SIEMENS

SIMATIC NET

SCALANCE S und SOFTNET Security Client

Betriebsanleitung

02/2011

C79000-G8900-C196-07

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
mit Warndreieck bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

VORSICHT
ohne Warndreieck bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass ein unerwünschtes Ergebnis oder Zustand eintreten kann, wenn der entsprechende Hinweis nicht beachtet wird.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Dokumentbestellnummer: C79000-G8900-C196-07
℗ 02/2011

Vorwort

Dieses Handbuch…

…unterstützt Sie bei der Inbetriebnahme der Security Module SCALANCE S602 / S612 / S613 sowie des SOFTNET Security Client. Die Varianten SCALANCE S602 / S612 / S613 werden im Folgenden mit SCALANCE S bezeichnet.

Neu in dieser Ausgabe

In dieser Ausgabe sind unter anderem folgende neue Funktionen berücksichtigt:

- **Security Configuration Tool V2.3**

  Für einen leichteren Umgang und um eine bessere Übersicht zu den verschiedenen Modularten zu erhalten, wurde die Handhabung der Moduleinbindung und des Modulaustausches neu konzeptioniert.

  Sie können einen SOFTNET Security Client V3.0 zusammen mit einem MD741-1 konfigurieren und die entsprechenden Konfigurationsdateien erzeugen (siehe GETTING STARTED Beispiel 5: Fernzugriff - VPN-Tunnel-Beispiel mit MD741-1 und SOFTNET Security Client (Seite 89)).

  Für den IKE-Modus (Phase 1) sind die Verschlüsselungsalgorithmen AES-128, AES-192 und AES-256 parametrierbar.

  Neben den Betriebssystemen Windows XP SP2 und Windows XP SP3 wird das Betriebssystem Windows 7 unterstützt (nicht die Home-Version).

- **SOFTNET Security Client V3.0**

  Für eine bessere Visualisierung und Diagnose der Zustände der Verbindungen wurden neue Icons implementiert und eine zusätzliche Diagnoseübersicht ("Erweiterte Diagnose") hinzugefügt.

  Für die Log-Konsole in der Tunnelübersicht können Sie nun Einstellungen vornehmen hinsichtlich der anzuzeigenden Meldungen und der Größe der Log-Dateien.

  Um bei volumenorientierten Verbindungen Kosten zu sparen, besteht die Möglichkeit, auf Kosten der Diagnosefähigkeit des SOFTNET Security Client V3.0 den Erreichbarkeitstest zu deaktivieren.

  Bei der Diagnose der Erreichbarkeit der Tunnelpartner kann es bei Tunneln über langsamere Übertragungswege (UMTS, GPRS, etc.) vorkommen, dass die Erreichbarkeit als negativ angezeigt wird, obwohl die Kommunikation prinzipiell funktioniert. Für diesen Fall kann die Wartezeit auf die Ping-Antwort (Erreichbarkeitstest) global erhöht werden.

  Der Verbindungsaufbau zu einem MD741-1 wird unterstützt. In diesem Zusammenhang kann eine dyn. DNS-Adresse konfiguriert werden (siehe GETTING STARTED Beispiel 5: Fernzugriff - VPN-Tunnel-Beispiel mit MD741-1 und SOFTNET Security Client (Seite 89)).

  Neben den Betriebssystemen Windows XP SP2 und Windows XP SP3 wird das Betriebssystem Windows 7 unterstützt (nicht die Home-Version).

- **Konfigurationsdaten für Modul MD 741-1**

  Um einen externen MD741-1 für einen Zugriff mit dem SOFTNET Security Client V3.0 zu konfigurieren, können Sie mit dem Security Configuration Tool V2.3 die Konfigurationsdaten in eine Textdatei ausleiten. (GETTING STARTED Beispiel 5: Fernzugriff - VPN-Tunnel-Beispiel mit MD741-1 und SOFTNET Security Client (Seite 89)).

Gültigkeitsbereich dieses Handbuchs

Dieses Handbuch ist für folgende Geräte und Komponenten gültig:

- SIMATIC NET SCALANCE S602 6GK5 602-0BA00-2AA3 - mit FW-Stand ab V2.3
- SIMATIC NET SCALANCE S612 V2 6GK5 612-0BA00-2AA3 - mit FW-Stand ab V2.3
- SIMATIC NET SCALANCE S613 V2 6GK5 613-0BA00-2AA3 - mit FW-Stand ab V2.3
- SIMATIC NET SOFTNET Security Client 6GK1 704-1VW02-0AA0 - ab Ausgabestand 2008
- Security Configuration Tool - Ausgabestand V2.3

Leserkreis

Dieses Handbuch wendet sich an Personen, welche die Inbetriebnahme der Security Module SCALANCE S sowie des SOFTNET Security Client in einem Netzwerk durchführen.

Weiterführende Dokumentation

Im Handbuch "SIMATIC NET Industrial Ethernet Twisted Pair- und Fiber Optic Netze" erhalten Sie zusätzliche Hinweise zu weiteren SIMATIC NET-Produkten, die Sie gemeinsam mit dem Security Module SCALANCE S in einem Industrial Ethernet Netzwerk betreiben können.

Sie können dieses Netzhandbuch beim Customer Support im Internet in elektronischer Form unter folgender Adresse herunterladen:

http://support.automation.siemens.com/WW/view/de/1172207
(http://support.automation.siemens.com/WW/view/de/1172207)

Normen und Zulassungen

Das Gerät SCALANCE S erfüllt die Anforderungen zur CE-Kennzeichnung. Ausführliche Hinweise hierzu finden Sie im Anhang dieses Betriebshandbuches.

In diesem Handbuch verwendete Symbole

Auf besondere Tipps werden Sie in dieser Anleitung mit diesem Symbol hingewiesen.

Das Symbol verweist auf besondere Literaturempfehlungen.

Dieses Symbol weist auf detailliertere Hilfestellung in der kontextabhängigen Hilfe hin. Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Literaturhinweise /.../

Hinweise auf weitere Dokumentationen sind mit Hilfe von Literaturnummern in Schrägstrichen /.../ angegeben. Anhand dieser Nummern können Sie dem Literaturverzeichnis am Ende des Handbuchs den Titel der Dokumentation entnehmen.

Inhalt

Einführung und Grundlagen

1

Mit SIMATIC NET SCALANCE S und SIMATIC NET SOFTNET Security Client haben Sie sich für das SIEMENS Sicherheits-Konzept entschieden, das den hohen Anforderungen geschützter Kommunikation in der industriellen Automatisierungstechnik gerecht wird.

Dieses Kapitel gibt Ihnen einen Überblick über die Sicherheitsfunktionen der Geräte und Komponenten

- Security Module SCALANCE S
- SOFTNET Security Client

Tipp:
Den schnellen Einstieg mit SCALANCE S finden Sie im Kapitel 3 "GETTING STARTED".

1.1 Einsatz von SCALANCE S612, S613 und SOFTNET Security Client

Umfassender Schutz - Aufgabe von SCALANCE S612 / S613

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall, NAT/NAPT-Router und VPN (Virtual Private Network) über IPsec-Tunnel schützen die Geräte SCALANCE S612 / S613 einzelne Geräte oder auch ganze Automatisierungszellen vor:

- Datenspionage
- Datenmanipulation
- unberechtigten Zugriffen

SCALANCE S612 / S613 ermöglicht diesen Schutz flexibel, rückwirkungsfrei, protokollunabhängig (ab Layer-2 gemäß IEEE 802.3) und ohne komplizierte Handhabung.

SCALANCE S612 / S613 und SOFTNET Security Client werden mit dem Projektierwerkzeug Security Configuration Tool konfiguriert.

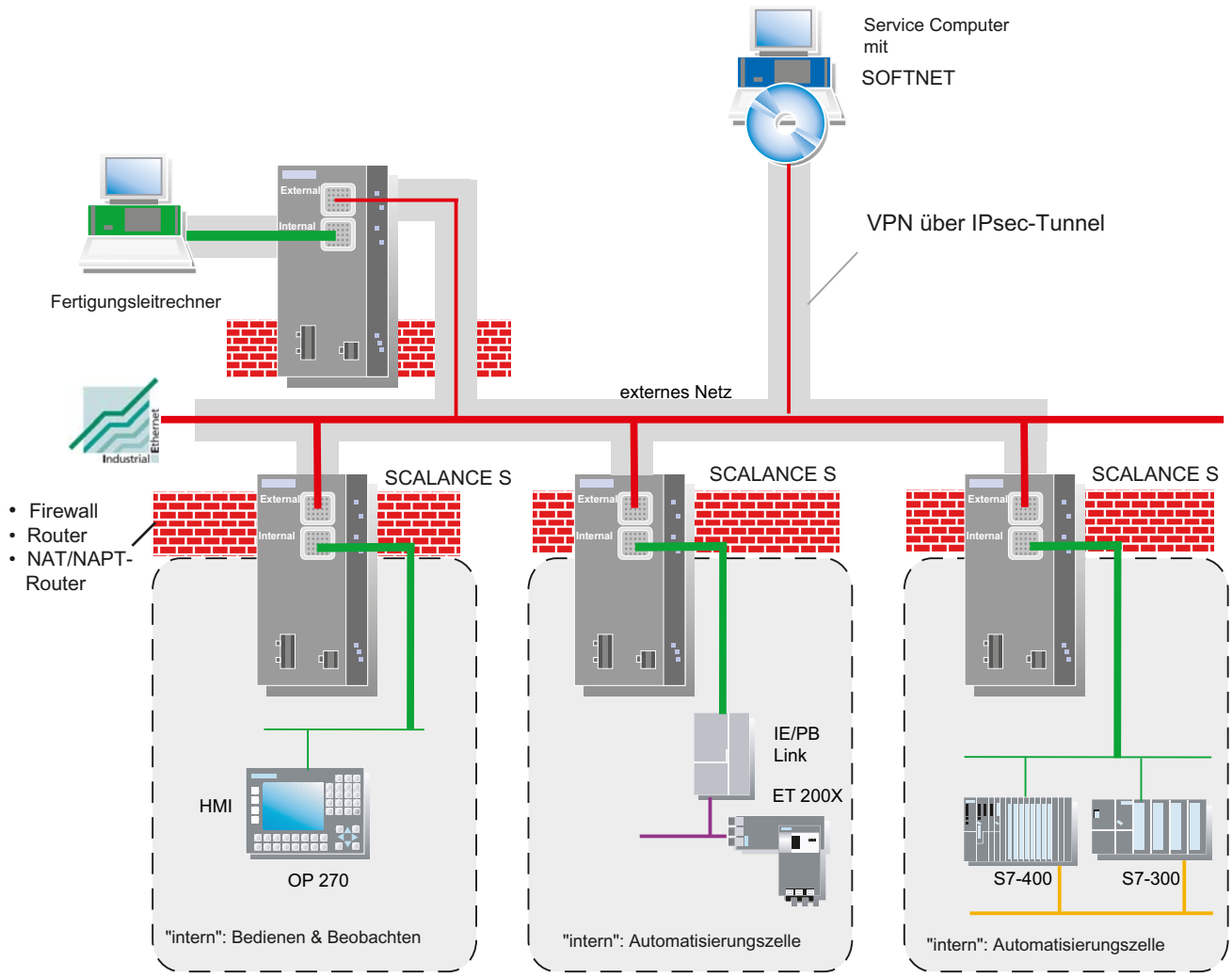


Bild 1-1 Netzkonfiguration mit SCALANCE S612 / S613

Sicherheitsfunktionen

- Firewall
  - IP-Firewall mit Stateful Packet Inspection;
  - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer-2-Telegramme; gilt nicht, wenn der Router-Betrieb genutzt wird)
  - Bandbreitenbegrenzung

  Alle Netzknoten, die sich im internen Netzsegment eines SCALANCE S befinden, werden durch dessen Firewall geschützt.
- Gesicherte Kommunikation durch IPsec-Tunnel

  SCALANCE S612 / S613 und SOFTNET Security Clients können per Projektierung zu Gruppen zusammengefasst werden. Zwischen allen SCALANCE S612 / S613 und einem SOFTNET Security Client einer Gruppe werden IPsec-Tunnel aufgebaut (VPN, Virtual Private Network). Alle internen Knoten dieser SCALANCE S können mittels dieser Tunnel gesichert miteinander kommunizieren.
- Protokollunabhängigkeit

  Die Tunnelung umfasst auch Ethernet-Telegramme gemäß IEEE 802.3 (Layer-2-Telegramme; gilt nicht, wenn der Router-Betrieb genutzt wird).

  Durch die IPsec-Tunnel werden sowohl IP-, als auch Non-IP-Telegramme übertragen.
- Router-Betrieb

  Indem Sie SCALANCE S als Router betreiben, verbinden Sie das interne Netz mit dem externen Netz. Das über SCALANCE S verbundene interne Netz wird somit zu einem eigenen Subnetz.
- Schutz für Geräte und Netzsegmente

  Die Schutzfunktion Firewall und VPN kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.
- Rückwirkungsfreiheit beim Einbau in flache Netze (Bridge-Betrieb)

  Interne Netzknoten können ohne Projektierung gefunden werden. Beim Einbau eines SCALANCE S612 / S613 in eine bestehende Netzinfrastruktur müssen daher die Endgeräte nicht neu konfiguriert werden.

  Das Modul versucht interne Teilnehmer zu finden; interne Teilnehmer, die auf diesem Weg nicht gefunden werden können, müssen dennoch projektiert werden.

PC/PG-Kommunikation im VPN - Aufgabe des SOFTNET Security Client

Mit der PC-Software SOFTNET Security Client sind gesicherte Fernzugriffe vom PC/PG auf Automatisierungsgeräte, die durch SCALANCE S geschützt sind, über öffentliche Netze hinweg, möglich.

Mittels des SOFTNET Security Client wird ein PC/PG automatisch so konfiguriert, dass er eine gesicherte IPsec Tunnelkommunikation im VPN (Virtual Private Network) zu einem oder mehreren SCALANCE S aufbauen kann.

PG/PC-Applikationen wie NCM Diagnose oder STEP7 können so über eine gesicherte Tunnel-Verbindung auf Geräte oder Netzwerke zugreifen, die sich in einem durch SCALANCE S geschützten internen Netz befinden.

Die PC-Software SOFTNET Security Client wird ebenfalls mit dem Projektierwerkzeug Security Configuration Tool konfiguriert; damit ist eine durchgängige Projektierung gewährleistet, die kein spezielles Security Know How erfordert.

Interne und Externe Netzknoten

SCALANCE S612 / S613 teilt Netzwerke in zwei Bereiche auf :

- internes Netz: geschützte Bereiche mit den "internen Knoten"

  Interne Knoten sind alle diejenigen Knoten, die von einem SCALANCE S abgesichert sind.

- externes Netz: ungeschützte Bereiche mit den "externen Knoten"

  Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

ACHTUNG
Die internen Netze werden als sicher (vertrauenswürdig) betrachtet. Verbinden Sie ein internes Netzsegment nur über SCALANCE S mit den externen Netzsegmenten. Weitere Verbindungswege zwischen dem internen und externen Netz dürfen nicht vorhanden sein!

1.2 Einsatz von SCALANCE S602

Firewall und Router - Aufgabe von SCALANCE S602

Durch die Kombination unterschiedlicher Sicherheitsmaßnahmen wie Firewall und NAT/NAPT-Router schützt das Gerät SCALANCE S602 einzelne Geräte oder auch ganze Automatisierungszellen vor:

- Datenspionage
- unberechtigten Zugriffen

SCALANCE S602 ermöglicht diesen Schutz flexibel und ohne komplizierte Handhabung.

SCALANCE S602 wird mit dem Projektierwerkzeug Security Configuration Tool konfiguriert.

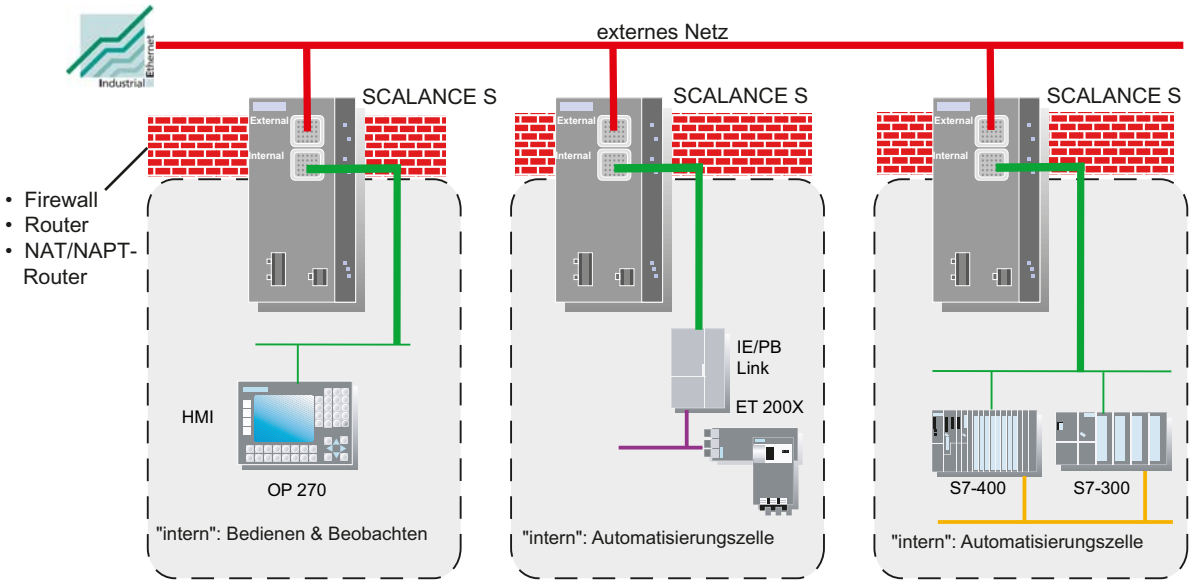


Bild 1-2 Netzkonfiguration mit SCALANCE S602

Sicherheitsfunktionen

- Firewall
  - IP-Firewall mit Stateful Packet Inspection;
  - Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3 (Layer-2-Telegramme; gilt nicht für S602, wenn der Router-Betrieb genutzt wird);
  - Bandbreitenbegrenzung

  Alle Netzknoten, die sich im internen Netzsegment eines SCALANCE S befinden, werden durch dessen Firewall geschützt.
- Router-Betrieb

  Indem Sie SCALANCE S als Router betreiben, entkoppeln Sie das interne Netz von dem externen Netz. Das von SCALANCE S verbundene interne Netz wird somit zu einem eigenen Subnetz; SCALANCE S muss als Router explizit über seine IP-Adresse adressiert werden.
- Schutz für Geräte und Netzsegmente

  Die Schutzfunktion Firewall kann sich über den Betrieb einzelner Geräte, mehrerer Geräte wie auch ganzer Netzsegmente erstrecken.
- Rückwirkungsfreiheit beim Einbau in flache Netze (Bridge-Betrieb)

  Beim Einbau eines SCALANCE S602 in eine bestehende Netzinfrastruktur müssen die Endgeräte nicht neu eingestellt werden.

Interne und Externe Netzknoten

SCALANCE S602 teilt Netzwerke in zwei Bereiche auf :

- internes Netz: geschützte Bereiche mit den "internen Knoten"

  Interne Knoten sind alle diejenigen Knoten, die von einem SCALANCE S abgesichert sind.

- externes Netz: ungeschützte Bereiche mit den "externen Knoten"

  Externe Knoten sind alle Knoten, die sich außerhalb der geschützten Bereiche befinden.

ACHTUNG
Die internen Netze werden als sicher (vertrauenswürdig) betrachtet. Verbinden Sie ein internes Netzsegment nur über SCALANCE S mit den externen Netzsegmenten. Weitere Verbindungswege zwischen dem internen und externen Netz dürfen nicht vorhanden sein!

1.3 Projektierung und Administration

Das Wichtigste zusammengefasst

Im Zusammenspiel mit dem Projektierwerkzeug Security Configuration Tool werden Sie zu einer einfachen und sicheren Anwendung der SCALANCE S-Module geführt:

- Projektierung ohne IT-Experten-Wissen mit dem Security Configuration Tool

  Mit dem Security Configuration Tool können auch Nicht-IT-Experten ein SCALANCE S-Modul einstellen. In einem erweiterten Modus können bei Bedarf komplexere Einstellungen vorgenommen werden.

- Gesicherte administrative Kommunikation

  Die Übertragung der Einstellungen zum SCALANCE S erfolgt über eine SSL-verschlüsselte Verbindung.

- Zugriffsschutz im Security Configuration Tool

  Durch die Benutzerverwaltung des Security Configuration Tool ist ein Zugriffsschutz für die SCALANCE S-Geräte und die Projektierdaten gewährleistet.

- Wechselmedium C-PLUG einsetzbar

  Der C-PLUG ist ein steckbares Wechselmedium, auf dem Konfigurationsdaten verschlüsselt abgespeichert sind. Er ermöglicht beim Austausch eines SCALANCE S die Konfiguration ohne PC/PG.

Produkteigenschaften und Inbetriebnahme 2

Dieses Kapitel macht Sie mit der Handhabung und allen wichtigen Eigenschaften des Gerätes SCALANCE S vertraut.

Sie erfahren, welche Montagemöglichkeiten bestehen und wie Sie das Gerät mit wenigen Schritten in Betrieb setzen.

Weitere Informationen

Wie Sie das Gerät für Standard-Anwendungen konfigurieren wird Ihnen kompakt im Kapitel "GETTING STARTED" gezeigt.

Details zur Projektierung und den Online-Funktionen finden Sie im Nachschlageteil dieses Handbuches.

2.1 Produkteigenschaften

Hinweis

Die angegebenen Zulassungen gelten erst dann als erteilt, wenn auf dem Produkt eine entsprechende Kennzeichnung angebracht ist.

2.1.1 Hardware-Merkmale und Funktionsübersicht

Folgende wesentliche Leistungsmerkmale bieten alle SCALANCE S Module:

Hardware

- Robustes Gehäuse mit Schutzart IP 30
- wahlweise Montage auf S7-300- oder DIN-Hutschiene 35mm
- redundante Spannungszuführung

- Meldekontakt
- erweiterter Temperaturbereich (-20 °C bis +70 °C SCALANCE S613)

Funktionsübersicht der Gerätetypen

Entnehmen Sie der folgenden Tabelle, welche Funktionen bei Ihrem Gerät unterstützt werden.

Hinweis

In diesem Handbuch werden alle Funktionen beschrieben. Bitte berücksichtigen Sie anhand der nachfolgenden Tabelle, welche Beschreibungen für das von Ihnen genutzte Gerät zutreffen.

Achten Sie auch auf die zusätzlichen Angaben in den Kapitel-Überschriften!

Tabelle 2- 1 Funktionsübersicht

Funktion	S602	S612 V1	S612 V2	S613 V1	S613 V2
Firewall	x	x	x	x	x
NAT/NAPT-Router	x	-	x	-	x
DHCP-Server	x	-	x	-	x
Netzwerk-Syslog	x	-	x	-	x
IPsec-Tunnel (VPN, Virtual Private Network)	-	x	x	x	x
SOFTNET Security Client	-	x	x	x	x

x Funktion wird unterstützt

- Funktion wird nicht unterstützt

2.1.2 Lieferumfang

Was wird mit dem SCALANCE S ausgeliefert ?

- Gerät SCALANCE S
- 2-poliger steckbarer Klemmenblock
- 4-poliger steckbarer Klemmenblock
- Informationen zum Produkt
- CD mit folgendem Inhalt:
  - Handbuch
  - Projektierungs-Software Security Configuration Tool

2.1.3 Auspacken und Prüfen

Auspacken, Prüfen

1. Überprüfen Sie das Paket auf Vollständigkeit.
2. Überprüfen Sie die Einzelteile auf Transportschäden.

⚠ WARNUNG
Nehmen Sie nur unbeschädigte Teile in Betrieb!

2.1.4 Anschluss an Ethernet

Anschlussmöglichkeiten

SCALANCE S verfügt über 2 RJ-45 Buchsen für den Anschluss an Ethernet.

Hinweis

An dem TP-Port in RJ–45 Ausführung können TP-Cords oder TP-XP-Cords mit einer Maximallänge von 10 m angeschlossen werden.

In Verbindung mit dem Industrial Ethernet FastConnect IE FC Standard Cable und IE FC RJ–45 Plug 180 ist eine gesamte Leitungslänge von maximal 100 m zwischen zwei Geräten zulässig.

