WEINZIERL

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

Remote access with the ETS

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

Table of contents

1 Introduction

This document describes the possibilities of remote access, e.g. with ETS, to a KNX installation via the Internet.

Remote access is an essential requirement for many KNX installations. On the one hand for the installer, who maintains and optimises the system remotely, on the other hand for the user of the object, who expects display and operating functions. Here, the Internet Protocol IP offers a continuous possibility to communicate from any location worldwide to the individual property.

At the same time, the use of the Internet entails the risk of unauthorized access. In order to prevent this, technical measures are required, which are listed below.

Remote access can either be carried out using NAT (Network Address Translation) or a VPN (Virtual Private Network). In addition to selecting the type of access, it is also possible to secure the KNX network using KNX Security.

Remote access is possible with all devices that support KNXnet/IP tunneling. These are the KNX IP Interface 731 / 732 secure, the KNX IP Router 751 / 752 secure, the KNX IP LineMaster 762 as well as the KNX IP BAOS 773, the KNX IP BAOS 774 and the KNX IP BAOS 777. In the following the term KNX IP devices is used.

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 efcp - 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

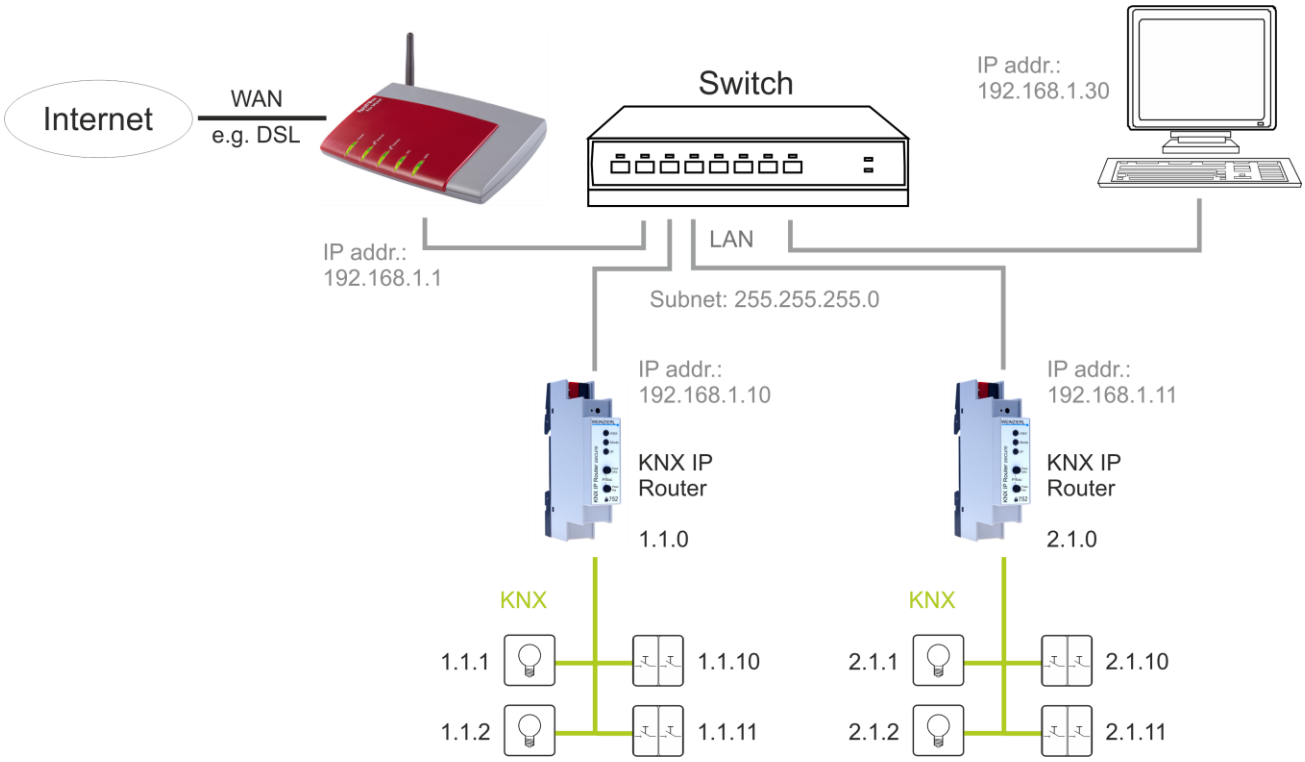

Figure 1: KNX installation

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 (192.168.5.1) 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 Necessary settings in the DSL router (FRITZ!Box 7490)

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. 192.168.5.30) 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.
Since Port 3671 is the official port for efcp - eFieldControl(EIBnet) of the KNX Association, it is advisable in the direction of Internet does not port the default to use it! As described in our example, we strongly recommend a port from the unreserved area between port 50000 and port 60000!

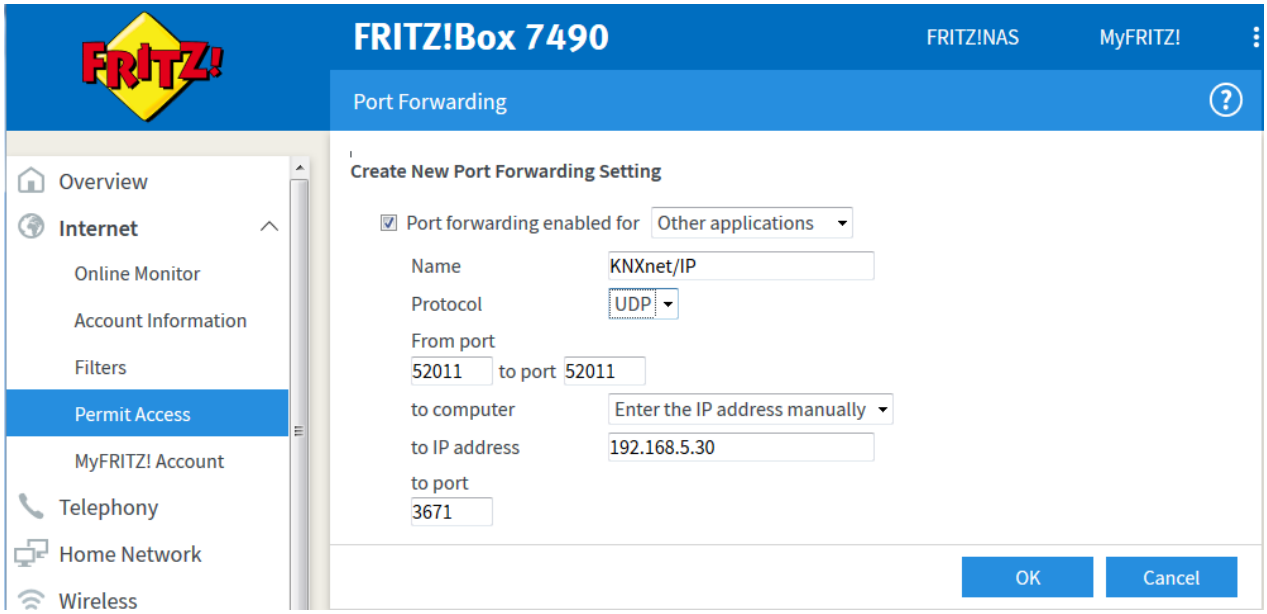

Figure 2: Settings in the DSL router (port forwarding for KNXnet/IP)

