Konfigurations-Handbuch

INSYS icom

Industrielle Datenkommunikation

VPN mit INSYS-Routern

IPsec-Teilnehmer mit zertifikatsbasierter Authentifizierung konfigurieren

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	11. 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 IPsec-Teilnehmer mit zertifikatsbasierter Authentifizierung einrichten können.

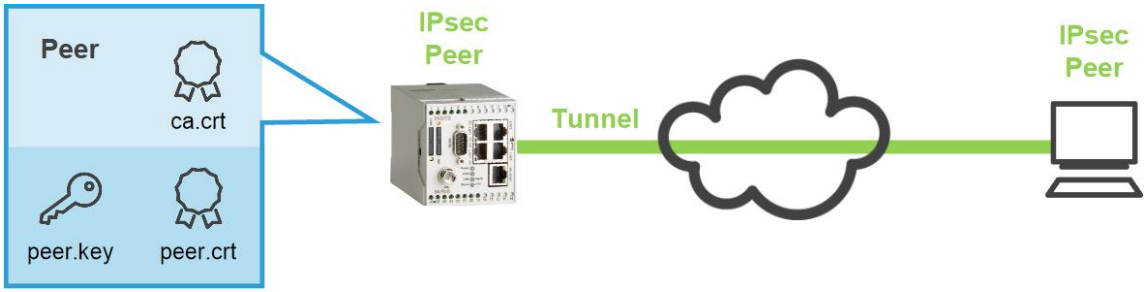


Abbildung 1: IPsec-Teilnehmer mit zertifikatsbasierter Authentifizierung konfigurieren

2 Kurzfassung

IPsec-Teilnehmer-Konfiguration

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

1. Im Menü → Dial-In / Dial-Out / LAN (ext) / WWAN die Seite → IPsec öffnen
2. CA-Zertifikat hochladen
3. Client-Zertifikat hochladen
4. Client-Schlüssel hochladen
5. „IPsec aktivieren“ markieren
6. „IP-Adresse oder Domainname der Gegenstelle“ eingeben
7. „Lokales Subnetz der Gegenstelle“ eingeben
8. DN der Gegenstelle bei „ID der Gegenstelle“ eingeben
9. „Main-Mode“ als „Authentifizierungs-Modus“ auswählen
10. „Authentifizierung mit Zertifikaten“ markieren
11. 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.

- **Zertifikate und Schlüssel hochladen**

So laden Sie die Zertifikate und Schlüssel hoch.

ⓘ *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 separater Configuration Guide) oder Ihnen zur Verfügung gestellt wurden:
öffentliches CA-Zertifikat, z.B. „ca.crt“
öffentliches Teilnehmer-Zertifikat, z.B. „peer.crt“
geheimer Teilnehmer-Schlüssel, z.B. „peer.key“

▶ *Falls Sie eine Datei erhalten haben, die Zertifikat und Schlüssel enthält (z.B. „peer.p12“), ersetzt diese die beiden Dateien für das Teilnehmer-Zertifikat und den Teilnehmer-Schlüssel. Ein Passwortschutz darf dabei jedoch nicht angewendet werden.*

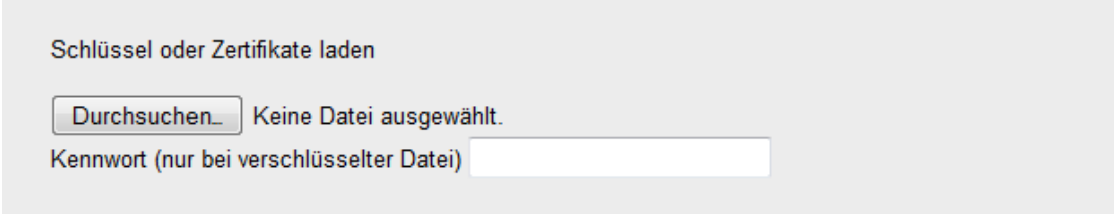
1. Wählen Sie im Menü die Seite → IPsec.

   ⓘ *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.

   ⓘ *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.



4. Wählen Sie die Datei mit dem CA-Zertifikat aus (z.B. „ca.crt“).
5. Klicken Sie zum Hochladen der Datei auf OK.

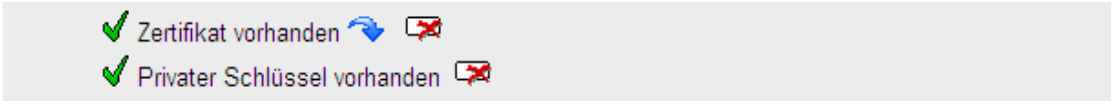
✓ Anstelle des roten „X“ bei „.. CA-Zertifikat …“ wird ein grüner Haken eingeblendet.

6. Klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf Durchsuchen.
7. Wählen Sie die Datei mit dem öffentlichen Zertifikat des Teilnehmers aus (z.B. „peer.crt“).
8. Klicken Sie zum Hochladen der Datei auf OK.

✓ Anstelle des roten „X“ bei „… Zertifikat …“ wird ein grüner Haken eingeblendet.

9. Klicken Sie im Abschnitt „Schlüssel oder Zertifikate laden“ auf Durchsuchen.
10. Wählen Sie die Datei mit dem geheimen Schlüssel des Teilnehmers aus (z.B. „peer.key“).
11. Klicken Sie zum Hochladen der Datei auf OK.

✓ Anstelle des roten „X“ bei „… Privater Schlüssel …“ wird ein grüner Haken eingeblendet.



✓ Das Hochladen der Zertifikate und Schlüssel ist damit abgeschlossen.

■ IPsec-Verbindung mit zertifikatsbasierter Authentifizierung konfigurieren

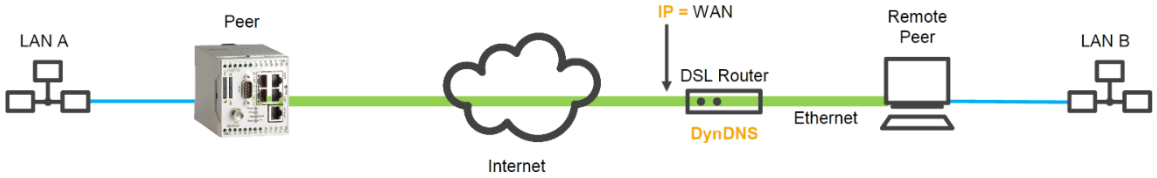
So konfigurieren Sie die IPsec-Verbindung zur Gegenstelle und die Authentifizierung mit Zertifikaten für einen IPsec-Teilnehmer.

→ Sie müssen den DN (Distinguished Name) der Gegenstelle wissen.

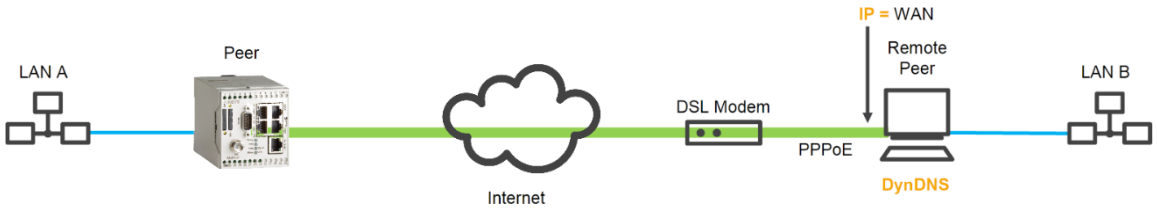
ⓘ *Der DN der Gegenstelle kann aus dem Zertifikat der Gegenstelle ausgelesen werden.*

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

ⓘ *Diese IP-Adresse hängt von der Architektur des Gegenstellen-Netzwerks ab. Befindet sich beispielsweise die Gegenstelle 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 die Gegenstelle eingerichtet sein.*



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



ⓘ *Hat die Gegenstelle keine feste IP-Adresse, kann auch ein DynDNS-Domain-Name eingegeben werden, der dann vom INSYS-Router aufgelöst wird. Dazu muss dann im DSL-Router (erstes Beispiel) bzw. in der Gegenstelle (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 → IPsec.