ACHTUNG
Die Ethernet-Anschlüsse an Port 1 und Port 2 werden vom SCALANCE S unterschiedlich behandelt und dürfen deshalb beim Anschluss an das Kommunikationsnetzwerk nicht verwechselt werden: • Port 1 - External Network obere RJ45-Buchse, rote Markierung = ungeschützter Netzwerk-Bereich; • Port 2 - Internal Network untere RJ45-Buchse, grüne Markierung = durch SCALANCE S geschütztes Netzwerk; Beim Vertauschen der Ports verliert das Gerät seine Schutzfunktion.

Autonegotiation

SCALANCE S unterstützt Autonegotiation.

Unter Autonegotiation versteht man, dass die Verbindungs- und Übertragungsparameter mit dem angesprochenen Netzknoten automatisch ausgehandelt werden.

MDI /MDIX Autocrossing-Funktion

SCALANCE S unterstützt die MDI / MDIX Autocrossing-Funktion.

Die MDI /MDIX Autocrossing-Funktion bietet den Vorteil einer durchgängigen Verkabelung, ohne dass externe, gekreuzte Ethernet-Kabel erforderlich sind. Fehlfunktionen bei vertauschten Send- und Empfangsleitungen werden dadurch verhindert. Die Installation wird dadurch wesentlich vereinfacht.

2.1.5 Spannungsversorgung

⚠ WARNUNG
Das Gerät SCALANCE S ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden. Das Netzteil für die Versorgung des SCALANCE S muss NEC Class 2 entsprechen (Spannungsbereich 18-32 V, Strombedarf 250 mA). Das Gerät darf nur mit einer Stromversorgungseinheit versorgt werden, die die Anforderungen der Klasse 2 für Stromversorgungen der "National Electrical Code,table 11 (b) " erfüllt. Bei einem Aufbau mit redundanter Stromversorgung (zwei getrennte Stromversorgungen) müssen beide diese Anforderungen erfüllen.

ACHTUNG
Schließen Sie den SCALANCE S niemals an Wechselspannung an oder an Gleichspannungen größer als 32 V DC an.

Der Anschluss der Spannungsversorgung erfolgt über einen 4-poligen steckbaren Klemmenblock. Die Spannungsversorgung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzteil mit der höheren Ausgangsspannung den SCALANCE S alleine. Die Spannungsversorgung ist hochohmig mit dem Gehäuse verbunden, um einen erdfreien Aufbau zu ermöglichen.

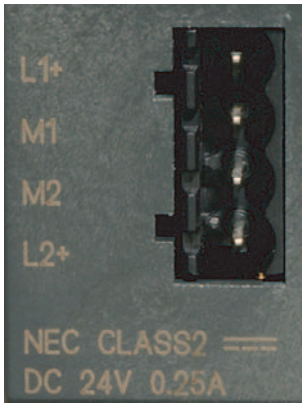


Bild 2-1 Spannungsversorgung

2.1.6 Meldekontakt

ACHTUNG
Der Meldekontakt darf mit maximal 100 mA belastet werden (Sicherheitsspannung (SELV), DC 24 V). Schließen Sie den SCALANCE S niemals an Wechselspannung an oder an Gleichspannungen größer als 32 V DC an.

Der Anschluss des Meldekontaktes erfolgt über einen 2-poligen steckbaren Klemmblock. Der Meldekontakt ist ein potentialfreier Schalter, mit dem Fehlerzustände durch Kontaktunterbrechung gemeldet werden.

Folgende Fehler können über den Meldekontakt signalisiert werden:

- Fehler in der Spannungsversorgung
- interne Fehler

Im Fehlerfall oder wenn SCALANCE S spannungslos ist, ist der Meldekontakt geöffnet. Bei fehlerfreiem Betrieb ist er geschlossen.

Bild 2-2 Meldekontakt

2.1.7 Reset-Taster - Rücksetzen der Konfiguration auf Werkseinstellung

SCALANCE S hat einen Reset-Taster. Der Reset-Taster befindet sich auf der Gehäuserückseite unter dem Schraubdeckel unmittelbar neben dem C-PLUG.

Der Reset-Taster ist gegen versehentliches Betätigen mechanisch geschützt.

ACHTUNG
Stellen Sie sicher, dass nur befugtes Personal Zugriff auf SCALANCE S hat.

Welche Funktion hat der Taster ?

Mit dem Reset-Taster können zwei Funktionen ausgelöst werden:

- Neustart

  Das Modul wird neu gestartet. Die geladene Konfiguration bleibt erhalten.

- Rücksetzen auf Werkseinstellungen

  Das Modul wird neu gestartet und in den Auslieferungszustand zurückversetzt. Eine geladene Konfiguration wird gelöscht.

Neustart - Gehen Sie so vor

1. Demontieren Sie ggf. das SCALANCE S-Modul, um Zugriff auf den Schacht zu erlangen.
2. Entfernen Sie den M32-Stopfen auf der Rückseite des Gerätes.

   Der Reset-Taster ist in einem Schacht auf der Rückseite des SCALANCE S direkt neben dem Steckplatz für den C-PLUG untergebracht. Dieser Schacht ist durch einen Stopfen mit Schraubverschluss gesichert. Der Taster befindet sich in einer dünnen Bohrung und ist dadurch vor versehentlichem Betätigen geschützt.

3. Drücken Sie den Reset-Taster kürzer als 5 Sekunden.

   Der Neustart dauert bis zu 2 Minuten. Während des Neustarts leuchtet die Fault-Anzeige gelb. Achten Sie darauf, dass die Spannungsversorgung währenddessen nicht unterbrochen wird.

   Nach Abschluss des Neustarts geht das Gerät automatisch in den Produktivbetrieb über. Die Fault-Anzeige leuchtet dann dauerhaft grün.

4. Verschließen Sie den Schacht mit dem M32-Stopfen und montieren Sie das Gerät.

Rücksetzen auf Werkseinstellungen - Gehen Sie so vor

ACHTUNG
Ist beim Rücksetzen auf Werkseinstellungen ein C-PLUG gesteckt, dann wird der C-PLUG gelöscht!

1. Demontieren Sie ggf. das SCALANCE S-Modul, um Zugriff auf den Schacht zu erlangen.
2. Entfernen Sie den M32-Stopfen auf der Rückseite des Gerätes.

   Der Reset-Taster ist in einem Schacht auf der Rückseite des SCALANCE S direkt neben dem Steckplatz für den C-PLUG untergebracht. Dieser Schacht ist durch einen Stopfen mit Schraubverschluss gesichert. Der Taster befindet sich in einer dünnen Bohrung und ist dadurch vor versehentlichem Betätigen geschützt.

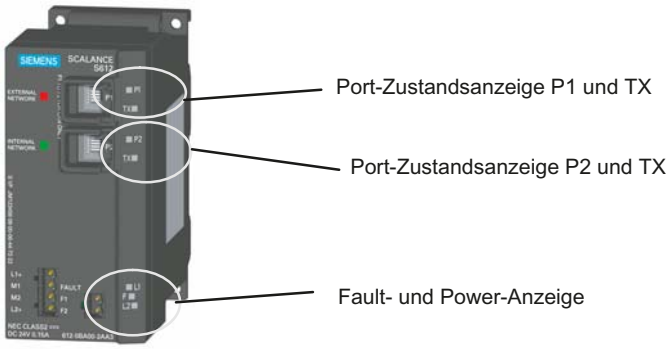
3. Drücken Sie den Reset-Taster und halten Sie ihn so lange gedrückt - länger als 5 Sekunden - bis die Fault-Anzeige gelb-rot blinkt.

   Der Rücksetzvorgang dauert bis zu 2 Minuten. Während des Rücksetzvorganges blinkt die Fault-Anzeige gelb-rot. Achten Sie darauf, dass die Spannungsversorgung währenddessen nicht unterbrochen wird.

   Nach Abschluss des Rücksetzvorganges startet das Gerät automatisch neu. Die Fault-Anzeige leuchtet dann dauerhaft gelb.

4. Verschließen Sie den Schacht mit dem M32-Stopfen und montieren Sie das Gerät.

2.1.8 Anzeigen



Fehleranzeige (Fault LED)

Anzeige des Betriebszustandes:

Zustand	Bedeutung
leuchtet rot	Modul erkennt einen Fehler. (Meldekontakt ist offen) Folgende Fehler werden erkannt: • Interner Fehler (beispielsweise: Anlauf fehlgeschlagen) • ungültiger C-PLUG (ungültige Formatierung)
leuchtet grün	Modul ist im Produktivbetrieb (Meldekontakt ist geschlossen).
leuchtet NICHT	Modul ist ausgefallen; keine Spannungsversorgung (Meldekontakt ist offen).
leuchtet gelb (Dauerlicht)	Modul ist im Anlauf. (Meldekontakt ist offen). Falls keine IP-Adresse vorhanden ist, bleibt das Modul in diesem Zustand.
blinkt abwechselnd gelb-rot	Modul setzt sich in den Auslieferungszustand zurück. (Meldekontakt ist offen).

Power-Anzeige (L1, L2)

Der Zustand der Spannungseinspeisung wird über 2 LEDs signalisiert:

Zustand	Bedeutung
leuchtet grün	Spannungsversorgung L1 bzw. L2 ist angeschlossen.
leuchtet nicht	Spannungsversorgung L1 bzw. L2 ist nicht angeschlossen oder <14 V (L+)
leuchtet rot	Spannungsversorgung L1 bzw. L2 ist im Betrieb ausgefallen oder <14 V (L+)

Portzustandsanzeigen (P1 und TX, P2 und TX)

Der Zustand der Schnittstellen wird über jeweils 2 LEDs für die beiden Anschlüsse signalisiert:

Zustand	Bedeutung
LED P1 / P2	
leuchtet grün	TP-Link vorhanden
blinkt / leuchtet gelb	Datenempfang an RX
aus	Kein TP-Link bzw. kein Datenempfang
LED TX	

Zustand	Bedeutung
blinkt / leuchtet gelb	Daten werden gesendet
aus	Keine Daten werden gesendet

2.1.9 Technische Daten

Anschlüsse	
Anschluss von Endgeräten oder Netzkomponenten über Twisted Pair	2xRJ–45-Buchsen mit MDI-X Belegung 10/100 Mbit/s (Halb-/Vollduplex)
Anschluss für Spannungsversorgung	1x4-poliger steckbarer Klemmenblock
Anschluss für Meldekontakt	1x2-poliger steckbarer Klemmenblock
Elektrische Daten	
Versorgungsspannung	Einspeisung DC 24 V (DC 18 bis 32 V) • redundant ausgeführt • Sicherheitskleinspannung (SELV)
Verlustleistung bei DC 24 V	3,84 W
Stromaufnahme bei Nennspannung	250 mA maximal
Zulässige Leitungslängen	
Anschluss über Industrial Ethernet FC TP Leitungen:	
0 - 100 m	Industrial Ethernet FC TP Standard Cable mit IE FC RJ–45 Plug 180 oder über Industrial Ethernet FC Outlet RJ–45 mit 0 - 90 m Industrial Ethernet FC TP Standard Cable + 10 m TP Cord
0 - 85 m	Industrial Ethernet FC TP Marine/Trailing Cable mit IE FC RJ–45 Plug 180 oder 0 - 75 m Industrial Ethernet FC TP Marine/Trailing Cable + 10 m TP Cord
Software-Mengengerüst bei VPN	
Anzahl der IPsec-Tunnel	
SCALANCE S612	64 maximal
SCALANCE S613	128 maximal
Software-Mengengerüst "Firewall"	
Anzahl Firewall-Regelsätze	
SCALANCE S602	256 maximal
SCALANCE S612	256 maximal
SCALANCE S613	256 maximal
Zulässige Umgebungsbedingungen/EMV	

Betriebstemperatur SCALANCE S602	0 °C bis +60 °C
Betriebstemperatur SCALANCE S612	0 °C bis +60 °C
Betriebstemperatur SCALANCE S613	-20 °C bis +70 °C
Lager-/Transporttemperatur	-40 °C bis +80 °C
Relative Feuchte im Betrieb	95 % (nicht kondensierend)
Betriebshöhe	bis 2000 m über NN bei max 56 °C Umbebungstemperatur bis 3000 m über NN bei max. 50 °C Umgebungstemperatur
Funkstörgrad	EN 50081-2 Class A
Störfestigkeit	EN 50082-2
Schutzart	IP 30
Zulassungen	
c-UL-us	UL 60950
	CSA C22.2 Nr. 60950
c-Ul-us for Hazardous Locations	UL 1604, UL 2279Pt.15
FM	FM 3611
C-TICK	AS/NZS 2064 (Class A).
CE	EN 50081-2, EN 50082-2
ATEX Zone 2	EN50021
MTBF	81,09 Jahre
Konstruktiver Aufbau	
Maße (B x H x T) in mm	60 x 125 x 124
Gewicht in g	780
Montagemöglichkeiten	• Hutschiene • S7-300 Profilschiene • Wandmontage
Bestellnummern	
SCALANCE S602	6GK5602-0BA00-2AA3
SCALANCE S612	6GK5612-0BA00-2AA3
SCALANCE S613	6GK5613-0BA00-2AA3
Handbuch "Industrial Ethernet TP- und Fiber Optic Netze"	6GK1970-1BA10-0AA0
Bestellnummern für Zubehör	
IE FC Stripping Tool	6GK1901-1GA00
IE FC Blade Cassettes	6GK1901-1GB00
IE FC TP Standard Cable	6XV1840 2AH10
IE FC TP Trailing Cable	6XV1840-3AH10
IE FC TP Marine Cable	6XV1840-4AH10
IE FC RJ–45 Plug 180 Packungseinheit = 1 Stück	6GK1 901-1BB10-2AA0

IE FC RJ–45 Plug 180 Packungseinheit = 10 Stück	6GK1 901-1BB10-2AB0
IE FC RJ–45 Plug 180 Packungseinheit = 50 Stück	6GK1 901-1BB10-2AE0

2.2 Montage

Hinweis

Die Anforderungen nach EN61000-4-5, Surge Prüfung auf Spannungsversorgungsleitungen, werden nur erfüllt bei Einsatz eines Blitzductor VT AD 24V Art. Nr. 918 402 .

Hersteller:
DEHN+SÖHNE GmbH+Co.KG, Hans Dehn Str.1, Postfach 1640, D-92306 Neumarkt

⚠ WARNUNG

Bei Einsatz unter Explosionsschutz Bedingungen (Zone 2) muss das Produkt SCALANCE S in ein Gehäuse eingebaut werden.

Im Geltungsbereich der ATEX 95 (EN 50021) muß dieses Gehäuse mindestens IP54 nach EN 60529 entsprechen.

WARNUNG
DAS GERÄT DARF NUR DANN AN DIE SPANNUNGSVERSORGUNG ANGESCHLOSSEN ODER VON IHR GETRENNT WERDEN, WENN EINE EXPLOSIONSGEFAHR MIT SICHERHEIT AUSGESCHLOSSEN WERDEN KANN.

Montagearten

Der SCALANCE S lässt mehrere Montagearten zu:

- Montage auf 35 mm DIN Hutschiene
- Montage auf einer SIMATIC S7-300 Profilschiene
- Wandmontage

Hinweis

Beachten Sie bei Installation und Betrieb die Aufbaurichtlinien und Sicherheitshinweise, die in dieser Beschreibung sowie im Handbuch SIMATIC NET Industrial Ethernet Twisted Pair- und Fiber Optic-Netze /1/ beschrieben sind.

ACHTUNG
Es wird empfohlen, das Gerät durch eine geeignete Abschattung gegen direktes Sonnenlicht zu schützen. Dies vermeidet eine unerwünschte Erwärmung des Gerätes und verhindert frühzeitige Alterung von Gerät und Verkabelung.

2.2.1 Hutschienenmontage

Montage

Montieren Sie den SCALANCE S auf einer 35 mm Hutschiene nach DIN EN 50022.

1. Hängen Sie die obere Rastführung des Geräts in die Hutschiene ein und drücken Sie es nach unten gegen die Hutschiene bis zum Einrasten.

2. Montieren Sie die elektrischen Anschlussleitungen und den Klemmenblock für den Meldekontakt.

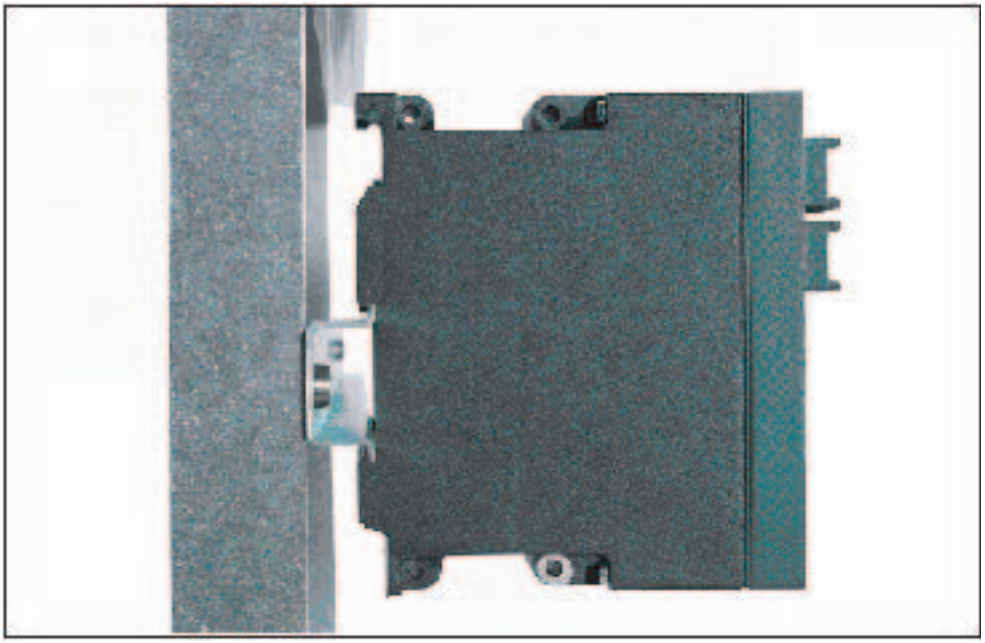


Bild 2-3 SCALANCE S Montage auf einer DIN-Hutschiene (35mm)

Demontage

Um den SCALANCE S von der Hutschiene abzunehmen:

1. Demontieren Sie zunächst die TP-Leitungen und ziehen Sie den Klemmblock für die Spannungsversorgung und den Meldekontakt ab.

2. Entriegeln Sie mit einem Schraubenzieher die Hutschienenverrastung an der Unterseite des Geräts und heben Sie danach das Gerät unten von der Hutschiene weg.

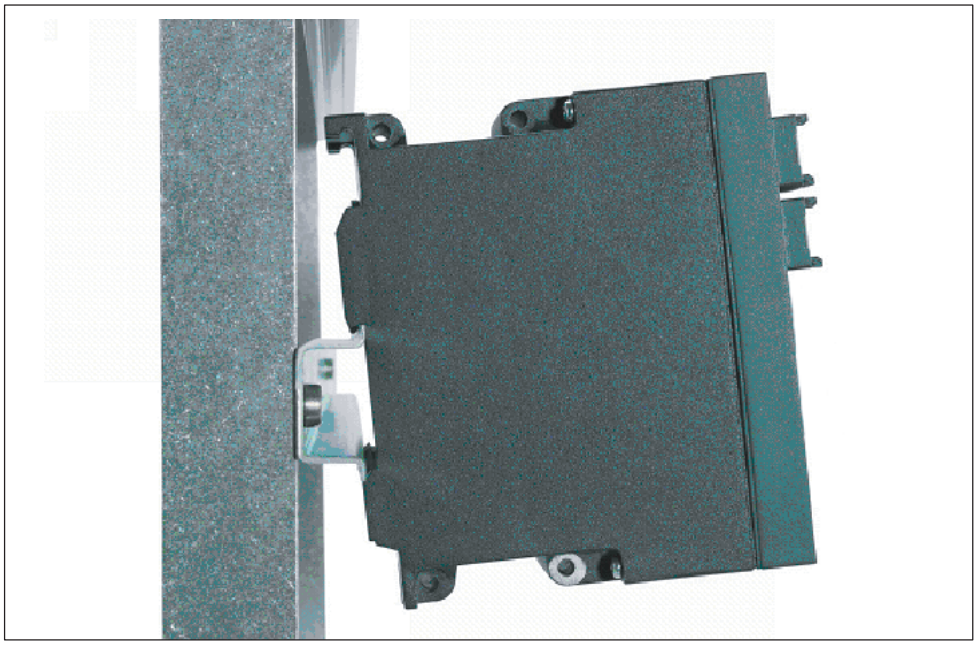


Bild 2-4 SCALANCE S Demontage von einer DIN-Hutschiene (35mm)

2.2.2 Profilschienenmontage

Montage auf einer SIMATIC S7-300 Profilschiene

1. Hängen Sie die Gehäuseführung an der Oberseite des SCALANCE S-Gehäuses in die S7-Profilschiene ein.

2. Verschrauben Sie das Gerät SCALANCE S an der Unterseite der Profilschiene.

Bild 2-5 SCALANCE S Montage auf einer SIMATIC S7-300-Profilschiene

2.2.3 Wandmontage

Montagematerial

Verwenden Sie zur Befestigung - beispielsweise an einer Betonwand:

- 4 Wanddübel mit 6 mm Durchmesser und 30 mm Länge
- Schrauben mit 3,5 mm Durchmesser und 40 mm Länge

Hinweis

Die Wandbefestigung muss so ausgelegt sein, dass sie mindestens das vierfache Eigengewicht des Geräts tragen kann.

2.2.4 Erdung

Hutschienenmontage

Die Erdung erfolgt über die Hutschiene.

S7-Profilschiene

Die Erdung erfolgt über die Geräterückseite und die Halsschraube.

Wandmontage

Die Erdung erfolgt durch die Befestigungsschraube über die lackfreie Bohrung.

ACHTUNG
Beachten Sie bitte, dass der SCALANCE S über eine Befestigungsschraube möglichst niederohmig geerdet werden muß.

2.3 Inbetriebnahme

ACHTUNG
Bitte lesen Sie vor der Inbetriebnahme unbedingt die Angaben in den Kapiteln "Produkteigenschaften" und "Montage" aufmerksam durch und befolgen Sie insbesondere die Anweisungen in den Sicherheitshinweisen.

Prinzip

Für den Betrieb eines SCALANCE S müssen Sie eine mit dem Security Configuration Tool projektierte Konfiguration laden. Dieser Vorgang wird nachfolgend beschrieben.

Eine Konfiguration eines SCALANCE S umfasst die IP-Parameter und die Einstellung von Firewall-Regeln und ggf. die Einstellung von IPsec-Tunneln (S612 / S613) oder Router-Betrieb.

Sie können grundsätzlich vor der Inbetriebnahme die vollständige Konfiguration zunächst offline projektieren und anschließend laden. Bei der ersten Konfiguration (Werkseinstellungen) verwenden Sie die auf dem Gerät aufgedruckte MAC-Adresse zur Adressierung.

Je nach Anwendung, werden Sie bei der Inbetriebnahme die Konfiguration in ein oder mehrere Module gleichzeitig laden.

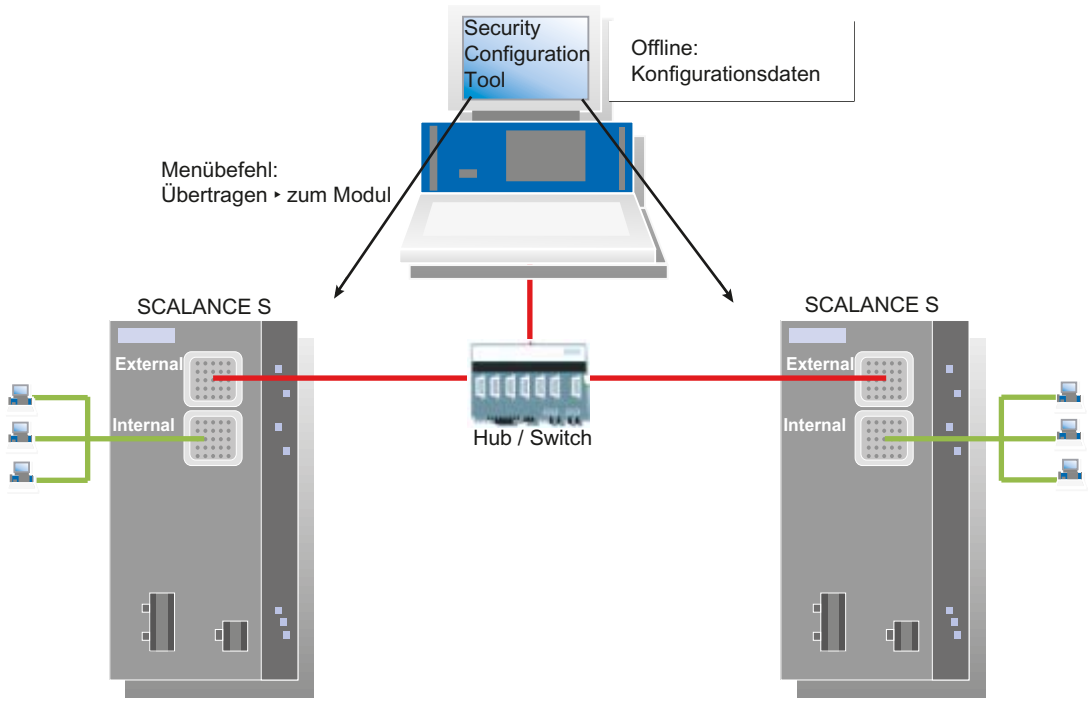


Bild 2-6 Übersichtsgrafik Inbetriebnahme

Werkseinstellungen

Mit den Werkseinstellungen (Lieferzustand oder nach "Rücksetzen auf Werkseinstellungen") hat das SCALANCE S nach dem Einschalten der Versorgungsspannung folgendes Verhalten:

- Eine IP-Kommunikation ist nicht möglich, da die IP-Einstellungen fehlen; insbesondere hat das SCALANCE S noch keine IP-Adresse.