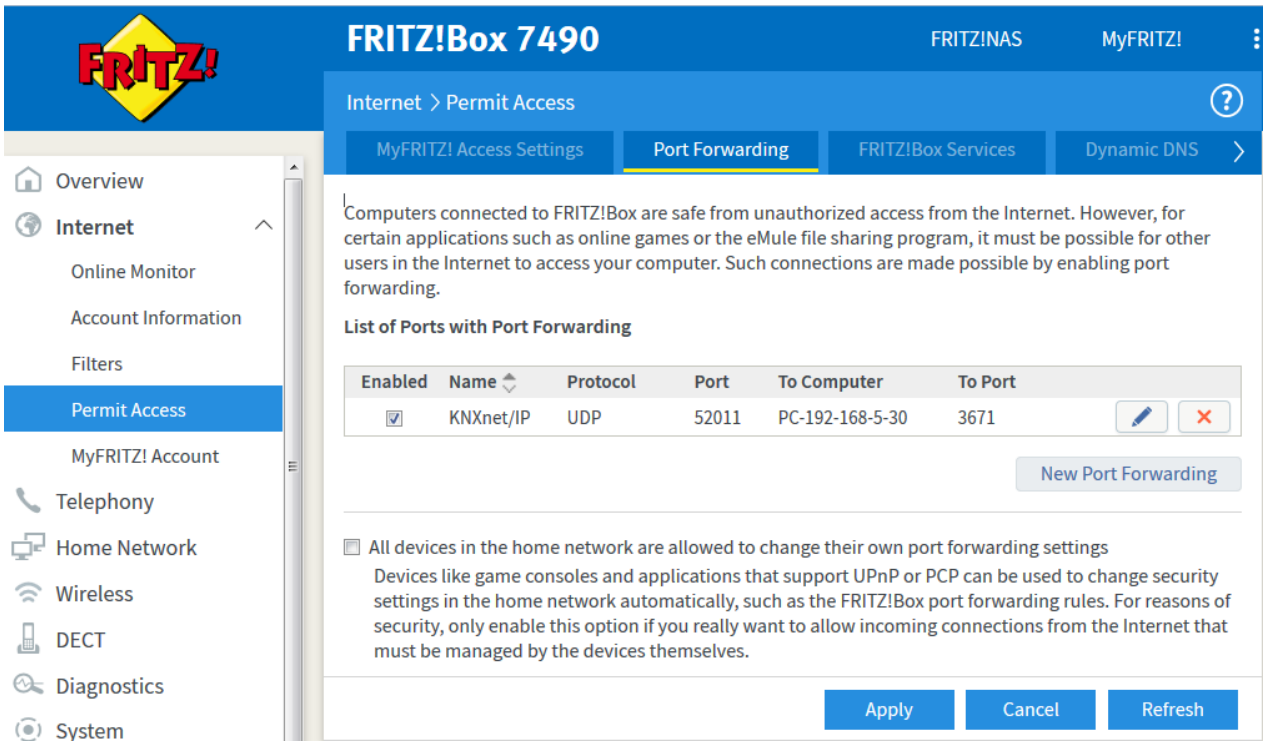

Figure 3: Settings in the DSL router (list of port forwarding's)

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 (192.168.5.30), subnet mask (255.255.255.0) and gateway IP address (192.168.5.1) must be specified.

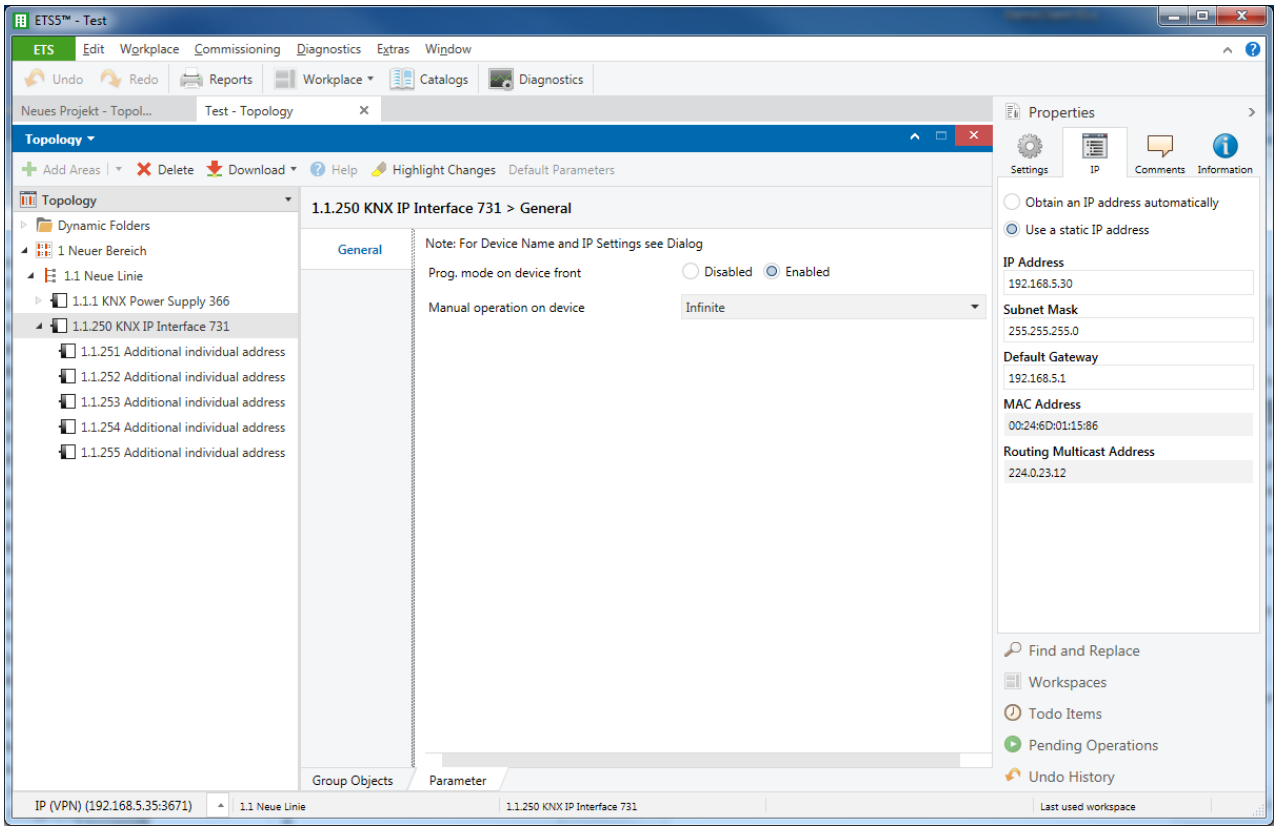

Figure 4: IP configuration (part 1)

