

VPN mit INSYS-Routern

OpenVPN-Server mit
zertifikatsbasierter
Authentifizierung
konfigurieren

Copyright © 2024 INSYS icom GmbH

Jede Vervielfältigung dieser Publikation ist verboten. Alle Rechte an dieser Publikation und an den Geräten liegen bei INSYS icom GmbH, Regensburg.

Warenzeichen und Firmenzeichen

Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

MNP ist ein eingetragenes Warenzeichen von Microcom, Inc.

IBM PC, AT, XT sind Warenzeichen von International Business Machine Corporation.

Windows™ ist ein Warenzeichen von Microsoft Corporation.

Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

INSYS® ist ein eingetragenes Warenzeichen der INSYS icom GmbH.

Die Prinzipien dieser Publikation können auf ähnliche Kombinationen übertragbar sein. In diesem Fall übernimmt INSYS icom GmbH weder Gewährleistung noch Support. Weiterhin kann nicht ausgeschlossen werden, dass andere als die beabsichtigten und hier beschriebenen Wirkungen oder Ergebnisse erzielt werden, wenn andere, ähnliche Komponenten kombiniert und verwendet werden. INSYS icom GmbH haftet nicht für etwaige, auftretende Schäden.

Herausgeber

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

Telefon +49 941 58692 0
Telefax +49 941 58692 45
E-Mail info@insys-icom.de
URL <http://www.insys-icom.de>

Druck 17. Jan. 2024
Artikel-Nr. -
Version 1.4
Sprache DE

1 Einführung

Allgemein

Die vorliegende Publikation bezieht sich auf eine Kombination von ausgewählten Hard- und Software-Komponenten der INSYS icom GmbH sowie anderer Hersteller. Alle Komponenten wurden mit dem Ziel kombiniert, bestimmte Ergebnisse und Wirkungen für bestimmte Anwendungen im Bereich der professionellen Datenübertragung zu realisieren.

Die genauen Bezeichnungen aller verwendeten Komponenten, auf die sich diese Publikation bezieht, sind in den Tabellen *Hardware*, *Zubehör* und *Software* am Ende dieser Publikation definiert.

Die in dieser Publikation verwendeten Symbole und Formatierungen sind im gleichnamigen Abschnitt im Gerätehandbuch näher erklärt.

Manche Konfigurationen oder Vorbereitungen, die in dieser Publikation vorausgesetzt werden, sind in anderen Publikationen beschrieben. Ziehen Sie daher auch immer die zugehörigen Geräte-Handbücher zu Rate. INSYS-Geräte mit Web-Interface zeigen Ihnen hilfreiche Informationen zu den Konfigurationsmöglichkeiten an, wenn Sie in der Kopfleiste auf „Hilfetexte anzeigen“ klicken.

Ziel dieser Publikation

Im Folgenden wird erklärt, wie Sie den INSYS-Router als OpenVPN-Server mit zertifikatsbasierter Authentifizierung einrichten können.

