

VPN with INSYS routers

Configuring OpenVPN client
with authentication via static
key

Introduction

Copyright © 2024 INSYS icom GmbH

Any duplication of this publication is prohibited. All rights on this publication and the devices are with INSYS icom GmbH Regensburg.

Trademarks

The use of a trademark not shown below is not an indication that it is freely available for use.

MNP is a registered trademark of Microcom Inc.

IBM PC, AT, XT are registered trademarks of International Business Machine Corporation.

Windows™ is a registered trademark of Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

INSYS® is a registered trademark of INSYS icom GmbH.

The principles of this publication may be transferred to similar combinations. INSYS icom GmbH does not assume liability or provide support in this case. Moreover, it cannot be excluded that other effects or results than described here are produced, if other, similar components are combined and used.

INSYS icom GmbH is not liable for possible damages.

Publisher

INSYS icom GmbH
Hermann-Köhl-Str. 22
D-93049 Regensburg
Germany

Phone +49 941 58692 0
Fax +49 941 58692 45
E-mail info@insys-icom.com
URL <http://www.insys-icom.com>

Print 17. Jan. 2024
Item No. -
Version 1.3
Language EN

1 Introduction

General

The present publication refers to a combination of selected hardware and software components of INSYS icom GmbH as well as other manufacturers. All components have been combined with the target to realize certain results and effects for certain applications in the field of professional data transfer.

All components have been prepared, configured and used as described in this publication. Thus, the desired results and effects have been achieved.

The exact descriptions of all used components, to which this publication refers, are described in the tables *Hardware*, *Accessories* and *Software* at the end of this publication.

The symbols and formatings used in this publication are explained in the correspondent section at the end of this publication.

Some configurations or preparations, which are precondition in this publication, are described in other publications. Therefore, always refer to the related device manuals. INSYS devices with web interface provide you with helpful information about the configuration possibilities, if you click on "display help text" in the header.

Target of this Publication

In the following, you will find a description of how to set up the INSYS router as OpenVPN client for an authentication with static key. This is reasonable for applications where only two devices connect to each other at a time.



Figure 1: Configure OpenVPN client for authentication with static key

2 Summary

OpenVPN Client Configuration

How to configure an INSYS router as OpenVPN client. You will find detailed step by step instructions in the following section.

1. Open in the menu → Dial-In / Dial-Out / LAN (ext) / WWAN the page → Open-VPN client
2. Upload static key
3. Check "Activate OpenVPN client"
4. Enter "IP address or domain name of remote site"
5. Check "No authentication or authentication with preshared key"
6. Enter local and remote IP address of the VPN tunnel
7. Enter "Netaddress of network behind the VPN tunnel" and "Netmask of network behind the VPN tunnel" if required
8. Save settings

3 Configuration

Provisions

Please prepare the following items before starting the configuration:

■ Connection to the INSYS router

- INSYS router is connected to power supply and ready for operation.
- You have access to the INSYS router via your web browser.
- Date and time are correctly set in the INSYS router.

■ Upload static key

How to upload the static key for an OpenVPN client.

i *You can upload new files with existing configuration as well. All other configuration settings are maintained except overwriting possibly present files.*

- The following file is required for uploading, which has been created before ("Creating a new static key") or provided for you by the server administrator: static key, e.g. "static.key"

i *OpenVPN client and OpenVPN server require the same static key!*

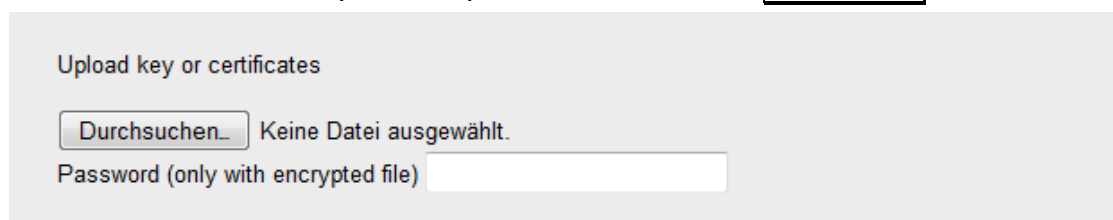
1. Select in the menu the page → OpenVPN client.