2.2.4 Establishing a connection with the ETS

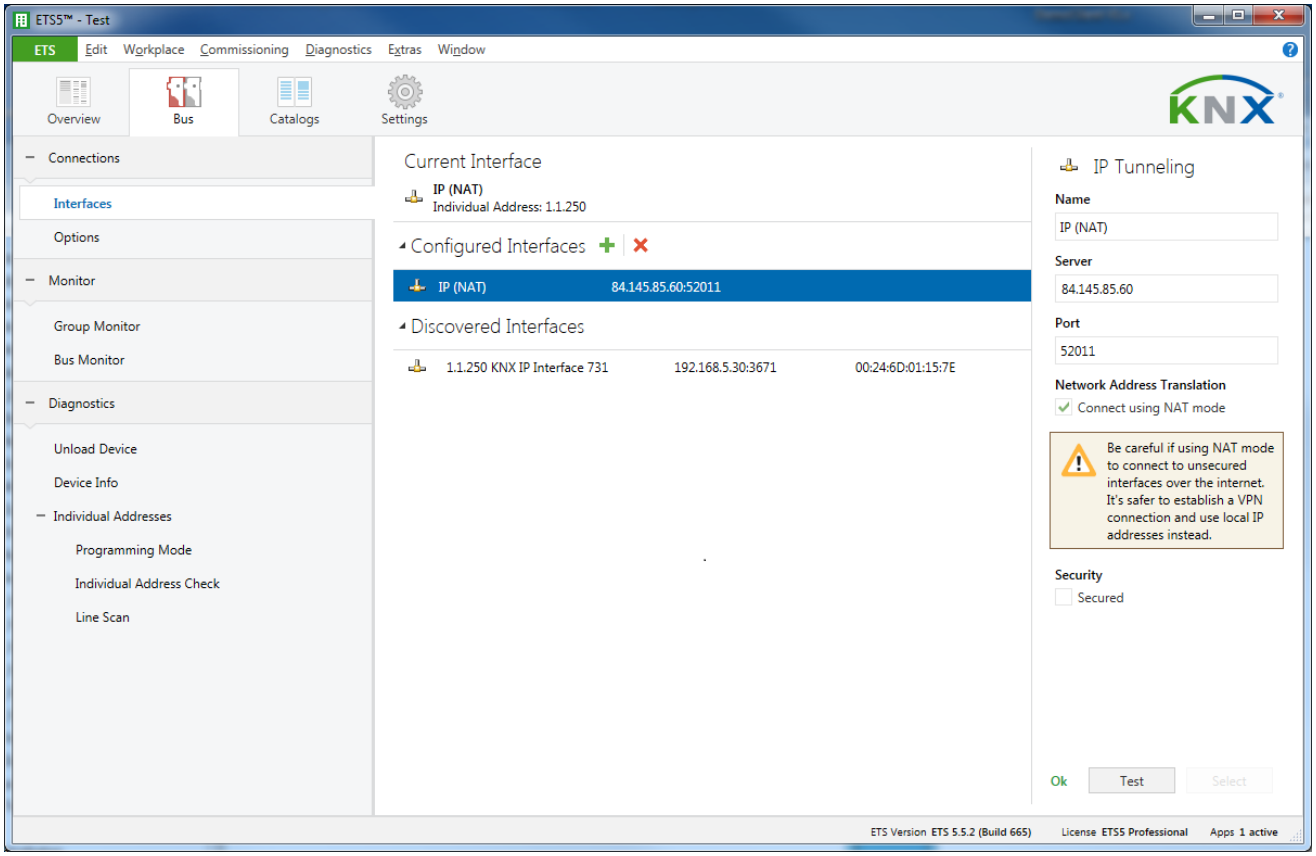

Figure 5: ETS Connection Manager

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 ‘Server’ 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)

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.

3.1.1 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.

3.1.2 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 Setting up the VPN-Tunnel

For the configuration of the Fritzbox 7490, a special tool is needed (fritz!box_configure_vpn_connection_english.exe). The tool can be downloaded from: www.en.avm.de

After a successful completion of the configuration, the tool will generate two configuration files.
One of this files is for import into the Fritzbox (in property B) the other one is for the AVM VPN client program (VPN client for the PC running ETS in property A) (see item 3.2.3).

Hint: setting up a VPN-tunnelling 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.

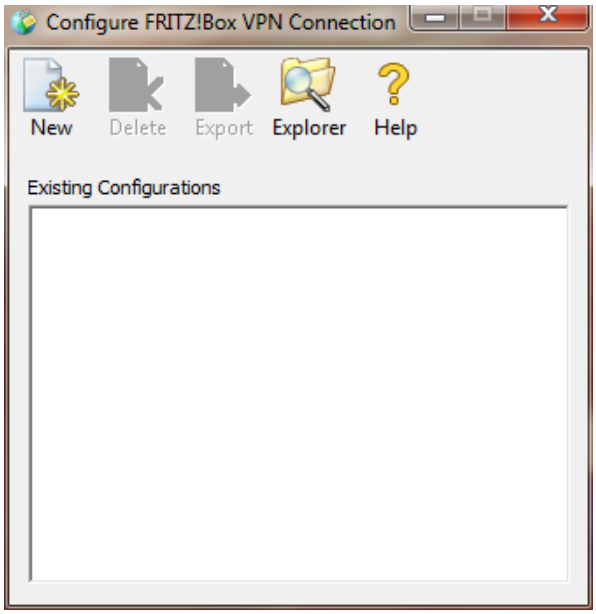

Figure 6: AVM VPN configuration tool

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.

