Konfigurations-Handbuch

INSYS icom

Industrielle Datenkommunikation

VPN mit INSYS-Routern

OpenVPN-Server 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	1.4
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 Authentifizierung über statischen Schlüssel einrichten können.

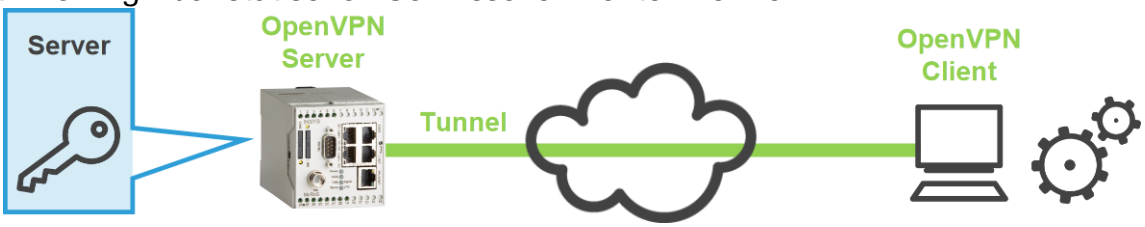


Abbildung 1: OpenVPN-Server mit Authentifizierung über statischen Schlüssel konfigurieren

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. „OpenVPN-Server aktivieren“ markieren
3. Einstellungen speichern
4. „Statischen Schlüssel neu erstellen“
5. „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“ markieren
6. Statischen Schlüssel herunterladen
7. „IP-Adresse oder Domainname der Gegenstelle“ eintragen
8. Lokale und entfernte IP-Adresse des VPN-Tunnels eingeben
9. Ggf. „Netzwerkadresse des Netzwerks hinter dem VPN-Tunnel“ und „Netzmaske des Netzwerks hinter dem VPN-Tunnel“ eingeben
10. 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.