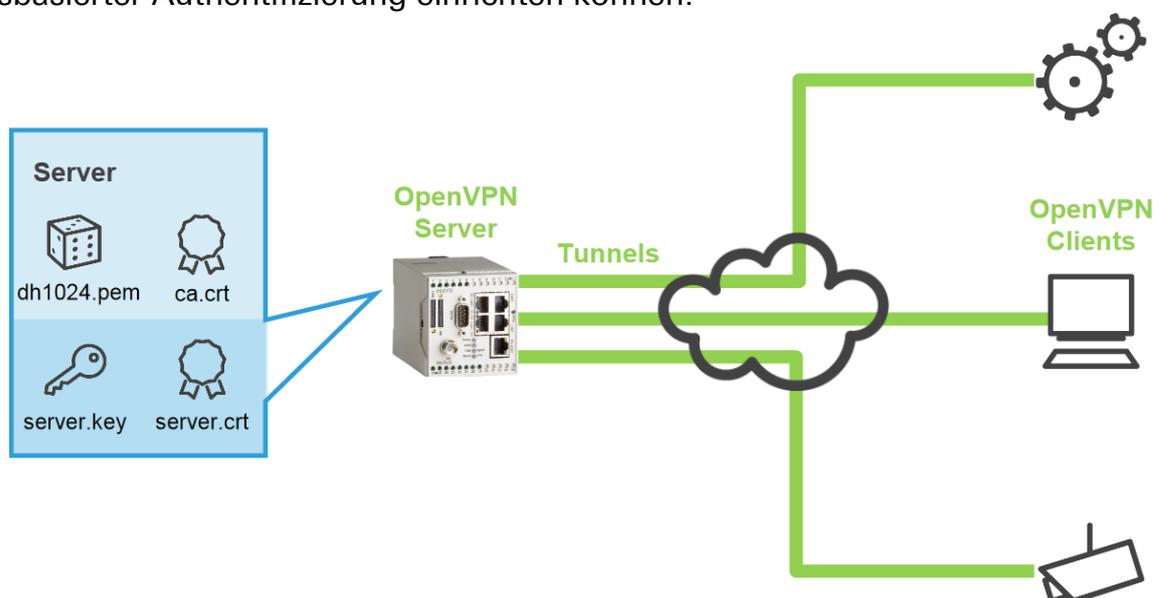


Abbildung 1: OpenVPN-Server mit zertifikatsbasierter Authentifizierung konfigurieren

2 Kurzfassung

OpenVPN-Server-Konfiguration

So konfigurieren Sie einen INSYS-Router als OpenVPN-Server. Detaillierte Schritt-für-Schritt-Anweisungen finden Sie im folgenden Kapitel.

1. Im Menü → Dial-In / Dial-Out / LAN (ext) / WWAN die Seite → OpenVPN-Server öffnen
2. CA-Zertifikat hochladen
3. Server-Zertifikat hochladen
4. Server-Schlüssel hochladen
5. „OpenVPN-Server aktivieren“ markieren
6. „Authentifizierung mit Zertifikaten“ markieren
7. Ggf. „IP-Adressen-Pool für die Clients“ anpassen
8. Ggf. „Neue Route zu Client-Netzwerk anlegen“
9. Einstellungen speichern

3 Konfiguration

Vorbereitungen

Bevor Sie mit der Konfiguration beginnen, bereiten Sie bitte folgende Punkte vor:

■ Verbindung mit dem INSYS-Router

- INSYS-Router ist mit der Stromversorgung verbunden und betriebsbereit.
- Sie haben Zugriff auf den INSYS-Router über Ihren Web-Browser.
- Datum und Zeit sind im INSYS-Router korrekt eingestellt.

■ Server-Zertifikate und -Schlüssel hochladen

So laden Sie die Zertifikate und Schlüssel für einen OpenVPN-Server hoch.

i *Sie können auch bei bestehender Konfiguration neue Dateien hochladen. Außer dem Überschreiben der evtl. vorhandenen Dateien bleiben alle anderen Konfigurationseinstellungen erhalten.*

- Zum Hochladen sind folgende Dateien erforderlich, die Sie vorher erstellt haben (siehe separates Konfigurationshandbuch) oder Ihnen zur Verfügung gestellt wurden:

öffentliches CA-Zertifikat, z.B. „ca.crt“

öffentliches Server-Zertifikat, z.B. „server.crt“

geheimer Server-Schlüssel, z.B. „server.key“

▶ *Falls Sie eine PKCS#12-Datei erhalten haben, die Zertifikate und Schlüssel enthält (z.B. „Server.p12“), enthält diese bereits sämtliche Dateien.*

1. Wählen Sie im Menü die Seite → OpenVPN-Server.

i *Diese Seite befindet sich je nach verwendetem INSYS-Router unter dem Menüpunkt Dial-In, Dial-Out, LAN (ext) oder WWAN.*

2. Scrollen Sie nach unten zu → Schlüssel oder Zertifikate laden.

i *Beim nachfolgenden Hochladen erkennt der INSYS-Router den Dateityp selbständig und ordnet die Datei richtig zu.*

3. Klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf Durchsuchen.

Schlüssel oder Zertifikate laden

Durchsuchen... Keine Datei ausgewählt.

Kennwort (nur bei verschlüsselter Datei)

4. Wählen Sie die Datei mit dem CA-Zertifikat aus (z.B. „ca.crt“).

5. Klicken Sie zum Hochladen der Datei auf OK.

✓ Anstelle des roten „X“ bei „... CA-Zertifikat ...“ wird ein grüner Haken eingeblendet.

✓ CA-Zertifikat vorhanden  

- Verfahren Sie in gleicher Weise mit dem öffentlichen Zertifikat des OpenVPN-Servers (z.B. „server.crt“) und dem geheimen Schlüssel des OpenVPN-Servers (z.B. „server.key“), um die beiden Dateien auf den INSYS-Router zu laden.

i Neben den Zertifikaten und Schlüsseln kann hier auf dieselbe Weise eine Certificate-Revocation-List (Zertifikats-Wiederrufliste) sowie ein neuer Diffie-Hellman-Parameter-Satz hochgeladen werden.