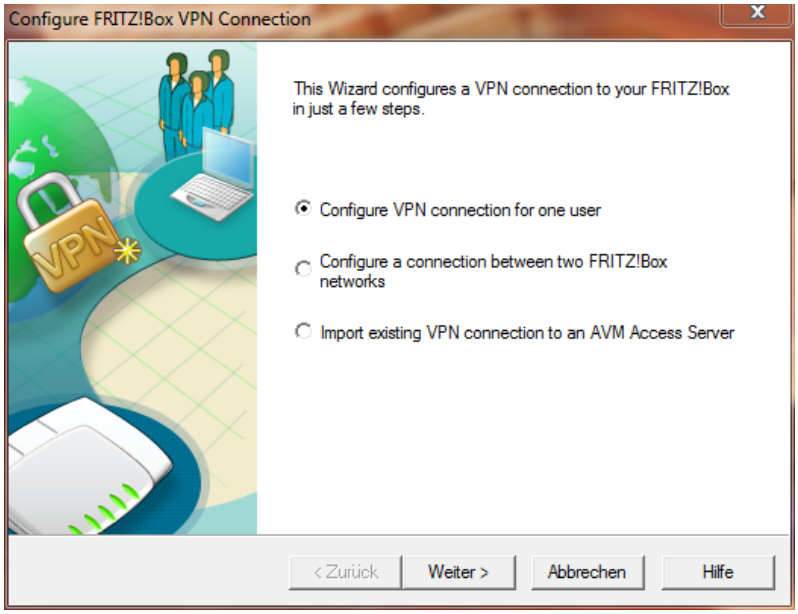

Figure 7: VPN mode option

In our example, we choose the ‘Configure VPN connection for one user’ option.

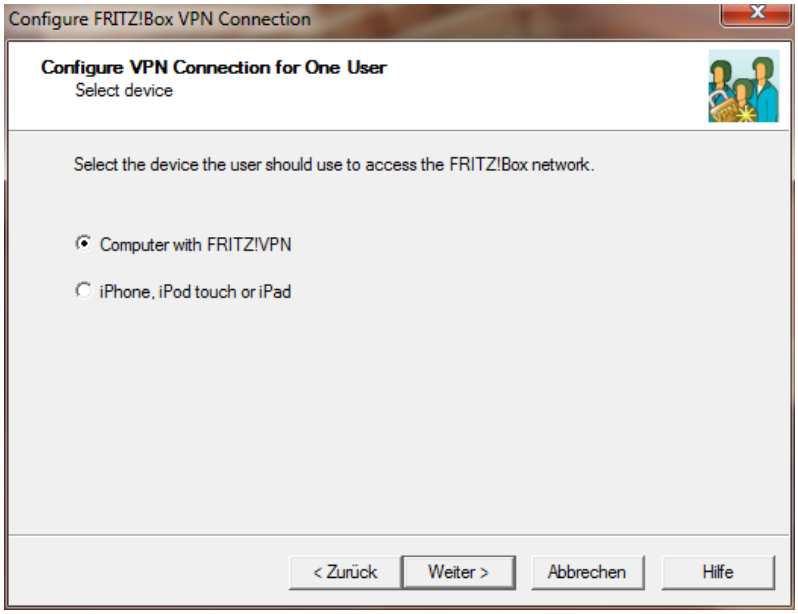

Figure 8: Choose platform

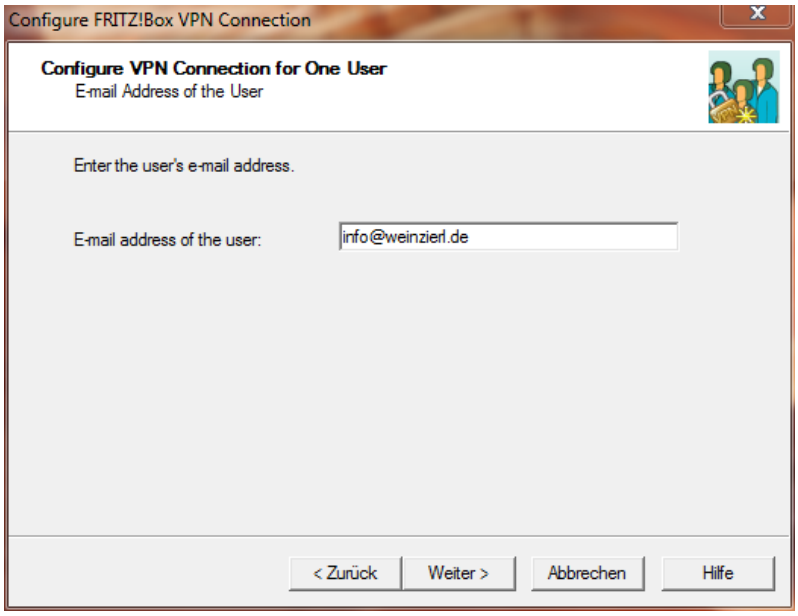

Figure 9: User e-mail

The next step is to create a user account with a specific name. In this example we choose an e-mail address but any name is allowed.

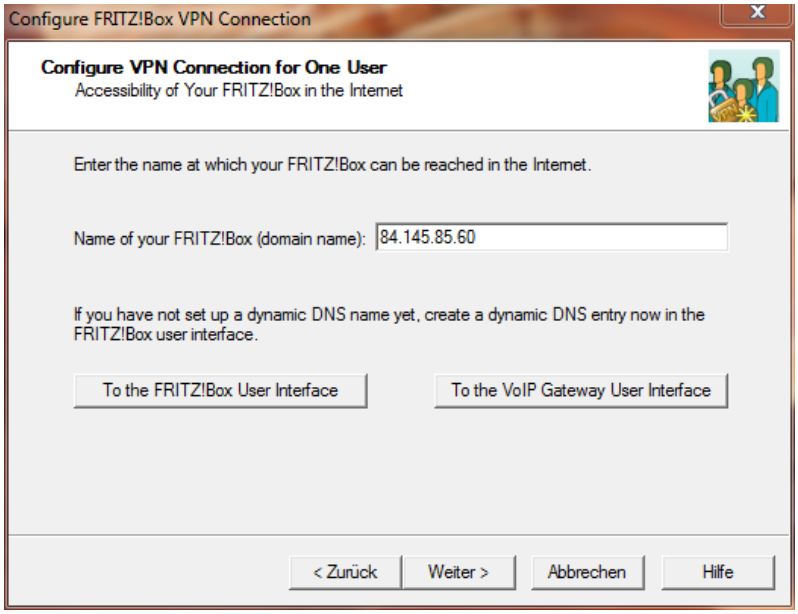

Figure 10: VPN-Server definition

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, …)

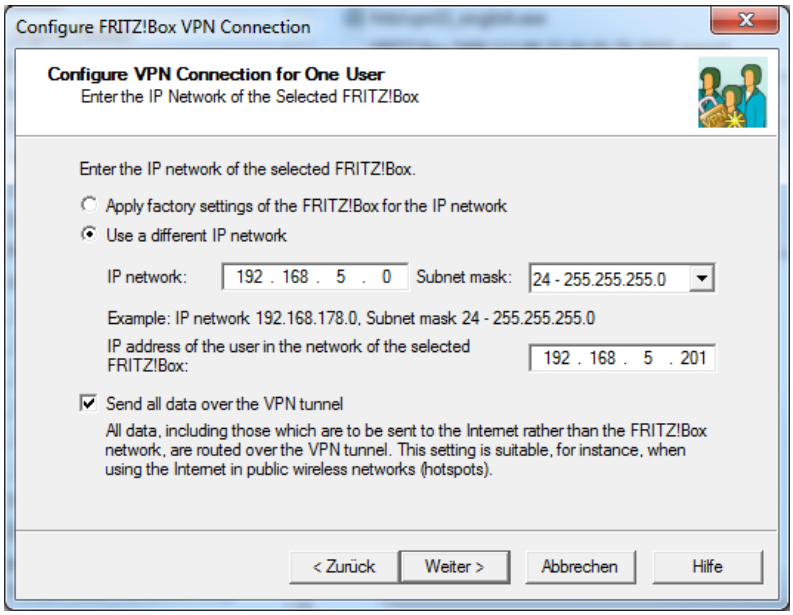

Figure 11: Subnet definition of LAN in building B

Hint: The 'IP address of the user in the network of the selected FRITZ!Box' has to be unique. Make sure that the choosen IP address is not already taken by another device or can be assigned by DHCP server of the FRITZ!Box.

