

## **VPN mit INSYS-Routern**

OpenVPN-Server mit  
Authentifizierung über  
statischen Schlüssel unter  
Windows 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](mailto:info@insys-icom.de)  
URL <http://www.insys-icom.de>

Druck 17. Jan. 2024  
Artikel-Nr. -  
Version 1.3  
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

In einem OpenVPN-Netzwerk kann auch ein Windows-PC als OpenVPN-Server fungieren. Informationen zu OpenVPN finden Sie unter <http://www.openvpn.eu>.

In dieser Publikation erfahren Sie, wie Sie einen Windows-PC als OpenVPN-Server mit Authentifizierung über statischen Schlüssel für ein OpenVPN-Netzwerk mit einem INSYS-Router als Client einrichten. Bei dieser Betriebsart ist nur eine Verbindung zu einem einzigen Client möglich.

Die vorliegende Publikation beschreibt die Vorgehensweise unter Windows 7. Gehen Sie bei einer Installation unter Windows Vista oder Windows XP analog vor.

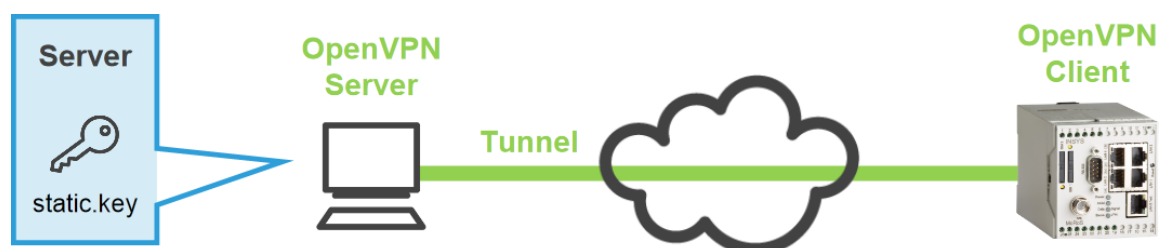


Abbildung 1: Windows-PC als OpenVPN-Server mit Authentifizierung über statischen Schlüssel

## 2 Konfiguration

### Vorbereitungen

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

- OpenVPN-Paket herunterladen
- OpenVPN-Paket auf Windows-PC installieren
- INSYS-Router als OpenVPN-Client konfigurieren und Konfigurationsdatei anzeigen
- Statischen Schlüssel hinterlegen



#### ■ OpenVPN-Paket herunterladen

So laden Sie das OpenVPN-Paket von unserer Homepage herunter.

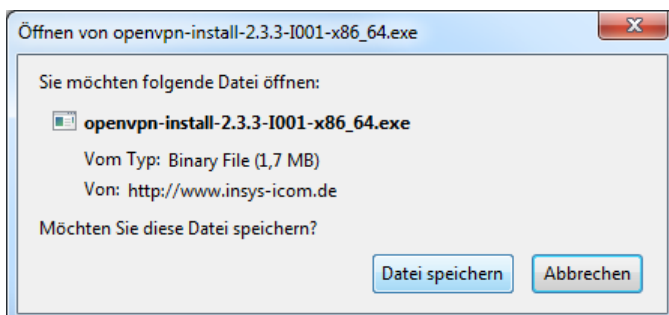
- PC mit ca. 1,5 MB freien Speicherplatz
- Webbrowser
- Internetverbindung

1. Öffnen Sie zum Download der Treiber <http://www.insys-icom.de/treiber/>.
2. Klicken Sie im Abschnitt „Router“ auf den Link für Ihre Windows-Version:

**i** Ihre Windows-Version (32 oder 64 Bit) finden Sie in der Systemsteuerung auf der Seite System im Abschnitt System unter Systemtyp.

| Router                                      |  |
|---|--|
| Treiber                                     | Datei  |
| OpenVPN-Installationsdatei - Windows 32 Bit |  <a href="#">OpenVPN 2.3.3 mit GUI (1,7 MB)</a> |
| OpenVPN-Installationsdatei - Windows 64 Bit |  <a href="#">OpenVPN 2.3.3 mit GUI (1,7 MB)</a> |

**i** Falls Ihnen eine aktuellere Version angeboten wird, wählen Sie diese.



3. Speichern Sie die Datei auf Ihrem PC.

✓ Damit haben Sie das OpenVPN-Paket herunter geladen.