  Sobald dem SCALANCE S-Modul durch Konfiguration eine gültige IP-Adresse zugewiesen wurde, ist das Modul auch über Router erreichbar (IP-Kommunikation ist dann möglich).

- Das Gerät hat eine fest voreingestellte MAC-Adresse; die MAC-Adresse ist auf dem Gerät aufgedruckt; diese müssen Sie bei der Projektierung eingeben.

- Die Firewall ist mit folgenden Firewall-Grundregeln vorkonfiguriert:

  – ungesicherter Datenverkehr vom Intern-Port zum Extern-Port und umgekehrt (extern ↔ intern) ist **nicht** möglich;

Der unkonfigurierte Zustand ist daran zu erkennen, dass die F-LED gelb leuchtet.

Siehe auch

Produkteigenschaften (Seite 17)

Montage (Seite 27)

2.3.1 Schritt 1: SCALANCE S Modul anschließen

Gehen Sie so vor:

1. Packen Sie zunächst das SCALANCE S aus und überprüfen Sie den unbeschädigten Zustand.
2. Schließen Sie die Spannungsversorgung an SCALANCE S an.

   Ergebnis: Nach dem Anschließen der Betriebsspannung leuchtet die Fault-LED (F) gelb.
3. Stellen Sie jetzt die physikalischen Netzwerkverbindungen her, indem Sie die Stecker der Netzwerkkabel in die dafür vorgesehenen Ports (RJ45-Buchsen) stecken.

   Verbinden Sie Port 1 (externer Port) mit dem externen Netzwerk, an dem der Projektier-PC/PG angeschlossen ist.

   Verbinden Sie Port 2 (interner Port) mit dem internen Netzwerk.

   Anmerkung:
   Sie können den Projektier-PC/PG bei der Inbetriebnahme prinzipiell zunächst an Port 1 oder Port 2 anschließen und auf den Anschluss von anderen Netzknoten verzichten, bis das Gerät mit einer Konfiguration versorgt ist. Beim Anschluss an Port 2 müssten Sie jedoch jedes einzelne SCALANCE S-Modul getrennt konfigurieren!
4. Fahren Sie nun mit dem nächsten Schritt "Projektieren und Laden" fort.

2.3.2 Schritt 2: Projektieren und Laden

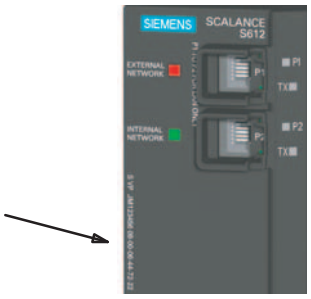
Im Folgenden wird beschrieben, wie Sie das SCALANCE S-Modul ausgehend von den Werkseinstellungen projektieren.

Gehen Sie so vor:

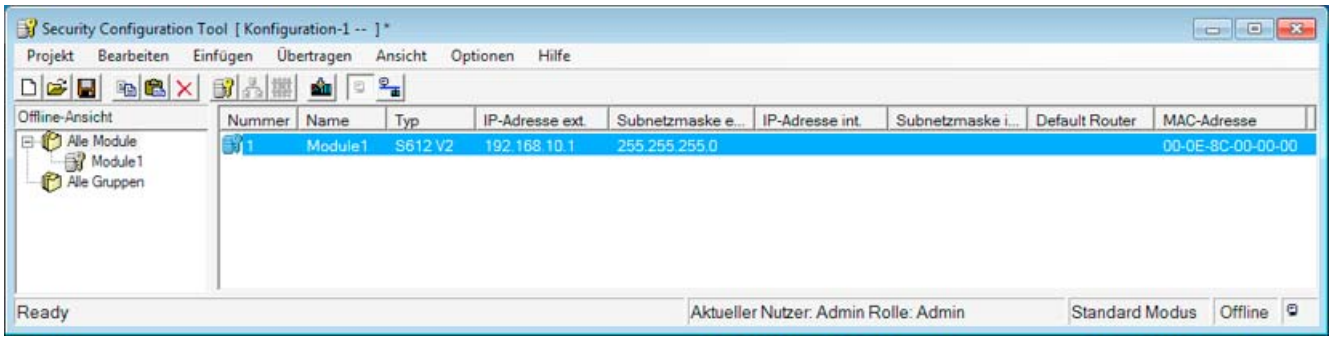
1. Starten Sie das mitgelieferte Projektierungswerkzeug Security Configuration Tool.
2. Wählen Sie den Menübefehl **Projekt ▸ Neu.**

   Sie werden aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Dem Benutzereintrag, den Sie hierbei festlegen, wird die Rolle eines Administrators zugewiesen.
3. Geben Sie einen Benutzernamen und ein Passwort ein und bestätigen Sie Ihre Eingabe; damit legen Sie ein neues Projekt an.
4. Es wurde automatisch der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" eingeblendet. Konfigurieren Sie jetzt Ihren Produkttyp, die Baugruppe und das Firmwarerelease.

5. Geben Sie in das Feld für die "MAC-Adresse" im Bereich "Konfiguration" die auf dem Modul-Gehäuse aufgedruckte MAC-Adresse im vorgegebenen Format ein.
   Sie finden diese Adresse auf der Frontseite des SCALANCE S-Moduls (siehe Bild).



6. Geben Sie die externe IP-Adresse und die externe Subnetzmaske im Bereich "Konfiguration" in die dafür vorgesehen Felder ein und bestätigen Sie den Dialog mit "OK". Daraufhin wird Ihr Modul in die Liste der konfigurierten Module aufgenommen.
7. Selektieren Sie Ihr Modul und geben Sie ggf. die IP-Adresse des Default-Routers ein indem Sie in die Spalte "Default Router" klicken.



optional: Projektieren Sie ggf. weitere Eigenschaften des Moduls und der Modulgruppen.

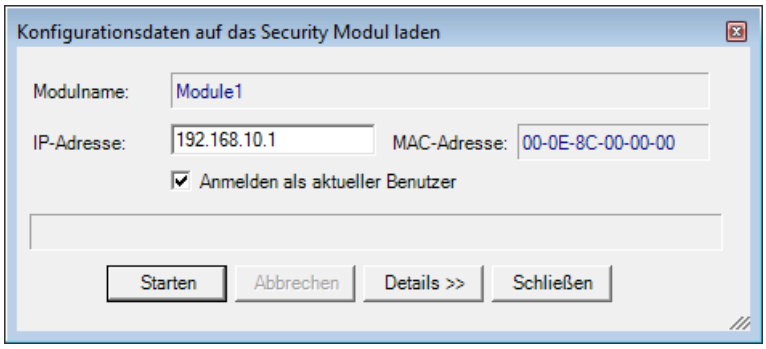
8. Speichern Sie das Projekt jetzt mit folgendem Menübefehl unter einem zweckmäßigen Namen ab:

   Projekt ▸ Speichern unter…

9. Wählen Sie folgenden Menübefehl:

   Übertragen ▸ An Modul...

   Der folgende Transfer-Dialog erscheint.



10. Durch Klicken auf die Schaltfläche "Starten" übertragen Sie die Konfiguration in das SCALANCE S-Modul.

    Ergebnis: Das SCALANCE S-Modul ist jetzt konfiguriert und kann auf IP-Ebene kommunizieren. Dieser Betriebszustand wird von der Fault-Anzeige-LED durch grünes Licht signalisiert.

2.4 C-PLUG (Configuration-Plug)

Anwendungsbereich

Der C-PLUG ist ein Wechselmedium zur Sicherung der Konfigurations- bzw. Projektierungsdaten des Grundgerätes (SCALANCE S). Dadurch stehen die Konfigurationsdaten bei einem Austausch des Grundgerätes weiterhin zur Verfügung.

Funktionsprinzip

Die Energie-Versorgung erfolgt durch das Grundgerät. Der C-PLUG behält in stromlosem Zustand alle Daten dauerhaft.

Einsetzen in C-PLUG Steckplatz

Der Steckplatz für den C-PLUG befindet sich auf der Geräterückseite. Zum Einsetzen des C-PLUG gehen Sie so vor:

1. Entfernen Sie den M32-Schraubdeckel.

2. Schieben Sie den C-PLUG in den vorgesehenen Schacht.
3. Verschließen Sie anschließend den Schacht mit dem M32-Schraubdeckel.

ACHTUNG
Betriebszustand beachten
Der C-PLUG darf nur im spannungslosen Zustand gesteckt oder gezogen werden!

Bild 2-7 C-PLUG in das Gerät einsetzen und C-PLUG mit Hilfe eines Schraubendrehers aus dem Gerät entnehmen

Funktion

Auf einem unbeschriebenen C-PLUG (Werkszustand) werden beim Geräteanlauf automatisch alle Konfigurationsdaten des SCALANCE S gesichert. Ebenso werden Änderungen der Konfiguration im laufenden Betrieb ohne Bedienereingriff auf dem C-PLUG gesichert.

Ein Grundgerät mit gestecktem C-PLUG verwendet beim Anlauf automatisch die Konfigurationsdaten eines gesteckten C-PLUG. Voraussetzung hierfür ist, dass die Daten von einem kompatiblen Gerätetyp geschrieben wurden.

Somit wird im Fehlerfall ein schneller und einfacher Austausch des Grundgerätes ermöglicht. Im Ersatzteilfall wird der C-PLUG aus der ausgefallenen Komponente entnommen und in das Ersatzteil gesteckt. Das Ersatzgerät verfügt nach Erstanlauf automatisch über die gleiche Gerätekonfiguration wie das ausgefallene Gerät.

Hinweis

Konsistente Projektdaten - MAC-Adresse anpassen

Die Projektierdaten sollten nach dem Austausch des Gerätes gegen ein Ersatzgerät insgesamt konsistent sein. Dazu sollten Sie die MAC-Adresse in der Projektierung an die auf dem Ersatzgerät aufgedruckte MAC-Adresse anpassen.

Wenn Sie im Ersatzgerät den bereits konfigurierten C-PLUG des ausgetauschten Gerätes verwenden, ist diese Maßnahme für den Anlauf und den Betrieb des Gerätes jedoch nicht zwingend erforderlich.

ACHTUNG

Rücksetzen auf Werkseinstellungen

Ist beim Rücksetzen auf Werkseinstellungen ein C-PLUG gesteckt, dann wird der C-PLUG gelöscht!

Verwenden eines nicht neuen C-PLUG

Verwenden Sie nur C-PLUGs, die für den jeweiligen SCALANCE S-Modultyp formatiert sind. Bereits in anderen Gerätetypen verwendete und für diese Gerätetypen formatierte C-PLUGs dürfen Sie nicht verwenden.

Entnehmen Sie der folgenden Tabelle, welchen C-Plug Sie für welchen SCALANCE S-Modultyp verwenden dürfen:

SCALANCE S-Modultyp	C-Plug formatiert von		
	S602	S612	S613
S602	x	-	-
S612	-	x	x *)
S613	-	x	x

- **x** C-Plug mit dem Modultyp verwendbar
- **-** C-Plug nicht mit dem Modultyp verwendbar
- ***)** Kompatibilität ist abhängig vom Mengengerüst.

Entnehmen des C-PLUG

Das Entnehmen des C-PLUG ist nur beim Ausfall (Hardwarefehler) des Grundgerätes notwendig.

ACHTUNG
Betriebszustand beachten
Der C-PLUG darf nur im spannungslosen Zustand entnommen werden !

Diagnose

Das Stecken eines C-PLUG, der die Konfiguration eines nicht kompatiblen Gerätetyps enthält sowie das unbeabsichtigte Entfernen des C-PLUG oder allgemeine Fehlfunktionen des C-PLUG werden über die Diagnosemechanismen des Endgerätes (Fault-Anzeige-LED rot) signalisiert.

2.5 Firmware übertragen

Neue Firmware-Ausgabestände können Sie mit dem Projektierungstool Security Configuration Tool in die SCALANCE S-Module laden.

Voraussetzungen

Zum Übertragen einer neuen Firmware auf ein SCALANCE S-Modul müssen folgende Voraussetzungen erfüllt sein:

- Sie müssen Administrator-Rechte für das Projekt besitzen;
- SCALANCE S muss mit einer IP-Adresse projektiert sein.

Die Übertragung ist sicher

Das Übertragen der Firmware erfolgt über eine gesicherte Verbindung und kann deshalb auch aus dem ungeschützten Netzwerk vorgenommen werden.

Die Firmware selbst ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur authentische Firmware auf das SCALANCE S-Modul geladen werden kann.

Die Übertragung kann im laufenden Betrieb vorgenommen werden

Die Übertragung der Firmware kann im laufenden Betrieb eines SCALANCE S-Moduls erfolgen. Die Kommunikation wird jedoch für die Dauer nach dem Ladevorgang bis zum automatisch abgelaufenen Neustart von SCALANCE S unterbrochen. Eine neu geladene Firmware wird erst nach diesem Neustart des SCALANCE S-Moduls aktiv.

Wurde die Übertragung gestört und abgebrochen, so startet die Baugruppe wieder mit dem alten Firmwarestand.

So führen Sie die Übertragung durch

Wählen Sie folgenden Menübefehl:

Übertragen ▸ Firmware übertragen...

GETTING STARTED 3

Schnell zum Ziel mit GETTING STARTED

Anhand eines einfachen Test-Netzwerkes lernen Sie hier den Umgang mit SCALANCE S und dem Projektierwerkzeug Security Configuration Tool kennen. Sie sehen, wie sich bereits ohne großen Projektieraufwand die Schutzfunktionen von SCALANCE S im Netz realisieren lassen.

Sie können hierbei an unterschiedlichen Sicherheits-Beispielen die Grundfunktionen von SCALANCE S / SOFTNET Security Client realisieren:

- Mit SCALANCE S612 / S613:
  - Konfiguration eines VPN mit SCALANCE S als IPsec-Tunnel-Endpunkte
  - Konfiguration eines VPN mit SCALANCE S und SOFTNET Security Client als IPsec-Tunnel-Endpunkte
- Mit allen SCALANCE S Modulen:
  - Konfiguration von SCLANCE S als Firewall
  - Konfiguration von SCALANCE S als NAT/NAPT-Router und Firewall
- Mit SOFTNET Security Client
  - Konfiguration eines VPN mit SCALANCE S und SOFTNET Security Client als IPsec-Tunnel-Endpunkte
  - Konfiguration eines VPN mit MD741-1 und SOFTNET Security Client als IPsec-Tunnel-Endpunkte

Wenn Sie mehr wissen möchten

Weitere Informationen entnehmen Sie bitte den Folgekapiteln in diesem Handbuch. Dort wird die gesamte Funktionalität detaillierter beschrieben.

Hinweis

Die in den Beispielen verwendeten IP-Einstellungen sind frei gewählt und funktionieren im isolierten Test-Netz konfliktfrei.

Im realen Netzverbund müssen Sie diese IP-Einstellungen der Netzwerkumgebung anpassen, um eventuelle Adress-Konflikte zu vermeiden.

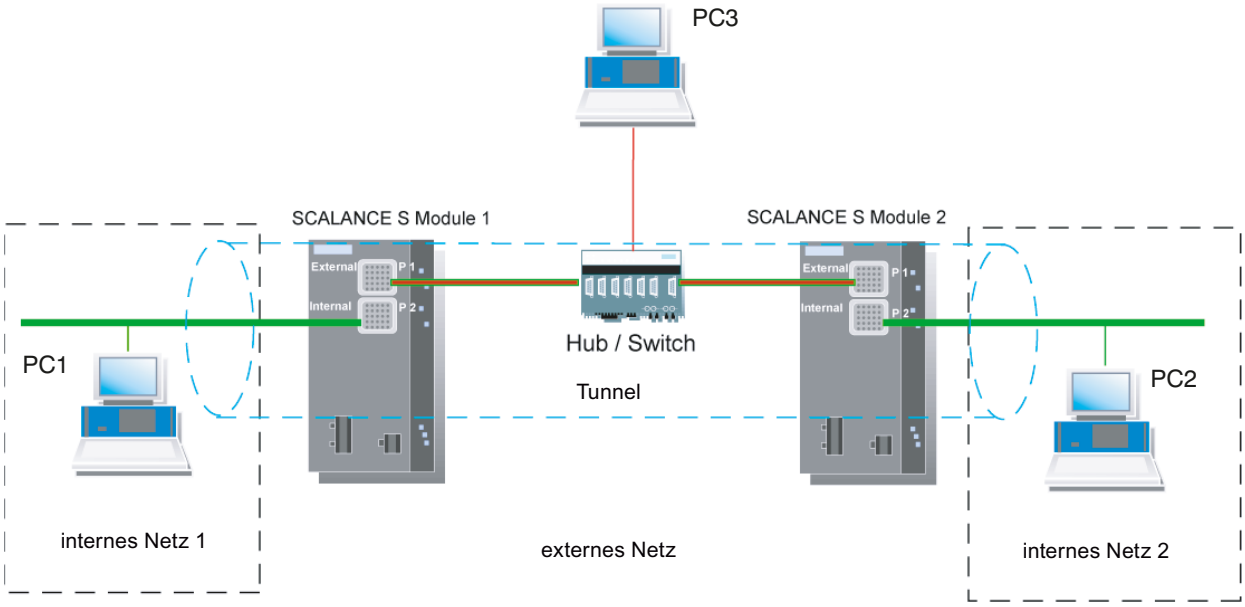
3.1 Beispiel 1: VPN-Tunnel - IPsec-Tunnel-Beispiel mit SCALANCE S612 / S613

3.1.1 Übersicht

In diesem Beispiel wird die Tunnelfunktion in der Projektierungssicht "Standard-Modus" projektiert. SCALANCE S-Modul 1 und SCALANCE S-Modul 2 bilden in diesem Beispiel die beiden Tunnelendpunkte für die gesicherte Tunnelverbindung.

Sie erreichen mit dieser Konfiguration, dass IP-Verkehr und Layer-2-Verkehr (lediglich Bridge-Modus) nur über die eingerichteten Tunnelverbindungen zwischen autorisierten Partnern möglich ist.

Aufbau des Testnetzes



- Internes Netzwerk - Anschluss an SCALANCE S Port 2 ("Internal Network"-Port)

  Im internen Netzwerk wird im Testaufbau der Netzknoten jeweils durch einen PC realisiert, der an den "Internal Network"-Port (Port 2, grün) eines SCALANCE S-Moduls angeschlossen ist.

  – PC1: Repräsentiert einen Teilnehmer des internen Netzwerks 1
  – PC2: Repräsentiert einen Teilnehmer des internen Netzwerks 2
  – SCALANCE S-Modul 1: SCALANCE S-Modul für das interne Netzwerk 1
  – SCALANCE S-Modul 2: SCALANCE S-Modul für das interne Netzwerk 2

- Externes Netzwerk - Anschluss an SCALANCE S Port 1 ("External Network"-Port)

  Das öffentliche, externe Netzwerk wird an den "External Network"-Port (Port 1, rot) eines SCALANCE S-Moduls angeschlossen.

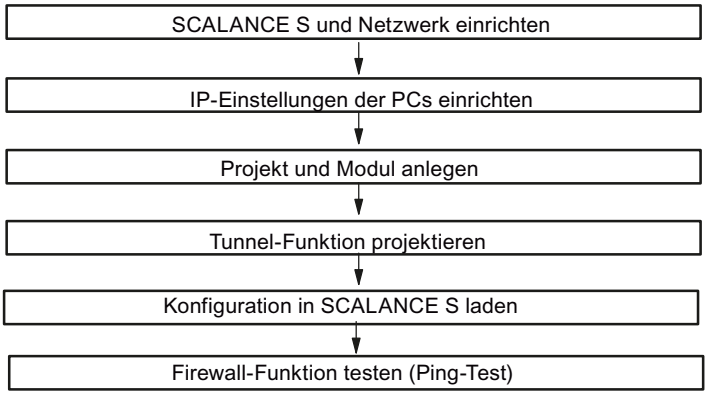
  PC3: PC mit der Konfigurationssoftware Security Configuration Tool

Erforderliche Geräte/Komponenten:

Für den Aufbau verwenden Sie folgende Komponenten:

- 2x SCALANCE S-Modul, (optional: eine oder zwei entsprechend montierte Hutschienen mit Montagematerial);
- 1x bzw. 2x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker (beide Module können auch aus einer gemeinsamen Stromversorgung betrieben werden);
- 1x PC auf dem das Projektierungswerkzeug "Security Configuration Tool" installiert ist;
- 2x PC in den internen Netzwerken für den Test der Konfiguration;
- 1x Netzwerk-Hub bzw. -Switch zum Aufbau der Netzwerkverbindungen mit den beiden SCALANCE S sowie den PCs/PGs;
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet.

Die folgenden Schritte in der Übersicht:



3.1.2 SCALANCE S und Netzwerk einrichten

Gehen Sie wie folgt vor:

1. Packen Sie zunächst die SCALANCE S Geräte aus und überprüfen Sie den unbeschädigten Zustand.
2. Schließen Sie die Spannungsversorgung an SCALANCE S an.

Ergebnis: Nach dem Anschließen der Betriebsspannung leuchtet die Fault-LED (F) gelb.

⚠ WARNUNG

Das Gerät SCALANCE S ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

Das Netzteil für die Versorgung des SCALANCE S muss NEC Class 2 entsprechen (Spannungsbereich 18-32 V, Strombedarf ca. 250 mA).

Beachten Sie für Montage und Anschluss der SCALANCE S-Module das Kapitel 2 "Produkteigenschaften und Inbetriebnahme".

1. Stellen Sie jetzt die physikalischen Netzwerkverbindungen her, indem Sie die Stecker der Netzwerkkabel in die dafür vorgesehenen Ports (RJ45-Buchsen) stecken:
   - Verbinden Sie PC1 mit Port 2 von Modul 1 und PC2 mit Port 2 von Modul 2.
   - Verbinden Sie Port 1 von Modul 1 und Port 1 von Modul 2 mit dem Hub/Switch.
   - Verbinden Sie PC3 ebenfalls mit dem Hub/Switch.
2. Schalten Sie jetzt die beteiligten PCs ein.

ACHTUNG

Die Ethernet-Anschlüsse an Port 1 und Port 2 werden vom SCALANCE S unterschiedlich behandelt und dürfen deshalb beim Anschluss an das Kommunikationsnetzwerk nicht verwechselt werden:

- Port 1 - External Network
  obere RJ45-Buchse, rote Markierung = ungeschützter Netzwerk-Bereich;
- Port 2 - Internal Network
  untere RJ45-Buchse, grüne Markierung = durch SCALANCE S geschütztes Netzwerk;

Beim Vertauschen der Ports verliert das Gerät seine Schutzfunktion.