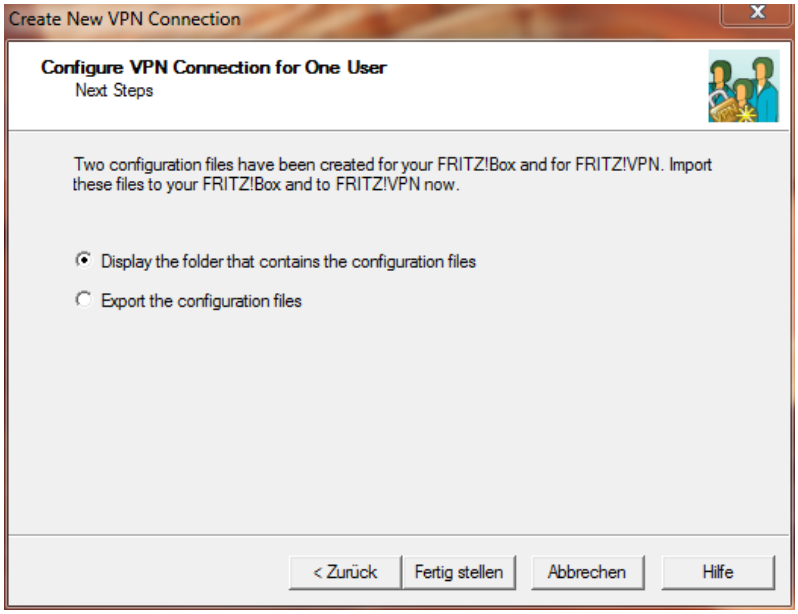

Figure 12: Finish the configuration wizard

Finally choose the option shown in figure 12. 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.

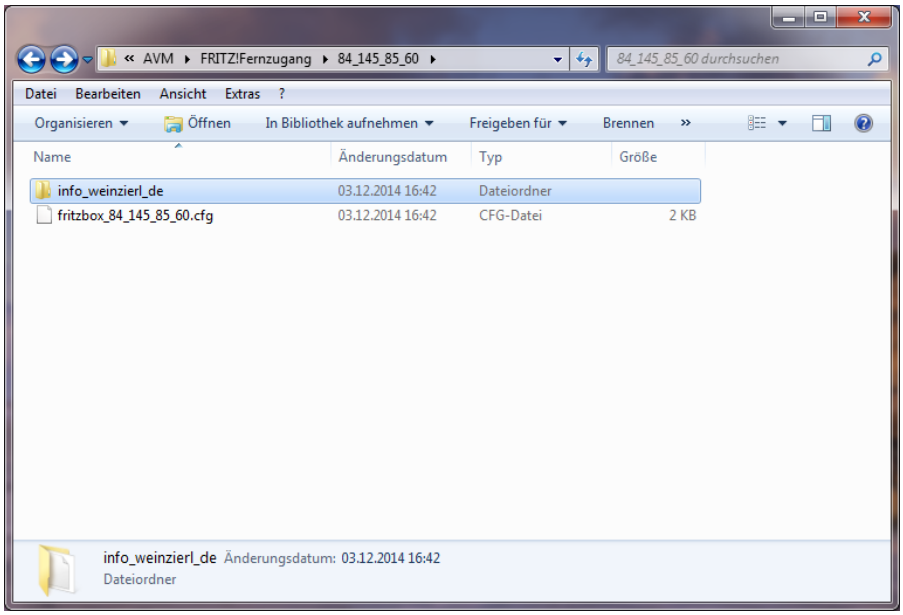

Figure 13: Folder with configuration file for VPN-Server

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 Fritbox in building B and creates a directory for the VPN user(s) in building A.

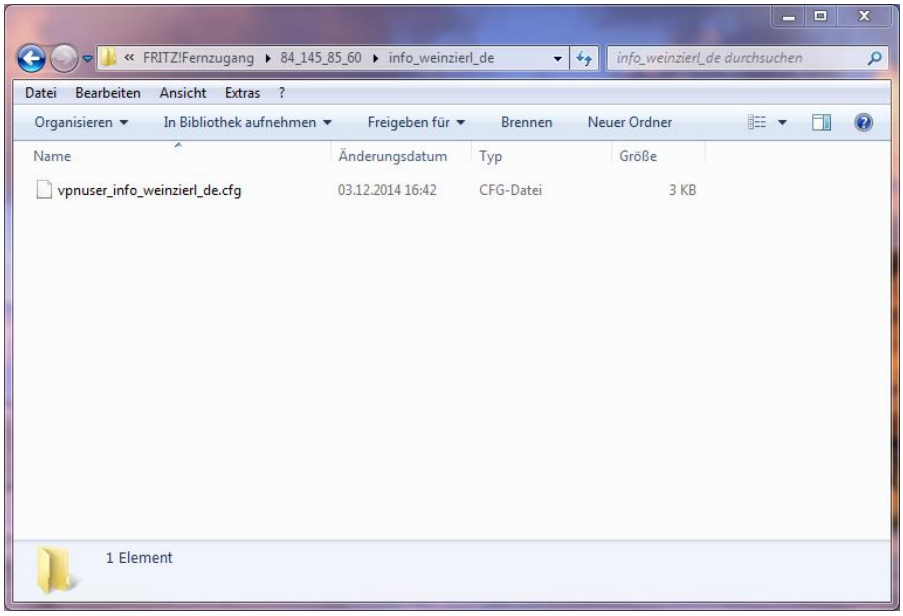

Figure 14: Folder with configuration file(s) for the user(s) (VPN client)

If additional users for VPN tunnel to building B are created, the individual configuration files will be stored in that folder (figure 13) as well.