#### ■ OpenVPN-Paket auf Windows-PC installieren

So installieren Sie die OpenVPN-GUI und die Programme zum Erstellen der Zertifikate und Schlüssel erfolgreich auf Ihrem PC.

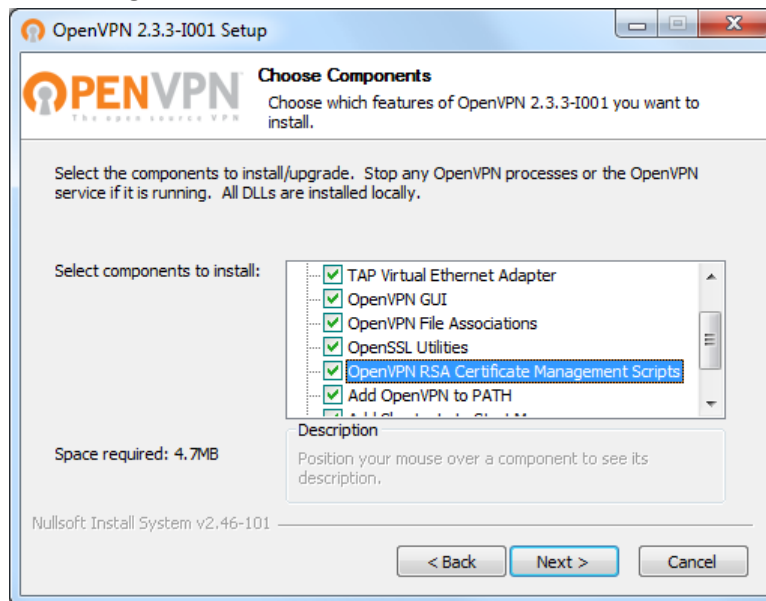
→ Sie haben das OpenVPN-Paket (Version 2.3.3 oder höher) von der INSYS Homepage [www.insys-icom.de/treiber](http://www.insys-icom.de/treiber) heruntergeladen.

1. Führen Sie die heruntergeladene Installationsdatei aus

- ▶ Falls eine Sicherheitsabfrage von Windows eingeblendet wird, bestätigen Sie diese.

2. Starten Sie den Setup Wizard und akzeptieren Sie die Lizenzhinweise.

- ✓ Das Fenster zur Auswahl der zu installierenden Komponenten wird angezeigt.



3. Markieren Sie die „OpenVPN RSA Certificate Management Scripts“, wählen Sie **Next >** und setzen Sie den Setup Wizard fort.

- ▶ Falls eine Warnung aus dem Windows-Log-Test eingeblendet wird, bestätigen Sie diese.

4. Klicken Sie nach dem Beenden der Installation zum Bestätigen **Finish**.

- ✓ Die OpenVPN-GUI, die SSL-Software und die Programme zum Erstellen der Zertifikate und Schlüssel befinden sich jetzt in den vorgegebenen Verzeichnissen (Standard: C:\Program Files\OpenVPN\).

| Name          | Änderungsdatum   | Typ               | Größe  |
|---------------|------------------|-------------------|--------|
| bin           | 04.06.2014 09:56 | Dateiordner       |        |
| config        | 04.06.2014 09:56 | Dateiordner       |        |
| doc           | 04.06.2014 09:56 | Dateiordner       |        |
| easy-rsa      | 04.06.2014 09:56 | Dateiordner       |        |
| log           | 04.06.2014 09:56 | Dateiordner       |        |
| sample-config | 04.06.2014 09:56 | Dateiordner       |        |
| icon.ico      | 25.06.2012 10:46 | IconView ICO File | 22 KB  |
| Uninstall.exe | 04.06.2014 09:56 | Anwendung         | 120 KB |

- ✓ Damit haben Sie das OpenVPN-Paket erfolgreich auf Ihrem PC installiert und die Vorbereitungen abgeschlossen.

### ■ INSYS-Router als OpenVPN-Client konfigurieren und Konfigurationsdatei anzeigen

So erzeugen Sie mit einem INSYS-Router, der als OpenVPN-Client konfiguriert ist, eine Konfigurationsdatei für den OpenVPN-Server. Dies ist die einfachste Art eine Konfigurationsdatei zu erstellen. Selbstverständlich kann diese auch manuell erstellt werden.

