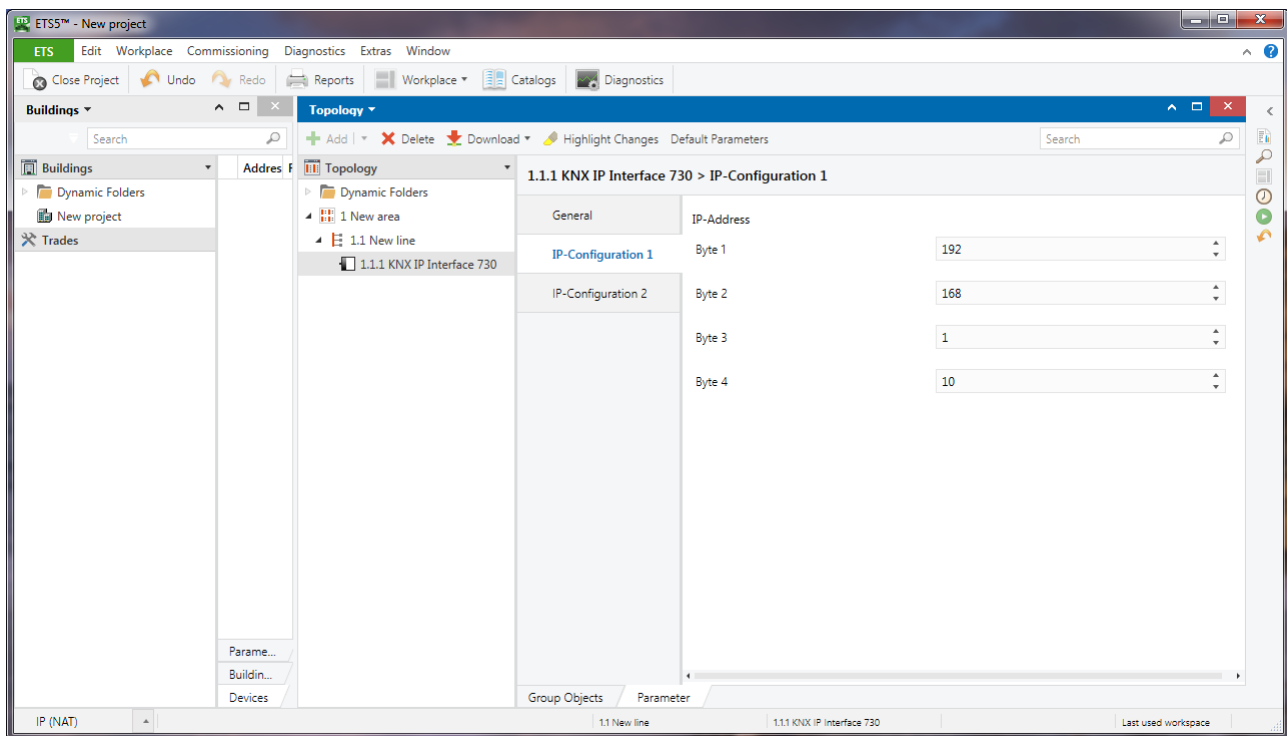


Figure 4: IP configuration (part 1)

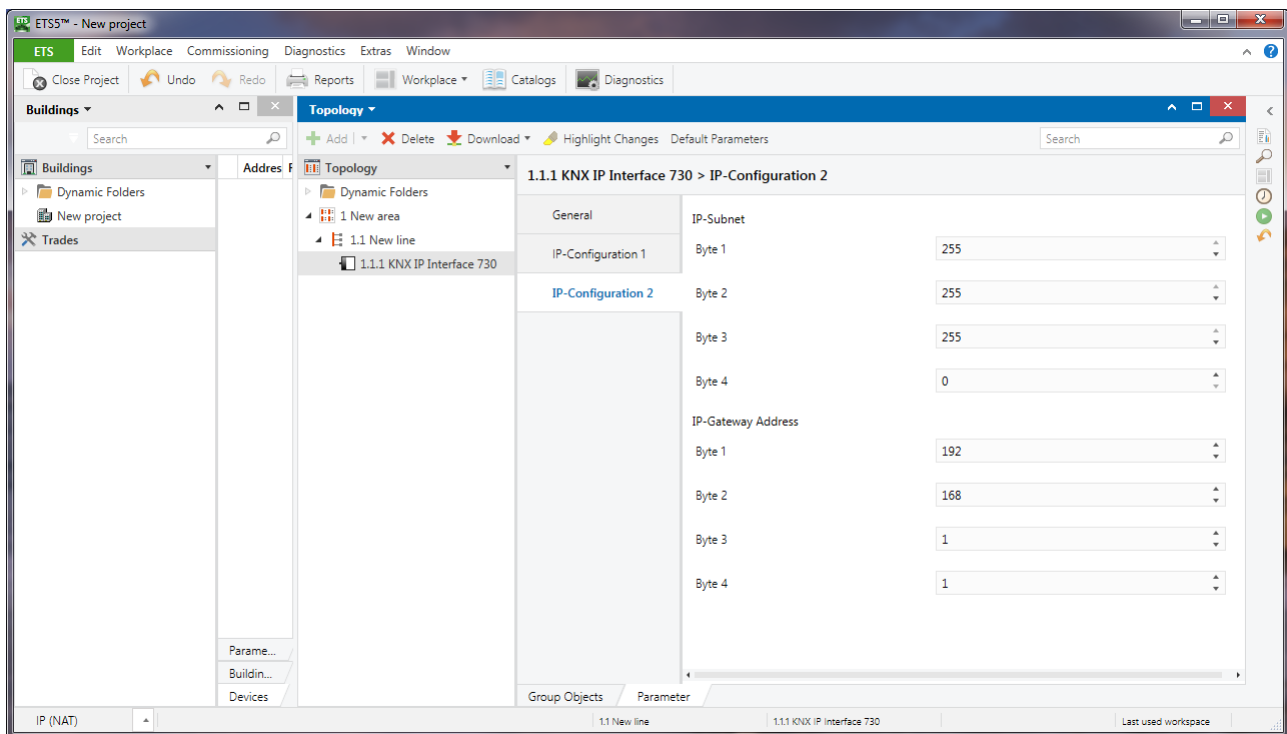


Figure 5: IP configuration (part 2)