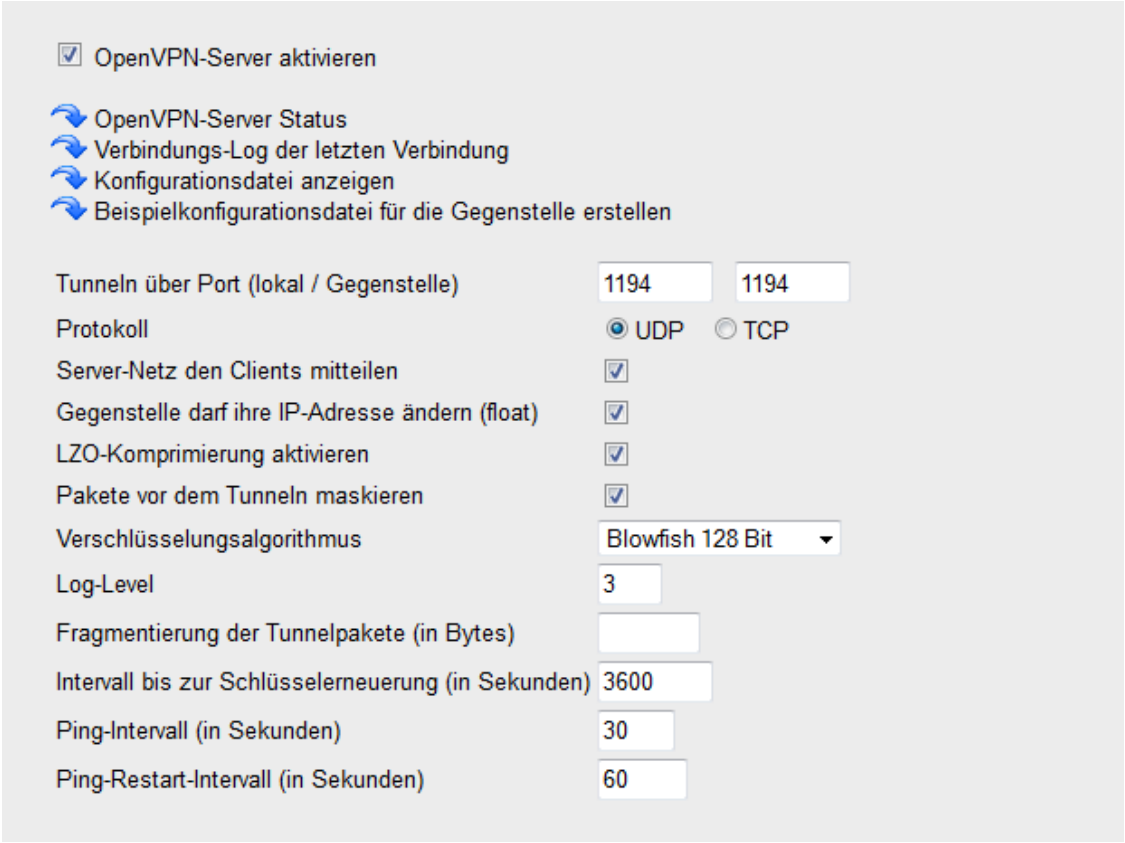
■ OpenVPN-Server konfigurieren

So konfigurieren Sie die Verbindungsdaten zur Gegenstelle für den Verbindungsaufbau des OpenVPN-Servers.

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

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

2. Markieren Sie die Checkbox „OpenVPN-Server aktivieren".

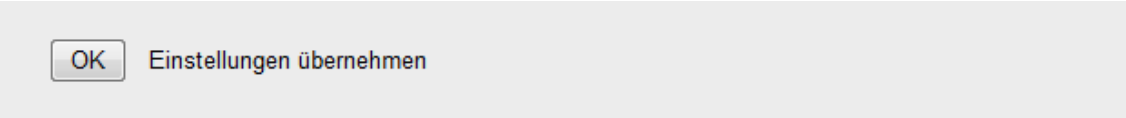


3. Konfigurieren Sie die weiteren OpenVPN-Parameter gemäß Ihrer Anwendung.

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

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



✓ Die Verbindungsdaten zur Gegenstelle für den Verbindungsaufbau des OpenVPN-Servers sind damit konfiguriert.

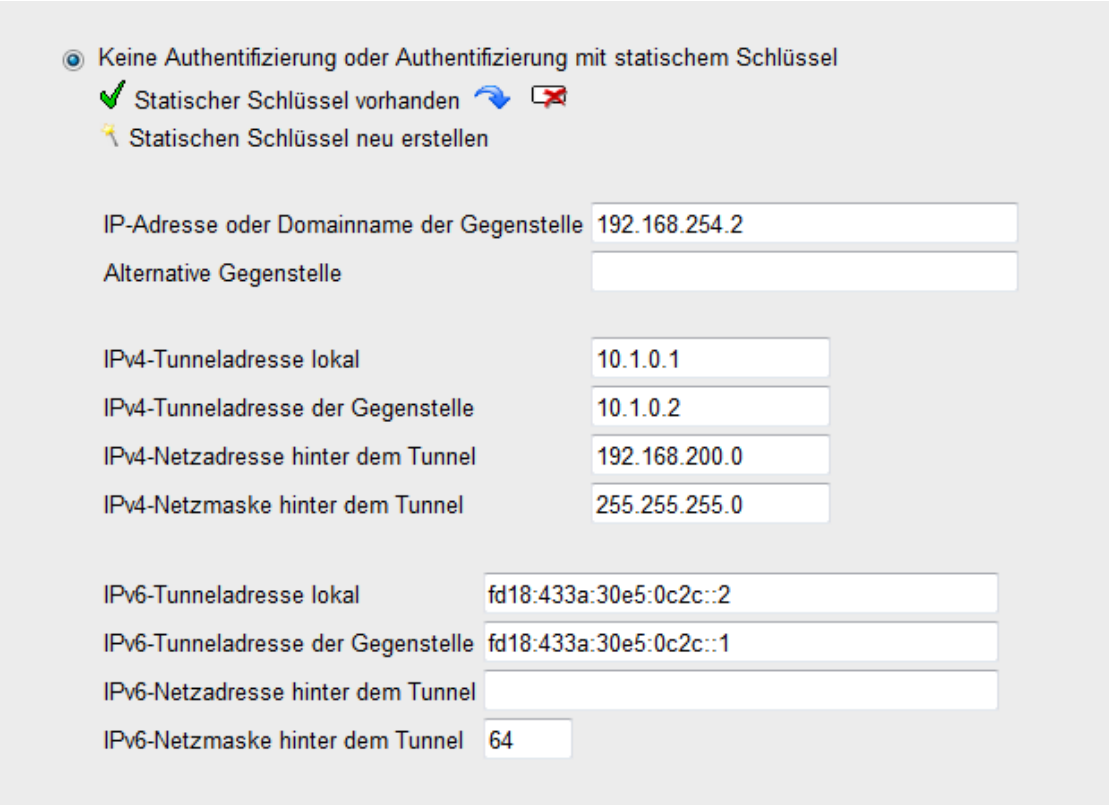
■ Authentifizierung mit statischem Schlüssel konfigurieren