1. Konfigurieren Sie einen INSYS-Router, der als OpenVPN-Client fungieren soll, entsprechend Ihrer Anwendung.

❶ *Eine detaillierte Beschreibung dazu finden Sie im Konfigurations-Handbuch „OpenVPN-Client mit Authentifizierung über statischen Schlüssel konfigurieren“.*

✓ Nach Abschluss dieser Vorgänge kann der INSYS-Router eine geeignete Konfigurationsdatei für den OpenVPN-Server erzeugen.

2. Klicken Sie nun auf den Link „Beispielkonfiguration für die Gegenstelle erstellen“, um diese Konfigurationsdatei anzuzeigen.

# Dies ist eine Beispielkonfiguration für einen OpenVPN-Server.  
# Text markieren und in die eigene Konfigurationsdatei kopieren (endet mit .ovpn).

```
# Noch anzupassende Parameter
remote 192.168.254.2 # IP-Adresse oder Domainname der Gegenstelle
ifconfig 10.1.0.1 10.1.0.2 # IP-Adresse des lokalen VPN Endpunkts, IP-Adresse des VPN Endpunkts der
Gegenstelle
secret static.key # Datei mit dem geheimen Schlüssel bei PSK Authentifizierung (Pre Shared
Key)

# Fixe Parameter
proto udp # Protokoll, das für den Tunnel benutzt wird
rport 1194 # Auf der Gegenstelle über diesen Port tunneln
lport 1194 # Lokal über diesen Port tunneln
comp-lzo # LZO Kompression aktivieren
cipher BF-CBC # Benutzer Verschlüsselungsalgorithmus
route 192.168.100.0 # Route in das Netzwerk hinter dem VPN-Tunnel
255.255.255.0
tun-mtu 1500 # Maximale Größe der Datenpakete
reneg-sec 3600 # Intervall bis zur Schlüsselerneuerung (in Sekunden)
ping 30 # Verbindungsprüfung nach Ablauf dieser Anzahl an Sekunden ohne
Datenverkehr
ping-restart 60 # Verbindung erneut aufbauen, wenn nach Ablauf dieser Anzahl an Sekunden
kein Ping von der Gegenstelle empfangen wurde
verb 3 # Ausführlichkeit der Log-Meldungen
dev tun # OpenVPN Netzwerkgerät
float # Akzeptiere Pakete von allen Rechnern (float)

# Alle Daten durch den VPN-Tunnel routen (zum Aktivieren # entfernen)
#redirect-gateway # Setze VPN-Tunnel als Standardroute
#route-method exe # Stabile Windowsrouten
#route-delay 2 # Routen nach Verzögerung setzen
```

3. Kopieren Sie den kompletten Text dieser Konfigurationsdatei in die Zwischenablage, um sie in einem folgenden Schritt in einen Texteditor einfügen zu können.

✓ Damit haben Sie eine Konfigurationsdatei für den OpenVPN-Server erstellt, die nun noch für Ihre Anwendung angepasst werden muss.

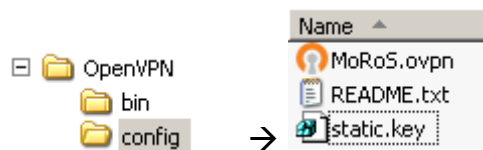
## ■ Statischen Schlüssel hinterlegen

So hinterlegen Sie den statischen Schlüssel für Ihre Anwendung.

- Dafür ist folgende Datei erforderlich, die Sie vorher mit Hilfe des INSYS-Routers erstellt haben („Statischen Schlüssel neu erstellen“) oder Ihnen vom Administrator des Systems zur Verfügung gestellt wurde:  
statischer Schlüssel, z.B. „static.key“

**i** *OpenVPN-Client und OpenVPN-Server benötigen denselben statischen Schlüssel!*

1. Kopieren Sie den statischen Schlüssel in das Arbeitsverzeichnis des OpenVPN-Pakets (Standard: C:\Program Files\OpenVPN\config).



- ✓ Damit verfügt der OpenVPN-Server über den erforderlichen Schlüssel.

## Konfiguration

Passen Sie nun die Beispielkonfiguration für Ihre Anwendung an. Dazu sind die folgenden Schritte erforderlich:

### ■ Konfigurationsdatei aus Beispielkonfiguration erzeugen

So erzeugen Sie aus der Beispielkonfiguration des INSYS-Routers eine Konfigurationsdatei für den OpenVPN-Server.

- Das OpenVPN-Paket ist auf dem Computer, der als Server fungieren soll, installiert.
- Sie haben mit einem INSYS-Router, der als OpenVPN-Client konfiguriert ist, die Beispielkonfiguration für die Gegenstelle aufgerufen und in die Zwischenablage kopiert.