2.2.4 Establishing a connection with the ETS

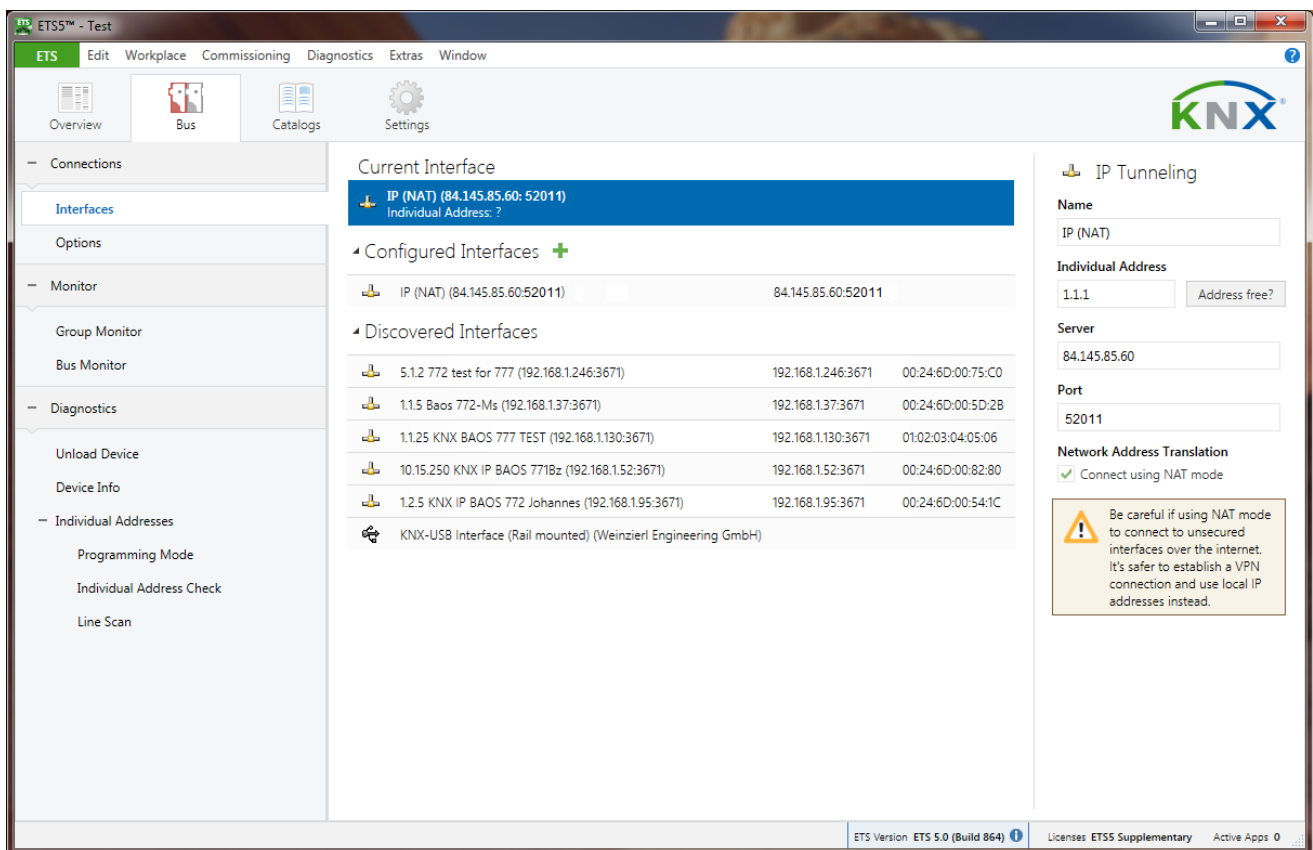


Figure 6: ETS Connection Manager

A separate connection should be created for remote access, such as "IP (NAT)" in the example shown here. Select "KNXnet/IP" for the type. In the "IP address" field, enter the public IP address of the remote KNX installation. The port 52011 specified here, must be the same as that one specified in the DSL router settings.

Important: The "Connect using NAT mode" box has to be checked!

Note: The IP address has to be entered manually since the devices cannot be scanned by ETS via the Internet.

Remote access by means of NAT requires at least ETS version 3.0f.

3 Remote access via a VPN

3.1 Virtual Private Network (VPN)

3.1.1 Introduction

A VPN is an extension of private networks. It can be used to enable remote access (site-to-end) and link private networks (site-to-site) via the Internet.

3.1.2 Site-to-end

A site-to-end VPN can be used to establish access to an internal network. For example, employees in the field can use it to dial into their company network.

3.1.3 Site-to-site

A site-to-site VPN can be used to link private networks. For example, a site-to-site VPN can link two remote company networks.

3.2 Remote access to a KNX/IP router using the Fritzbox 7490

As an example, the remote connection via the Internet between a PC in building A running the ETS software and a KNX installation behind a Fritzbox 7490 DSL router in building B is explained. The KNX system topology of building B is similar to that one shown in Figure 1. Through a VPN tunnel, the ETS in property A communicates securely via the internet with KNX system in property B.

3.2.1 Configuration of the VPN-Server

For setting up a VPN server on a Fritzbox 7490, a special tool is needed (FRITZ!Box-Fernzugang_einrichten.exe).

The tool can be downloaded from: www.avm.de

After successful completion of the configuration, the tool will generate two configuration files.

One of this files is for importing into the Fritzbox the other one is for the AVM VPN client program (see item 3.2.3).

Hint: setting up a VPN-tunneling connection via a AVM Fritzbox router is only possible by using the additional AVM VPN-Client. The Windows VPN-Client is incompatible with the Fritzbox VPN-Server.

