Konfigurations-Handbuch

INSYS icom

Industrielle Datenkommunikation

VPN mit INSYS-Routern

IPsec-Teilnehmer mit Authentifizierung durch Passphrase für Scalance konfigurieren

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	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 Authentifizierung durch eine Passphrase für eine Verbindung mit einem SIEMENS Scalance S Security Module einrichten können.

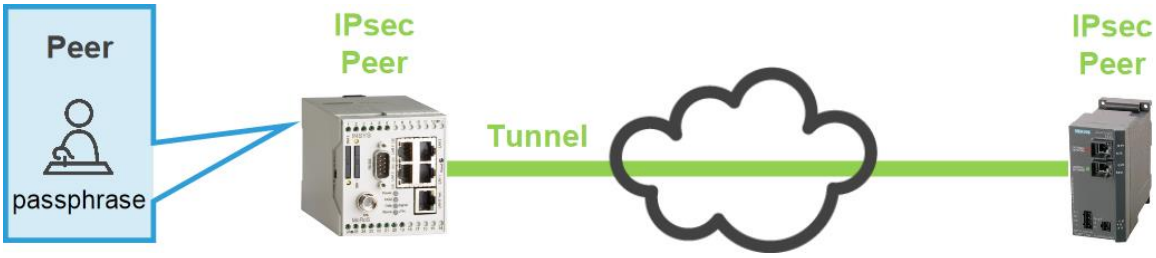


Abbildung 1: IPsec-Teilnehmer mit Authentifizierung durch Passphrase für SIEMENS Scalance S konfigurieren

2 Kurzfassung

IPsec-Teilnehmer-Konfiguration

So konfigurieren Sie einen INSYS-Router als IPsec-Teilnehmer für eine Verbindung mit einem SIEMENS Scalance S. Detaillierte Schritt-für-Schritt-Anweisungen finden Sie im folgenden Kapitel.

1. „IPsec aktivieren“ markieren
2. „IP-Adresse oder Domainname der Gegenstelle“ eingeben
3. „Lokales Subnetz der Gegenstelle“ eingeben
4. IPsec-Parameter entsprechend der Scalance-Konfiguration einstellen
5. „Authentifizierung mit Passphrase (PSK)“ markieren
6. Passphrase eingeben
7. Einstellungen speichern

3 Konfiguration

Vorbereitungen

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

- **Scalance-Konfiguration**

→ Siemens Security Configuration Tool ist auf dem Konfigurations-PC installiert.
→ Der erweiterte Modus des Security Configuration Tool ist aktiviert (Strg+E).
→ Eine Gruppe ist im Security Configuration Tool für die entsprechende IPsec-Verbindung erstellt. Die Gruppe ist für eine Authentifizierung über Preshared Key konfiguriert und ein Schlüssel (Passphrase) ist eingegeben.
→ Scalance ist konfiguriert und in der Gruppe enthalten. Für den Scalance muss Routing aktiviert und konfiguriert sein. Routing kann nur aktiviert werden, wenn der Scalance als Typ S612V2 konfiguriert ist (Siehe Handbuch für Scalance).

- **Verbindung mit dem INSYS-Router**

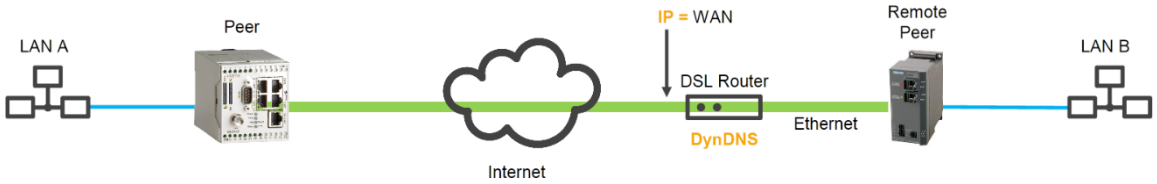
→ INSYS-Router ist mit der Stromversorgung verbunden und betriebsbereit.
→ Sie haben Zugriff auf den INSYS-Router über Ihren Web-Browser.
→ Datum und Zeit sind im INSYS-Router korrekt eingestellt.