- ✓ Für jede hochgeladene Datei erscheint ein grüner Haken anstatt eines roten Kreuzes. Das Hochladen der Zertifikate und Schlüssel ist damit abgeschlossen.

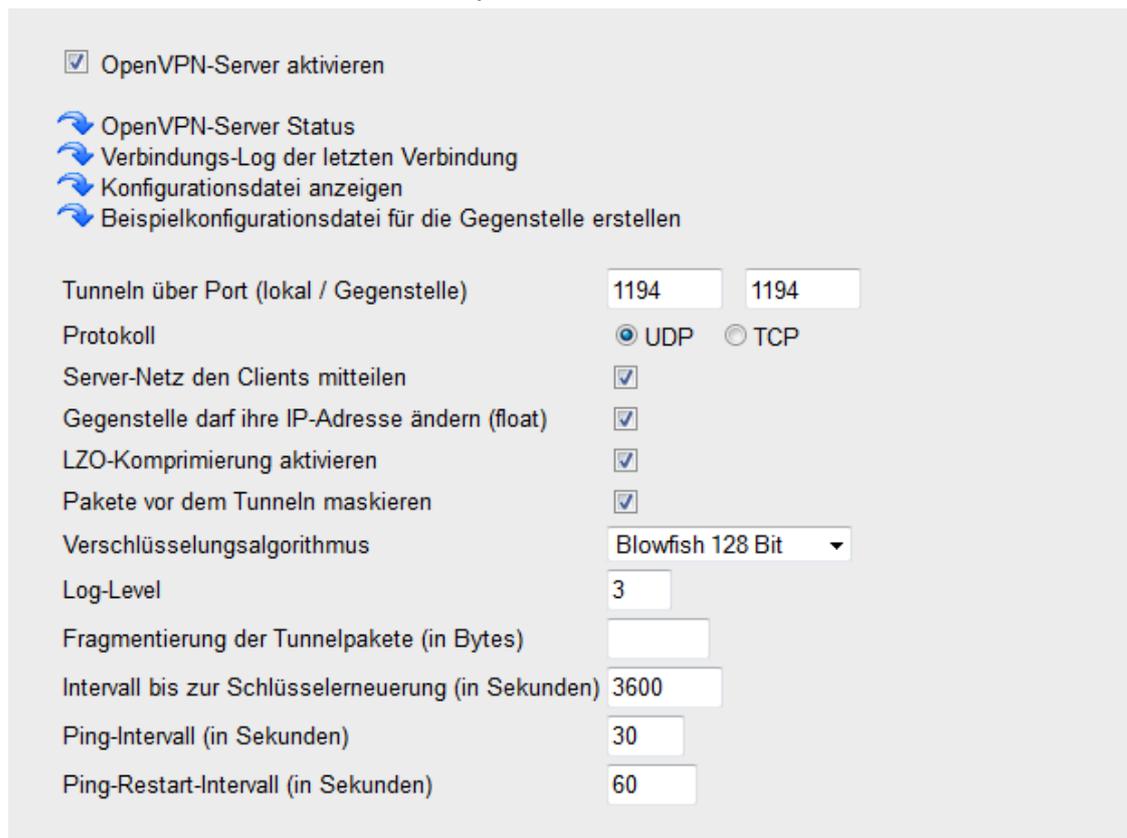
■ OpenVPN-Server mit zertifikatsbasierter Authentifizierung konfigurieren

So konfigurieren Sie die Verbindungsdaten zur Gegenstelle für den Verbindungsaufbau des VPN-Servers und die Authentifizierung mit Zertifikaten.

- Wählen Sie im Menü die Seite → OpenVPN-Server.

i Diese Seite befindet sich je nach verwendetem INSYS-Router unter dem Menüpunkt Dial-In, Dial-Out, LAN (ext) oder WWAN.

- Markieren Sie die Checkbox „OpenVPN-Server aktivieren“.



