

VPN mit INSYS-Routern

OpenVPN-Server mit
zertifikatsbasierter
Authentifizierung 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
URL <http://www.insys-icom.de>

Druck 17. Jan. 2024
Artikel-Nr. -
Version 1.6
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 zertifikatsbasierter Authentifizierung für ein OpenVPN-Netzwerk mit INSYS Routern als Clients einrichten.

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

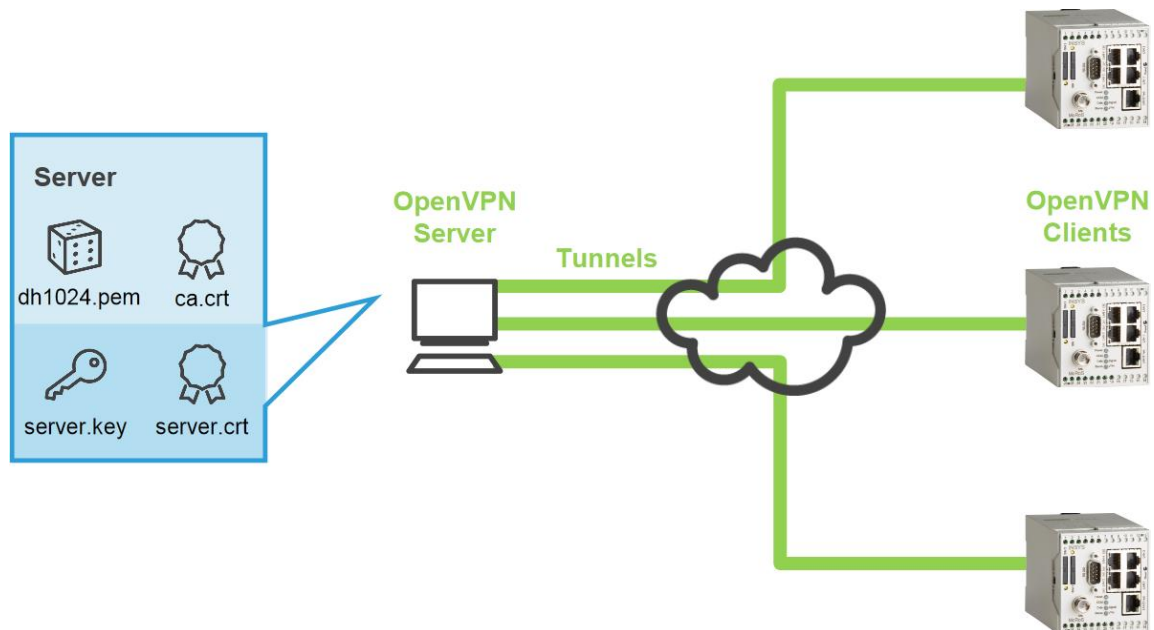


Abbildung 1: Windows-PC als OpenVPN-Server mit zertifikatsbasierter Authentifizierung

2 Konfiguration

Vorbereitungen

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

- OpenVPN-Paket herunterladen
- OpenVPN-Paket auf Windows-PC installieren
- Zertifikatsstruktur erzeugen
- INSYS-Router als OpenVPN-Client konfigurieren und Konfigurationsdatei anzeigen



■ OpenVPN-Paket herunterladen

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

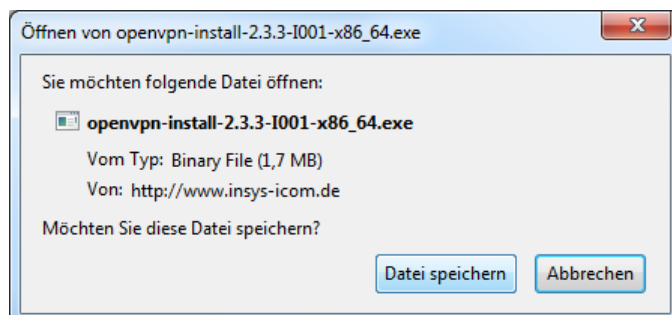
- PC mit ca. 1,5 MB freien Speicherplatz
- Webbrowser
- Internetverbindung

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	 OpenVPN 2.3.3 mit GUI (1,7 MB)
OpenVPN-Installationsdatei - Windows 64 Bit	 OpenVPN 2.3.3 mit GUI (1,7 MB)

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.