IPsec-Verbindung mit Authentifizierung durch Passphrase für Scalance S konfigurieren

So konfigurieren Sie die IPsec-Verbindung mit Authentifizierung durch Passphrase zu einem Scalance S.

→ Sie müssen die über das Internet erreichbare IP-Adresse oder den Domain-Namen des Scalance S wissen.

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



1. Wählen Sie im Menü die Seite → IPsec.

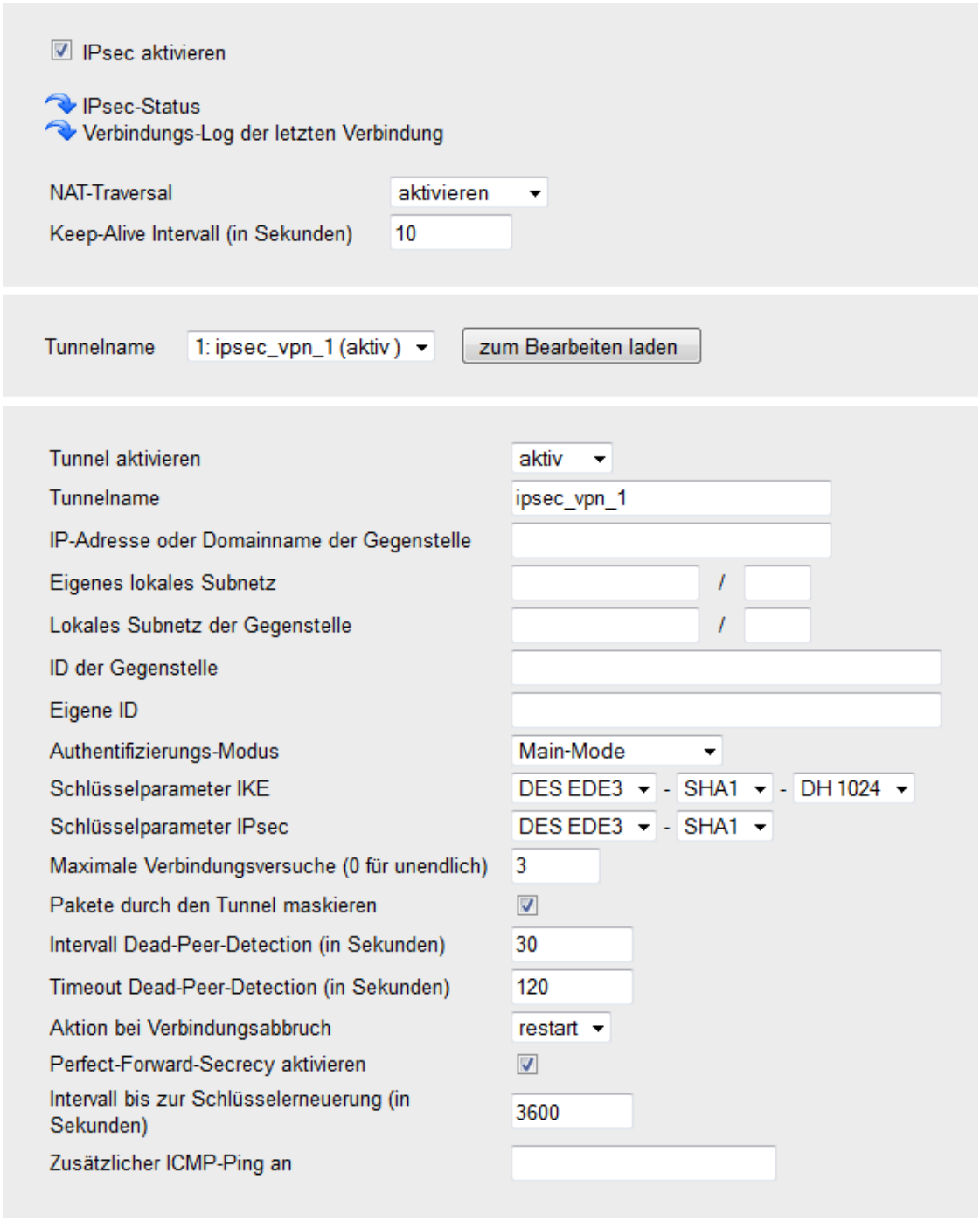
   ⓘ *Diese Seite befindet sich je nach verwendetem INSYS-Router unter dem Menüpunkt Dial-In, Dial-Out, LAN (ext) oder WWAN.*

