

VPN mit INSYS-Routern

OpenVPN-Client 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-Client mit zertifikatsbasierter Authentifizierung einrichten können.

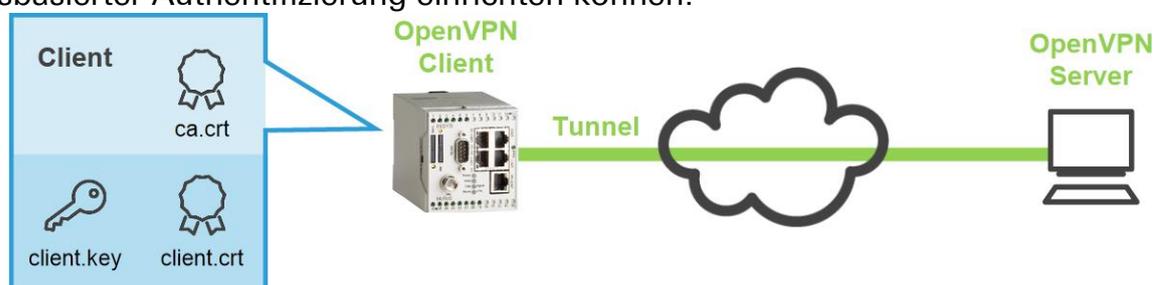


Abbildung 1: OpenVPN-Client mit zertifikatsbasierter Authentifizierung konfigurieren

2 Kurzfassung

OpenVPN-Client-Konfiguration

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

1. Im Menü → Dial-In / Dial-Out / LAN (ext) / WWAN die Seite → OpenVPN-Client öffnen
2. CA-Zertifikat hochladen
3. Client-Zertifikat hochladen
4. Client-Schlüssel hochladen
5. „OpenVPN-Client aktivieren“ markieren
6. „IP-Adresse oder Domainname der Gegenstelle“ eingeben
7. „Authentifizierung mit Zertifikaten“ markieren
8. Ggf. „Zertifikat der Gegenstelle prüfen“ markieren
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.

■ Client-Zertifikate und -Schlüssel hochladen

So laden Sie die Zertifikate und Schlüssel für einen OpenVPN-Client 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 Client-Zertifikat, z.B. „client.crt“

geheimer Client-Schlüssel, z.B. „client.key“

▶ *Falls Sie eine PKCS#12-Datei erhalten haben, die Zertifikate und Schlüssel enthält (z.B. „Client_1.p12“), enthält diese bereits sämtliche Dateien.*

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

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 → Authentifizierung mit Zertifikaten.

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-Clients (z.B. „client.crt“) und dem geheimen Schlüssel des OpenVPN-Clients (z.B. „client.key“), um die beiden Dateien auf den INSYS-Router zu laden.

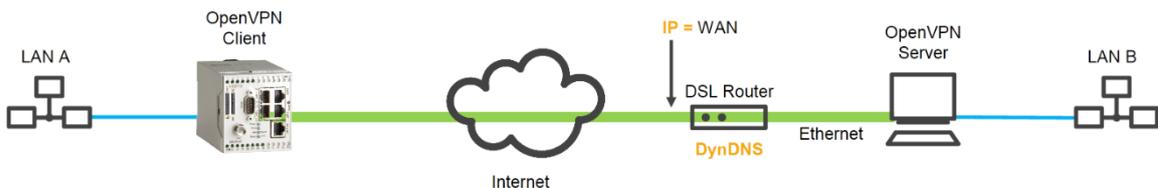
✓ Für jede hochgeladene Datei erscheint ein grüner Haken anstatt eines roten Kreuzes. Das Hochladen der Zertifikate und Schlüssel ist damit abgeschlossen.