Konfiguration

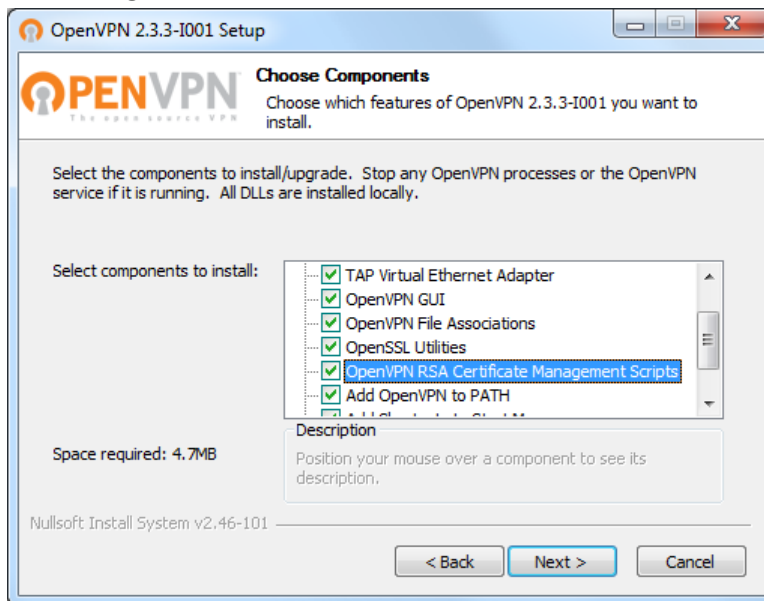
→ Sie haben das OpenVPN-Paket (Version 2.3.3 oder höher) von der INSYS Homepage www.insys-icom.de/treiber heruntergeladen.

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.

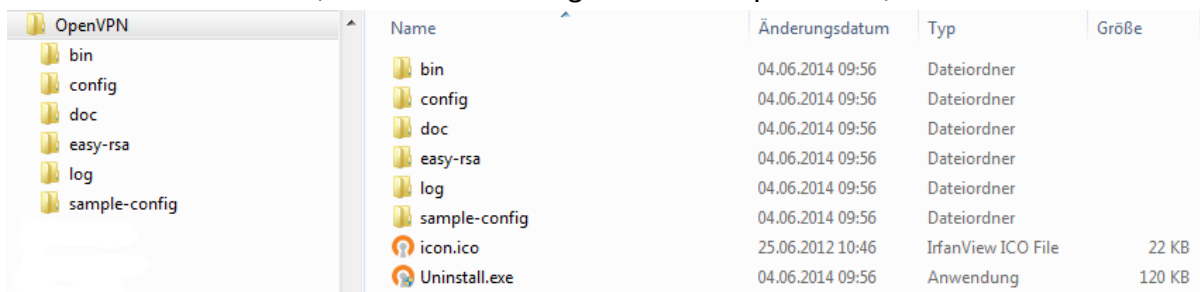


3. Markieren Sie die „OpenVPN RSA Certificate Management Scripts“, wählen Sie **Next >** und setzen Sie den Setup Wizard fort.

▶ 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\).



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

■ Zertifikatsstruktur erzeugen

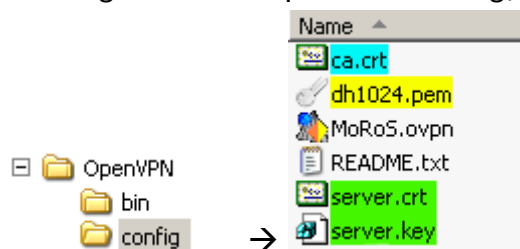
So erzeugen Sie eine Zertifikatsstruktur für Ihre Anwendung.