3.1.3 IP-Einstellungen der PCs einrichten

Die PCs sollten für den Test folgende IP-Adresseinstellungen erhalten:

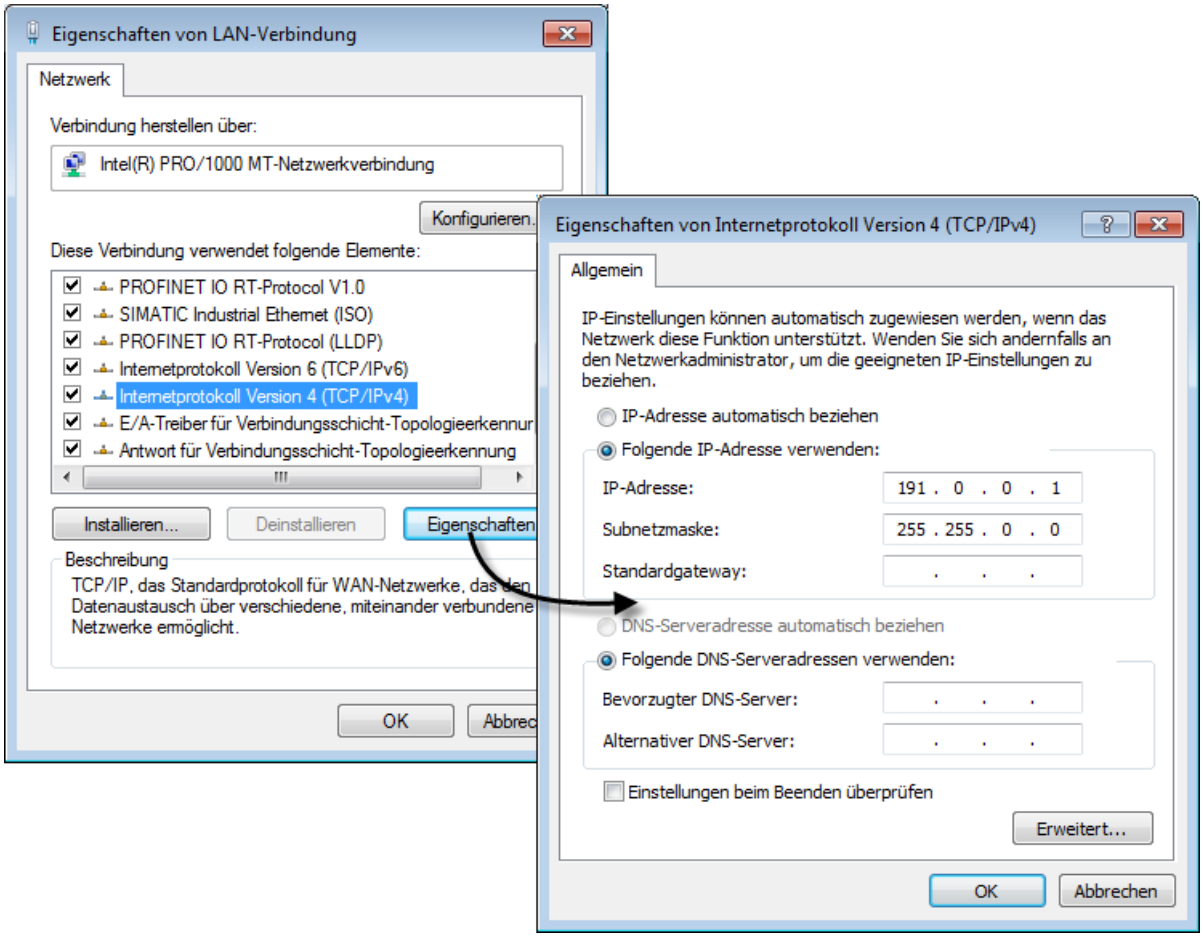
PC	IP-Adresse	Subnetzmaske
PC1	191.0.0.1	255.255.0.0
PC2	191.0.0.2	255.255.0.0
PC3	191.0.0.3	255.255.0.0

Gehen Sie jeweils bei PC1, PC2 und PC3 folgendermaßen vor:

1. Öffnen Sie auf dem betreffenden PC die Systemsteuerung mit folgendem Menübefehl:

   Start ▸ Systemsteuerung

2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4(TCP/IPv4)" und klicken Sie die Schaltfläche "Eigenschaften".



4. Wählen Sie im Dialog "Eigenschaften von Internetprotokoll Version 4(TCP/IPv4)" das Optionsfeld "Folgende IP-Adresse verwenden:" aus und geben Sie jetzt die dem PC zugeordneten Werte aus der Tabelle "*IP-Einstellungen der PCs einrichten*" in die dafür vorgesehenen Felder ein.

   Schließen Sie die Dialoge mit "OK" ab und verlassen Sie die Systemsteuerung.

3.1.4 Projekt und Module anlegen

Gehen Sie so vor:

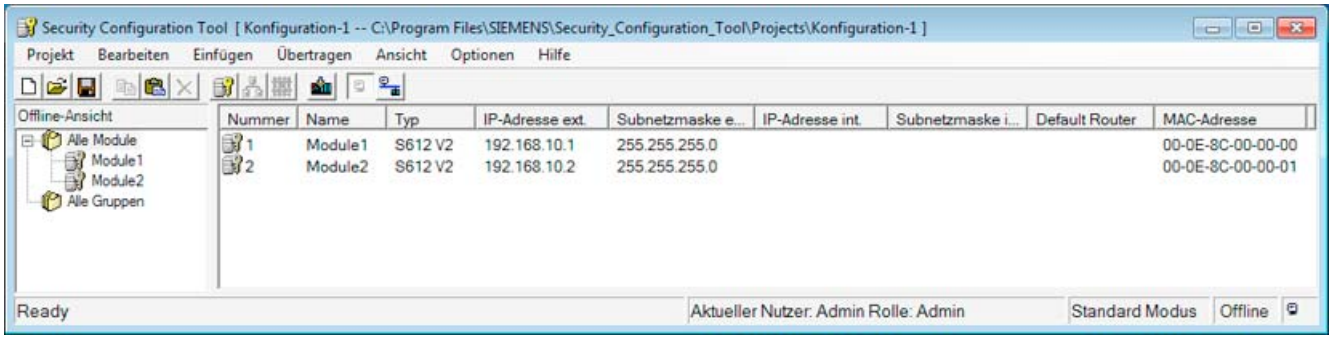
1. Starten Sie die Projektierungssoftware Security Configuration Tool auf PC3.
2. Erzeugen Sie ein neues Projekt mit folgendem Menübefehl:

   Projekt ▸ Neu

   Sie werden aufgefordert einen Benutzernamen und ein Passwort anzugeben. Dem Benutzereintrag, den Sie hierbei festlegen, wird die Rolle eines Administrators zugewiesen.
3. Geben Sie einen Benutzernamen und ein Passwort ein und bestätigen Sie Ihre Eingabe; damit legen Sie ein neues Projekt an.
4. Es wurde automatisch der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" eingeblendet. Konfigurieren Sie jetzt Ihren Produkttyp, die Baugruppe und das Firmwarerelease und schließen Sie am Ende den Dialog mit "OK".
5. Erzeugen Sie ein zweites Modul mit folgendem Menübefehl:
   Einfügen ▸ Modul

   Konfigurieren Sie jetzt Ihren Produkttyp, die Baugruppe und das Firmwarerelease und scließen Sie am Ende den Dialog mit "OK".

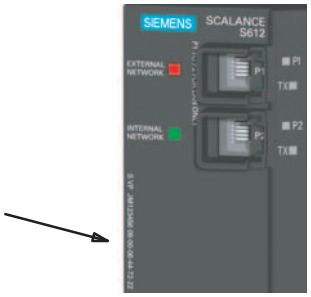
   Dieses Modul erhält automatisch einen Namen entsprechend den Voreinstellungen für das Projekt und ebenfalls voreingestellte Parameterwerte. Die IP-Adresse ist gegenüber "Module1" weitergezählt, also unterschiedlich.



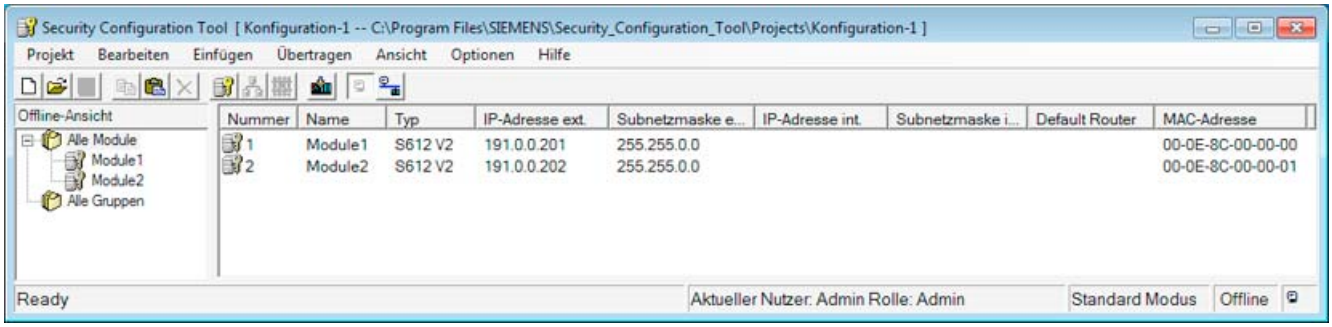
6. Klicken Sie im Navigationsbereich auf "Alle Module" und anschließend im Inhaltsbereich auf die Zeile mit "Module1".

7. Klicken Sie jetzt in die Spalte "MAC-Adresse" und geben Sie diese im vorgegebenen Format ein.

   Sie finden diese Adresse auf der Frontseite des SCALANCE S-Moduls (siehe Bild).



8. Klicken Sie jetzt in die Spalte "IP-Adresse ext." und geben Sie diese im vorgegebenen Format ein und passen Sie ebenso die Subnetzmaske an.
   - für Modul 1: IP-Adresse: 191.0.0.201 Subnetzmaske: 255.255.0.0
   - für Modul 2: IP-Adresse: 191.0.0.202 Subnetzmaske: 255.255.0.0



9. Wiederholen Sie die Schritte 6. bis 8. mit "Module 2".

3.1.5 Tunnelverbindung projektieren

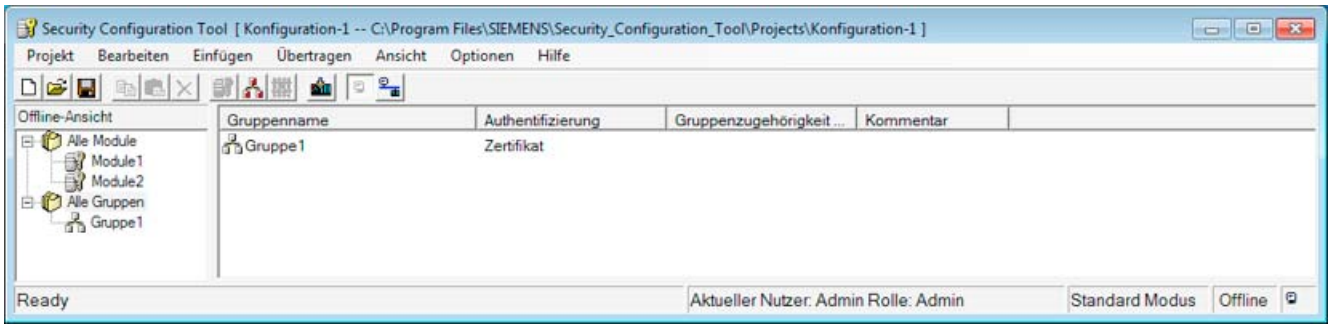
Zwei SCALANCE S können genau dann einen IPsec-Tunnel für die gesicherte Kommunikation aufbauen, wenn sie im Projekt der gleichen Gruppe zugeordnet sind.

Gehen Sie so vor:

1. Selektieren Sie im Navigationsbereich "Alle Gruppen" und erzeugen Sie mit folgendem Menübefehl eine neue Gruppe:

Einfügen ▸ Gruppe

Diese Gruppe erhält automatisch den Namen "Gruppe1".



2. Selektieren Sie im Inhaltsbereich das SCALANCE S-Modul "Module1" und ziehen Sie es auf "Gruppe1" im Navigationsbereich.

   Das Modul ist jetzt dieser Gruppe zugeordnet bzw. Mitglied dieser Gruppe.

   Die Farbe des Schlüsselsymbols des Modul-Icons schlägt hierbei von grau nach blau um.

3. Selektieren Sie im Inhaltsbereich das SCALANCE S-Modul "Module 2" und ziehen Sie es auf "Gruppe1" im Navigationsbereich.

   Das Modul ist jetzt ebenso dieser Gruppe zugeordnet.

4. Speichern Sie dieses Projekt jetzt mit dem folgenden Menübefehl unter einem zweckmäßigen Namen ab:

   Projekt ▸Speichern unter...

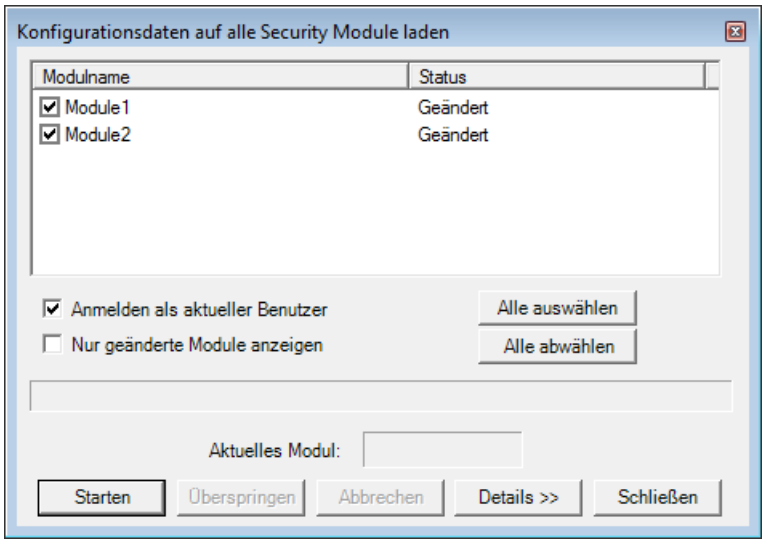
Die Konfiguration der Tunnelverbindung ist damit abgeschlossen.

3.1.6 Konfiguration in SCALANCE S laden

Gehen Sie so vor:

1. Rufen Sie mit folgendem Menübefehl den folgenden Dialog auf:

Übertragen ▸ An alle Module…



2. Selektieren Sie beide Module über die Schaltfläche "Alle auswählen".
3. Starten Sie den Ladevorgang über die Schaltfläche "Starten".

Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das SCALANCE S automatisch neu gestartet und die neue Konfiguration aktiviert.

Ergebnis: SCALANCE S im Produktivbetrieb

SCALANCE S befindet sich jetzt im Produktivbetrieb. Dieser Betriebszustand wird von der Fault-Anzeige-LED durch grünes Licht signalisiert.

Die Inbetriebsetzung der Konfiguration ist damit abgeschlossen und die beiden SCALANCE S können einen Kommunikationstunnel aufbauen, über den Netzknoten aus den beiden internen Netzwerken gesichert kommunizieren können.

3.1.7 Tunnelfunktion testen (Ping-Test)

Wie können Sie die konfigurierte Funktion testen ?

Die Funktionstests können Sie wie nachfolgend beschrieben mit einem Ping-Kommando durchführen.

Alternativ können Sie auch andere Kommunikationsprogramme für den Test der Konfiguration verwenden.

ACHTUNG
Bei Windows kann die Firewall standardmäßig so eingestellt sein, dass PING-Kommandos nicht passieren können. Sie müssen ggf. die ICMP-Dienste vom Typ Request und Response freischalten.

Testabschnitt 1

Testen Sie nun die Funktion der zwischen PC1 und PC2 aufgebauten Tunnelverbindung wie folgt:

1. Rufen Sie auf dem PC2 in der Startleiste den folgenden Menübefehl auf:

   Start ▸ Alle Programme ▸ Zubehör ▸ Eingabeaufforderung

2. Eingabe des Ping-Kommandos von PC1 an den PC2 (IP-Adresse 191.0.0.2)

   Unmittelbar in die Kommandozeile des aufgeblendeten Fensters "Eingabeaufforderung", an der Cursor-Position, geben Sie den Befehl

   ping 191.0.0.2

   ein.

   Sie erhalten daraufhin folgende Meldung: (positive Antwort von PC2).

Ergebnis

Wenn die IP-Telegramme PC2 erreicht haben, gibt die "Ping-Statistik" für 191.0.0.2 folgendes aus:

- Gesendet = 4
- Empfangen = 4
- Verloren = 0 (0% Verlust)

Da keine andere Kommunikation zugelassen war, können diese Telegramme nur durch den VPN-Tunnel transportiert worden sein.

Testabschnitt 2

Wiederholen Sie nun den Test , indem Sie ein Ping-Kommando von PC3 aus absetzen.

1. Rufen Sie auf dem PC3 in der Startleiste den folgenden Menübefehl auf:

Start ► Alle Programme ► Zubehör ► Eingabeaufforderung

2. Setzen Sie erneut das gleiche Ping-Kommando (**ping 191.0.0.2**) im Fenster der Eingabeaufforderung von PC3 aus ab.

   Sie erhalten daraufhin folgende Meldung: (keine Antwort von PC2).

Ergebnis

Die IP-Telegramme von PC3 können PC2 nicht erreichen, da weder eine Tunnelkommunikation zwischen diesen Geräten konfiguriert ist, noch normaler IP-Datenverkehr erlaubt ist.

Das wird in der "Ping-Statistik" für 191.0.0.2 folgendermaßen angegeben:

- Gesendet = 4
- Empfangen = 0
- Verloren = 4 (100% Verlust)

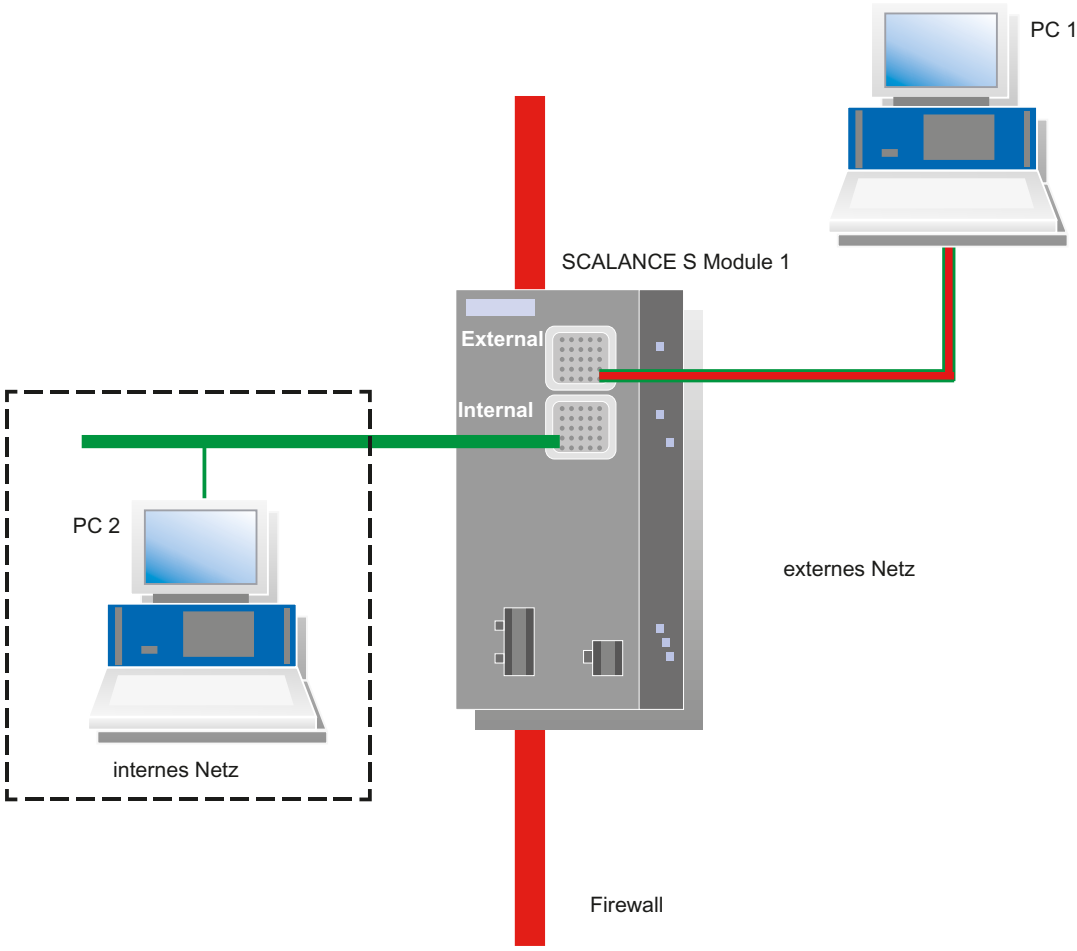
3.2 Beispiel 2: Firewall - SCALANCE S als Firewall betreiben

3.2.1 Übersicht

In diesem Beispiel projektieren Sie die Firewall in der Projektierungssicht "Standard-Modus". Der Standard-Modus beinhaltet vordefinierte Regelsätze für den Datenverkehr.

Sie erreichen mit dieser Konfiguration, dass IP-Verkehr nur vom internen Netz initiiert werden kann; aus dem externen Netz wird nur die Antwort zugelassen.

Aufbau des Testnetzes



- Internes Netzwerk - Anschluss an SCALANCE S Port 2

  Im internen Netzwerk wird im Testaufbau der Netzknoten durch einen PC realisiert, der an den "Internal Network"-Port (Port 2, grün) eines SCALANCE S-Moduls angeschlossen ist.

  – PC2: Repräsentiert einen Teilnehmer des internen Netzwerks

  – SCALANCE S-Modul 1: SCALANCE S-Modul für das interne Netzwerk

- Externes Netzwerk - Anschluss an SCALANCE S Port 1

  Das öffentliche, externe Netzwerk wird an den "External Network"-Port (Port 1, rot) eines SCALANCE S-Moduls angeschlossen.

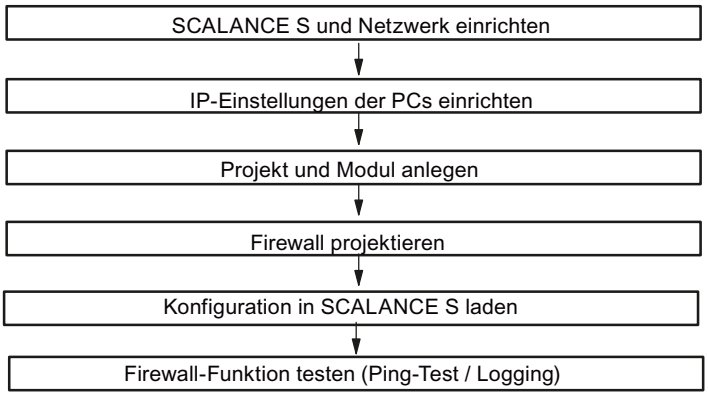
  – PC1: PC mit der Konfigurationssoftware Security Configuration Tool

Erforderliche Geräte/Komponenten:

Für den Aufbau verwenden Sie folgende Komponenten:

- 1x SCALANCE S, (zusätzlich optional: eine entsprechend montierte Hutschiene mit Montagematerial)
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker
- 1x PC auf dem das Projektierungswerkzeug Security Configuration Tool installiert ist
- 1x PC im internen Netz für den Test der Konfiguration
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet

Die folgenden Schritte in der Übersicht:



3.2.2 SCALANCE S und Netzwerk einrichten

Gehen Sie so vor:

1. Packen Sie zunächst das SCALANCE S aus und überprüfen Sie den unbeschädigten Zustand.
2. Schließen Sie die Spannungsversorgung an SCALANCE S an.

   Ergebnis: Nach dem Anschließen der Betriebsspannung leuchtet die Fault-LED (F) gelb.

⚠ WARNUNG

Das Gerät SCALANCE S ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

Das Netzteil für die Versorgung des SCALANCE S muss NEC Class 2 entsprechen (Spannungsbereich 18-32 V, Strombedarf ca. 250 mA).

Beachten Sie für Montage und Anschluss der SCALANCE S-Module das Kapitel 2 "Produkteigenschaften und Inbetriebnahme"

3. Stellen Sie jetzt die physikalischen Netzwerkverbindungen her, indem Sie die Stecker der Netzwerkkabel in die dafür vorgesehenen Ports (RJ45-Buchsen) stecken:
   – Verbinden Sie PC2 mit Port 2 von Modul 1.
   – Verbinden Sie PC1 mit Port 1 von Modul 1.
4. Schalten Sie jetzt die beteiligten PCs ein.

ACHTUNG

Die Ethernet-Anschlüsse an Port 1 und Port 2 werden vom SCALANCE S unterschiedlich behandelt und dürfen deshalb beim Anschluss an das Kommunikationsnetzwerk nicht verwechselt werden:

- Port 1 - External Network
  obere RJ45-Buchse, rote Markierung = ungeschützter Netzwerk-Bereich;
- Port 2 - Internal Network
  untere RJ45-Buchse, grüne Markierung = durch SCALANCE S geschütztes Netzwerk;

Beim Vertauschen der Ports verliert das Gerät seine Schutzfunktion.