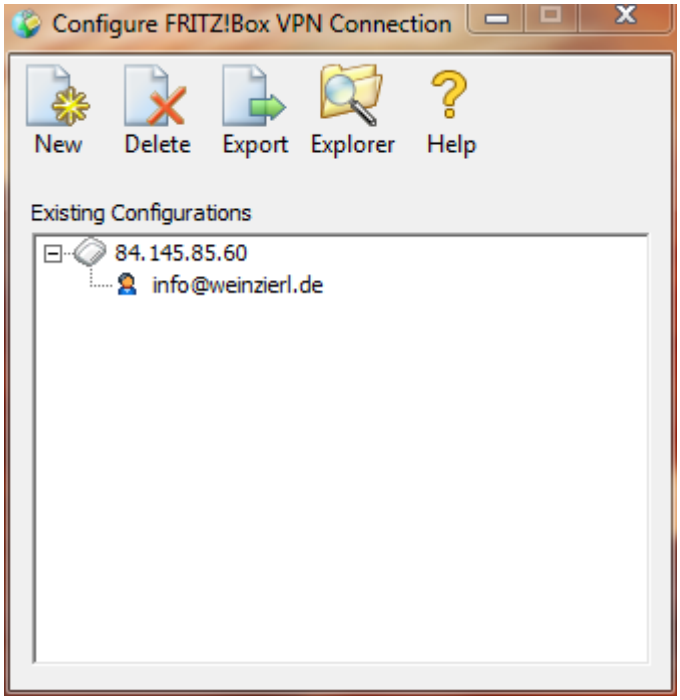

Figure 15: complete configuration of the VPN

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)

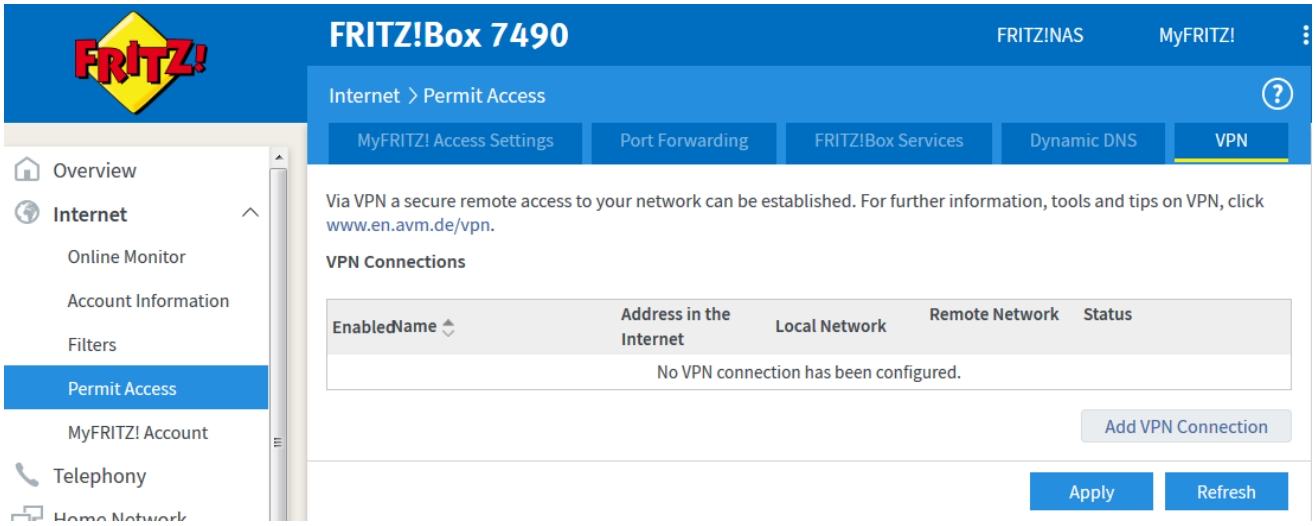

Figure 16: Fritzbox VPN-Server - add a connection

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’.