1. Erzeugen Sie eine Zertifikatsstruktur für Ihre Anwendung.

i Eine detaillierte Beschreibung dieses Vorgangs finden Sie in unseren Configuration Guides „X509.V3-Zertifikate für VPNs mit easy-rsa erzeugen“ bzw. „X509.V3-Zertifikate für VPNs mit XCA erzeugen“.

- ✓ Damit haben Sie eine Zertifikatsstruktur bestehend aus Zertifikaten und Schlüsseln für CA, Server und Clients, sowie einem Diffie-Hellman-Parametersatz erzeugt.

2. Kopieren Sie **Server-Schlüssel und -Zertifikat**, **CA-Zertifikat** und **Diffie-Hellman-Parametersatz** in das Arbeitsverzeichnis des OpenVPN-Pakets (Standard: C:\Program Files\OpenVPN\config).



- ▶ Falls Sie eine PKCS#12-Datei erhalten haben, die Zertifikate und Schlüssel enthält (z.B. „Server.p12“), enthält diese bereits sämtliche Dateien. Kopieren Sie in dem Fall nur diese Datei und den Diffie-Hellman-Parametersatz in obiges Verzeichnis.

- ✓ Damit verfügt der OpenVPN-Server über die erforderlichen Schlüssel und Zertifikate.

■ 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.

→ Sie haben eine Zertifikatsstruktur für Ihre Anwendung erzeugt.

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 zertifikatsbasierter Authentifizierung 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
server 10.1.0.0 255.255.255.0 # IP-Adresse oder Domainname der Gegenstelle
ca ca.crt # Datei mit dem Zertifikat der Certification Authority (CA)
key private.key # Privater (und geheimer) Schlüssel in Verbindung mit einem Zertifikat
cert certificate.crt # Datei mit dem Zertifikat
dh dh.pem # Datei mit den Diffie-Hellman-Parametern

# 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 # Benutzter Verschlüsselungsalgorithmus
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 Logmeldungen
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
```

3. Kopieren Sie den kompletten Text dieser Konfigurationsdatei in die Zwischenablage, um sie im nächsten 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.

Konfiguration

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

- Konfigurationsdatei aus Beispielkonfiguration erzeugen
- Konfigurationsdatei für Routing anpassen

■ 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.
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 server 10.1.0.0 255.255.255.0 # IP-Adressen-Pool des OpenVPN-Servers
6 ca ca.crt # Datei mit dem Zertifikat der Certification Authority (CA)
7 key server.key # Privater (und geheimer) Schlüssel in Verbindung mit einem Zertifikat
8 cert server.crt # Datei mit dem Zertifikat
9 dh dh1024.pem # Datei mit den Diffie-Hellman-Parametern
10
11 # Fixe Parameter
12 proto udp # Protokoll, das für den Tunnel benutzt wird
13 rport 1194 # Auf der Gegenstelle über diesen Port tunneln
14 lport 1194 # Lokal über diesen Port tunneln
15 comp-lzo # LZO Kompression aktivieren
16 cipher BF-CBC # Benutzer Verschlüsselungsalgorithmus
17 tun-mtu 1500 # Maximale Größe der Datenpakete
18 reneg-sec 3600 # Intervall bis zur Schlüsselerneuerung (in Sekunden)
19 ping 30 # Verbindungsprüfung nach Ablauf dieser Anzahl an Sekunden ohne Datenverkehr
20 ping-restart 60 # Verbindung erneut aufbauen, wenn nach Ablauf dieser Anzahl an Sekunden
    kein Ping von der Gegenstelle empfangen wurde
21 verb 9 # Ausführlichkeit der Logmeldungen
22 dev tun # OpenVPN Netzwerkgerät
23 float # Akzeptiere Pakete von allen Rechnern (float)
24
25 # Alle Daten durch den VPN-Tunnel routen (zum Aktivieren # entfernen)
26 #redirect-gateway # Setze VPN-Tunnel als Standardroute
27 route-method exe # Stabile Windowsrouten
28 #route-delay 2 # Routen nach Verzögerung setzen

