

VPN mit INSYS-Routern

OpenVPN-Client mit
Authentifizierung über
statischen Schlüssel
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 1.3
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

Im Folgenden wird erklärt, wie Sie den INSYS-Router als OpenVPN-Client für eine Authentifizierung mit statischem Schlüssel einrichten können. Dies ist für Anwendungen sinnvoll, bei denen sich nur jeweils zwei Geräte zu einem Zeitpunkt miteinander verbinden.

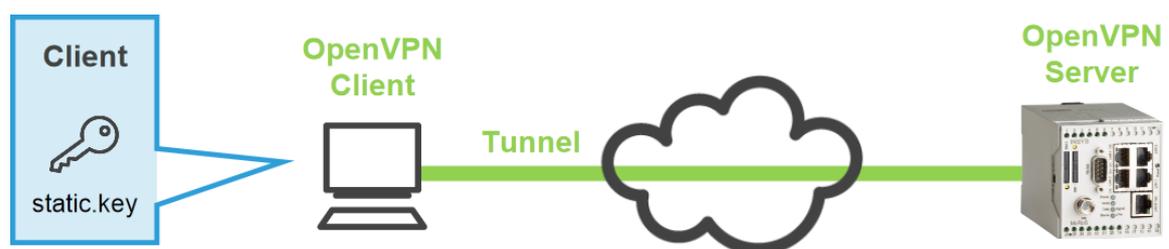


Abbildung 1: OpenVPN-Client für Authentifizierung mit statischem Schlüssel konfigurieren

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. Statischen Schlüssel hochladen
3. „OpenVPN-Client aktivieren“ markieren
4. „IP-Adresse oder Domainname der Gegenstelle“ eingeben
5. „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“ markieren
6. Lokale und entfernte IP-Adresse des VPN-Tunnels eingeben
7. Ggf. „Netzwerkadresse des Netzwerks hinter dem VPN-Tunnel“ und „Netzmaske des Netzwerks hinter dem VPN-Tunnel“ eingeben
8. 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.

■ Statischen Schlüssel hochladen

So laden Sie den statischen 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 ist folgende Datei erforderlich, die Sie vorher erstellt haben („Statischen Schlüssel neu erstellen“) oder Ihnen vom Administrator des Servers zur Verfügung gestellt wurde:
statischer Schlüssel, z.B. „static.key“

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

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 → Schlüssel oder Zertifikate laden.

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

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

Schlüssel oder Zertifikate laden

Keine Datei ausgewählt.

Kennwort (nur bei verschlüsselter Datei)

4. Wählen Sie die Datei mit dem statischen Schlüssel aus (z.B. „static.key“).

5. Klicken Sie zum Hochladen der Datei auf **OK**.

✓ Anstelle des roten „X“ bei „... statischer Schlüssel vorhanden“ wird ein grüner Haken eingeblendet.

✓ Statischer Schlüssel vorhanden  

Konfiguration

► Über den Link „Statischen Schlüssel neu erstellen“ können Sie auch einen neuen statischen Schlüssel im INSYS-Router erstellen. Über den Download-Link (blauer Pfeil) kann dieser auch heruntergeladen und auf den Server geladen werden.

❗ Wenn Sie keinen statischen Schlüssel hochladen, wird keine Authentifizierung verwendet. Dies wird nicht empfohlen und ist nur für Testzwecke sinnvoll, weil ohne Authentifizierung auch keine Verschlüsselung der durch den Tunnel gesendeten Daten erfolgt.

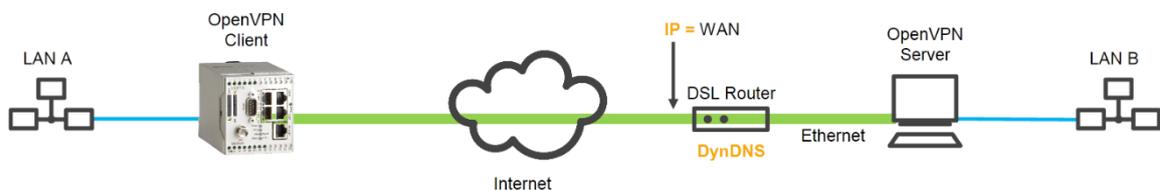
✓ Das Hochladen des statischen Schlüssels ist damit abgeschlossen.