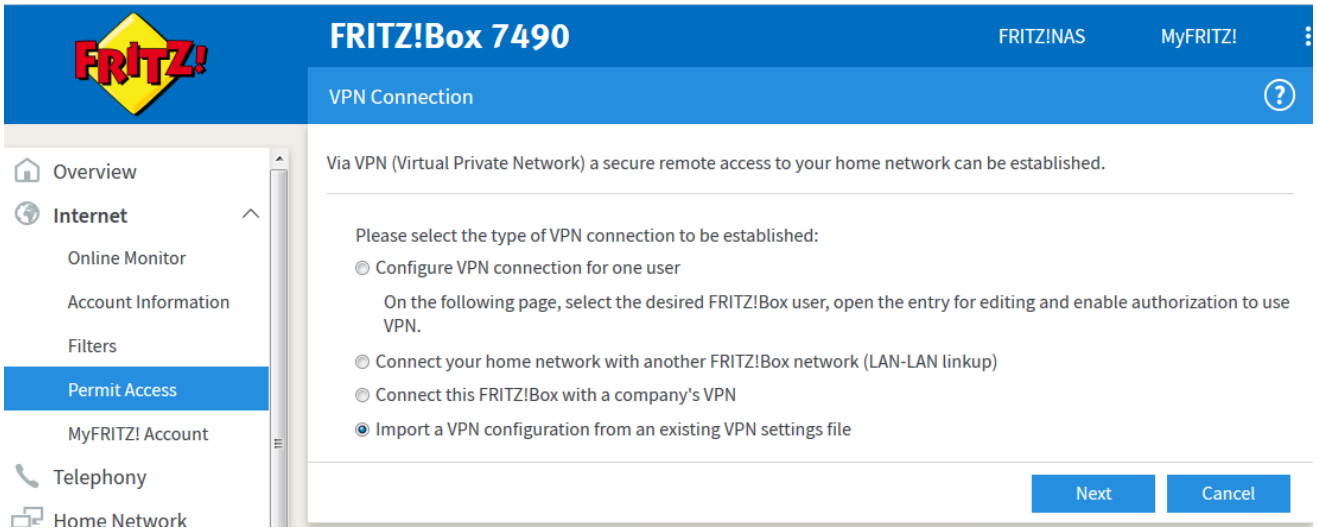

Figure 17: Fritzbox VPN-Server – choose means of configuration

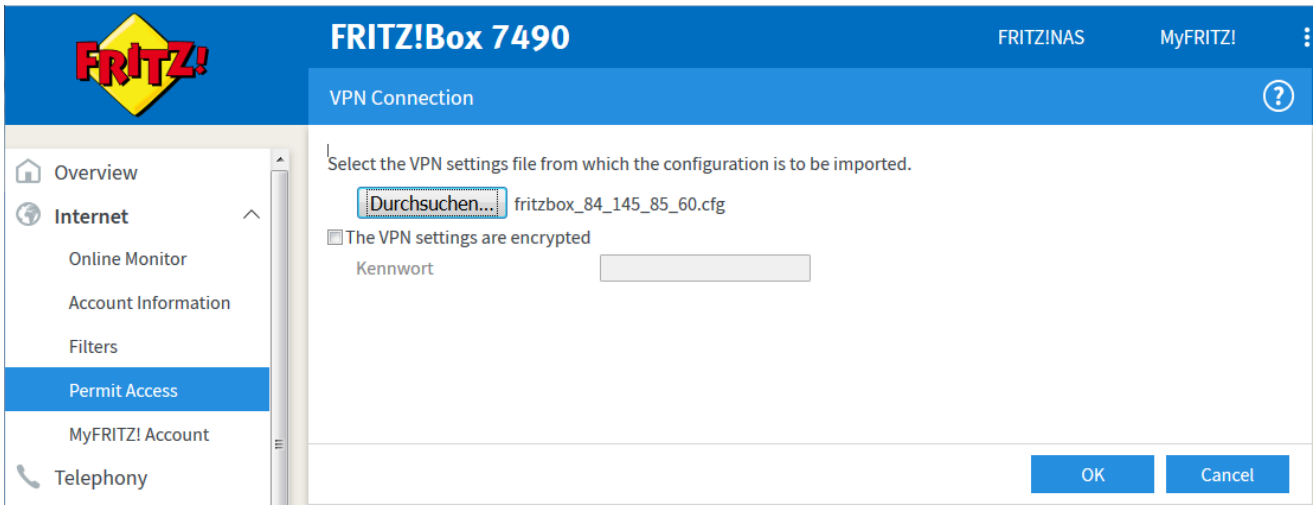

Figure 18: Fritzbox VPN-Server – choose the configuration file on your local system

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

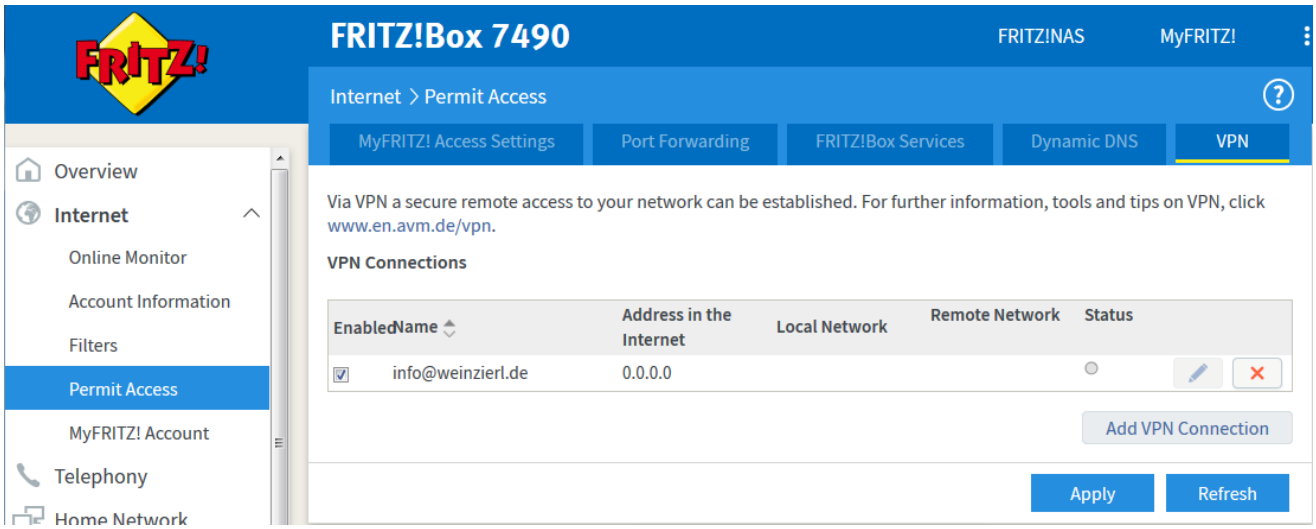

Figure 19: Fritzbox VPN-Server – opening the VPN connection

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:

https://en.avm.de/service/vpn/overview/

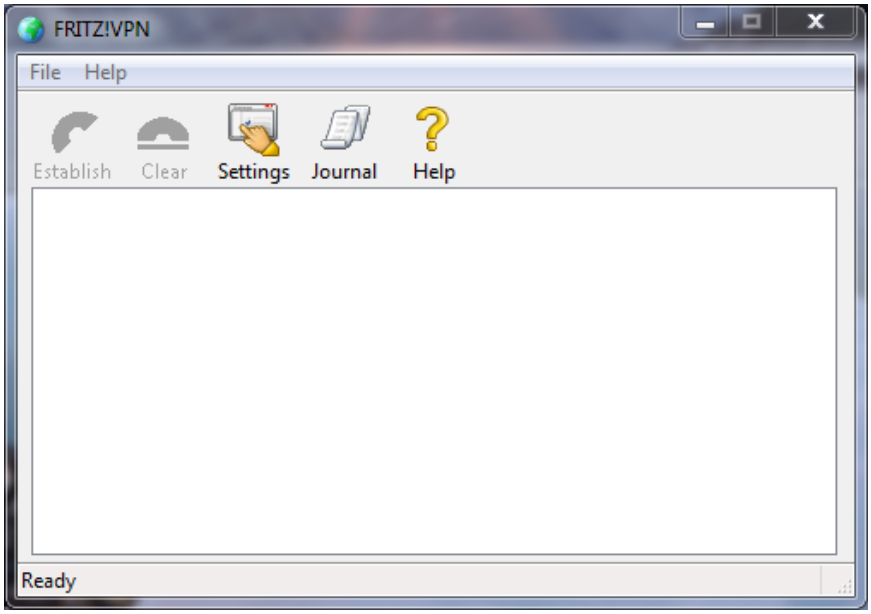

Figure 20: AVM VPN-Client

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.