```

5. Passen Sie die Dateinamen für CA-Zertifikat, Server-Zertifikat und -Schlüssel und Diffie-Hellman-Parameter entsprechend den zuvor erzeugten Dateien an (hier Zeilen 6 bis 9).
 - ▶ Falls Sie eine PKCS#12-Datei erhalten haben, die Zertifikate und Schlüssel enthält (z.B. „Server.p12“), enthält diese bereits sämtliche Dateien. Löschen Sie in diesem Fall die Zeilen 6 bis 8 und fügen Sie stattdessen eine Zeile für diese Datei ein (z.B. „pkcs12 server.p12“).
6. Passen Sie ggf. den Adresspool für das interne VPN-Routing an, wenn bereits benutzte Netzwerke in diesem Bereich liegen (hier Zeile 5).
7. Entfernen Sie das Symbol „#“, um den Befehl „route-method exe“ zu aktivieren (hier Zeile 27).
8. Entfernen Sie das Symbol „#“, um den Befehl „route-delay 2“ zu aktivieren (hier Zeile 28).
 - ✓ Damit haben Sie eine Konfigurationsdatei aus der Beispielkonfiguration erzeugt. Damit kann sich ein OpenVPN-Client am Server anmelden. Das korrekte Routing muss aber noch angepasst werden.

■ Konfigurationsdatei für Routing anpassen

So passen Sie die Konfigurationsdatei für den OpenVPN-Server an Ihre Anwendung an.

- Das OpenVPN-Paket ist auf dem Computer, der als Server fungieren soll, installiert.
- Sie haben eine Konfigurationsdatei für den OpenVPN-Server erstellt und im Texteditor geöffnet.

1. Fügen Sie für das Routing ins Server-Netzwerk am Ende der Konfigurationsdatei neue Zeilen mit dem Befehl **push** hinzu, mit dem die Routen vom Server zum Client „gepusht“ werden. Der Server-IP-Adressbereich muss damit jedem Client mitgeteilt werden.

```
29 # Route für die Clients anlegen
30 # Server-Netzwerk
31 push "route 192.168.200.0 255.255.255.0"
```

2. Legen Sie das Verzeichnis fest, in dem sich die Dateien für das Routing ins Client-Netzwerk befinden, welche die IP-Adressbereiche hinter den jeweiligen Clients definieren (z.B. Verzeichnis „ccd“).

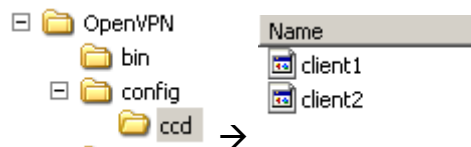
```
33 # Routen für die Clients festlegen
34 client-config-dir ccd
```

i Damit der Server zum richtigen Client routen kann, wird hier die Verknüpfung von IP-Adressbereich und „common name“ hergestellt.

3. Legen Sie ein Verzeichnis mit genau demselben Namen wie oben festgelegt unter dem Arbeitsverzeichnis des OpenVPN-Pakets an (z.B. C:\Program Files\OpenVPN\config\ccd).

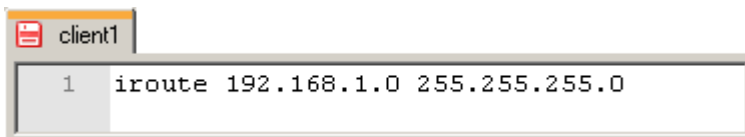


4. Erstellen Sie in diesem Verzeichnis für jeden Client eine Textdatei, welche den IP-Adressbereich hinter dem Client definiert. Der Dateiname dieser Textdatei muss identisch mit dem „common name“ des Clients sein und darf keine Dateiendung haben.