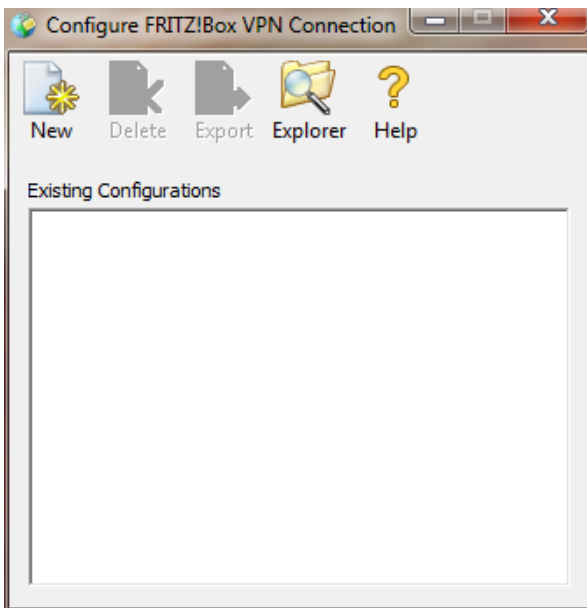


Figure 7: AVM VPN configuration tool

Using the AVM VPN configuration tool, all data for setting up the VPN connection will be collected. By clicking the option “New” the following window appears.

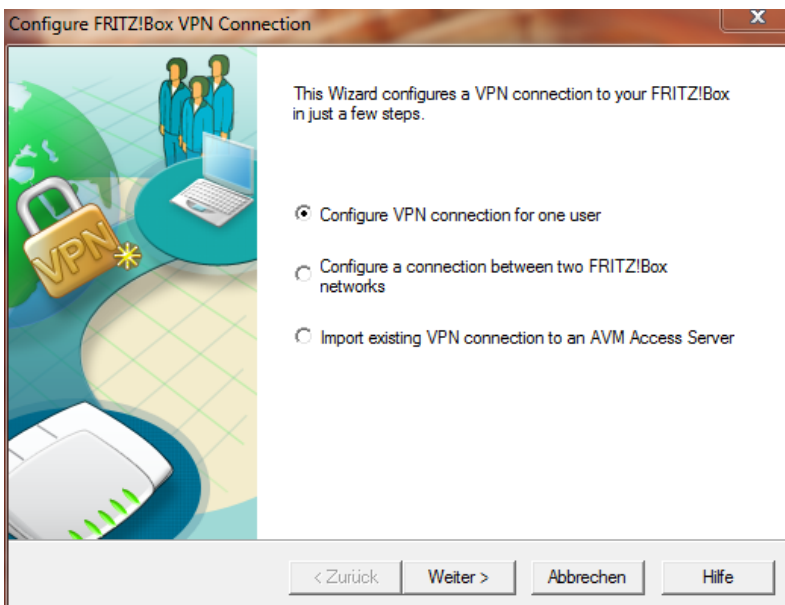


Figure 8: VPN mode option

In our example, we choose the “Configure VPN connection for one user” option.

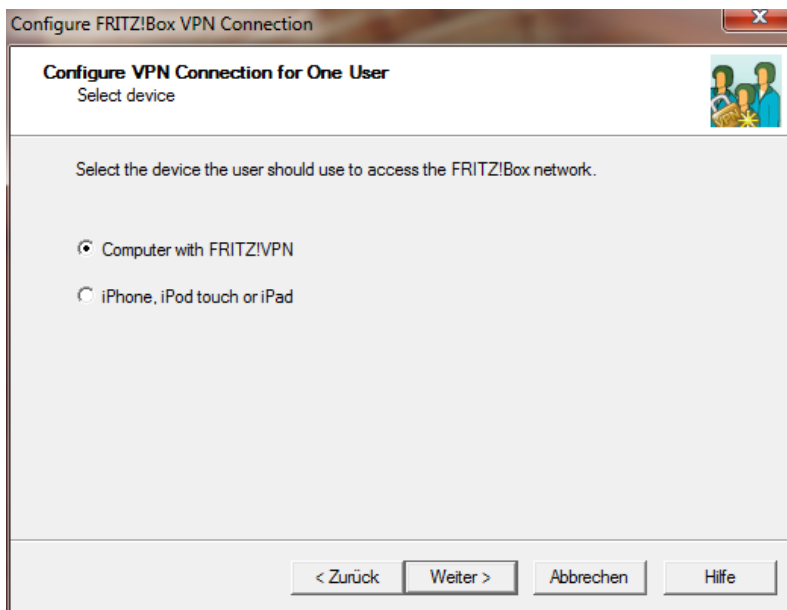


Figure 9: Platform options

To fill in your e-mail address in the next window is optional.

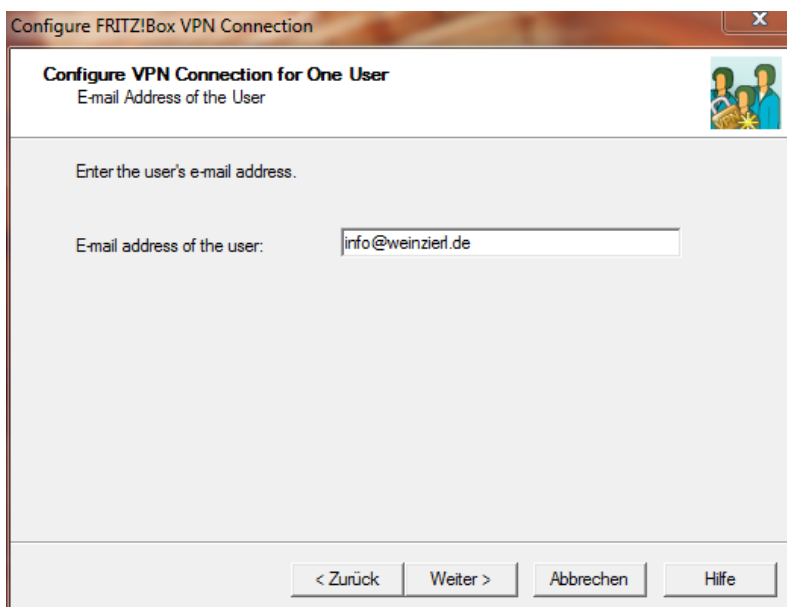


Figure 10: User e-mail

The next step is to create a user account with a specific name.