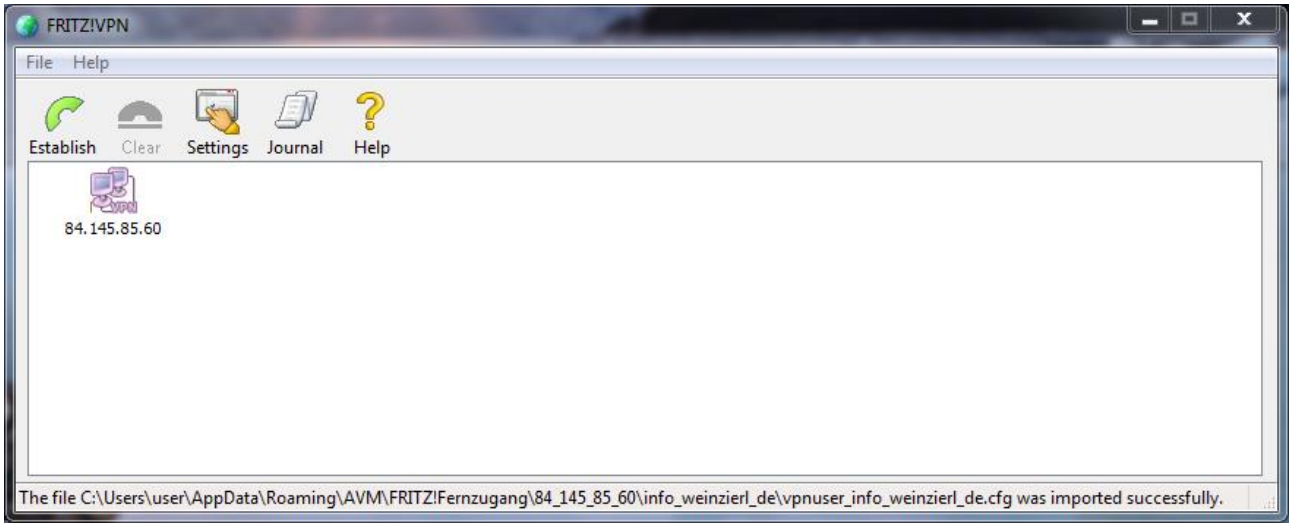

Figure 21: AVM VPN-Client – connect

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

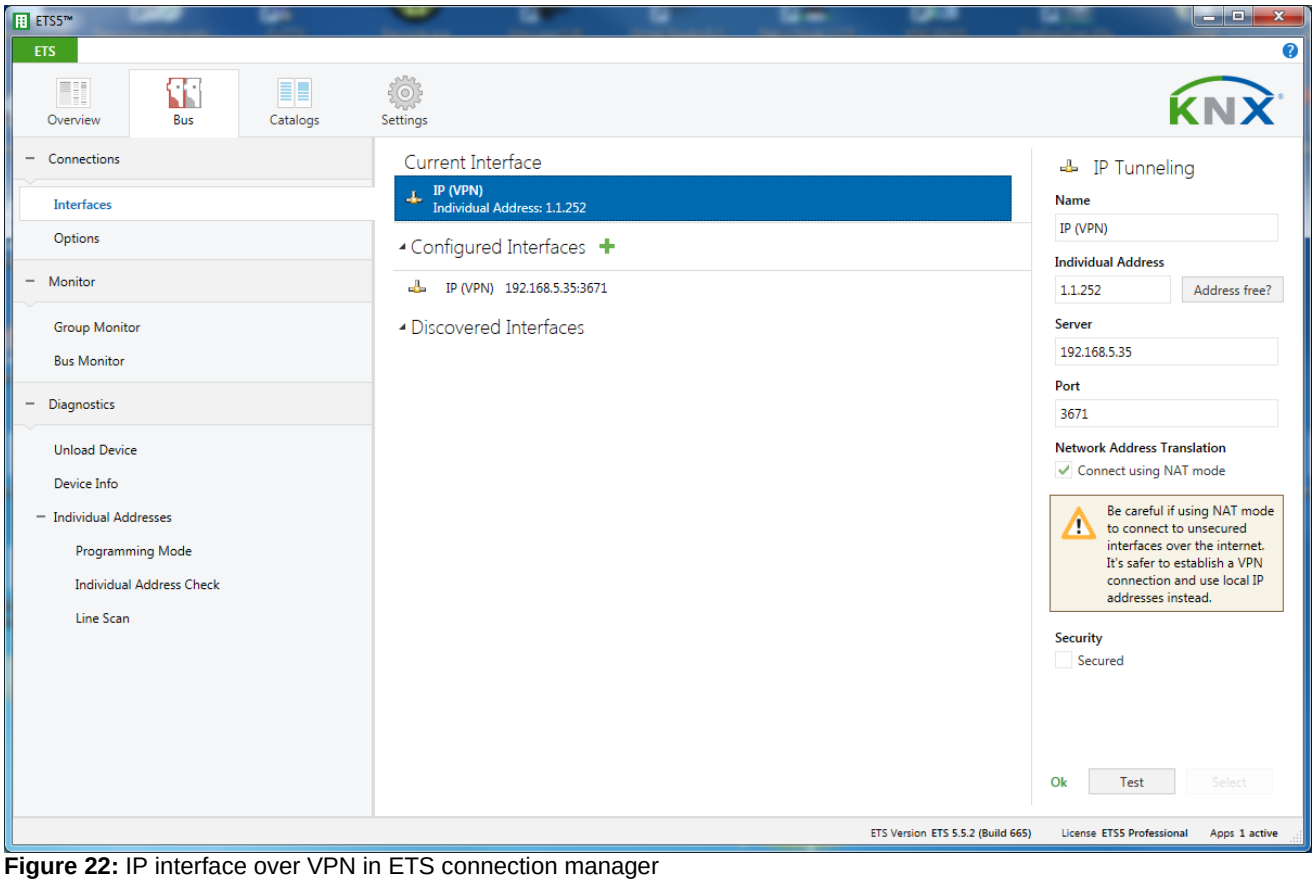

Figure 22: IP interface over VPN in ETS connection manager

In order to establish an 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 have to fill in the static IP-address of the KNX IP Interface in the subnet of building B. In our example this is the IP address of the first KNX IP Router (192.168.5.35)

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.

4 KNX IP Security

The alternative KNX IP Security follows an alternative approach, but is based on the same encryption methods as KNX Data Security. KNX IP Security is a pragmatic approach based on the assumption that there is an essential point of attack at the IP level. KNX Twisted Pair is assumed to be relatively secure as a purely local medium located in the wall. On the other hand, IP communication is often connected to the Internet and can therefore be attacked remotely.
KNX IP Security secures KNX IP communication while communication on KNX TP remains unencrypted. The main advantage of this approach is that the existing KNX TP devices and installations can continue to be used unchanged. Only the KNX IP devices, i.e. essentially KNX IP interfaces and KNX IP routers, must be replaced.
KNX IP includes the routing protocol, which is used for IP backbones, but also represents the KNX IP medium. On the other hand, the tunneling protocol is used to enable a client (e.g. ETS) to access a TP line via IP. While KNX IP routers usually implement both protocols, KNX IP interfaces only support the tunneling function.
As different as the two applications of KNX IP are, so different are the respective extensions for security. With the Secure Routing protocol, which is based on UDP Multicast, a common key is used to encrypt all KNX IP routing communication. A special feature is the telegram counter during routing. This is time-based and thus represents a time stamp that allows obsolete telegrams to be detected. The common system time is continuously synchronised between the devices.
With the tunneling protocol, the client and KNX IP device (KNXnet/IP server) first establish a secure channel using the so-called Diffie-Hellmann method. Only then are the user ID and password transferred. A new feature of KNX Secure Tunneling is the possibility of establishing the connection with TCP.

5 Combination of remote access and KNX secure

Due to the different remote access possibilities and the possibility of KNX secure or KNX unsecure the following constellations are possible.

	NAT	VPN
KNX unsecure	Warning! unprotected	OK
KNX secure	OK	optimal protection

Remote access via NAT and KNX unsecure is completely unprotected and should never be used. Optimum protection results are reached by simultaneous use of KNX Security and VPN.