ⓘ *Beachten Sie dabei die Groß- und Kleinschreibung!*

5. Tragen Sie den Befehl **iroute** mit Angabe des entsprechenden IP-Adressbereichs in jede Datei ein.



ⓘ *In diese Textdatei kommt nur eine einzige Zeile!*

6. Fügen Sie am Ende der Konfigurationsdatei neue Zeilen mit dem Befehl **route** hinzu, um dem Betriebssystem die IP-Adressbereiche mitzuteilen, welche durch den/die Tunnel geroutet werden sollen (im folgenden Beispiel wird von 2 Clients ausgegangen).

```
36 # Windows-Routen hinzufügen
37 route 192.168.1.0 255.255.255.0
38 route 192.168.2.0 255.255.255.0
```

▶ *Wenn auch Client-to-Client-Verbindungen zugelassen werden sollen, müssen noch folgende Schritte durchgeführt werden.*

7. Fügen Sie eine neue Zeile mit dem Befehl **client-to-client** hinzu, um Verbindungen zwischen den einzelnen Clients zuzulassen.

```
40 # Verbindungen von Client zu Client zulassen
41 client-to-client # Befehl für Client zu Client
```

8. Wenn Sie alle Clients gleich behandeln wollen, d.h. jeder Client darf mit jedem Client kommunizieren, fügen Sie am Ende der Konfigurationsdatei neue Zeilen mit dem Befehl **push** hinzu. Damit werden jedem Client alle Client-Adressbereiche (außer dem eigenen) mitgeteilt, so dass wieder eine direkte Kommunikation möglich ist.

```
42 # Client-Netzwerke (1 Eintrag je Client)
43 push "route 192.168.1.0 255.255.255.0"
44 push "route 192.168.2.0 255.255.255.0"
```

▶ *Wenn aus Sicherheitsgründen nur bestimmte Clients mit bestimmten Clients kommunizieren dürfen, dürfen obige **push**-Befehle nicht in die Server-Konfigurationsdatei eingetragen werden. In diesem Fall muss in der Textdatei (im Unterverzeichnis „ccd“) des Clients, der kommunizieren darf,*

Konfiguration

der **push**-Befehl nach dem Befehl **iroute** eingefügt werden. Für jeden von diesem Client aus erreichbaren Client muss eine Zeile eingefügt werden.

9. Speichern Sie die geänderte Konfigurationsdatei ab.

- ✓ Damit haben Sie die Konfigurationsdatei an Ihre Anwendung angepasst.

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.

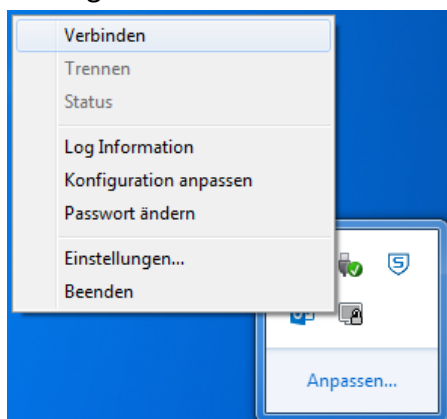
- Das OpenVPN-Paket ist auf dem Computer, der als Server fungieren soll, installiert.
- Sie haben Server-Zertifikat und –Schlüssel, CA-Zertifikat und Diffie-Hellman-Parametersatz im OpenVPN-Arbeitsverzeichnis abgelegt.
- Sie haben die Konfigurationsdatei an Ihre Anwendung angepasst.

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.*

1. Öffnen Sie die Systemsteuerung über Start → Einstellungen → Systemsteuerung.
2. Doppelklicken Sie im Abschnitt „Systemsteuerung“ den Eintrag „Verwaltung“.
3. Doppelklicken Sie im Abschnitt „Verwaltung“ den Eintrag „Dienste“.
4. Doppelklicken Sie im Abschnitt „Dienste“ den Eintrag „OpenVPNService“.
5. 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
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