3.2.3 IP-Einstellungen der PCs einrichten

Die PCs sollten für den Test folgende IP-Adresseinstellungen erhalten:

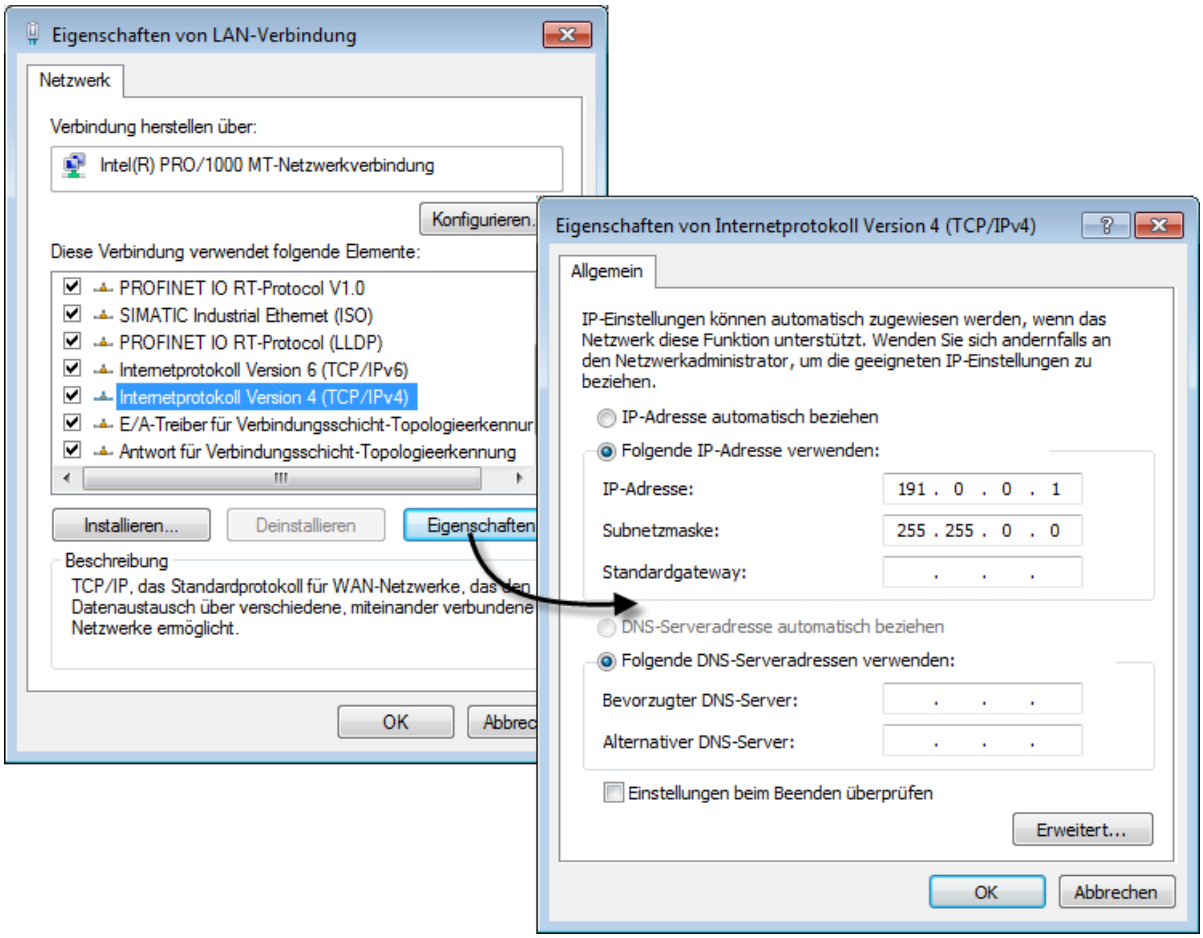
PC	IP-Adresse	Subnetzmaske
PC1	191.0.0.1	255.255.0.0
PC2	191.0.0.2	255.255.0.0

Gehen Sie dazu jeweils bei PC1und PC2 folgendermaßen vor:

1. Öffnen Sie auf dem betreffenden PC die Systemsteuerung mit folgendem Menübefehl:

Start ▸ Systemsteuerung

2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4(TCP/IPv4)" und klicken Sie die Schaltfläche "Eigenschaften".



4. Wählen Sie im Dialog "Eigenschaften von Internetprotokoll Version 4(TCP/IPv4)" das Optionsfeld "Folgende IP-Adresse verwenden:" aus und geben Sie jetzt die dem PC zugeordneten Werte aus der Tabelle "*IP-Einstellungen der PCs einrichten*" in die dafür vorgesehenen Felder ein.

   Schließen Sie die Dialoge mit "OK" ab und verlassen Sie die Systemsteuerung.

3.2.4 Projekt und Modul anlegen

Gehen Sie so vor:

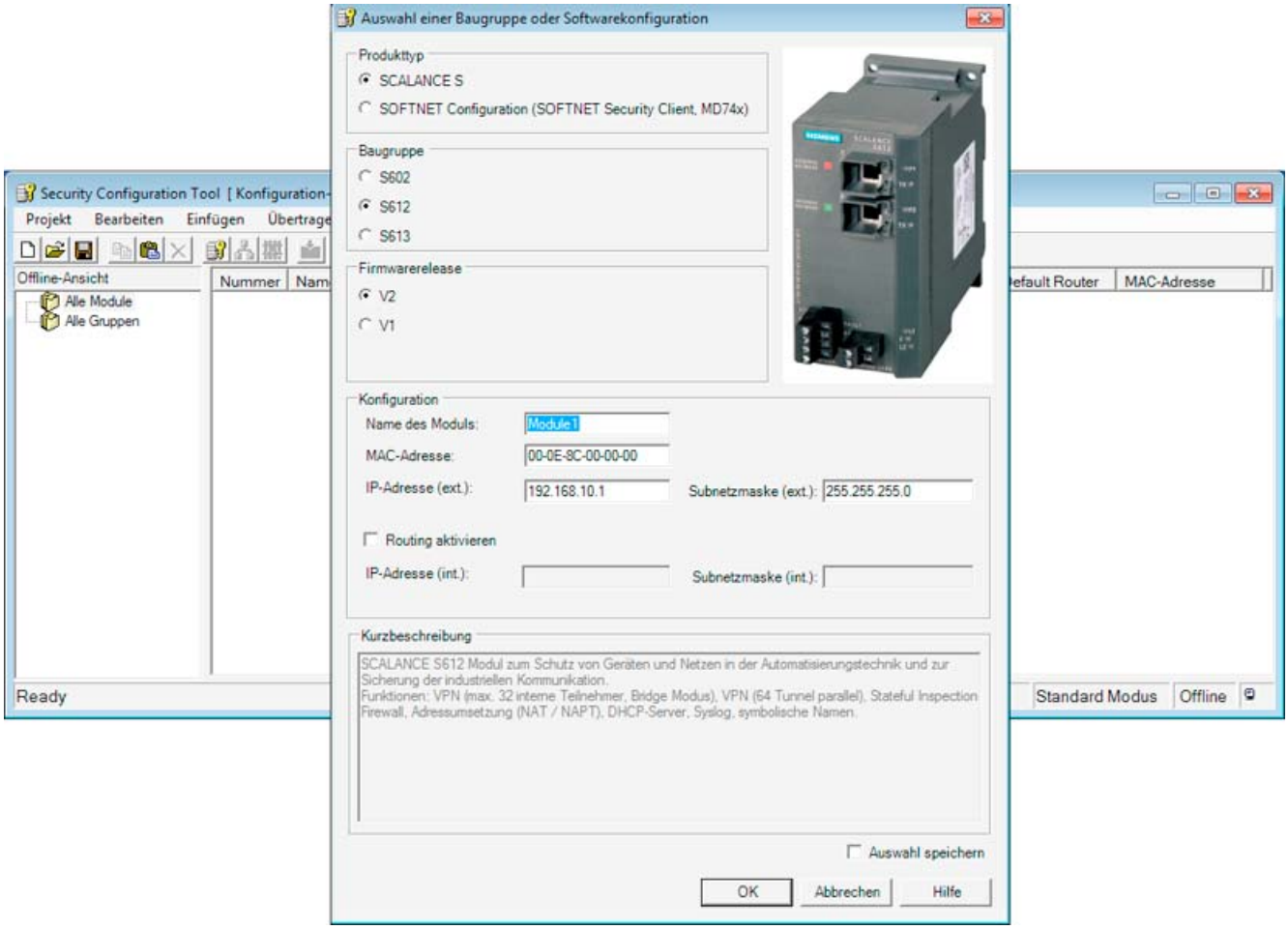
1. Installieren und starten Sie die Projektierungssoftware Security Configuration Tool auf PC1.

2. Erzeugen Sie mit folgendem Menübefehl ein neues Projekt:

   Projekt ▸ Neu

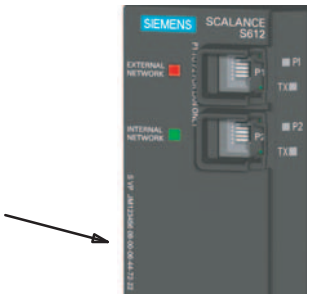
   Sie werden aufgefordert einen Benutzernamen und ein Passwort anzugeben. Dem Benutzereintrag, den Sie hierbei festlegen, wird die Rolle eines Administrators zugewiesen.

3. Geben Sie einen Benutzernamen und ein Passwort ein und bestätigen Sie Ihre Eingabe; damit legen Sie ein neues Projekt an.

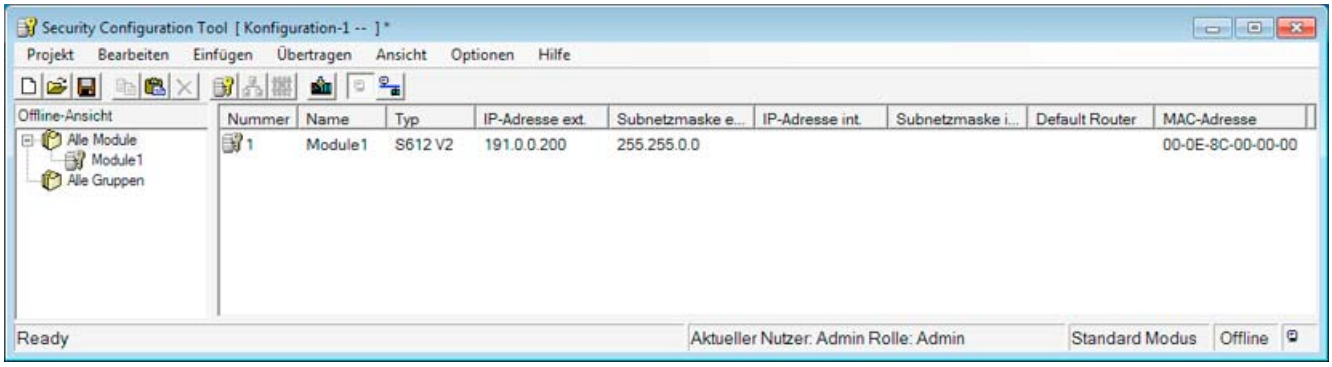


4. Es wurde automatisch der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" eingeblendet. Konfigurieren Sie jetzt Ihren Produkttyp, die Baugruppe und das Firmwarerelease.

5. Geben Sie in das Feld für die "MAC-Adresse" im Bereich "Konfiguration" die auf dem Modul-Gehäuse aufgedruckte MAC-Adresse im vorgegebenen Format ein.
   Sie finden diese Adresse auf der Frontseite des SCALANCE S-Moduls (siehe Bild).



6. Geben Sie ebenso im vorgegebenen Format die externe IP-Adresse (191.0.0.200) und die externe Subnetzmaske (255.255.0.0) ein und bestätigen Sie den Dialog mit "OK". Daraufhin wird Ihr Modul in die Liste der konfigurierten Module aufgenommen.



3.2.5 Firewall projektieren

Im Standard-Modus ist eine einfache Bedienung der Firewalleinstellungen durch vordefinierte Regelsätze gegeben. Durch Anklicken können diese Regelsätze aktiviert werden.

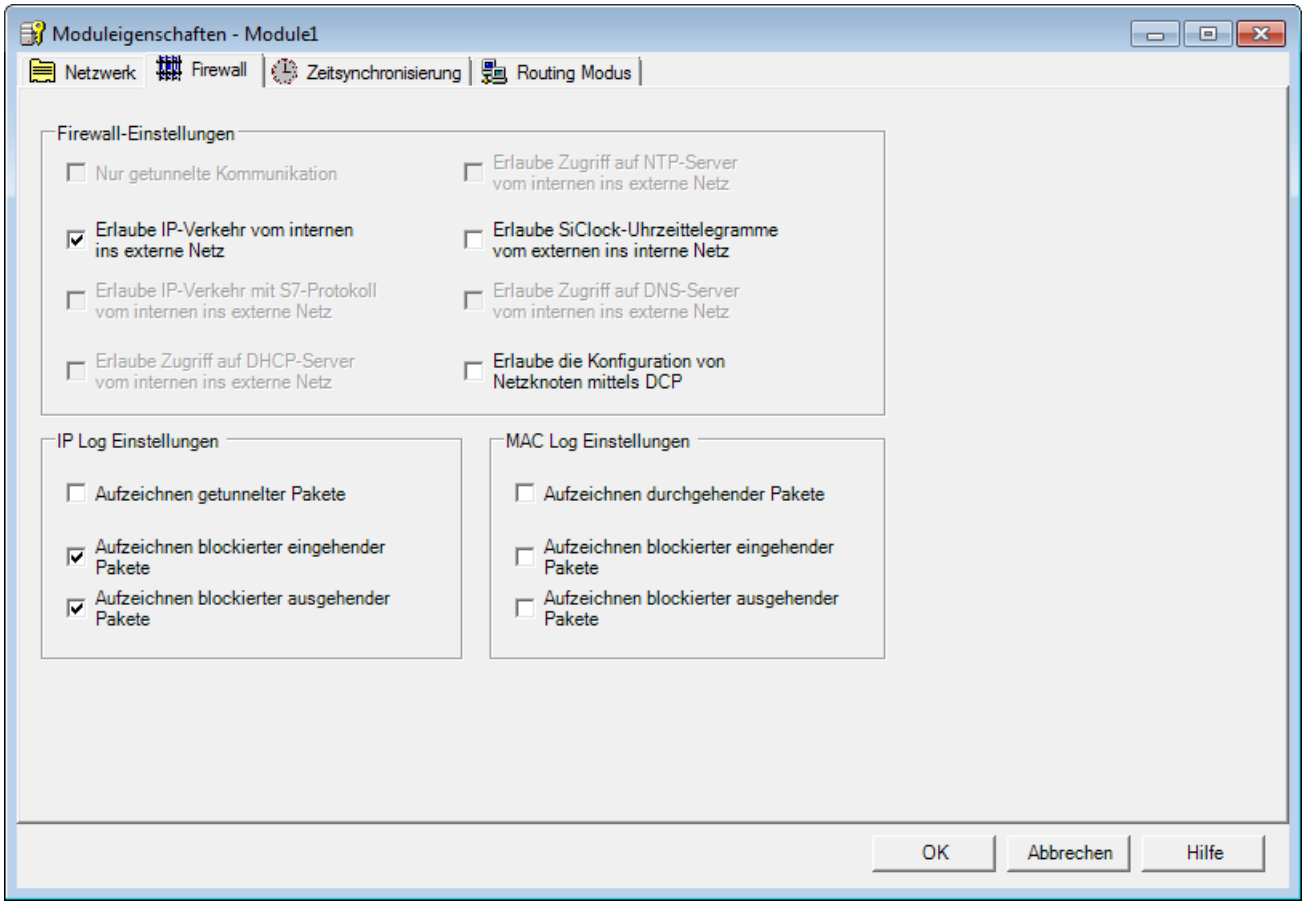
Gehen Sie so vor:

1. Markieren Sie im Inhaltsbereich die Zeile "Module1".
2. Wählen Sie folgenden Menübefehl:

   Bearbeiten ▸ Eigenschaften…

3. Wählen Sie im aufgeblendeten Dialog das Register "Firewall".

4. Schalten Sie die Option wie nachfolgend dargestellt ein:



   Sie erreichen damit, dass IP-Verkehr nur vom internen Netzwerk initiiert werden kann; aus dem externen Netzwerk wird nur die Antwort zugelassen.

5. Wählen Sie zusätzlich die Log-Optionen an, um den Datenverkehr aufzuzeichnen.
6. Schließen Sie den Dialog mit "OK" ab.
7. Speichern Sie dieses Projekt jetzt mit dem folgenden Menübefehl unter einem zweckmäßigen Namen ab:

   Projekt ▸ Speichern unter…

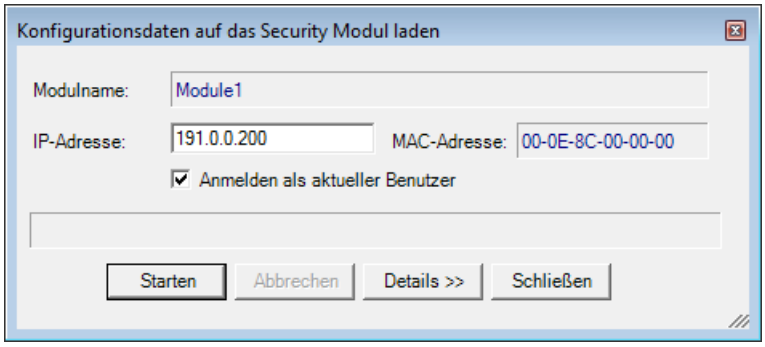
3.2.6 Konfiguration in SCALANCE S laden

Gehen Sie so vor:

1. Selektieren Sie im Inhaltsbereich das Modul.

2. Wählen Sie folgenden Menübefehl:

   Übertragen ▸ An Modul…



3. Starten Sie den Ladevorgang über die Schaltfläche "Starten".

Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das SCALANCE S-Modul automatisch neu gestartet und die neue Konfiguration aktiviert.

Ergebnis: SCALANCE S im Produktivbetrieb

SCALANCE S befindet sich jetzt im Produktivbetrieb. Dieser Betriebszustand wird von der Fault-Anzeige-LED durch grünes Licht signalisiert.

Die Inbetriebsetzung der Konfiguration ist damit abgeschlossen und SCALANCE S schützt jetzt über die eingerichtete Firewall das interne Netz (PC 2) gemäß der projektierten Regel: "Erlaube IP-Verkehr vom internen ins externe Netz".

3.2.7 Firewallfunktion testen (Ping-Test)

Wie können Sie die konfigurierte Funktion testen ?

Die Funktionstests können Sie wie nachfolgend beschrieben mit einem Ping-Kommando durchführen.

Alternativ können Sie auch andere Kommunikationsprogramme für den Test der Konfiguration verwenden.

ACHTUNG
Bei Windows kann die Firewall standardmäßig so eingestellt sein, dass PING-Kommandos nicht passieren können. Sie müssen ggf. die ICMP-Dienste vom Typ Request und Response freischalten.

Testabschnitt 1

Testen Sie nun die Funktion der Firewall-Konfiguration zunächst bei zugelassenem abgehenden IP-Datenverkehr wie folgt:

1. Rufen Sie auf dem PC2 in der Startleiste folgenden Menübefehl auf:

   Start ▸ Alle Programme ▸ Zubehör ▸ Eingabeaufforderung

2. Eingabe des Ping-Kommandos von PC2 an den PC1 (IP-Adresse 191.0.0.1)

   Geben Sie unmittelbar in die Kommandozeile des aufgeblendeten Fensters "Eingabeaufforderung", an der Cursor-Position, den folgenden Befehl ein:

   ping 191.0.0.1

   Sie erhalten daraufhin folgende Meldung: (positive Antwort von PC1).

Ergebnis

Wenn die IP-Telegramme PC1 erreicht haben, gibt die "Ping-Statistik" für 191.0.0.1 folgendes aus:

- Gesendet = 4
- Empfangen = 4
- Verloren = 0 (0% Verlust)

Die Ping-Telegramme konnten aufgrund der Projektierung vom internen Netz ins externe Netz gelangen. Der PC im externen Netz hat auf die Ping-Telegramme geantwortet. Durch die "Stateful-Inspektion"-Funktion der Firewall werden die Antworttelegramme, die nun vom externen Netz kommen, automatisch ins interne Netz weitergeleitet.

Testabschnitt 2

Testen Sie nun die Funktion der Firewall-Konfiguration bei gesperrtem abgehenden IP-Datenverkehr wie folgt:

1. Rufen Sie erneut den Firewall-Dialog, wie bereits vorher durchgeführt, auf.
2. Schalten Sie im Register "Firewall" die Option "Erlaube IP-Verkehr vom internen ins externe Netz" wieder aus.

   Schließen Sie den Dialog mit "OK".

3. Laden Sie jetzt die geänderte Konfiguration erneut auf das SCALANCE S-Modul.
4. Nach fehlerfrei durchgeführtem Ladevorgang geben Sie erneut das gleiche Ping-Kommando (**ping 191.0.0.1**) im Fenster der Eingabeaufforderung von PC2, wie bereits durchgeführt, ein.

   Sie erhalten daraufhin folgende Meldung: (keine Antwort von PC1).

Ergebnis

Die IP-Telegramme von PC2 können PC1 jetzt nicht erreichen, da der Datenverkehr aus dem "internen Netz" (PC2) zum "externen" Netz (PC1) nicht erlaubt ist.

Das wird in der "Ping-Statistik" für 191.0.0.1 folgendermaßen angegeben:

- Gesendet = 4
- Empfangen = 0
- Verloren = 4 (100% Verlust)

3.2.8 Firewall-Datenverkehr aufzeichnen (Logging)

Beim SCALANCE S ist standardmäßig die lokale Aufzeichnung von System-, Audit- und Paketfilter-Ereignissen eingeschaltet.

Zusätzlich haben Sie im Verlauf dieses Beispieles bei der Firewall-Projektierung die Log-Optionen für den gesamten Datenverkehr aktiviert.

Sie können sich daher im Online-Modus die aufgezeichneten Ereignisse ausgeben lassen.

Gehen Sie so vor:

1. Wechseln Sie jetzt auf dem PC1 im Security Configuration Tool mit folgendem Menübefehl in die Online-Betriebsart:

   Ansicht ▸ Online
2. Wählen Sie folgenden Menübefehl:

   Bearbeiten ▸ Online Diagnose…
3. Wählen Sie das Register "Paketfilter Log".

4. Betätigen Sie die Schaltfläche "Starte Lesen".
5. Quittieren Sie den aufgeblendeten Dialog mit OK.

   Ergebnis: Die Log-Einträge werden aus dem SCALANCE S ausgelesen und hier ausgegeben.

3.3 Beispiel 3: Firewall und Router - SCALANCE S als Firewall und Router betreiben

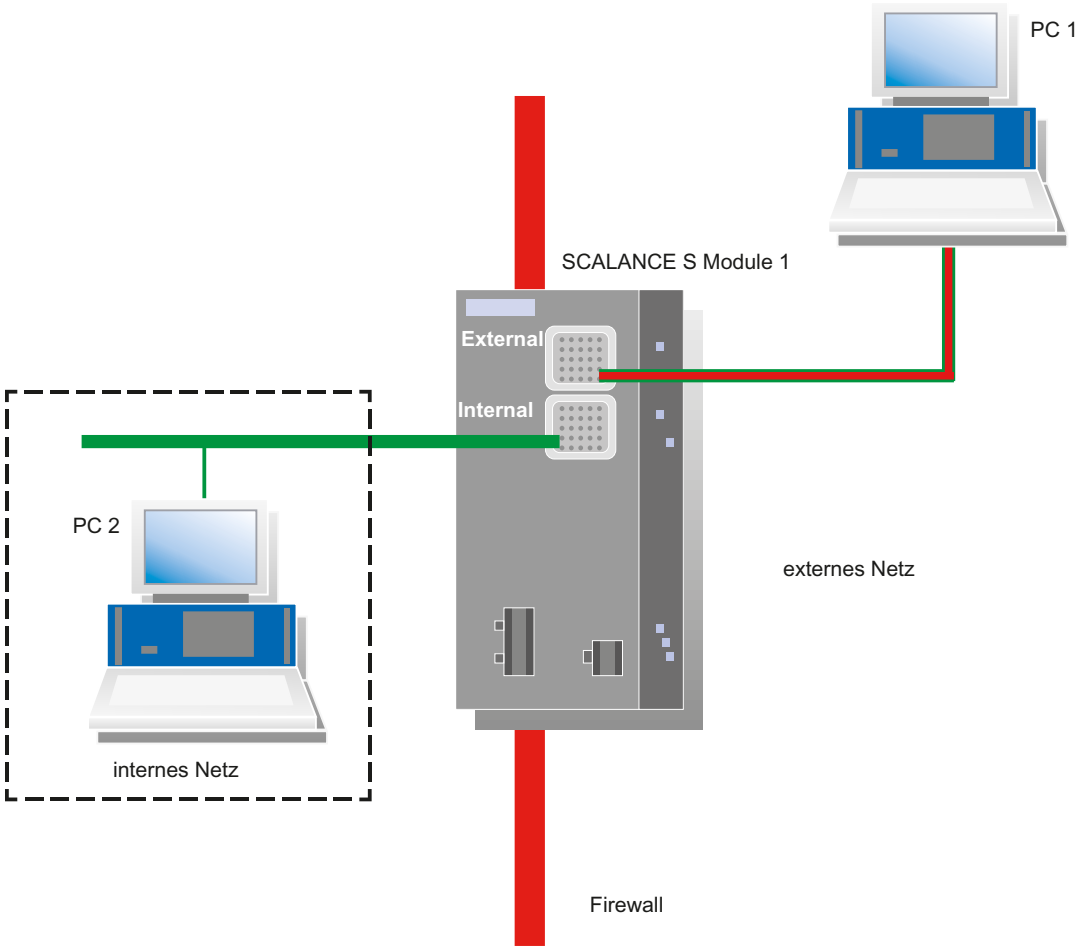
3.3.1 Übersicht

In diesem Beispiel projektieren Sie den NAT-Router-Betrieb. Die Projektierung erfolgt in der Projektierungssicht "Erweitert-Modus".