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

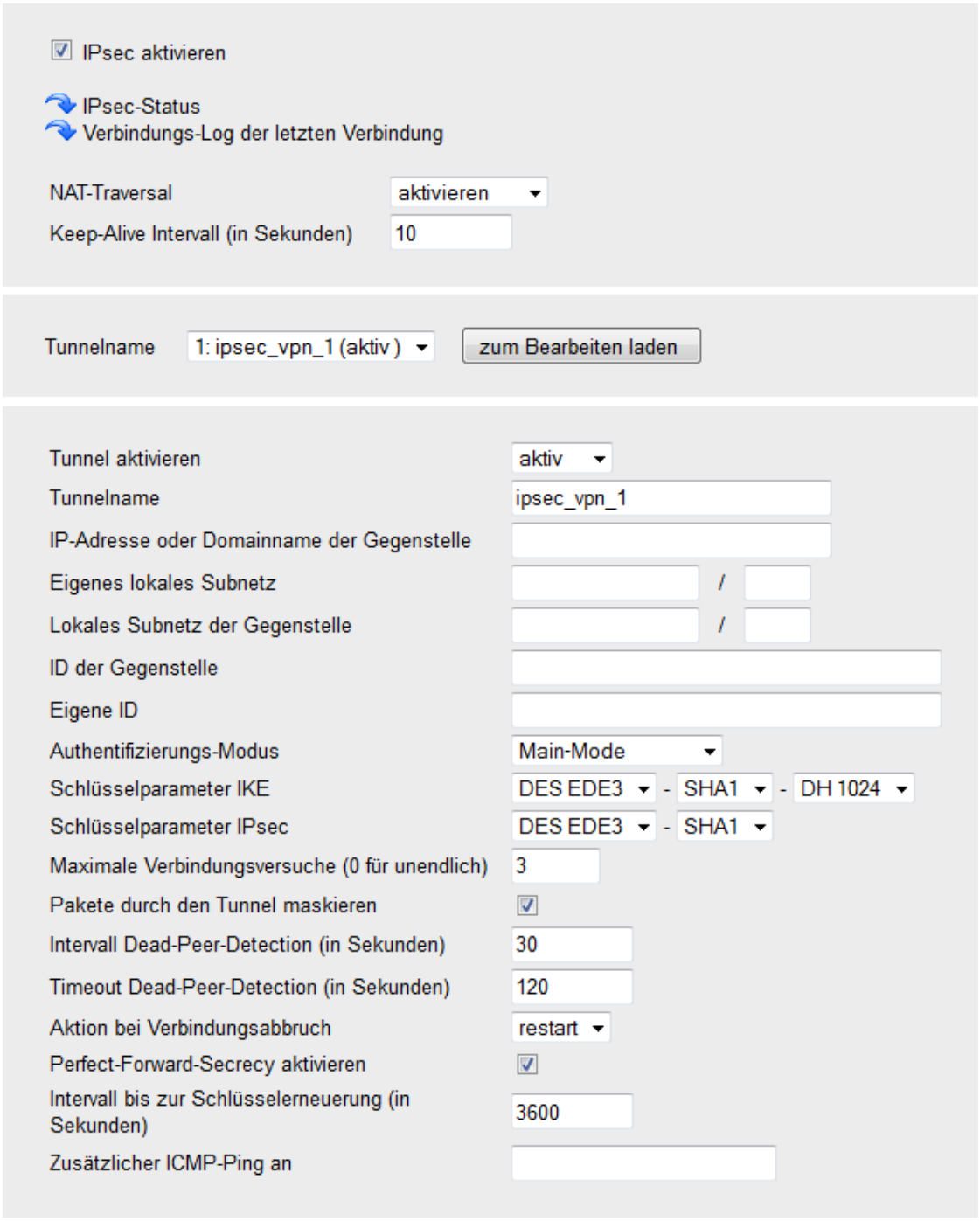
3. Markieren Sie die Checkbox „IPsec aktivieren“.
4. Tragen Sie die im Internet erreichbare IP-Adresse oder den Domain-Namen der Gegenstelle in das Feld „IP-Adresse oder Domainname der Gegenstelle“ ein.

   ⓘ *Wenn Sie hier keine Eintragung vornehmen, kann der IPsec-Teilnehmer keine Verbindung zur Gegenstelle aufbauen, sondern nur annehmen.*

5. Tragen Sie das lokale Subnetz der Gegenstelle in das Feld „Lokales Subnetz der Gegenstelle“ ein.
6. Tragen Sie den DN (Distinguished Name) der Gegenstelle bei „ID der Gegenstelle“ ein.

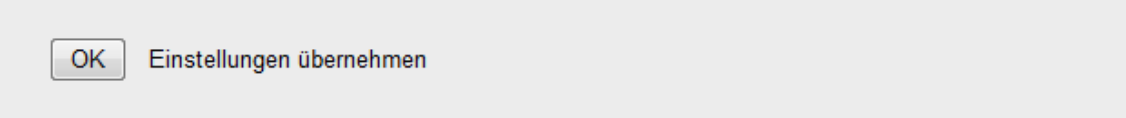
   ⓘ *Je nach Gegenstelle kann es auch erforderlich sein, hier eine andere ID einzutragen.*

7. Wählen Sie „Main-Mode“ als „Authentifizierungs-Modus“.



8. Konfigurieren Sie die weiteren IPsec-Parameter gemäß den Anforderungen Ihrer Verbindung oder der Konfiguration der Gegenstelle.
9. Scrollen Sie nach unten zu → Authentifizierung mit Zertifikaten.
10. Markieren Sie die Option „Authentifizierung mit Zertifikaten“.

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



✓ Die IPsec-Verbindung zur Gegenstelle 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