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

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

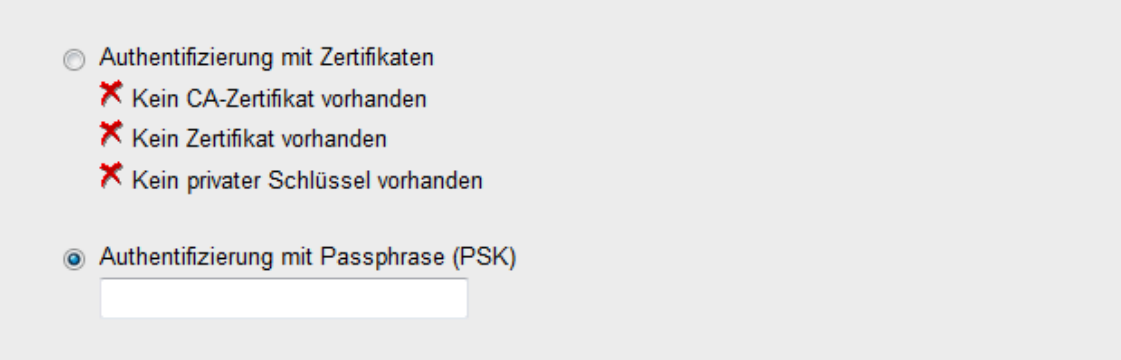
4. Tragen Sie das lokale Subnetz des Scalance S in das Feld „Lokales Subnetz der Gegenstelle“ ein.
5. Konfigurieren Sie die IPsec-Parameter gemäß Konfiguration des Scalance S.

   ⓘ *Die Konfiguration des Scalance S kann angezeigt werden, indem Sie im Security Configuration Tool die entsprechende Gruppe auswählen und im Kontextmenü Eigenschaften auswählen. Die erweiterten Einstellungen Phase 1 entsprechen den Schlüsselparametern IKE und die erweiterten Einstellungen Phase 2 entsprechen den Schlüsselparametern IPsec.*

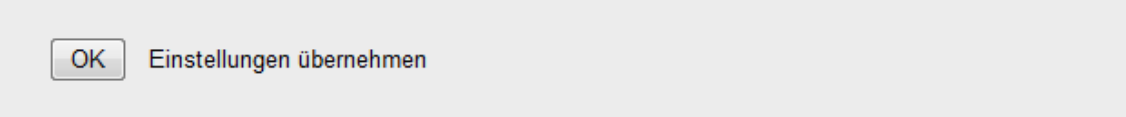


6. Konfigurieren Sie ggf. die weiteren IPsec-Parameter gemäß den Anforderungen Ihrer Verbindung bzw. der Konfiguration des Scalance S.
7. Scrollen Sie nach unten zu → Authentifizierung mit Zertifikaten.
8. Markieren Sie die Option „Authentifizierung mit Passphrase (PSK)“.
9. Geben Sie die Passphrase in das darunterliegende Feld ein.

   ⓘ *Die Passphrase ist der im Security Configuration Tool eingegebene Schlüssel.*



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



✓ Die IPsec-Verbindung zum Scalance S ist damit konfiguriert. Ein erfolgreicher Verbindungsaufbau wird durch Leuchten der grünen LED „Status / VPN“ angezeigt und kann auf der Seite „IPsec“ über den Link „Verbindungslog der letzten Verbindung“ verifiziert werden.

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
Security Module	Siemens	Scalance S	-

Tabelle 1: Verwendete Hardware

Software

Bezeichnung	Hersteller	Typ	Version
Betriebssystem	Microsoft	Windows 7	SP1
Browser	Mozilla	Firefox	^30
Konfigurations-Tool	Siemens	Security Configuration Tool	2.01

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