■ Verbindungsdaten zur Gegenstelle und zertifikatsbasierte Authentifizierung konfigurieren

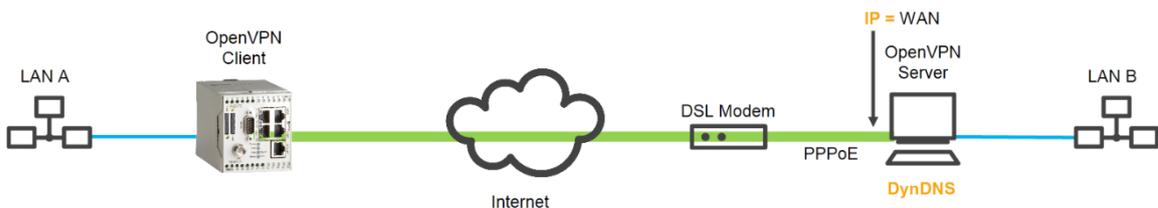
So konfigurieren Sie die Verbindungsdaten zur Gegenstelle für den Verbindungsaufbau des VPN-Clients und die Authentifizierung mit Zertifikaten.

→ Sie müssen die über das Internet erreichbare IP-Adresse oder den Domain-Namen der Gegenstelle wissen.

i Diese IP-Adresse hängt von der Architektur des Server-Netzwerks ab. Befindet sich beispielsweise der Server wie in der folgenden Abbildung hinter einem DSL-Router, muss dessen WAN-IP-Adresse verwendet werden. Im DSL-Router muss eine entsprechende Port-Weiterleitung des Tunnels an den Server eingerichtet sein.



i Befindet sich der Server wie in der folgenden Abbildung direkt an einem DSL-Modem ohne dazwischen liegenden Router, muss die IP-Adresse des Servers verwendet werden.



i Hat der Server keine feste IP-Adresse, kann auch ein DynDNS-Domain-Name eingegeben werden, der dann vom Client aufgelöst wird. Dazu muss dann im DSL-Router (erstes Beispiel) bzw. im Server (zweites Beispiel) DynDNS aktiviert werden. Hinweise dazu finden Sie in der Dokumentation des jeweiligen Geräts. Im INSYS-Router muss dazu auch ein DNS-Server eingetragen sein.

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

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-Client aktivieren“.
- Tragen Sie die im Internet erreichbare IP-Adresse oder den Domain-Namen des OpenVPN-Servers bei „IP-Adresse oder Domainname der Gegenstelle“ ein.

OpenVPN-Client aktivieren

[↩ OpenVPN-Client Status](#)
[↩ Verbindungs-Log der letzten Verbindung](#)
[↩ Konfigurationsdatei anzeigen](#)
[↩ Beispielkonfigurationsdatei für die Gegenstelle erstellen](#)

IP-Adresse oder Domainname der Gegenstelle
 Alternative Gegenstelle
 Tunneln über Port (lokal / Gegenstelle)
 Protokoll UDP TCP
 IP-Adresse oder Domainname des Proxy-Servers
 HTTP SOCKS5
 Port
 Benutzername
 Kennwort

Default-Route setzen (redirect-gateway)
 Lokale Adresse und Port fixieren (nobind)
 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)
 Zusätzlicher ICMP-Ping an

5. Konfigurieren Sie die weiteren OpenVPN-Parameter gemäß der Konfiguration Ihres Servers.

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.

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

Authentifizierung mit Zertifikaten

✓ CA-Zertifikat vorhanden  

✓ Zertifikat vorhanden  

✓ Privater Schlüssel vorhanden 

Benutzername

Kennwort

Zertifikatstyp der Gegenstelle überprüfen

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

8. Markieren Sie ggf. die Checkbox „Zertifikat der Gegenstelle prüfen“.

i *Client prüft Serverzertifikat auf Zertifizierung durch die gemeinsame Zertifizierungsstelle (CA-Zertifikat). Dies ist nicht unbedingt erforderlich und abhängig vom Server.*

▶ *Zusätzlich zur Authentifizierung mit Zertifikaten kann der Server auch noch die Authentifizierung mit Benutzername/Kennwort erfordern.*

9. Klicken Sie zum Speichern bei „Einstellungen übernehmen“ auf **OK**.

Einstellungen übernehmen

✓ Die Gegenstelle für den Verbindungsaufbau des VPN-Clients 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