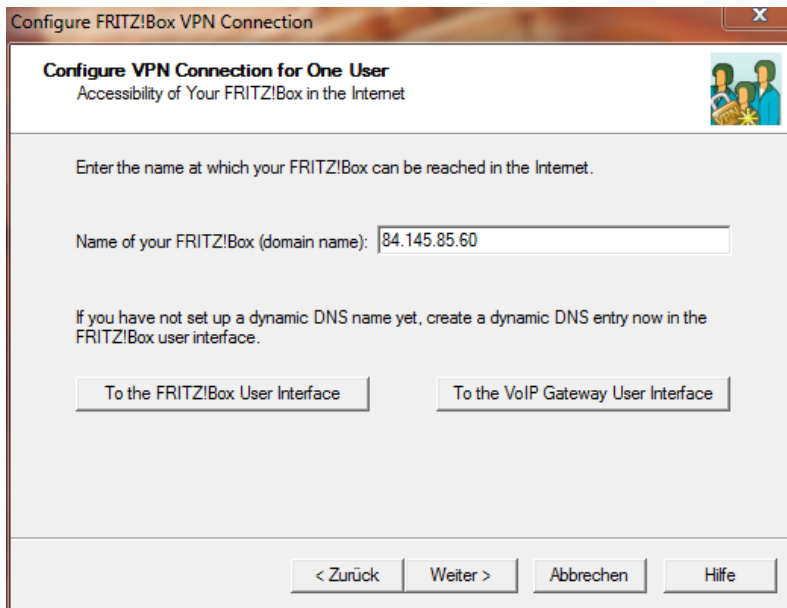


Figure 11: VPN-Server definition

In the window above, you have to specify the Fritzbox in building B. You either fill in its static IP address (from ISP) or a DNS account name (provided for example from www.dyn.com, www.selfhost.de, ...)

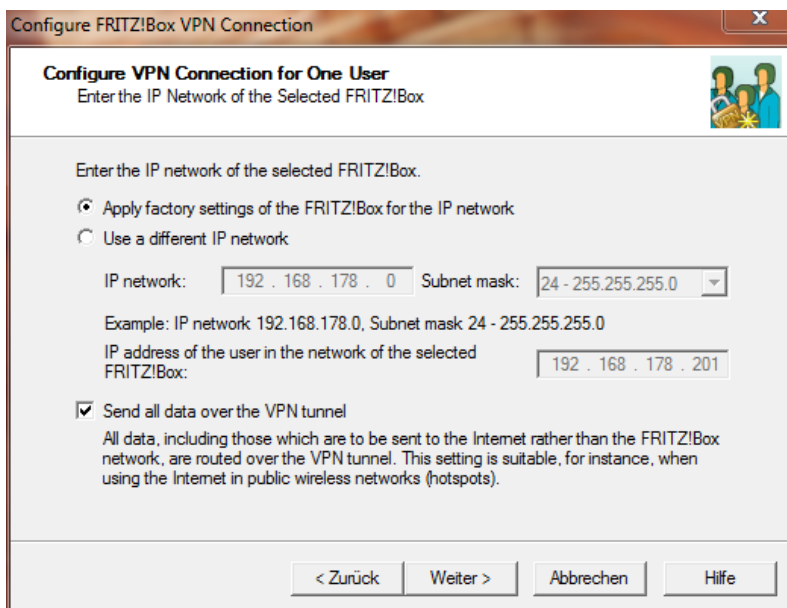


Figure 11: Subnet definition of LAN in building B

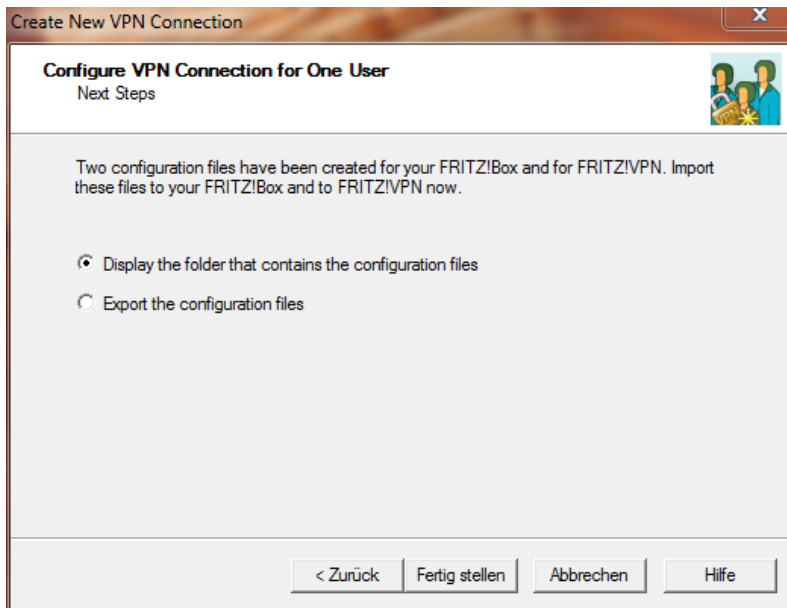


Figure 13: Finish the configuration wizard

Finally choose the option shown in figure 13. The wizard will direct you to the windows folder in which it has created the configuration files for the Fritzbox and the AVM-VPN-Client.

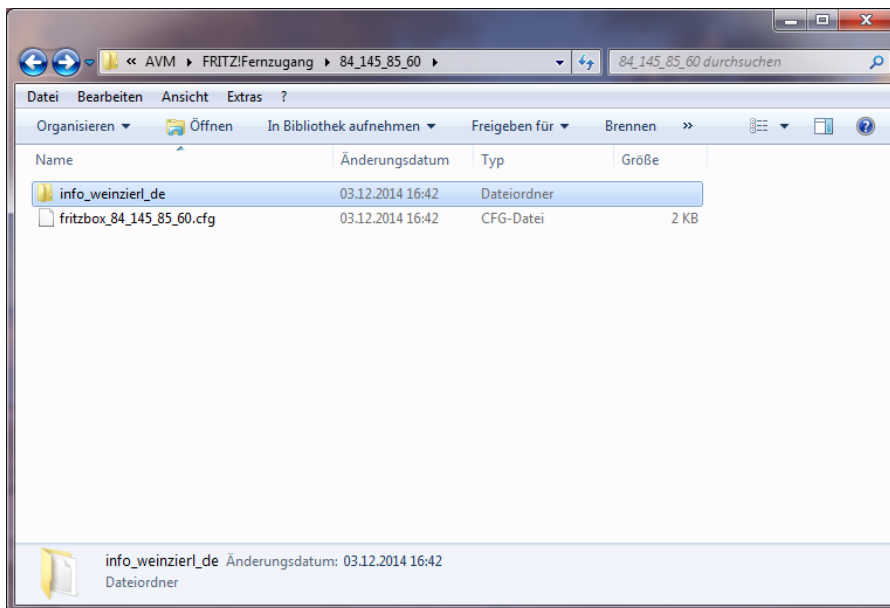


Figure 14: Folder with configuration file for VPN-Server

The Wizard will create a directory in:

...\User\AppData\Roaming\AVM\FRITZ!Fernzugang\

The directory name will be the name of the Fritzbox in building B.

Within this directory the wizard stores the .cfg file for Fritzbox in building B and creates a directory for the VPN user(s) in building A.

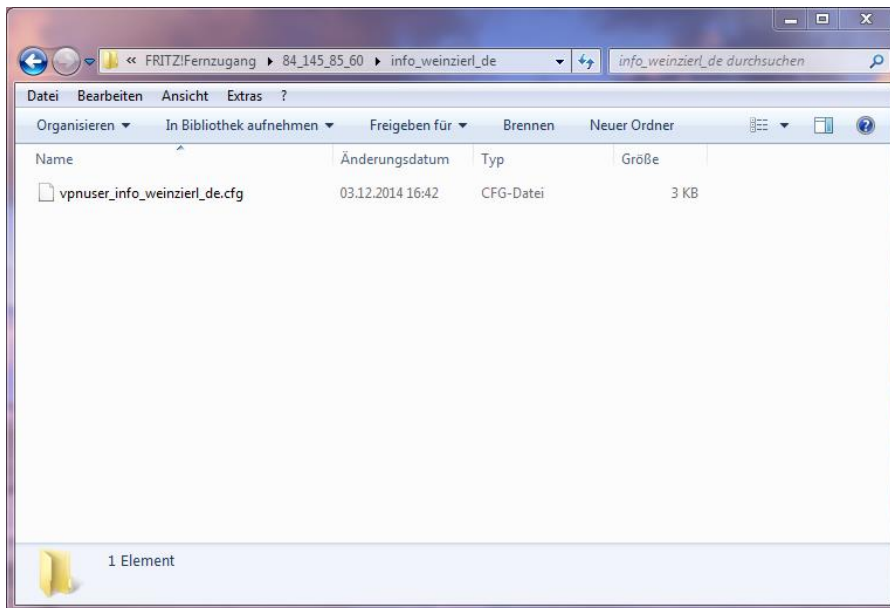


Figure 15: Folder with configuration file(s) for the user(s) (VPN client)

If additional users for VPN tunnel to building B are created, the individual configuration files will be stored in that folder (figure 15) as well.

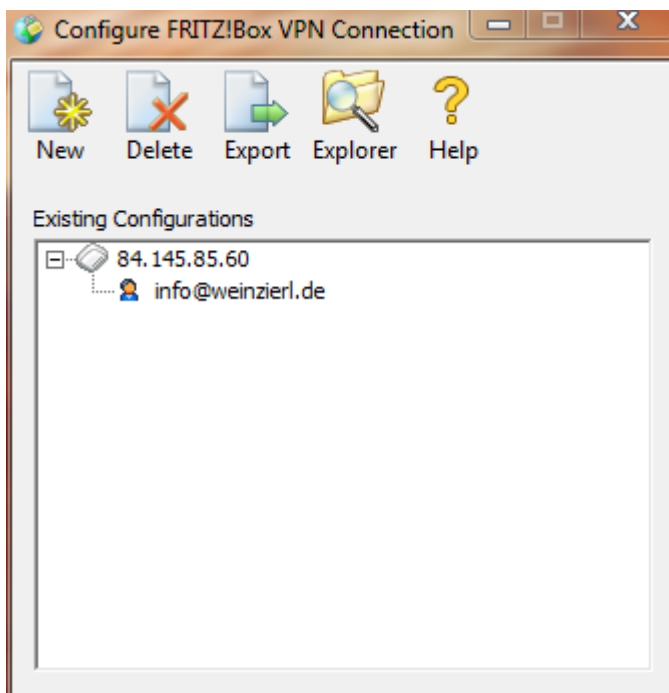


Figure 16: complete configuration of the VPN

Now, we've finished the VPN configuration.

All necessary data for the Fritzbox and the AVM VPN-Client are stored in the configuration files.

The configuration wizard automatically generates a password (shared key) for the VPN tunnelling connection.

