

VPN with INSYS routers

Configuring OpenVPN server
with certificate-based
authentication

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 1.4
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 server with certificate-based authentication.

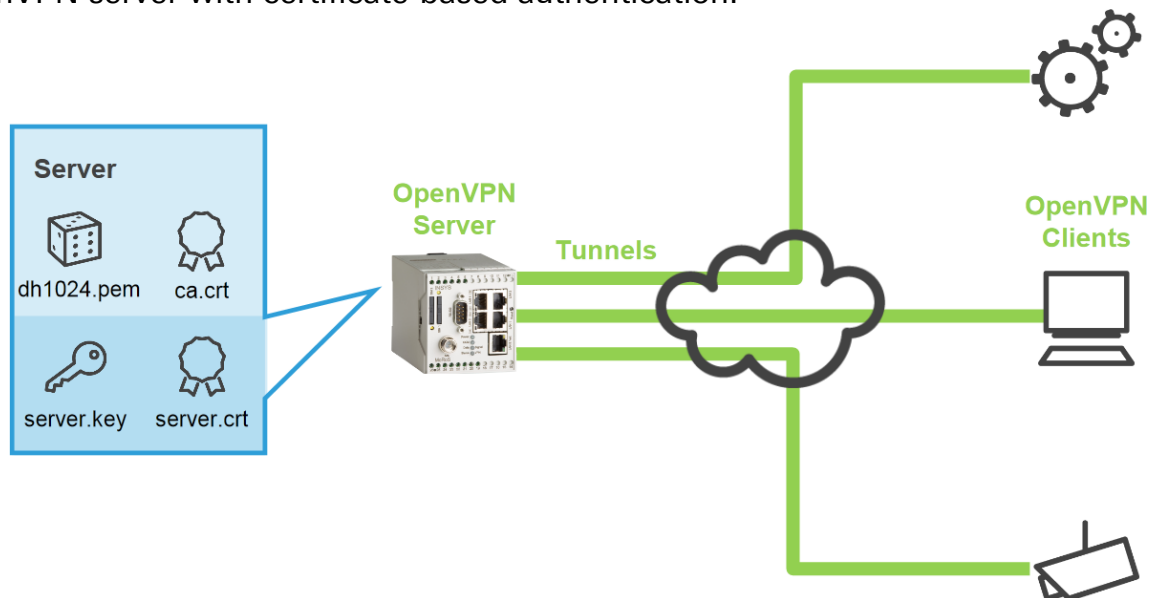


Figure 1: Configure the OpenVPN server with certificate-based authentication

2 Summary

OpenVPN Server Configuration

How to configure an INSYS router as OpenVPN server. 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 server
2. Upload CA certificate
3. Upload server certificate
4. Upload server key
5. Check "Activate OpenVPN server"
6. Check "Authentication based on certificate"
7. Adjust "IP address pool for clients" if required
8. "Create new route to a client network" if required
9. 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.

■ Uploading Server Certificates and Keys

How to upload the certificates and keys for an OpenVPN server.

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

- The following files are required for uploading, which have been created before (refer to separate Configuration Guide) or provided for you:

public CA certificate, e.g. "ca.crt"

public server certificate, e.g. "server.crt"

secret server key, e.g. "server.key"

▶ *If you have received a PKCS#12 file that contains certificates and key (e.g. "Server.p12"), this already contains all files.*

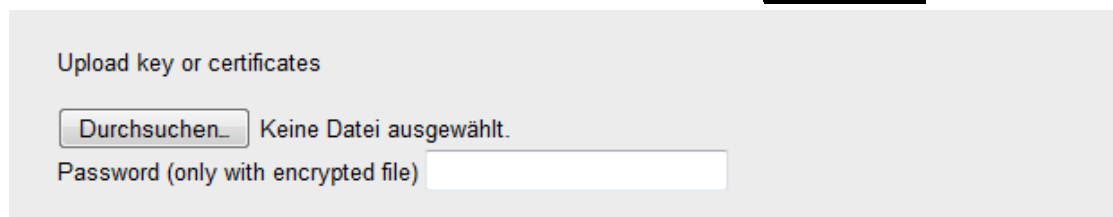
1. Select in the menu the page → OpenVPN server.

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

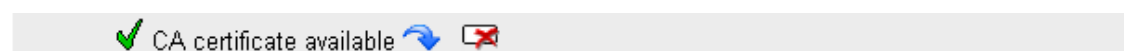
Keine Datei ausgewählt.

Password (only with encrypted file)

4. Select the file with the CA certificate (e.g. "ca.crt").

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

✓ A green check mark appears instead of the red "X" at "... CA certificate ...".



Configuration

- Proceed accordingly for the public certificate of the OpenVPN server (e.g. "server.crt") and the secret key of the OpenVPN server (e.g. "server.key") in order to upload both files to the INSYS router.

i Besides certificates and keys, a Certificate Revocation List as well as a new Diffie-Hellman parameter set can be uploaded here in the same way.

- ✓ A green check mark appears instead of the red cross for each uploaded file. Uploading the certificates and keys is completed with this.

■ Configure the OpenVPN server with certificate-based authentication

How to configure the connection data to the remote terminal for the connection set-up of the VPN server and the authentication with certificates.

- Select in the menu the page → OpenVPN server.

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

- Check the check box "Activate OpenVPN server".

Activate OpenVPN server

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

Tunnelling over port (local / remote)

Protocol UDP TCP

Inform clients about server network

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)

- Configure the further OpenVPN parameters according to your application.

i The default settings can be maintained for most applications. It is important that client and server have a consistent configuration.

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.

- Scroll down to → Authentication based on certificate.

Authentication based on certificate
 Diffie Hellman parameters available
 No Certificate Revocation List available
 CA certificate available
 Certificate available
 Private key available

Allow communication between clients

IPv4 address pool / Netmask /
 IPv6 address pool / Netmask /

Create new route to a client network

Name in certificate
 IPv4 net address / netmask /
 IPv6 net address / netmask /
 VPN IPv4 address

Existing routes to client networks

| delete | Name in certificate | Net address | Netmask | VPN IPv4 address |
|--------------------------|---------------------|---------------|---------------|------------------|
| <input type="checkbox"/> | client1 | 192.168.200.0 | 255.255.255.0 | |

5. Select the "Authentication based on certificate" option.
6. Adjust the "IP address pool for clients" if conflicts occur.
 - The tunnel addresses are only used for internal VPN routing and must only be adjusted, if they overlap with already used IP ranges.*
7. Create routes to client networks, if required.
 - As more than one tunnel are possible at the same time, the server must know the networks of the clients and apply the according routes. A route entry consists of "Name in certificate" (Common Name), "Net address" and "Netmask address". With the help of these routes, the server will determine which data packets are sent through which tunnel to the correct client. To differentiate the tunnels, the routes are determined according to the "common name" of a client certificate, which was sent to the server during the authentication.*
8. Click at "Confirm all" to save the settings.

Confirm all

- The OpenVPN server 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