1. Wechseln Sie in das Arbeitsverzeichnis des OpenVPN-Pakets (Standard: C:\Program Files\OpenVPN\config).
2. Erstellen Sie dort eine neue Textdatei und geben Sie ihr einen Dateinamen mit der Endung „.ovpn“ (z.B. „server.ovpn“).

**i** *Prüfen Sie, ob Ihr Texteditor der Datei nicht die Endung „.txt“ angehängt hat. Je nach Windows-Konfiguration kann es auch sein, dass die Anzeige dieser Endung unterdrückt wird, obwohl sie vorhanden ist.*

**i** *Es können auch mehrere verschiedene Konfigurationsdateien im Arbeitsverzeichnis vorhanden sein.*

3. Öffnen Sie diese Datei mit einem Texteditor.

## Konfiguration

### 4. Kopieren Sie die vorher erzeugte Beispielkonfiguration in diese Datei.

```
server.ovpn
1 # Dies ist eine Beispielkonfiguration für einen OpenVPN-Server.
2 # Text markieren und in die eigene Konfigurationsdatei kopieren (endet mit .ovpn).
3
4 # Noch anzupassende Parameter
5 remote 192.168.254.2 # IP-Adresse oder Domainname der Gegenstelle
6 ifconfig 10.1.0.1 10.1.0.2 # IP-Adresse des lokalen VPN Endpunkts, IP-Adresse des VPN Endpunkts der Gegenstelle
7 secret static.key # Datei mit dem geheimen Schlüssel bei PSK Authentifizierung (Pre Shared Key)
8 # Fixe Parameter
9 proto udp # Protokoll, das für den Tunnel benutzt wird
10 rport 1194 # Auf der Gegenstelle über diesen Port tunneln
11 lport 1194 # Lokal über diesen Port tunneln
12 comp-lzo # LZO Kompression aktivieren
13 cipher BF-CBC # Benutzter Verschlüsselungsalgorithmus
14 route 192.168.100.0 255.255.255.0 # Route in das Netzwerk hinter dem VPN-Tunnel
15 tun-mtu 1500 # Maximale Größe der Datenpakete
16 reneg-sec 3600 # Intervall bis zur Schlüsselerneuerung (in Sekunden)
17 ping 30 # Verbindungsprüfung nach Ablauf dieser Anzahl an Sekunden ohne Datenverkehr
18 ping-restart 60 # Verbindung erneut aufbauen, wenn nach Ablauf dieser Anzahl an Sekunden kein Ping
   von der Gegenstelle empfangen wurde
19 verb 3 # Ausführlichkeit der Log-Meldungen
20 dev tun # OpenVPN Netzwerkgerät
21 float # Akzeptiere Pakete von allen Rechnern (float)
22
23 # Alle Daten durch den VPN-Tunnel routen (zum Aktivieren # entfernen)
24 #redirect-gateway # Setze VPN-Tunnel als Standardroute
25 route-method exe # Stabile Windowsrouten
26 route-delay 2 # Routen nach Verzögerung setzen
```

### 5. Passen Sie den Dateinamen für den statischen Schlüssel entsprechend an (hier Zeile 7).

### 6. Passen Sie ggf. die Adresse der Gegenstelle an (hier Zeile 5).

**i** *Dies kann erforderlich sein, wenn diese IP-Adresse in einem verwendeten Adressbereich liegt. Diese IP-Adresse sollte immer in einem nicht verwendeten, privaten Adressbereich liegen. Auf diese Angabe darf nicht verzichtet werden.*

### 7. Entfernen Sie das Symbol „#“, um den Befehl „route-method exe“ zu aktivieren (hier Zeile 25).

### 8. Entfernen Sie das Symbol „#“, um den Befehl „route-delay 2“ zu aktivieren (hier Zeile 26).

✓ Damit haben Sie eine Konfigurationsdatei aus der Beispielkonfiguration erzeugt. Damit kann sich ein OpenVPN-Client am Server anmelden.