■ Verbindungsdaten zur Gegenstelle und Authentifizierung mit statischem Schlüssel konfigurieren

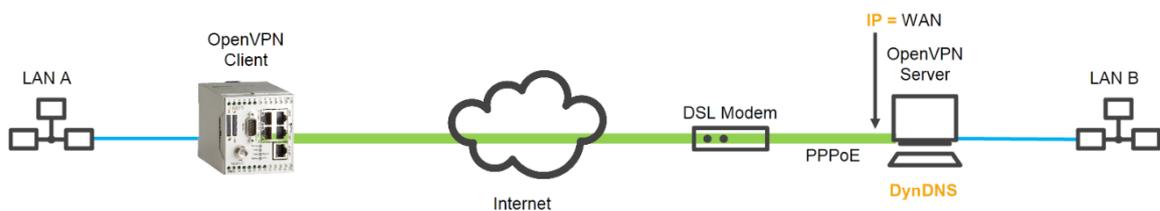
So konfigurieren Sie die Verbindungsdaten zur Gegenstelle für den Verbindungsaufbau des VPN-Clients und die Authentifizierung mit statischem Schlüssel.

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

❗ Diese IP-Adresse hängt von der Architektur des Server-Netzwerks ab. Beinhaltet 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.



❗ 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.



❗ 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.

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

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

3. Markieren Sie die Checkbox „OpenVPN-Client aktivieren“.

4. 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 Status](#)
[Verbindungslog 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

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 OpenVPN-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 → Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel.

Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel

Statischer Schlüssel vorhanden [↩](#) [✖](#)
 Statischen Schlüssel neu erstellen

IP-Adresse des VPN-Tunnels lokal

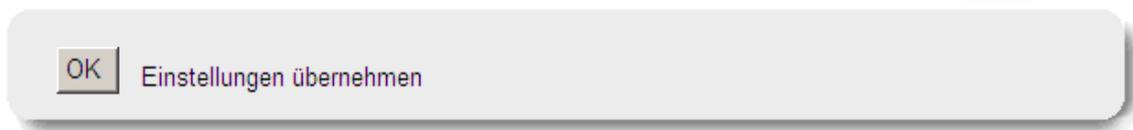
IP-Adresse des VPN-Tunnels der Gegenstelle

Netzwerkadresse des Netzwerks hinter dem VPN-Tunnel

Netzmaske des Netzwerks hinter dem VPN-Tunnel

Konfiguration

7. Markieren Sie die Option „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“.
8. Geben Sie die IP-Adresse des lokalen Tunnelendes in das Feld „IP-Adresse des VPN-Tunnels lokal“ und die IP-Adresse des entfernten Tunnelendes in das Feld „IP-Adresse des VPN-Tunnels der Gegenstelle“ ein.
 - ❗ *Diese IP-Adressen müssen an der VPN-Gegenstelle des Servers „spiegelverkehrt“ eingetragen sein, d.h. die Adresse, die am Server das lokale Tunnelende darstellt, ist am Client das entfernte Tunnelende, und umgekehrt. In den meisten Fällen können hier die Standardeinstellungen verwendet werden.*
9. Geben Sie gegebenenfalls die Netzwerkadresse des Netzwerks, zu dem der VPN-Tunnel aufgebaut werden soll, in das Feld „Netzwerkadresse des Netzwerks hinter dem VPN-Tunnel“ und die Netzmaske dieses Netzwerks in das Feld „Netzmaske des Netzwerks hinter dem VPN-Tunnel“ ein.
 - ❗ *Dies ist nur dann erforderlich, wenn die IP-Adressen in einem Netzwerk sind, das entweder lokal oder an der Gegenstelle bereits benutzt wird. Die IP-Adresse eines Netzes ist in diesem Fall eine Adresse, die mit „0“ endet, z.B. 192.168.200.0. Die Netzmaske ist in diesem Fall 255.255.255.0.*
10. Klicken Sie zum Speichern bei „Einstellungen übernehmen“ auf OK.



- ✓ Die Gegenstelle für den Verbindungsaufbau des OpenVPN-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