3.2.2 Setting up the VPN-Server (Fritzbox)

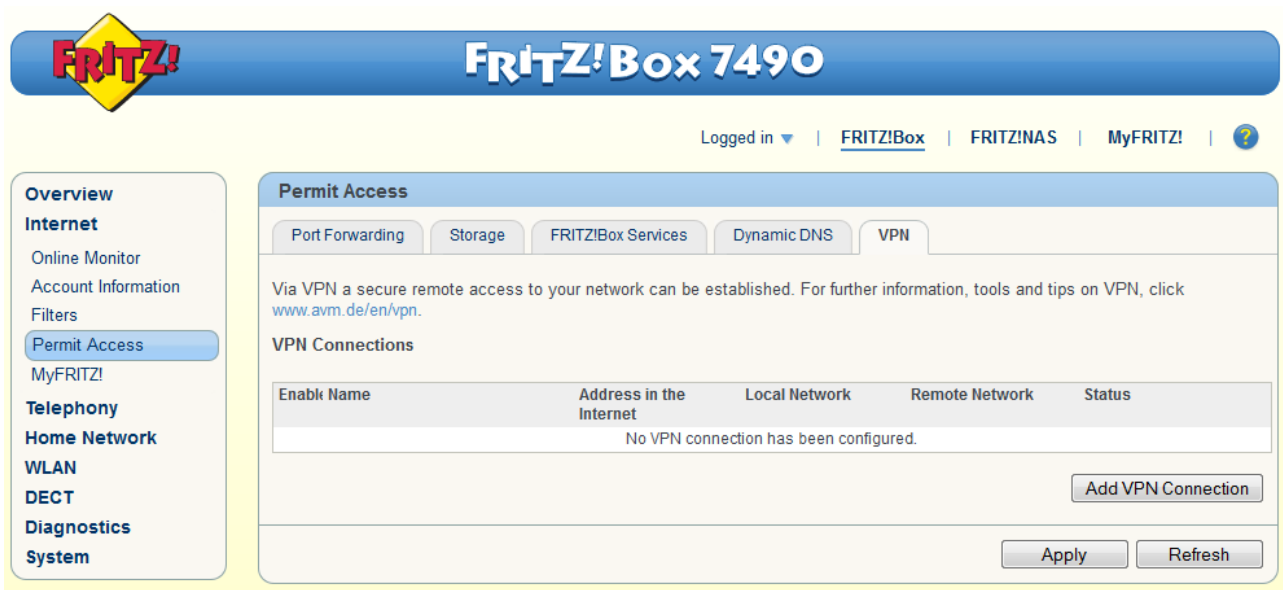


Figure 17: Fritzbox VPN-Server - add a connection

Hint: Within this menu you can also find the index tab „Dynamic DNS“. Within this option you can configure your DynDNS account.

For setting up the VPN-Server you have to choose tab “VPN” and then press the button “Add VPN Connection”.

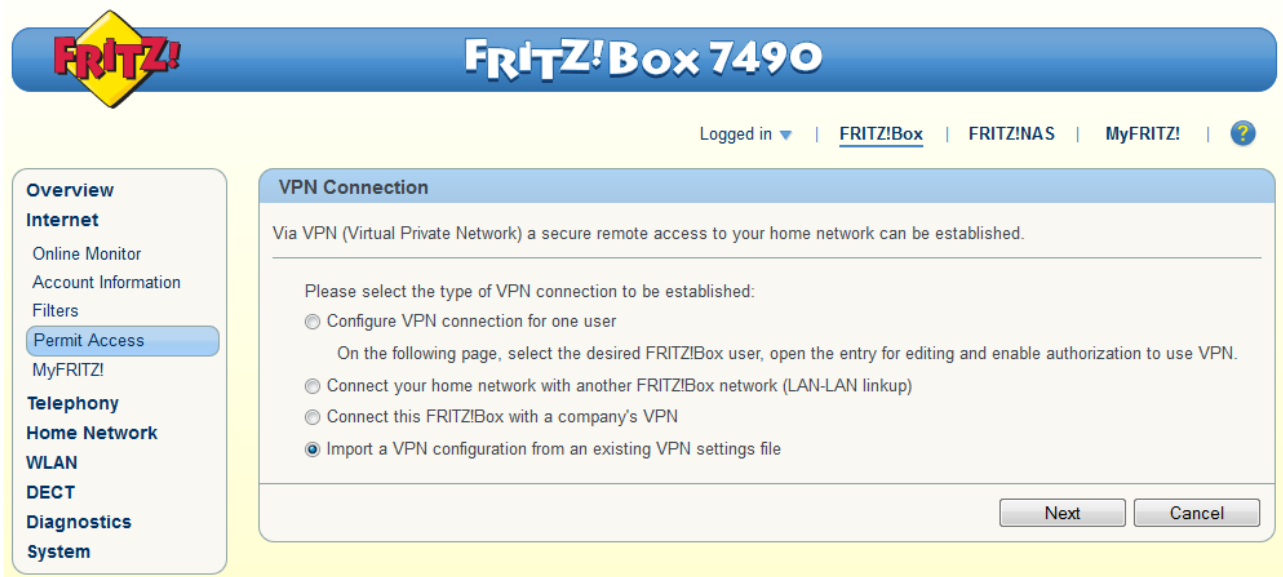


Figure 18: Fritzbox VPN-Server – choose means of configuration

You’ve got to choose “Import a VPN configuration from an existing VPN settings file” because we’ve already defined the configuration data with AVM setup wizard.

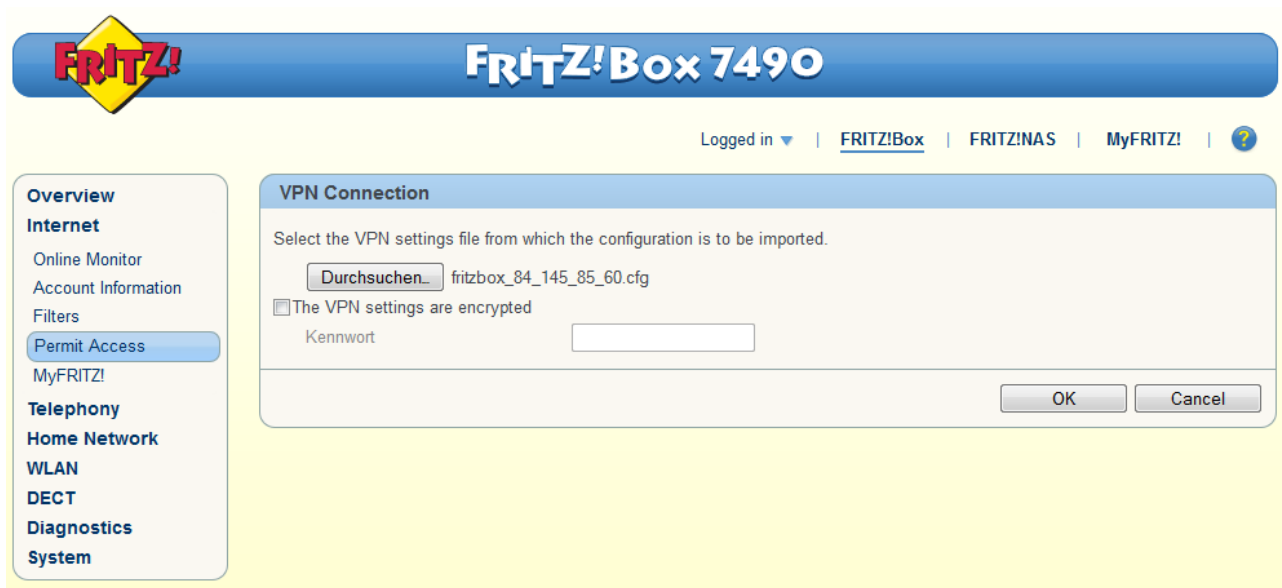


Figure 19: Fritzbox VPN-Server – choose the configuration file on your local system

Select the path to the fritzbox_84_145_85_60.cfg file which was stored by the wizard.