i *This page is under the menu item Dial-In, Dial-Out, LAN (ext), or WWAN depending on the used INSYS router.*

2. Scroll down to → Upload key or certificates.

i *The INSYS router detects the file type automatically and assigns the file correctly during the following upload.*

3. Click in the section "Upload key or certificates" on **Browse...**.



Upload key or certificates




Keine Datei ausgewählt.

Password (only with encrypted file)

4. Select the file with the static key (e.g. "static.key").

5. Click **OK** to upload the file.

- ✓ A green check mark appears instead of the red "X" at "... preshared key available ...".

 Preshared key available  

- ▶ *You can also generate a new static key in the INSYS router using the "Generate a new static key" link. This can also be downloaded using the download link (blue arrow) and then uploaded to the server.*

Configuration

i No authentication will be used if you don't upload a static key. This is not recommended and only useful for test purposes because the data sent through the tunnel will not be encrypted without authentication.

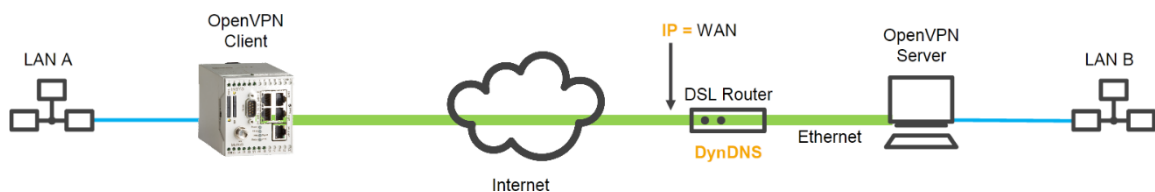
✓ Uploading the static key is completed with this.

■ Configuring Connection Data to Remote Terminal and Authentication with Static Key

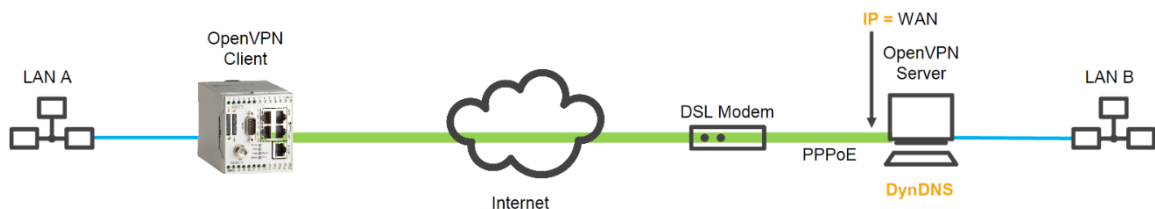
How to configure the connection data to the remote terminal for the connection set-up of the VPN client and the authentication with static key.

→ You must know the IP address accessible via the internet or the domain name of the remote terminal.

i This IP address depends on the architecture of the server network. If the server is behind a DSL router like in the following figure for example, its WAN IP address must be used. A corresponding port forwarding rule of the tunnel to the server must be present in the DSL router.



i If the server is directly connected to a DSL modem without intermediate router like in the following figure, the IP address of the server must be used.



i If the server has no fixed IP address, a DynDNS domain name can also be entered, which will then be resolved by the client. For this, DynDNS must be enabled in the DSL router (first example) or in the server (second example). Information about this can be found in the documentation of the respective devices. A DNS server must also be entered in the INSYS router for this.

2. Select in the menu the page → OpenVPN client.

i This page is under the menu item Dial-In, Dial-Out, or LAN (ext) depending on the used INSYS router.