Sie erreichen mit der hier vorgestellten Konfiguration, dass alle vom internen Subnetz an den Teilnehmer PC1 im externen Netz gesendeten Telegramme die Firewall passieren können. Nach außen werden die Telegramme mit einer auf die IP-Adresse des SCALANCE S transformierten IP-Adresse sowie einer dynamisch vergebenen Port-Nummer weitergeleitet.

Aus dem externen Netz wird nur die Antwort auf diese Telegramme zugelassen.

Aufbau des Testnetzes



- Internes Netzwerk - Anschluss an SCALANCE S Port 2

  Im internen Netzwerk wird im Testaufbau der Netzknoten durch einen PC realisiert, der an den "Internal Network"-Port (Port 2, grün) eines SCALANCE S-Moduls angeschlossen ist.

  – PC2: Repräsentiert einen Teilnehmer des internen Netzwerks

  – SCALANCE S-Modul 1: SCALANCE S-Modul für das interne Netzwerk

- Externes Netzwerk - Anschluss an SCALANCE S Port 1

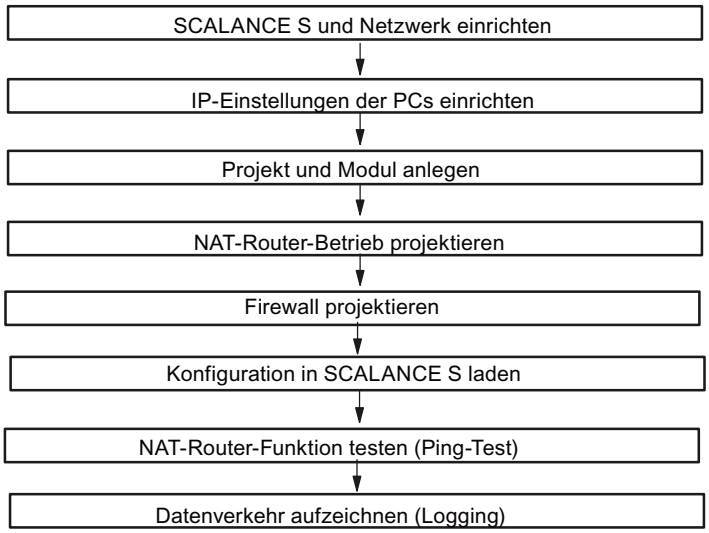
  Das öffentliche, externe Netzwerk wird an den "External Network"-Port (Port 1, rot) eines SCALANCE S-Moduls angeschlossen.
  PC1: PC mit der Konfigurationssoftware Security Configuration Tool

Erforderliche Geräte/Komponenten:

Für den Aufbau verwenden Sie folgende Komponenten:

- 1x SCALANCE S, (zusätzlich optional: eine entsprechend montierte Hutschiene mit Montagematerial);
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker;
- 1x PC auf dem das Projektierungswerkzeug Security Configuration Tool installiert ist;
- 1x PC im internen Netzwerk für den Test der Konfiguration;
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet.

Die folgenden Schritte in der Übersicht:



3.3.2 SCALANCE S und Netzwerk einrichten

Gehen Sie so vor:

1. Packen Sie zunächst das SCALANCE S aus und überprüfen Sie den unbeschädigten Zustand.
2. Schließen Sie die Spannungsversorgung an SCALANCE S an.

   Ergebnis: Nach dem Anschließen der Betriebsspannung leuchtet die Fault-LED (F) gelb.

⚠ WARNUNG

Das Gerät SCALANCE S ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

Das Netzteil für die Versorgung des SCALANCE S muss NEC Class 2 entsprechen (Spannungsbereich 18-32 V, Strombedarf ca. 250 mA).

Beachten Sie für Montage und Anschluss der SCALANCE S-Module das Kapitel 2 "Produkteigenschaften und Inbetriebnahme"

3. Stellen Sie jetzt die physikalischen Netzwerkverbindungen her, indem Sie die Stecker der Netzwerkkabel in die dafür vorgesehenen Ports (RJ45-Buchsen) stecken:
   – Verbinden Sie PC2 mit Port 2 von Modul 1.
   – Verbinden Sie PC1 mit Port 1 von Modul 1.
4. Schalten Sie jetzt die beteiligten PCs ein.

ACHTUNG

Die Ethernet-Anschlüsse an Port 1 und Port 2 werden vom SCALANCE S unterschiedlich behandelt und dürfen deshalb beim Anschluss an das Kommunikationsnetzwerk nicht verwechselt werden:

- Port 1 - External Network
  obere RJ45-Buchse, rote Markierung = ungeschützter Netzwerk-Bereich;
- Port 2 - Internal Network
  untere RJ45-Buchse, grüne Markierung = durch SCALANCE S geschütztes Netzwerk;

Beim Vertauschen der Ports verliert das Gerät seine Schutzfunktion.

3.3.3 IP-Einstellungen der PCs einrichten

Die PCs sollten für den Test folgende IP-Adresseinstellungen erhalten:

PC	IP-Adresse	Subnetzmaske	Standardgateway
PC1	192.168.10.100	255.255.255.0	192.168.10.1
PC2	172.10.10.100	255.255.255.0	172.10.10.1

Unter Standardgateway sind die IP-Adressen anzugeben, die dem SCALANCE S-Modul in der nachfolgenden Projektierung für die interne und externe Schnittstelle zugewiesen werden:

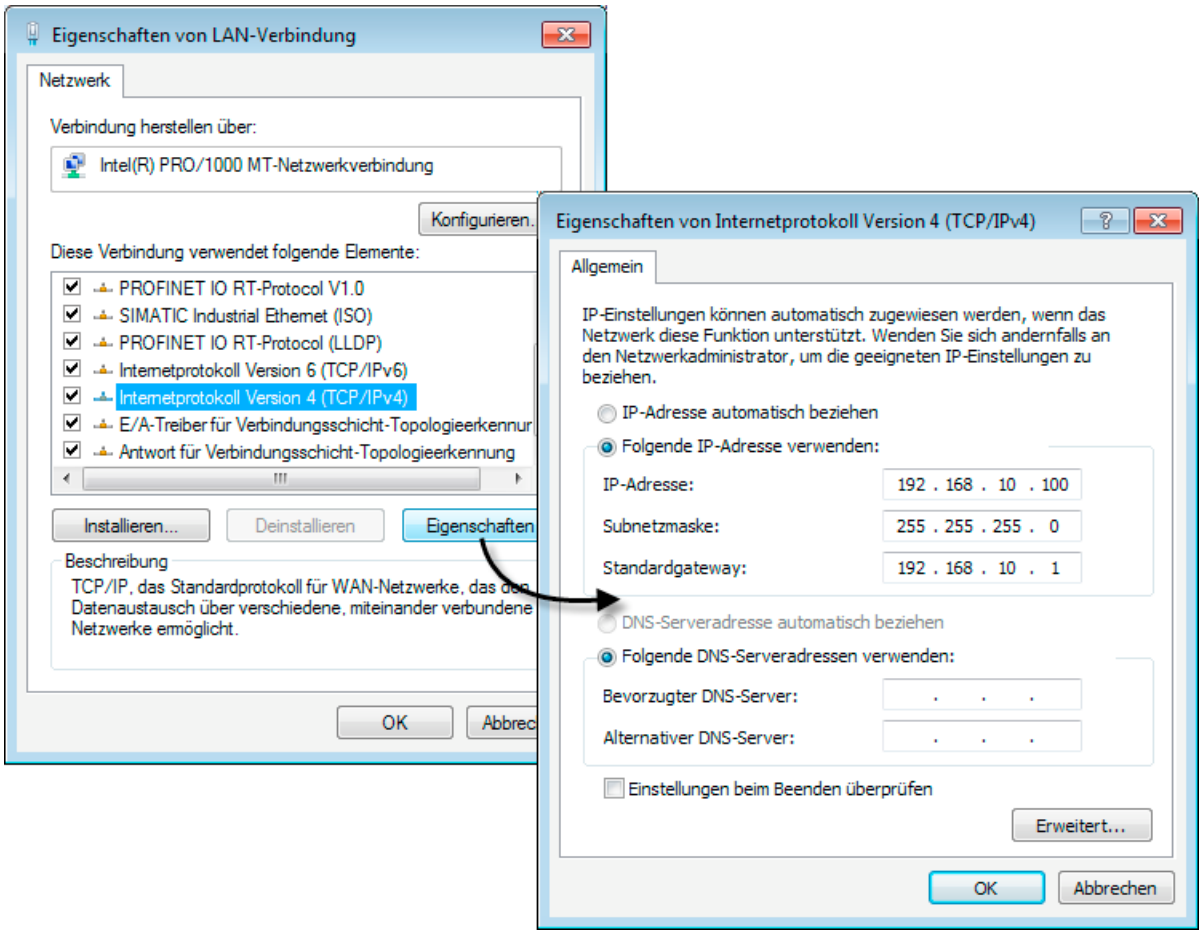
- PC1 verwendet die externe Schnittstelle.
- PC2 verwendet die interne Schnittstelle.

Gehen Sie jeweils bei PC1und PC2 folgendermaßen vor:

1. Öffnen Sie auf dem betreffenden PC die Systemsteuerung mit folgendem Menübefehl:

   Start ▸ Systemsteuerung

2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4(TCP/IPv4)" und klicken Sie die Schaltfläche "Eigenschaften".



4. Wählen Sie im Dialog "Eigenschaften von Internetprotokoll Version 4(TCP/IPv4)" das Optionsfeld "Folgende IP-Adresse verwenden:" aus und geben Sie jetzt die dem PC zugeordneten Werte aus der Tabelle "*IP-Einstellungen der PCs einrichten*" in die dafür vorgesehenen Felder ein.

   Schließen Sie die Dialoge mit "OK" ab und verlassen Sie die Systemsteuerung.

3.3.4 Projekt und Modul anlegen

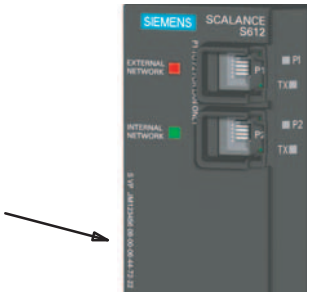
Gehen Sie so vor:

1. Installieren und starten Sie die Projektierungssoftware Security Configuration Tool auf PC1.
2. Erzeugen Sie mit folgendem Menübefehl ein neues Projekt:

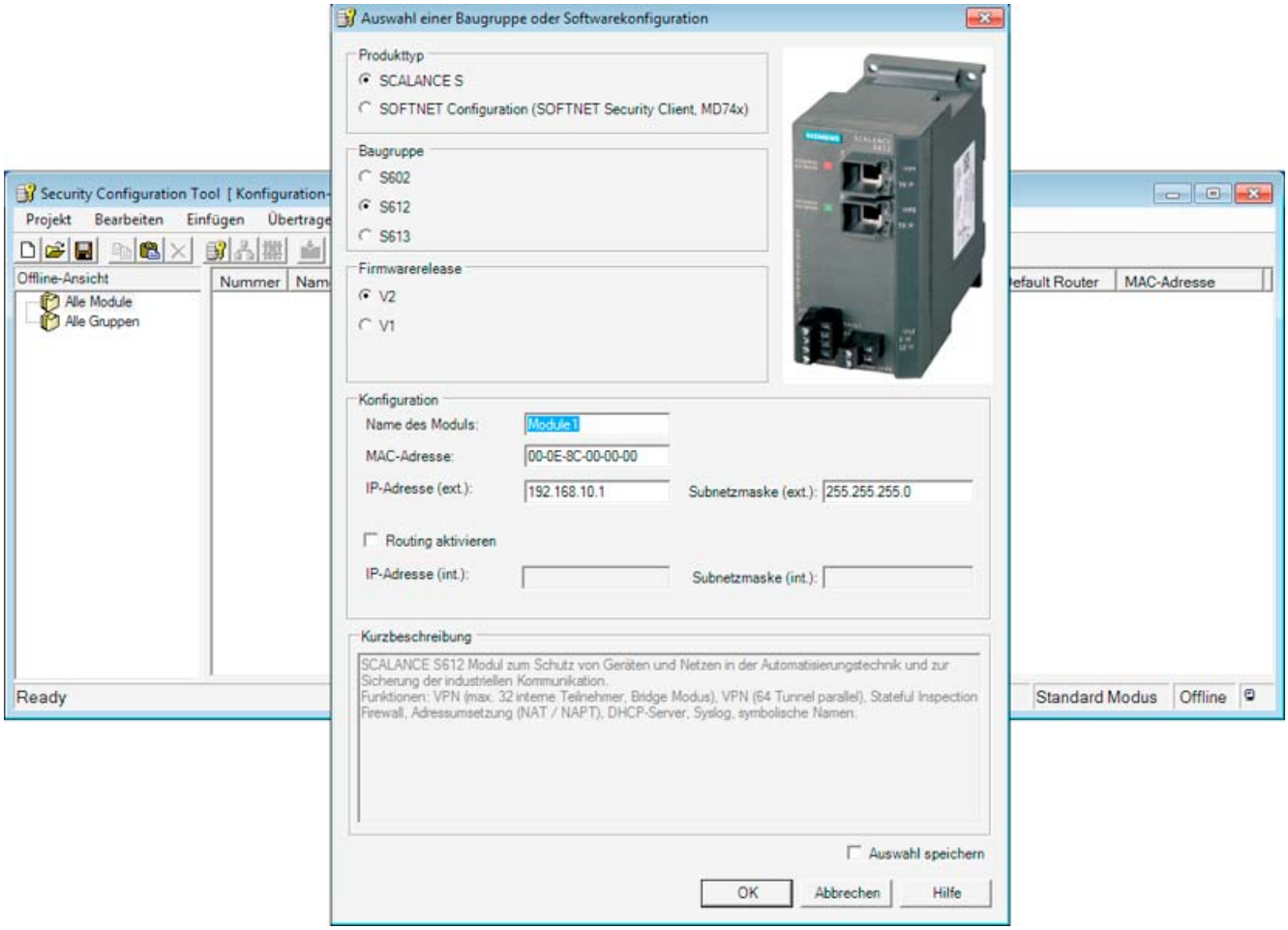
   Projekt ▸ Neu

   Sie werden aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Dem Benutzereintrag, den Sie hierbei festlegen, wird die Rolle eines Administrators zugewiesen.
3. Geben Sie einen Benutzernamen und ein Passwort ein und bestätigen Sie Ihre Eingabe; damit legen Sie ein neues Projekt an.
4. Es wurde automatisch der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" eingeblendet. Konfigurieren Sie jetzt Ihren Produkttyp, die Baugruppe und das Firmwarerelease.
5. Geben Sie in das Feld für die "MAC-Adresse" im Bereich "Konfiguration" die auf dem Modul-Gehäuse aufgedruckte MAC-Adresse im vorgegebenen Format ein.

   Sie finden diese Adresse auf der Frontseite des SCALANCE S-Moduls (siehe Bild).



6. Geben Sie ebenso im vorgegebenen Format die externe IP-Adresse (192.168.10.1) und die externe Subnetzmaske (255.255.255.0) ein und bestätigen Sie den Dialog mit "OK". Daraufhin wird Ihr Modul in die Liste der konfigurierten Module aufgenommen.



3.3.5 NAT-Router-Betrieb projektieren

Der häufige Einsatzfall, dass alle internen Teilnehmer Telegramme in das externe Netz senden und durch die NAT-Funktionalität deren IP-Adresse verborgen werden sollen, ist bei SCALANCE S vorkonfiguriert. Wie nachfolgend gezeigt wird, können Sie durch einfaches Anklicken im Routing-Modus dieses Verhalten aktivieren.

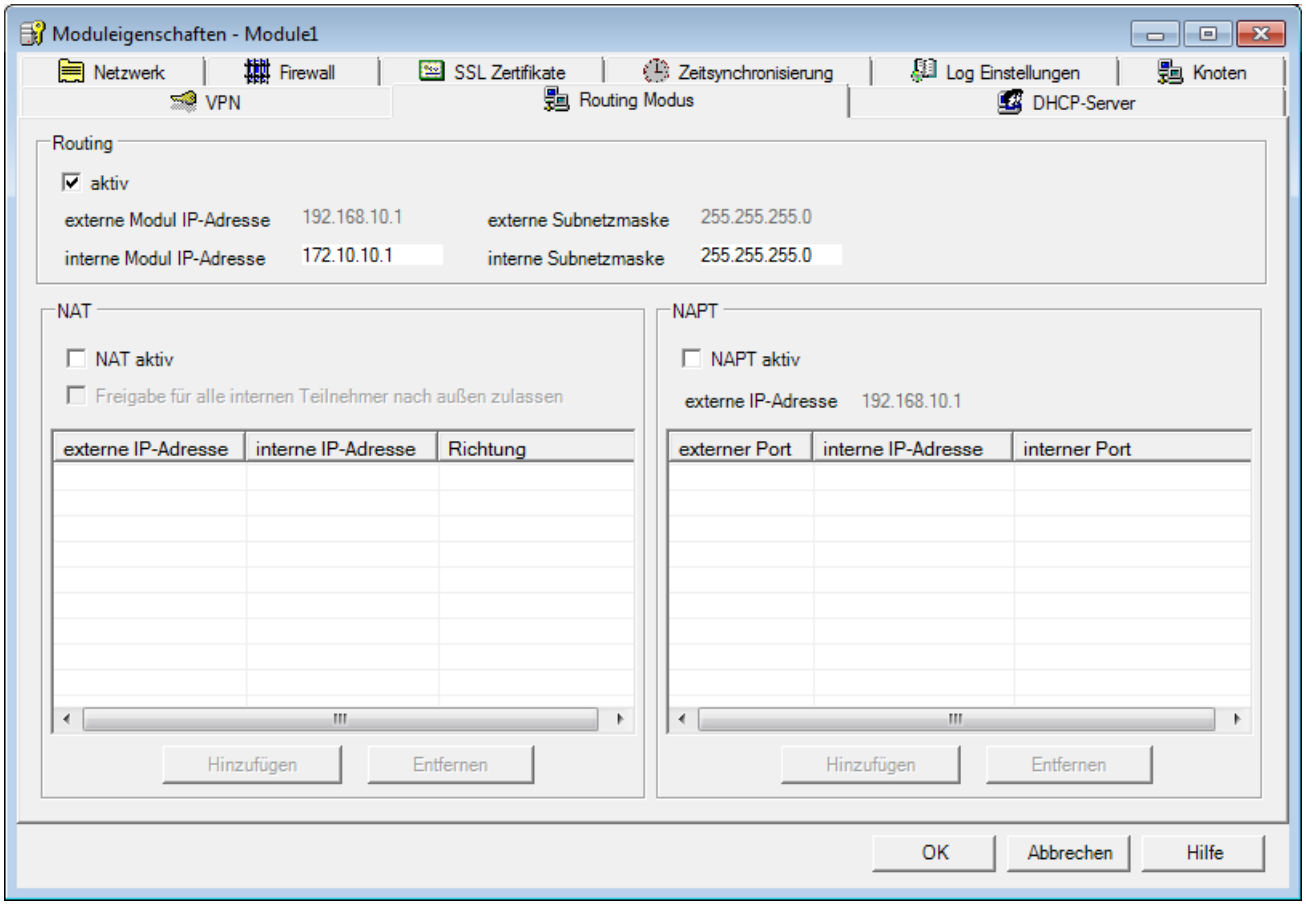
Router-Betrieb aktivieren - Gehen Sie so vor:

1. Schalten Sie zunächst die Projektierungsansicht in den Erweitert-Modus um.
2. Wählen Sie hierzu folgenden Menübefehl:

   Ansicht ▸ Erweitert-Modus

3. Doppelklicken Sie nun auf das SCALANCE S-Modul. Sie öffnen damit den Dialog zum Einstellen der Moduleigenschaften.

4. Wählen Sie im aufgeblendeten Dialog das Register "Routing Modus".



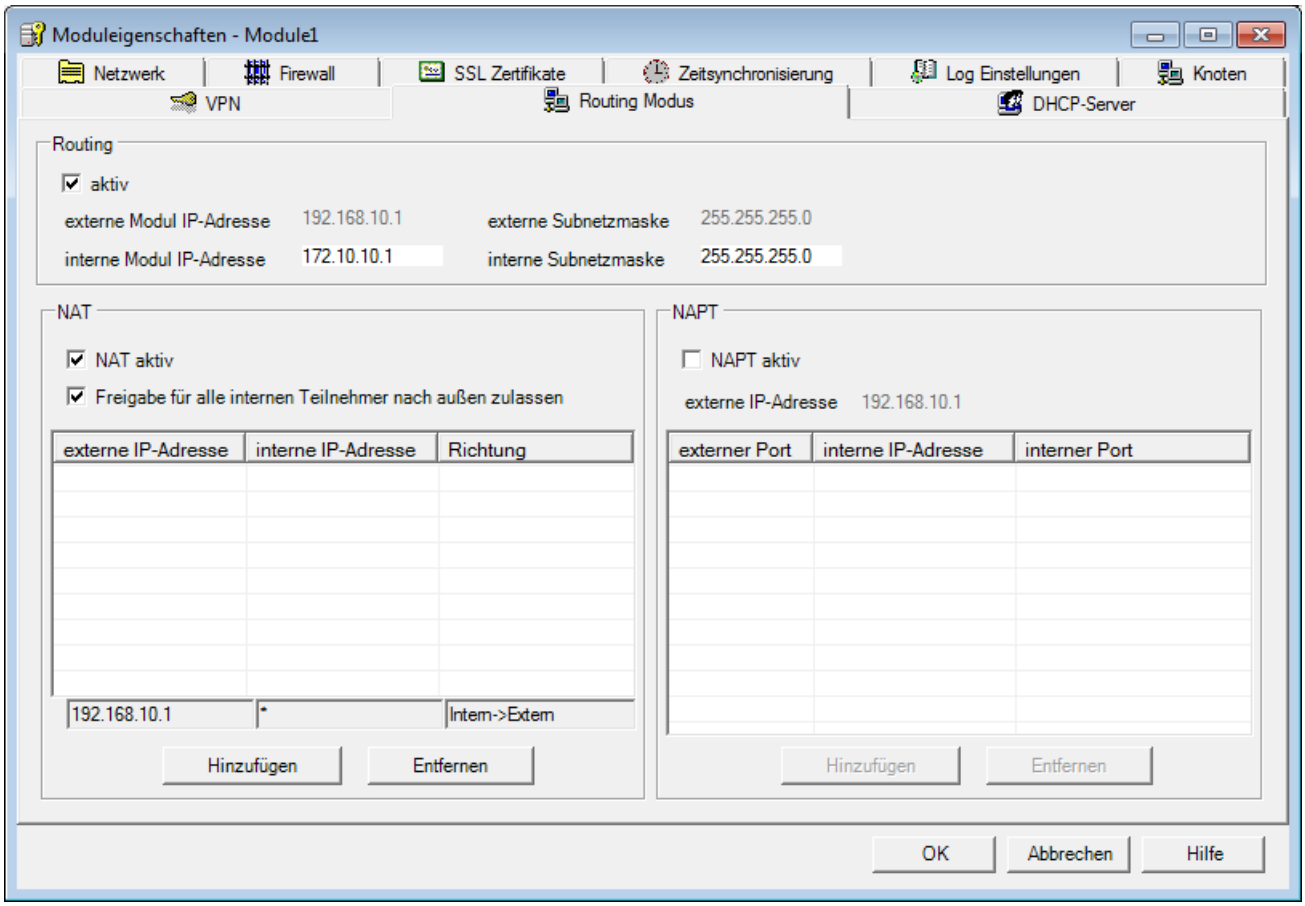
5. Wählen Sie im Eingabebereich "Routing" die Option "aktiv".
6. Ergänzen Sie nun im Eingabebereich "Routing" die Adressangaben für die Schnittstelle des SCALANCE S zum internen Subnetz wie folgt:
   - interne Modul IP-Adresse: 172.10.10.1
   - interne Subnetzmaske: 255.255.255.0

NAT-Router-Betrieb für interne Teilnehmer aktivieren - Gehen Sie so vor:

Nun geht es darum, die für den NAT-Betrieb geforderte Adressumsetzung zu konfigurieren.