OpenVPN-Server aktivieren

 OpenVPN-Server Status
 Verbindungs-Log der letzten Verbindung
 Konfigurationsdatei anzeigen
 Beispielkonfigurationsdatei für die Gegenstelle erstellen

Tunneln über Port (lokal / Gegenstelle)

Protokoll UDP TCP

Server-Netz den Clients mitteilen

Gegenstelle darf ihre IP-Adresse ändern (float)

LZO-Komprimierung aktivieren

Pakete vor dem Tunneln maskieren

Verschlüsselungsalgorithmus

Log-Level

Fragmentierung der Tunnelpakete (in Bytes)

Intervall bis zur Schlüsselerneuerung (in Sekunden)

Ping-Intervall (in Sekunden)

Ping-Restart-Intervall (in Sekunden)

- Konfigurieren Sie die weiteren OpenVPN-Parameter gemäß Ihrer Anwendung.

i Für die meisten Anwendungsfälle können die Grundeinstellungen beibehalten werden. Wichtig ist, dass Client und Server eine übereinstimmende Konfiguration aufweisen.

- i** Über den Link „Konfigurationsdatei anzeigen“ können Sie die Einstellungen in der OpenVPN-Syntax kontrollieren. Über den Link „Beispielkonfigurationsdatei für die Gegenstelle anzeigen“ können Sie sich möglicherweise an der Gegenstelle vorzunehmende Einstellungen anzeigen lassen.

4. Scrollen Sie nach unten zu → Authentifizierung mit Zertifikaten.

Authentifizierung mit Zertifikaten

- ✓ Diffie-Hellman-Parameter vorhanden
- ✗ Keine Certificate Revocation List vorhanden
- ✓ CA-Zertifikat vorhanden
- ✓ Zertifikat vorhanden
- ✓ Privater Schlüssel vorhanden

Kommunikation zwischen Clients erlauben

IPv4-Adress-Pool / Netzmaske /

IPv6-Adress-Pool / Netzmaske /

Neue Route zu Client-Netzwerk anlegen

Name im Zertifikat

IPv4-Netzadresse / Netzmaske /

IPv6-Netzadresse / Netzmaske /

VPN-IPv4-Adresse

Bestehende Routen zu Client-Netzwerken

löschen	Name im Zertifikat	Netzadresse	Netzmaske	VPN-IPv4-Adresse
<input type="checkbox"/>	client1	192.168.200.0	255.255.255.0	

5. Markieren Sie die Option „Authentifizierung mit Zertifikaten“.

6. Passen Sie ggf. den „IP-Adressen-Pool für die Clients“ an, falls Konflikte auftreten.

- i** Die Tunneladressen werden nur für das interne VPN-Routing verwendet und müssen nur angepasst werden, wenn sie sich mit bereits verwendeten IP-Bereichen überschneiden.

7. Legen Sie ggf. Routen zu Client-Netzwerken an.

- i** Weil mehrere Tunnel gleichzeitig möglich sind, muss der Server die Netzwerke der Clients kennen und die entsprechenden Routen anlegen. Ein Routeneintrag besteht aus "Name im Zertifikat" (Common Name), "Netzwerkadresse" und "Netzwerkmaske". Mit Hilfe dieser Routen bestimmt der Server, welche Datenpakete durch welchen Tunnel zum richtigen Client gesendet werden sollen. Zur Unterscheidung der Tunnel werden die Routen anhand des "Common Name" eines Client-Zertifikates bestimmt, das bei der Authentifizierung zum Server gesendet wurde.

8. Klicken Sie zum Speichern bei „Einstellungen übernehmen“ auf .

Konfiguration

Einstellungen übernehmen

- ✓ Der OpenVPN-Server ist damit konfiguriert.

4 Verwendete Komponenten

Bitte beachten Sie: Die zum Betrieb notwendigen Spannungsversorgungen von Geräten sind hier nicht einzeln aufgeführt. Falls nicht im Lieferumfang enthalten, stellen Sie diese bitte vor Ort bereit.

Hardware

Bezeichnung	Hersteller	Typ	Version
Router	INSYS	INSYS-Router	Firmware 2.12.1

Tabelle 1: Verwendete Hardware

Software

Bezeichnung	Hersteller	Typ	Version
Betriebssystem	Microsoft	Windows 7	SP1
Browser	Mozilla	Firefox	30

Tabelle 2: Verwendete Software

Deutschland

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

Telefon +49 941 58692 0
Telefax +49 941 58692 45
E-Mail info@insys-icom.de
URL www.insys-icom.de

Czech Republic

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

Telefon +420 377 429 952
Telefax +420 377 429 952
Mobil +420 777 651 188
E-Mail info@insys-icom.cz
URL www.insys-icom.cz