3. Check the check box "Activate OpenVPN client".

4. Enter the IP address accessible via the internet or the domain name of the OpenVPN server into "IP address or domain name of remote site".

Activate OpenVPN client

[↻ OpenVPN current state](#)
[↻ Display log of last connection](#)
[↻ Display configurations file](#)
[↻ Create sample configuration file for remote terminal](#)

IP address or domain name of remote site

Alternative remote site

Tunnelling over port (local / remote)

Protocol UDP TCP

Bind to local address and port

Remote terminal is allowed to change its IP address (float)

Activate LZO compression

Masquerade packets before tunnelling

Cipher algorithm

Log level

Fragment packets (in bytes)

Interval for renegotiation of data channel key (in seconds)

Ping interval (in seconds)

Ping restart interval (in seconds)


Additional ICMP ping to

5. Configure the further OpenVPN parameters according to the configuration of your OpenVPN server.

i You can check the settings in OpenVPN syntax using the "Display configuration file" link. You can display settings, which might be suitable for the remote terminal, using the "Create sample configuration file for remote terminal" link.

6. Scroll down to → No authentication or authentication with preshared key.

No authentication or authentication with preshared key

Preshared key available [↻](#) 
 Generate a new static key

IP address of VPN tunnel local

IP address of VPN tunnel remote

Netaddress of network behind the VPN tunnel

Netmask of network behind the VPN tunnel

7. Select the option "No authentication or authentication with preshared key".

8. Enter the IP address of the local tunnel end into the "IP address of VPN tunnel local" field and the IP address of the remote tunnel end into the "IP address of VPN tunnels remote" field.

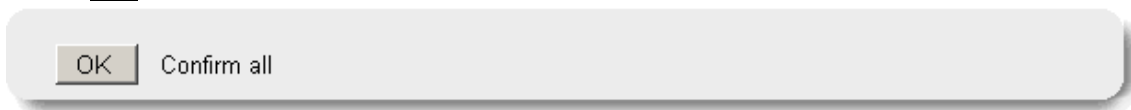
Configuration

i *These IP addresses must be swapped at the VPN remote terminal of the server, i.e. the address, which is the local tunnel end at the server, is the remote tunnel end at the client, and vice versa. The default settings can be used here in most cases.*

9. If required, enter the network address of the network, to which the VPN tunnel is to be established, into the "Netaddress of the network behind the VPN tunnel" field and the netmask of this network into the "Netmask of network behind the VPN tunnel" field.

i *This is only necessary, if the IP addresses are in a network, which is already used either local or at the remote terminal. In this case, the IP address of a network is an address ending with "0", e.g. 192.168.200.0. The network mask in this case is 255.255.255.0.*

10. Click **OK** at "Confirm all" to save the settings.



- ✓ The remote terminal for the connection set-up of the OpenVPN client is configured with this.

4 Used Components

Please observe: The power supply units required to operate devices are not listed here in detail. Take care for a provision at the site, if they are not part of the scope of delivery.

Hardware

Description	Manufacturer	Type	Version
Router	INSYS	INSYS router	Firmware 2.12.1

Table 1: Used hardware

Software

Description	Manufacturer	Type	Version
Operating system	Microsoft	Windows 7	SP1
Browser	Mozilla	Firefox	30

Table 2: Used software

Germany

INSYS icom GmbH
Hermann-Köhl-Str. 22
93049 Regensburg
Germany

Phone +49 941 58692 0
Fax +49 941 58692 45

E-mail info@insys-icom.com
URL www.insys-icom.com

Czech Republic

INSYS icom CZ, s.r.o.
Slovanská alej 1993 / 28a
326 00 Plzeň-Východní Předměstí
Czech Republic

Phone +420 377 429 952
Fax +420 377 429 952
Mobile +420 777 651 188

E-mail info@insys-icom.cz
URL www.insys-icom.cz