1. Wählen Sie hierzu im Eingabebereich "NAT" die beiden Optionen "NAT aktiv" und "Freigabe für alle internen Teilnehmer zulassen".

Sie erkennen, dass im Eingabebereich "NAT" die Adressumsetzungsliste am Ende durch einen Eintrag ergänzt wurde. Der Eintrag "*" in der Spalte "interne IP-Adresse" steht nun stellvertretend für alle Teilnehmer im internen Netz.



2. Schließen Sie jetzt den Dialog mit "OK" ab.

Jetzt ist nur noch dafür zu sorgen, dass die Firewall die Telegramme von intern nach extern passieren lässt.

3.3.6 Firewall projektieren

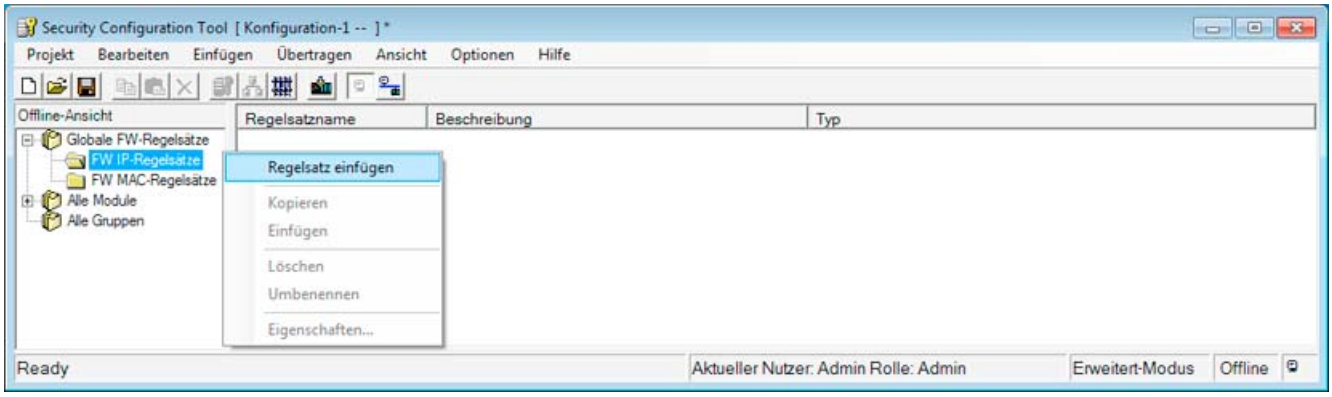
Sie müssen nun einen Regelsatz definieren, der den Telegrammverkehr für den internen Teilnehmer (PC2) zum Teilnehmer im externen Netzwerk (PC1) zulässt.

Zusätzlich zeigt Ihnen das Beispiel, wie Sie einen Regelsatz global definieren und einem Modul zuweisen können. Wenn Sie weitere Module im selben Projekt konfigurieren würden, würde es dann genügen, den einmal definierten Regelsatz den weiteren Modulen per "Drag and Drop" zuzuweisen; vorausgesetzt natürlich, dass hierbei dieselbe Regel zur Anwendung kommen soll.

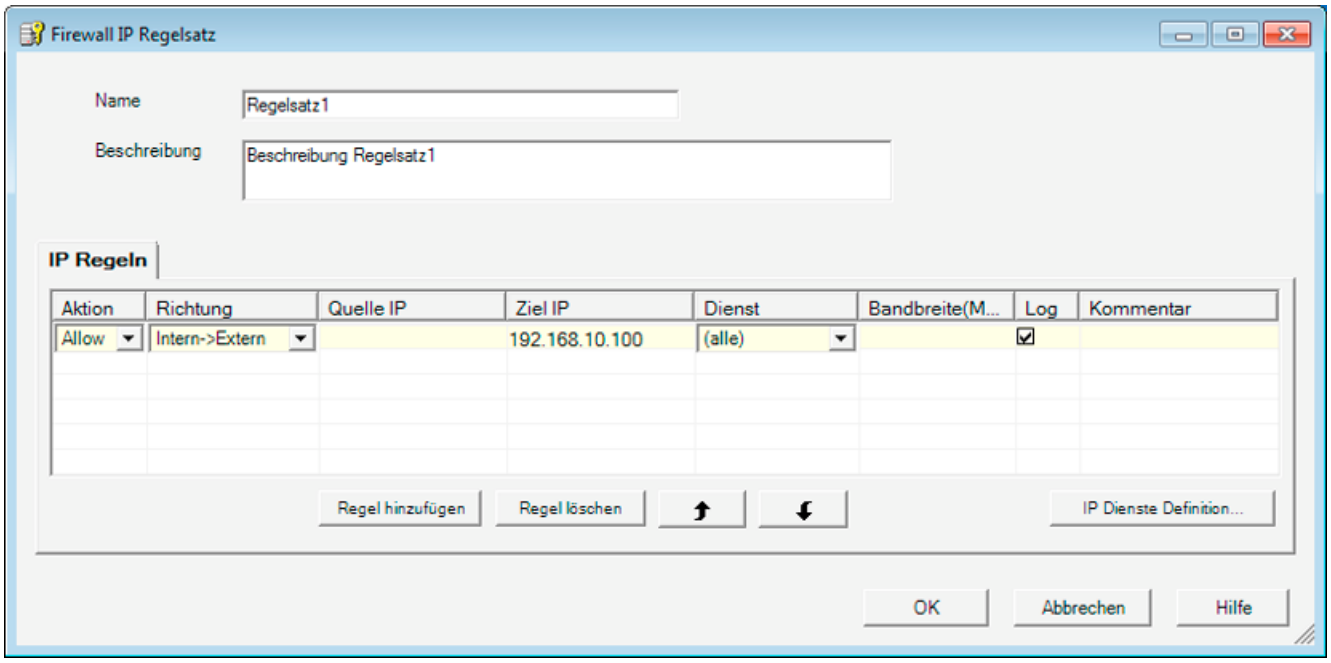
Globalen Regelsatz definieren - Gehen Sie so vor:

1. Öffnen Sie im Navigationsbereich das Objekt "Globale FW-Regelsätze" und markieren Sie darunter das Objekt "FW IP-Regelsätze".
2. Wählen Sie über die rechte Maustaste folgenden Menübefehl:

   Regelsatz einfügen



3. Tragen Sie im aufgeblendeten Dialog einen Regelsatz wie nachfolgend dargestellt ein:



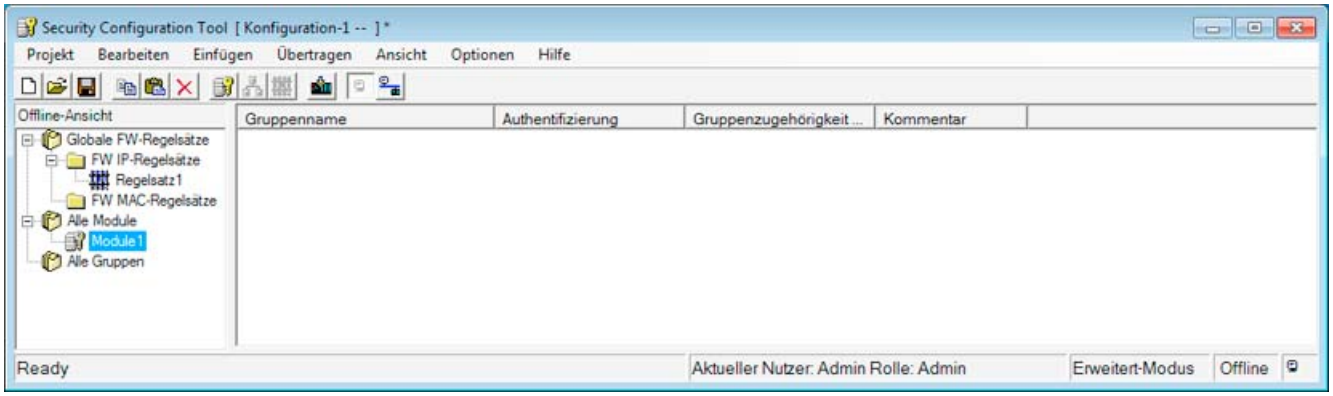
4. Klicken Sie in der Spalte "Log" in die Zeile des neuen Regelsatzes. Damit wird die Option Paketfilter-Logging aktiviert. Telegramme, auf die die definierte Regel angewendet wird, werden dann aufgezeichnet.

   Diese Aufzeichnung werden Sie im hier gezeigten Beispiel beim abschließenden Test der Konfiguration nutzen.

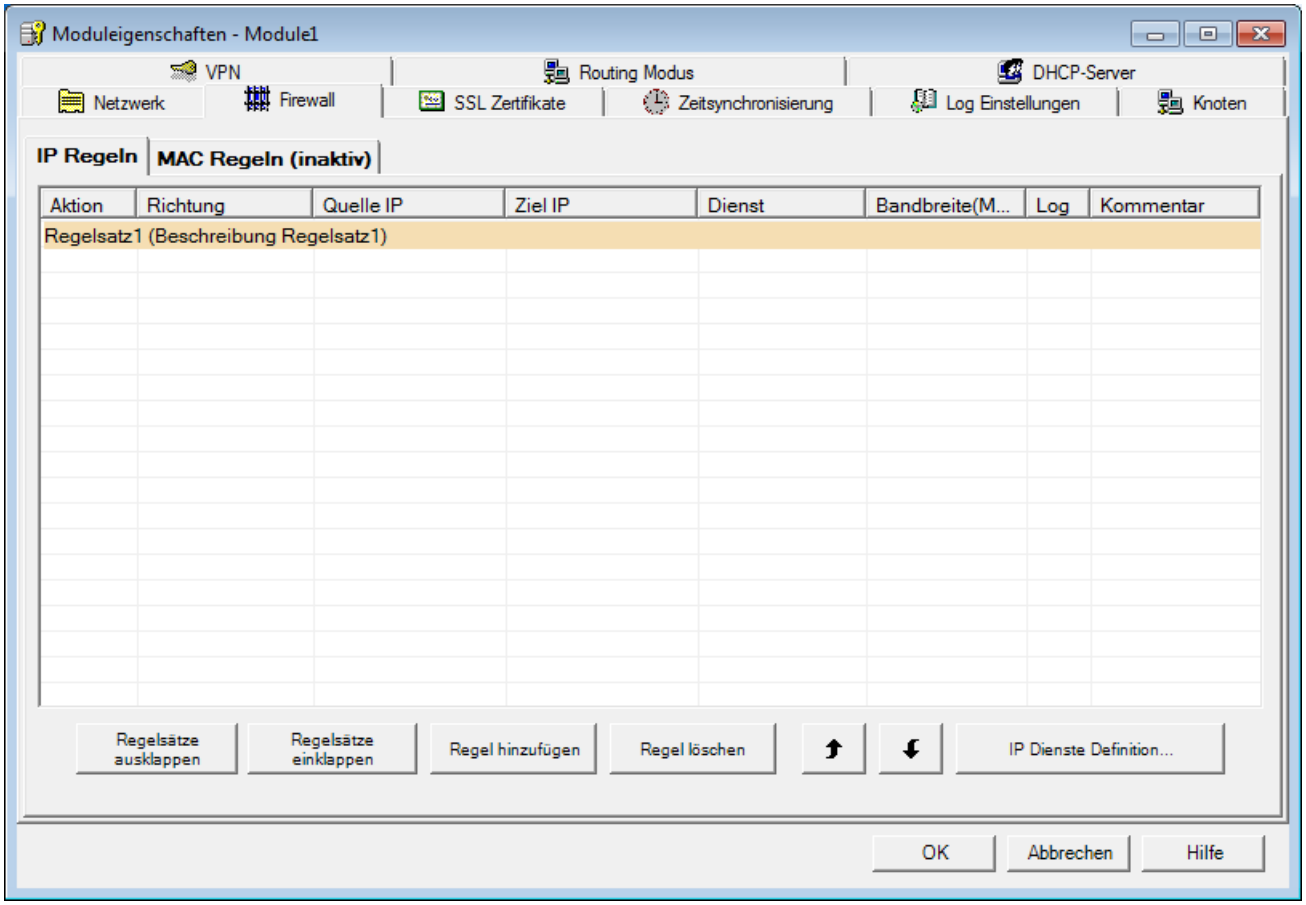
5. Schließen Sie den Dialog mit "OK" ab.

Globalen Regelsatz zuweisen - Gehen Sie so vor:

1. Markieren Sie im Navigationsbereich das Objekt "Module1" und ziehen Sie es bei gedrückter linker Maustaste auf den neu angelegten globalen Firewall-Regelsatz.



2. Sie können die Zuweisung kontrollieren, indem Sie nochmals den Dialog zum Einstellen der Moduleigenschaften öffnen und dort das Register "Firewall" wählen.



Sie sehen, dass die globale Firewall-Regel dort hinterlegt wurde.

3. Indem Sie die Schaltfläche "Regelsätze ausklappen" betätigen, können Sie den Regelsatz im Detail einblenden.

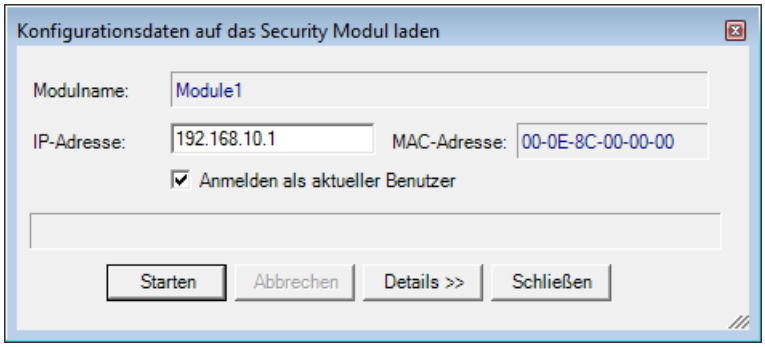
Damit ist nun die Offline-Konfiguration abgeschlossen.

3.3.7 Konfiguration in SCALANCE S laden

Gehen Sie so vor:

1. Selektieren Sie im Inhaltsbereich das Modul.
2. Wählen Sie folgenden Menübefehl:

   Übertragen ▸ An Modul…



3. Starten Sie den Ladevorgang über die Schaltfläche "Starten".

   Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das SCALANCE S-Modul automatisch neu gestartet und die neue Konfiguration aktiviert.

Ergebnis: SCALANCE S im Produktivbetrieb

SCALANCE S befindet sich jetzt im Produktivbetrieb. Dieser Betriebszustand wird von der Fault-Anzeige-LED durch grünes Licht signalisiert.

Die Inbetriebsetzung der Konfiguration ist damit abgeschlossen und SCALANCE S schützt jetzt über die eingerichtete Firewall das interne Netz (PC 2) gemäß der projektierten Regel: "Erlaube abgehenden IP-Verkehr" vom internen ins externe Netz.

3.3.8 NAT-Router-Funktion testen (Ping-Test)

Wie können Sie die konfigurierte Funktion testen ?

Die Funktionstests können Sie wie nachfolgend beschrieben mit einem Ping-Kommando durchführen. Um die Auswirkung des NAT-Router-Betriebes erkennen zu können, verwenden Sie die Möglichkeit des Paketfilter-Logging an der Firewall-Schnittstelle.

Zur Erinnerung: Bei der Definition der globalen Firewall-Regel haben Sie bereits die Option für das Paketfilter-Logging eingeschaltet.

Anmerkung zum Ping-Kommando: Alternativ können Sie auch andere Kommunikationsprogramme für den Test der Konfiguration verwenden.

ACHTUNG
Bei Windows kann die Firewall standardmäßig so eingestellt sein, dass PING-Kommandos nicht passieren können. Sie müssen ggf. die ICMP-Dienste vom Typ Request und Response freischalten.

Testabschnitt 1 - Ping-Kommando absetzen

Testen Sie nun die Funktion des NAT-Router-Betriebes bei IP-Datenverkehr von intern nach extern wie folgt:

1. Rufen Sie auf dem PC2 in der Startleiste folgenden Menübefehl auf:

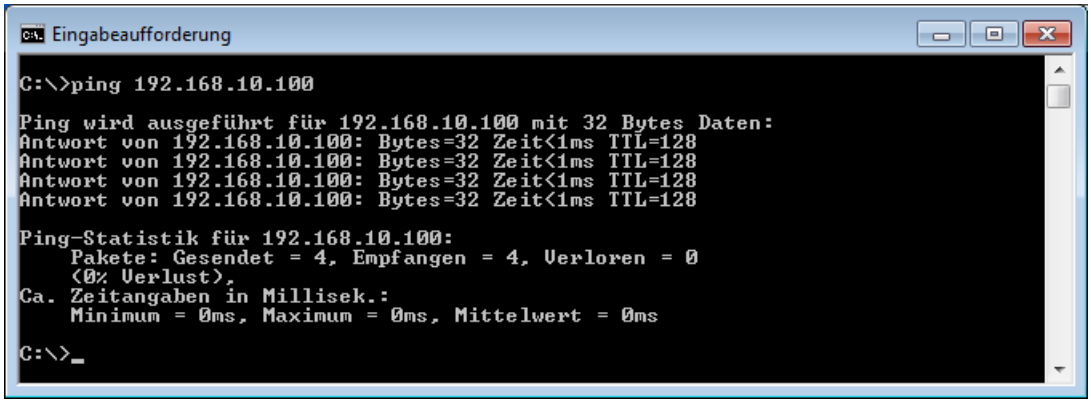
   Start ▸ Alle Programme ▸ Zubehör ▸ Eingabeaufforderung

2. Eingabe des Ping-Kommandos von PC2 an den PC1 (IP-Adresse 192.168.10.100)

   Geben Sie unmittelbar in die Kommandozeile des aufgeblendeten Fensters "Eingabeaufforderung", an der Cursor-Positionden folgenden Befehl ein:

   ping 192.168.10.100

   Sie erhalten daraufhin folgende Meldung: (positive Antwort von PC1).



Testabschnitt 2 - Ergebnis auswerten

1. Gehen Sie nun im Security Configuration Tool in den Online-Modus. Wählen Sie hierzu den folgenden Menübefehl:

   Ansicht ▸ Online

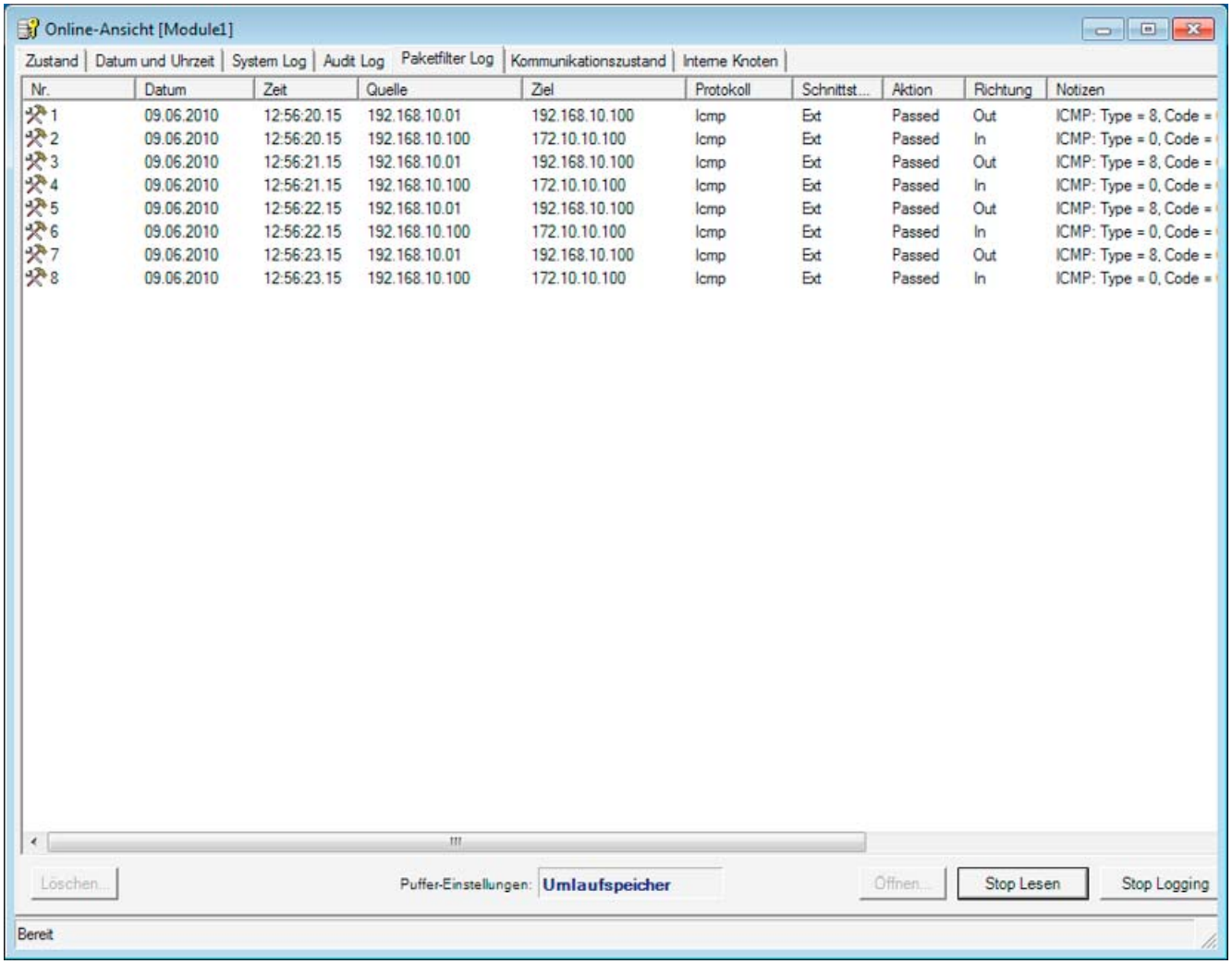
2. Markieren Sie das zu bearbeitende Modul und wählen Sie zum Öffnen des Online-Dialoges den Menübefehl

   Bearbeiten ▸ Online Diagnose...

   Wählen Sie das Register "Paketfilter Log"

3. Betätigen Sie die Schaltfläche "Starte Lesen".
4. Quittieren Sie den aufgeblendeten Dialog mit "OK".

   Ergebnis: Die Log-Einträge werden aus dem SCALANCE S ausgelesen und hier ausgegeben.



Ergebnis

In den Ausgabezeilen der Aufzeichnung erkennen Sie Folgendes:

- Ausgabezeile 1

  Die IP-Adressen der Telegramme von PC2 an PC1 werden an der Schnittstelle zum externen Netz mit der externen IP-Adresse des SCALANCE S-Moduls (192.168.10.01) gezeigt. Dies entspricht der erwarteten Adressumsetzung (Anmerkung: die zusätzliche Port-Zuweisung ist hier nicht sichtbar).

- Ausgabezeile 2

Die Antworttelegramme werden mit der Zieladresse des Teilnehmers im internen Subnetz (PC2: 172.10.10.100) angezeigt. Sie erkennen daran, dass die Adressumsetzung bereits erfolgt ist, bevor das Antworttelegramm die Firewall passiert.