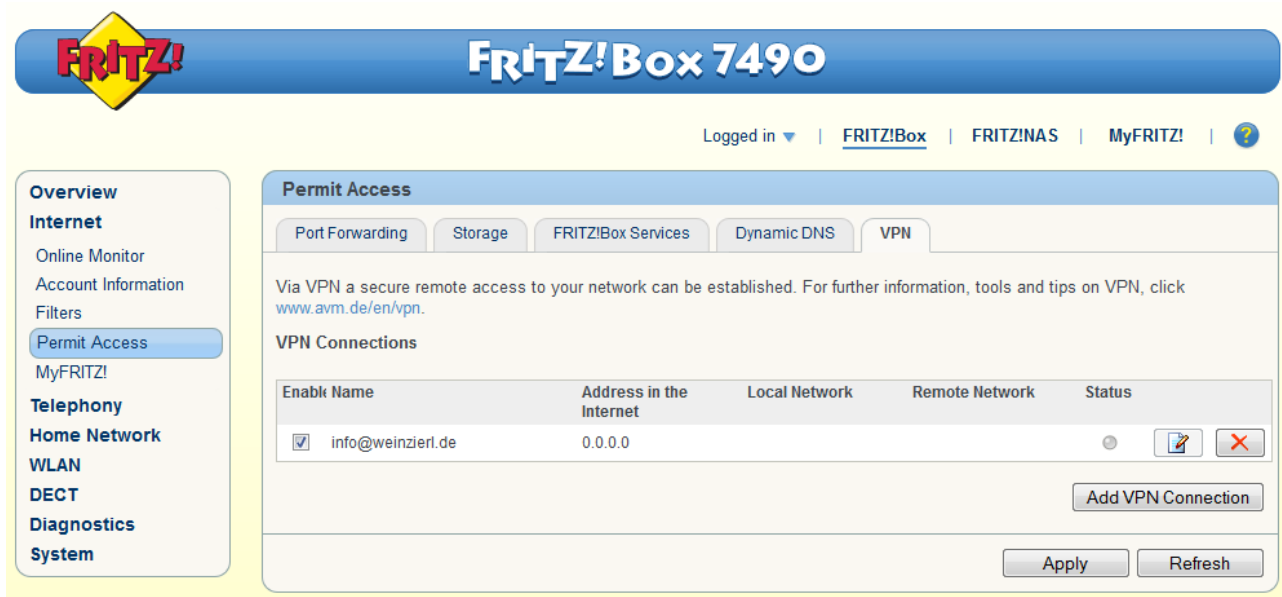


Figure 20: Fritzbox VPN-Server – opening the VPN connection

3.2.3 Setting up the VPN-Client (PC)

To enable the client to connect to the VPN-Server, a VPN-Client tool of company AVM is needed. The VPN-Client program can be downloaded here:

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

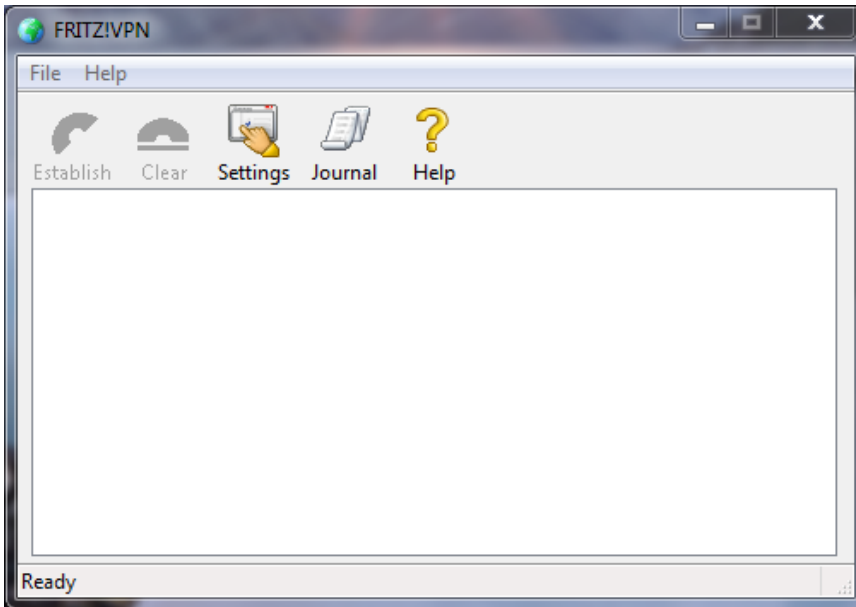


Figure 21: AVM VPN-Client

The configuration of the client connection is done by importing the `vpnuser_info_weinzierl_de.cfg` created by the wizard. Go to “Settings” and import the file into the VPN-Client.