So konfigurieren Sie die Authentifizierung mit statischem Schlüssel für einen OpenVPN-Server und erstellen den Schlüssel für den OpenVPN-Client.

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

ⓘ *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 → Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel.



3. Klicken Sie auf den Link „Statischen Schlüssel neu erstellen“.

✓ Ein neuer statischer Schlüssel wird erstellt und anstelle des roten „X“ bei „Kein statischer Schlüssel vorhanden“ wird ein grüner Haken eingeblendet.

ⓘ *Wenn kein statischer Schlüssel vorhanden ist, 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.*

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

4. Klicken Sie auf den blauen Pfeil hinter „Statischer Schlüssel vorhanden“ zum Herunterladen des erzeugten statischen Schlüssels und speichern Sie diesen.

   ⓘ *Dieser statische Schlüssel muss auch auf den Client hochgeladen werden, um eine Verbindung zu ermöglichen.*

   ▶ *Sie können auch einen bereits vorhandenen statischen Schlüssel verwenden, indem Sie diesen im Abschnitt „Schlüssel und Zertifikate laden“ hochladen. Derselbe Schlüssel muss auch auf dem Client vorhanden sein.*

5. Markieren Sie die Option „Keine Authentifizierung oder Authentifizierung mit statischem Schlüssel“.
6. Passen Sie ggf. die Daten des OpenVPN-Clients bei „IP-Adresse oder Domainname der Gegenstelle“ ein.

   ⓘ *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.*

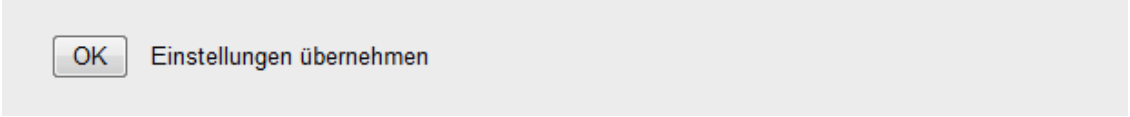
7. Geben Sie die IP-Adresse des lokalen Tunnelendes in das Feld „IP-Adresse des VPN-Tunnels lokal“ und die IP-Adresse des entfernten Tunnel-Endes in das Feld „IP-Adresse des VPN-Tunnels der Gegenstelle“ ein.

   ⓘ *Diese IP-Adressen müssen an der VPN-Gegenstelle des Clients „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.*

8. 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.*

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



✓ Die Authentifizierung über statischen Schlüssel 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 Repulic

INSYS icom CZ, s.r.o.
Slovanská alej 1993 / 28a
326 00 Plzen-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