## Inbetriebnahme



Starten Sie nun den OpenVPN-Server, um zusammen mit den Clients ein OpenVPN-Netzwerk aufzubauen. Dazu sind folgende Schritte erforderlich:

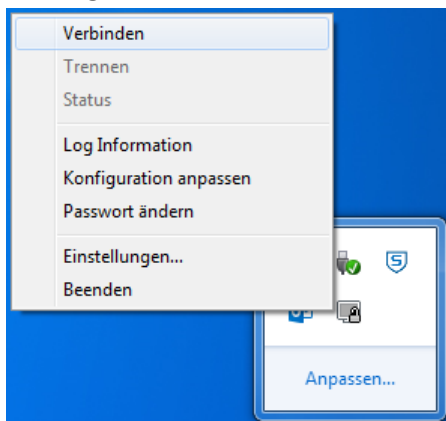
### ■ OpenVPN-Server starten

So starten Sie den OpenVPN-Server bei laufendem Rechner. Diese Option über die GUI ist geeignet zum Testen der Konfiguration. Die Option, den OpenVPN-Server automatisch mit dem Rechner zu starten, ist weiter unten beschrieben.

- Das OpenVPN-Paket ist auf dem Computer, der als Server fungieren soll, installiert.
- Sie haben den statischen Schlüssel im OpenVPN-Arbeitsverzeichnis abgelegt.
- Sie haben die Konfigurationsdatei an Ihre Anwendung angepasst.



1. Starten Sie die OpenVPN GUI über Start → Programme → OpenVPN → OpenVPN GUI oder das Desktop-Icon.
  - ❗ *Unter Windows 7 und Windows Vista muss die OpenVPN GUI explizit „als Administrator ausgeführt“ (über das Kontext-Menü) werden. Es ist nicht ausreichend als Administrator angemeldet zu sein, wenn die OpenVPN GUI gestartet wird.*
2. Klicken Sie ggf. auf das Symbol zum Einblenden der ausgeblendeten Symbole in der Task-Leiste .
3. Klicken Sie mit der rechten Maustaste auf das Symbol der OpenVPN GUI  und wählen Sie Verbinden (bzw. server → Connect (server bezeichnet hier Ihre Konfigurationsdatei; in unserem Beispiel server.ovpn)).



- ✓ Damit haben Sie den OpenVPN-Server gestartet. Das Symbol der OpenVPN GUI wird grün dargestellt. Der OpenVPN-Server ist nun bereit, Client-Verbindungen anzunehmen. Ein Log der Verbindungen kann über den Menüpunkt „View Log“ angezeigt werden.
  - ▶ *Zum automatischen Starten des OpenVPN-Servers mit dem Start des Rechners kann auch der entsprechende Dienst aktiviert werden.*
  - ❗ *In diesem Fall werden Instanzen für alle Konfigurationsdateien, die sich im Arbeitsverzeichnis des OpenVPN-Pakets befinden, gestartet. Löschen Sie daher alle nicht benötigten Konfigurationsdateien aus dem Verzeichnis.*
4. Öffnen Sie die Systemsteuerung über Start → Einstellungen → Systemsteuerung.
  5. Doppelklicken Sie im Abschnitt „Systemsteuerung“ den Eintrag „Verwaltung“.
  6. Doppelklicken Sie im Abschnitt „Verwaltung“ den Eintrag „Dienste“.
  7. Doppelklicken Sie im Abschnitt „Dienste“ den Eintrag „OpenVPNService“.
  8. Ändern Sie den „Starttyp“ auf „Automatisch“ und klicken Sie auf „OK“.
- ✓ Damit haben Sie den OpenVPN-Server für einen automatischen Start beim Hochfahren des Rechners konfiguriert.

### 3 Verwendete Komponenten

#### Software

| Bezeichnung    | Hersteller  | Typ             | Version |
|----------------|-------------|-----------------|---------|
| OpenVPN-Paket  | Open Source | OpenVPN mit GUI | 2.3.3   |
| Betriebssystem | Microsoft   | Windows         | 7       |

Tabelle 1: Verwendete Software

## 4 Weiterführende Informationen

### 4.1 Literatur

OpenVPN

Das Praxisbuch

ISBN: 978-3-8362-1197-0

Verlag: Galileo Computing

OpenVPN

Grundlagen, Konfiguration, Praxis

ISBN: 978-3-89864-396-2

Verlag: dpunkt.verlag

### 4.2 Weblinks

OpenVPN Technologies, Inc.:

<http://www.openvpn.net>

OpenVPN e.V.:

<http://www.openvpn.eu>

## **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](mailto:info@insys-icom.de)  
URL [www.insys-icom.de](http://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](mailto:info@insys-icom.cz)  
URL [www.insys-icom.cz](http://www.insys-icom.cz)