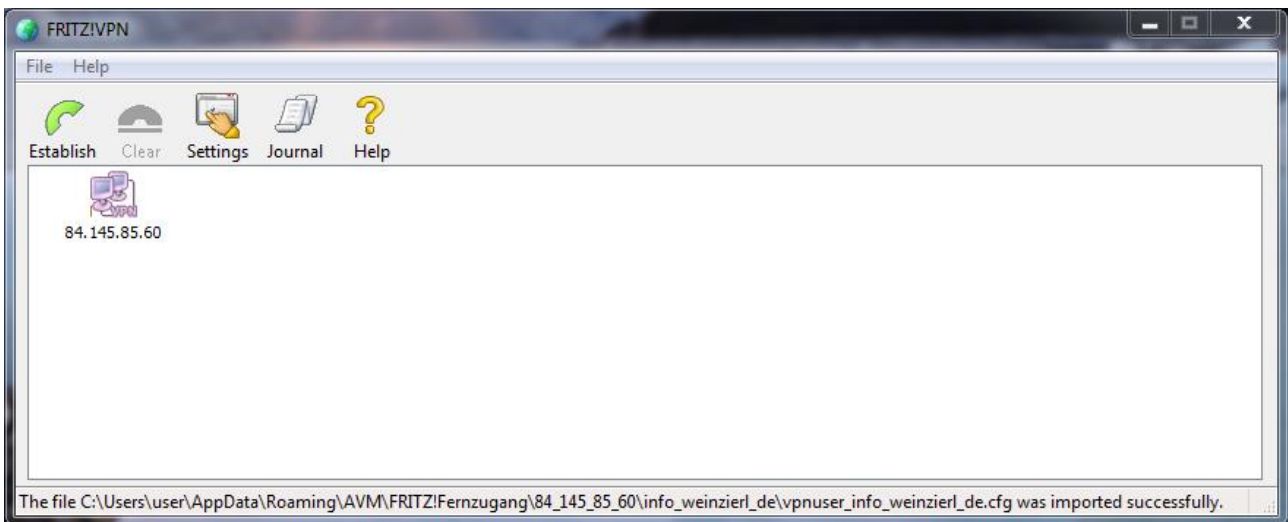


Figure 22: AVM VPN-Client – connect

To connect to the VPN-Server on Fritzbox in building B, select the icon named “84.145.85.60” and click on the option “Establish”

Now the AVM VPN-Client program will connect to the VPN-Server on Fritzbox in building B.

3.2.4 Accessing the remote KNX IP device with the ETS

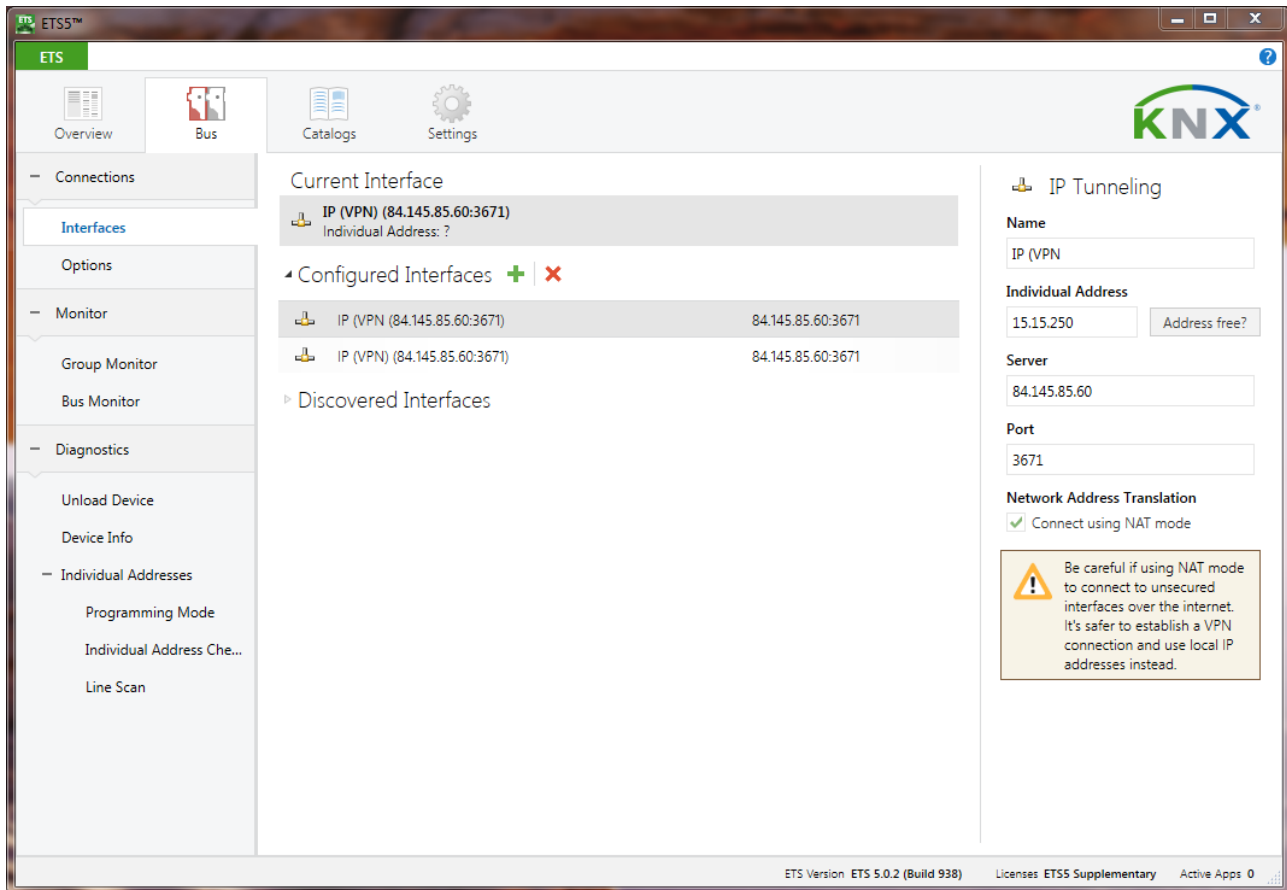


Figure 23: IP interface over VPN in ETS connection manager

In order to establish a ETS connection via the VPN connection, you have to configure the KNX IP interface manually. It is not possible for ETS to identify the interface automatically via the VPN connection. Within the "Server" text box you either fill in the static IP-Address of Fritzbox in building B or the DynDNS account.

Hint: The "Connect using NAT mode" checkbox has to be activated. Despite the fact that the connection is not established in NAT mode, this option enables certain initialisations which are necessary for a KNXnet/IP connection.

3.2.5 Alternatives

Apart from the Fritzbox (AVM) used in this example, a VPN can be built with other devices as well. Devices of this type are available from Linksys, Netgear, DrayTek etc. Besides all embedded solutions also a PC running "OpenVPN" can be used.