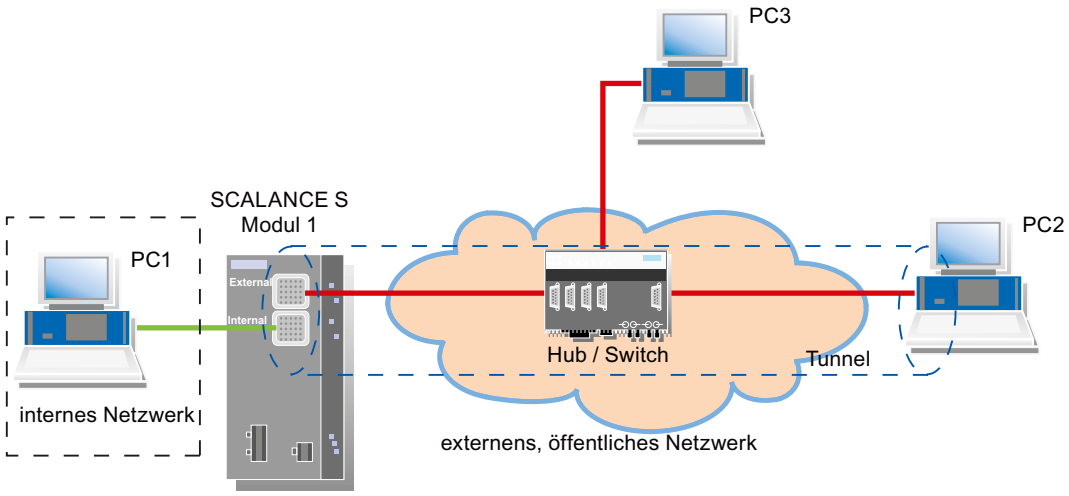
3.4 Beispiel 4: Fernzugriff - VPN-Tunnel-Beispiel mit SCALANCE S612 / S613 und SOFTNET Security Client

3.4.1 Übersicht

In diesem Beispiel wird die VPN-Tunnelfunktion in der Projektierungssicht "Standard-Modus" projektiert. Ein SCALANCE S und der SOFTNET Security Client bilden in diesem Beispiel die beiden Tunnelendpunkte für die gesicherte Tunnelverbindung über ein öffentliches Netzwerk.

Sie erreichen mit dieser Konfiguration, dass IP-Verkehr nur über die eingerichteten VPN-Tunnelverbindungen zwischen autorisierten Partnern möglich ist.

Aufbau des Testnetzes



- Internes Netzwerk - Anschluss an SCALANCE S Port 2 ("Internal Network"-Port)

  Im internen Netzwerk wird im Testaufbau ein Netzknoten durch einen PC realisiert, der an den "Internal Network"-Port (Port 2, grün) eines SCALANCE S-Moduls angeschlossen ist.

  – PC1: repräsentiert einen Teilnehmer des internen Netzwerks

  – SCALANCE S Modul 1: SCALANCE S-Modul für den Schutz des internen Netzwerks

- Externes, öffentliches Netzwerk - Anschluss an SCALANCE S Port 1 ("External Network"-Port)

  Das externe, öffentliche Netzwerk wird an den "External Network"-Port (Port 1, rot) eines SCALANCE S-Moduls angeschlossen.

  – PC2: PC mit der Konfigurationssoftware Security Configuration Tool und der Software SOFTNET Security Client für den sicheren VPN-Zugang in das interne Netzwerk

  – PC3: Test-PC für Testabschnitt 2

Hinweis

Im Beispiel wird stellvertretend für ein externes, öffentliches WAN ein lokales Netz zur prinzipiellen Erläuterung der entsprechenden Funktionsweise zu Hilfe genommen.

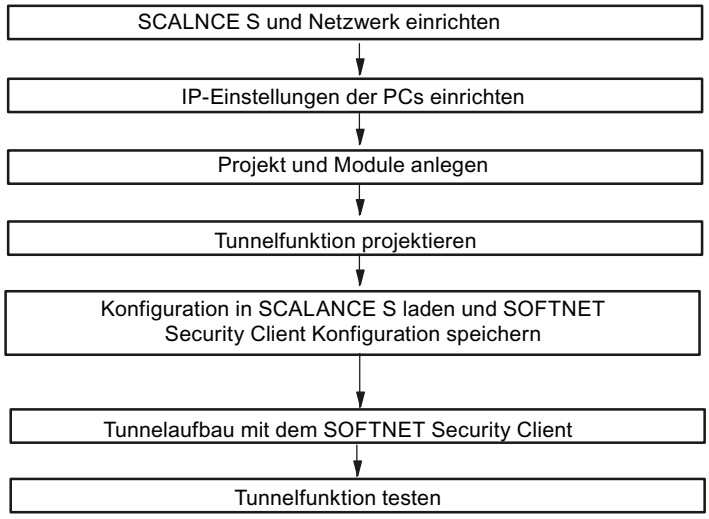
Erläuterungen bezüglich der Nutzung eines WANs werden an den entsprechenden Stellen gegeben.

Erforderliche Geräte/Komponenten:

Für den Aufbau verwenden Sie folgende Komponenten:

- 1x SCALANCE S-Modul, (optional: eine entsprechend montierte Hutschiene mit Montagematerial);
- 1x 24V-Stromversorgungen mit Kabelverbindung und Klemmenblockstecker;
- 1x PC auf dem das Projektierungswerkzeug "Security Configuration Tool" und der VPN-Client "SOFTNET Security Client" installiert ist;
- 1x PC im internen Netz für den Test der Konfiguration;
- 1x PC im externen Netz für den Test der Konfiguration;
- 1x Netzwerk-Hub bzw. -Switch zum Aufbau der Netzwerkverbindungen mit dem SCALANCE S-Modul sowie den PCs;
- die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet.

Die folgenden Schritte in der Übersicht:



3.4.2 SCALANCE S und Netzwerk einrichten

Gehen Sie wie folgt vor:

1. Packen Sie zunächst das SCALANCE S Gerät aus und überprüfen Sie den unbeschädigten Zustand.
2. Schließen Sie die Spannungsversorgung an das SCALANCE S Modul an.

Ergebnis: Nach dem Anschließen der Betriebsspannung leuchtet die Fault-LED (F) gelb.

⚠ WARNUNG

Das Gerät SCALANCE S ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsanschlüsse nur Sicherheitskleinspannungen (SELV) nach IEC950/EN60950/ VDE0805 angeschlossen werden.

Das Netzteil für die Versorgung des SCALANCE S muss NEC Class 2 entsprechen (Spannungsbereich 18-32 V, Strombedarf ca. 250 mA).

Beachten Sie für Montage und Anschluss der SCALANCE S-Module das Kapitel 2 "Produkteigenschaften und Inbetriebnahme ".

1. Stellen Sie jetzt die physikalischen Netzwerkverbindungen her, indem Sie die Stecker der Netzwerkkabel in die dafür vorgesehenen Ports (RJ45-Buchsen) stecken:

- Verbinden Sie PC1 mit Port 2 von Modul 1.
- Verbinden Sie Port 1 von Module 1 mit dem Hub/Switch.
- Verbinden Sie PC2 und PC3 ebenfalls mit dem Hub/Switch.

2. Schalten Sie jetzt die beteiligten PCs ein.

Hinweis

Für die Nutzung eines WAN als externes, öffentliches Netzwerk sind die Verbindungen zum Hub/Switch mit den Verbindungen zum WAN (Internetzugang) zu ersetzen.

ACHTUNG

Die Ethernet-Anschlüsse an Port 1 und Port 2 werden vom SCALANCE S unterschiedlich behandelt und dürfen deshalb beim Anschluss an das Kommunikationsnetzwerk nicht verwechselt werden:

- Port 1 - "External Network"
  obere RJ45-Buchse, rote Markierung = ungeschützter Netzwerkbereich;
- Port 2 - "Internal Network"
  untere RJ45-Buchse, grüne Markierung = durch SCALANCE S geschütztes Netzwerk;

Beim Vertauschen der Ports verliert das Gerät seine Schutzfunktion.

3.4.3 IP-Einstellungen der PCs einrichten

Die PCs sollten für den Test folgende IP-Adress-Einstellungen erhalten.

PC	IP-Adresse	Subnetzmaske	Standardgateway
PC1	192.168.0.1	255.255.255.0	192.168.0.201
PC2	191.0.0.2	255.255.0.0	191.0.0.201
PC3	191.0.0.3	255.255.0.0	191.0.0.201

Unter Standardgateway sind die IP-Adressen anzugeben, die dem SCALANCE S-Modul in der nachfolgenden Projektierung für die interne und externe Schnittstelle zugewiesen werden:

- PC1 verwendet die interne Schnittstelle.
- PC2 und PC3 verwenden die externe Schnittstelle.

Hinweis

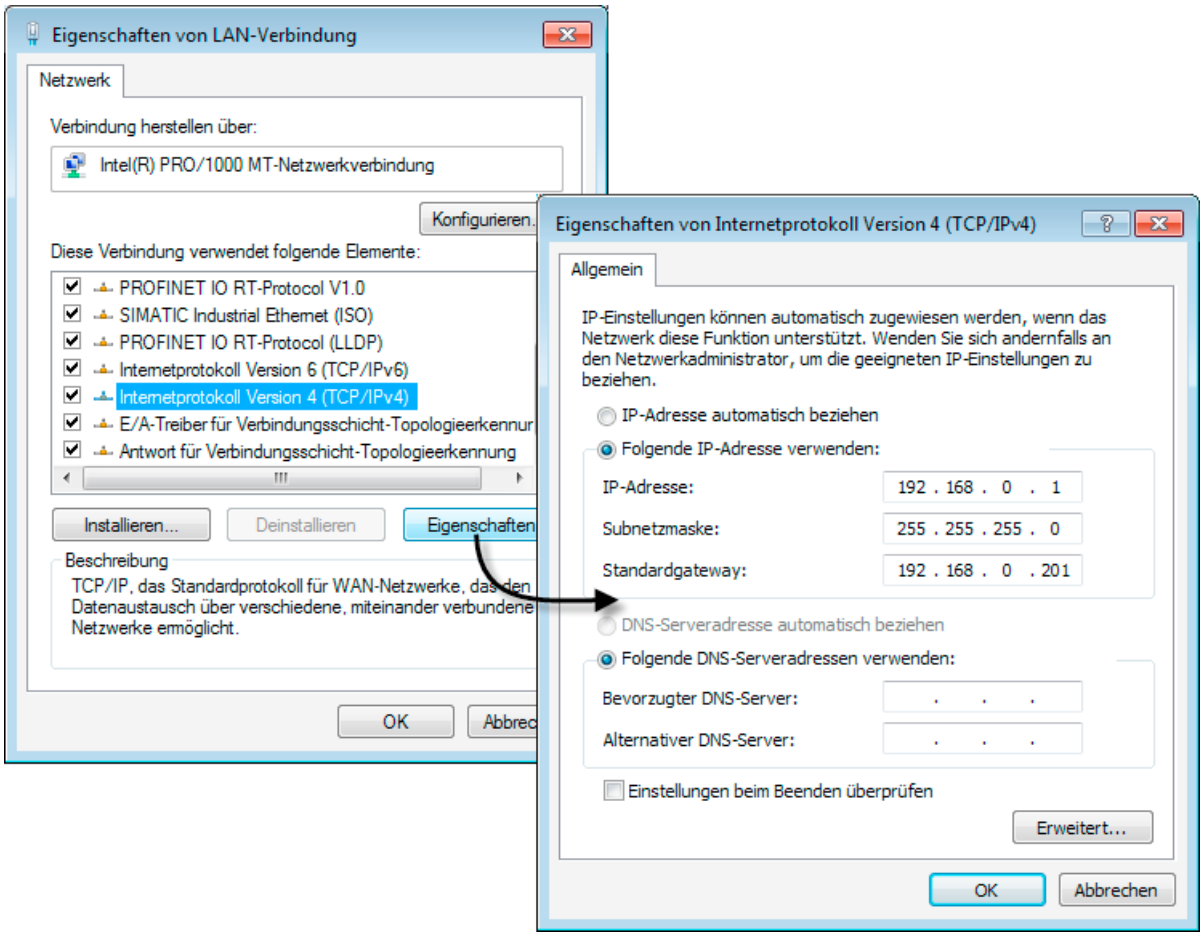
Für die Nutzung eines WAN als externes, öffentliches Netzwerk sind auf PC2 und PC3 die jeweiligen IP-Einstellungen für die Verbindung mit dem WAN (Internet) einzurichten.

Gehen Sie bei PC1, PC2 und PC3 jeweils folgendermaßen vor:

1. Öffnen Sie auf dem betreffenden PC die Systemsteuerung mit folgendem Menübefehl:

   Start ▸ Systemsteuerung

2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter" und wählen Sie aus dem Navigationsmenü links die Option "Adaptereinstellungen ändern".
3. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4(TCP/IPv4)" und klicken Sie die Schaltfläche "Eigenschaften".



4. Wählen Sie im Dialog "Eigenschaften von Internetprotokoll Version 4(TCP/IPv4)" das Optionsfeld "Folgende IP-Adresse verwenden:" aus und geben Sie jetzt die dem PC zugeordneten Werte aus der Tabelle "*IP-Einstellungen der PCs einrichten*" in die dafür vorgesehenen Felder ein.

   Schließen Sie die Dialoge mit "OK" ab und verlassen Sie die Systemsteuerung.

3.4.4 Projekt und Module anlegen

Gehen Sie wie folgt vor:

1. Starten Sie die Projektierungssoftware Security Configuration Tool auf PC2.
2. Erzeugen Sie ein neues Projekt mit folgendem Menübefehl:

   Projekt ► Neu

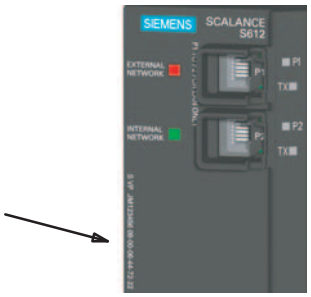
   Sie werden aufgefordert einen Benutzernamen und ein Passwort anzugeben. Dem Benutzereintrag, den Sie hierbei festlegen, wird automatisch die Rolle eines Administrators zugewiesen.
3. Geben Sie einen Benutzernamen und ein Passwort ein und bestätigen Sie Ihre Eingabe, damit legen Sie ein neues Projekt an.
4. Es wurde automatisch der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" eingeblendet. Konfigurieren Sie jetzt Ihren Produkttyp, die Baugruppe und das Firmwarerelease und schließen Sie am Ende den Dialog mit "OK".
5. Erzeugen Sie ein zweites Modul mit folgendem Menübefehl:

   Einfügen ► Modul

   Konfigurieren Sie jetzt den Produkttyp "SOFTNET Configuration", die Baugruppe "SOFTNET Security Client" und das Firmwarerelease Ihrer SOFTNET Security Client Version und schließen Sie am Ende den Dialog mit "OK".

   Dieses Modul erhält automatisch einen Namen entsprechend den Voreinstellungen für das Projekt.
6. Klicken Sie im Navigationsbereich auf "Alle Module" und anschließend im Inhaltsbereich auf die Zeile mit "Module1".
7. Klicken Sie jetzt in die Spalte "MAC-Adresse" und geben Sie diese im vorgegebenen Format ein.

   Sie finden diese Adresse auf der Frontseite des SCALANCE S-Moduls (siehe Bild).



8. Klicken Sie jetzt in die Spalte "IP-Adresse ext.", geben Sie diese im vorgegebenen Format ein und passen Sie ebenso die Subnetzmaske an.
   Für Module1: IP-Adresse: 191.0.0.201, Subnetzmaske: 255.255.0.0

   Hinweis

   Für die Nutzung eines WAN als externes, öffentliches Netzwerk geben Sie als "IP-Adresse ext." Ihre vom Provider erhaltene statische IP-Adresse an über welche das SCALANCE S-Modul dann im WAN (Internet) erreichbar ist.

   Damit das SCALANCE S-Modul Pakete über das WAN (Internet) versenden kann müssen Sie als "Default Router" Ihren DSL-Router eintragen.

   Wenn Sie einen DSL-Router als Internet Gateway nutzen, müssen an diesem mindestens die folgenden Ports weitergeleitet werden:

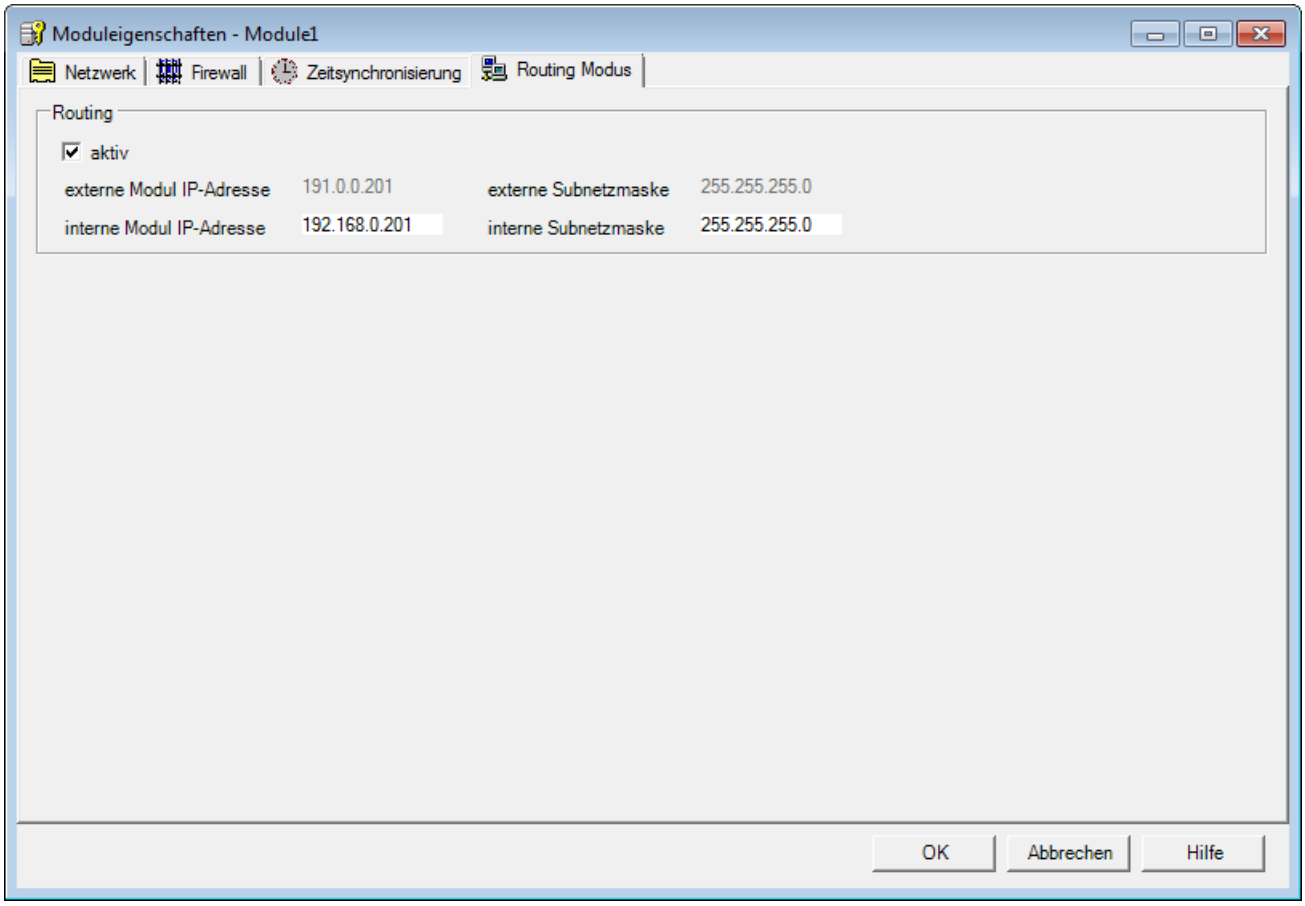
   • Port 500 (ISAKMP)

   • Port 4500 (NAT-T)

   Bei Konfigurationsdownloads (nicht durch einen aktiven Tunnel) muss zusätzlich der Port 443 (HTTPS) weitergeleitet werden.

9. Öffnen Sie jetzt das Eigenschaftsmenü von "Module1" indem Sie den Eintrag selektieren, die rechte Maustaste betätigen und den Menüpunkt "Eigenschaften…" auswählen.

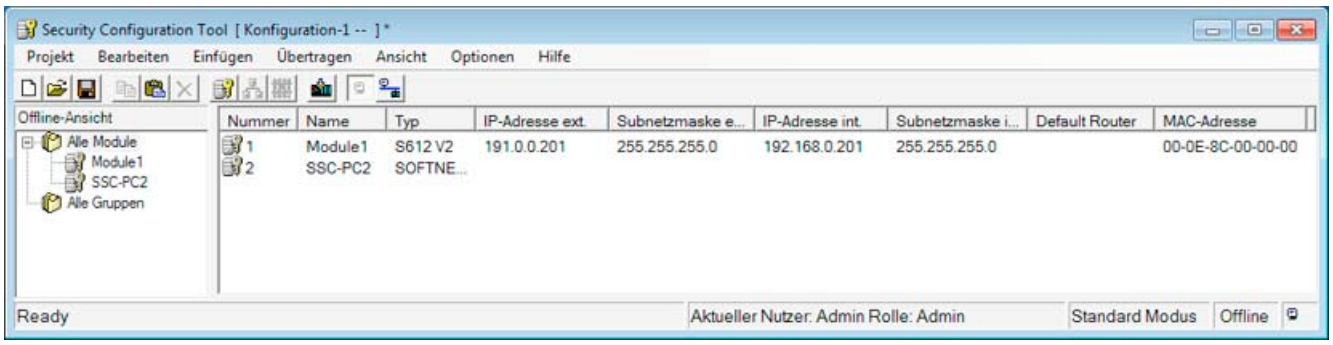
10. Schalten Sie jetzt entsprechend der folgenden Ansicht in der Registerkarte "Routing Modus" den Routing Modus aktiv, tragen Sie die interne IP-Adresse (192.168.0.201) und die Subnetzmaske (255.255.255.0) des SCALANCE S Modul ein und bestätigen Sie mit "OK".



11. Klicken Sie im Navigationsbereich auf "Alle Module" und anschließend im Inhaltsbereich auf die Zeile mit "Module2".
12. Klicken Sie in die Spalte "Name" und geben Sie den Namen "SSC-PC2" ein.

Der SOFTNET Security Client benötigt keine weiteren Einstellungen.

Ihre Ansicht sollte jetzt ähnlich dem folgenden Bild entsprechen.



3.4.5 Tunnelverbindung projektieren

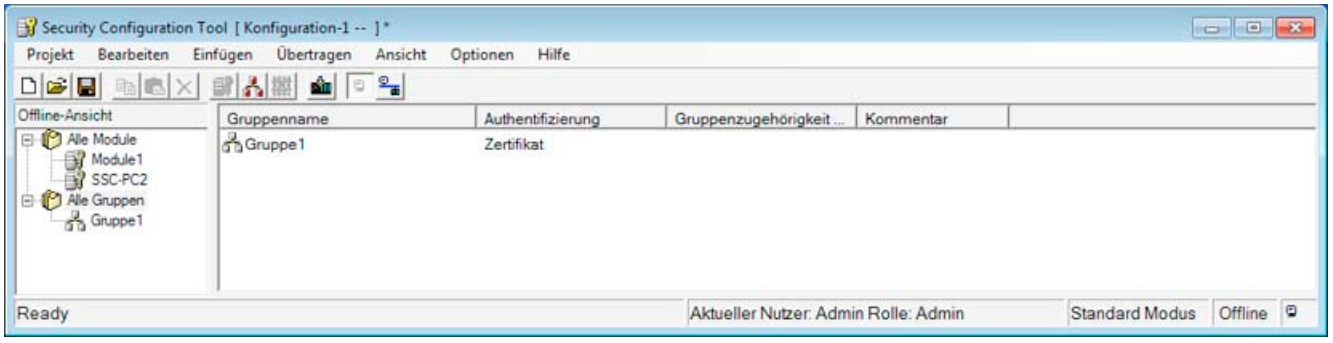
Ein SCALANCE S und der SOFTNET Security Client können genau dann einen IPsec-Tunnel für die gesicherte Kommunikation aufbauen, wenn sie im Projekt der gleichen Gruppe zugeordnet sind.

Gehen Sie wie folgt vor:

1. Selektieren Sie im Navigationsbereich "Alle Gruppen" und erzeugen Sie mit folgendem Menübefehl eine neue Gruppe:

   Einfügen ► Gruppe

   Diese Gruppe erhält automatisch den Namen "Gruppe1".



2. Selektieren Sie im Inhaltsbereich das SCALANCE S Module "Module1" und ziehen Sie es auf "Gruppe1" im Navigationsbereich.

   Das Modul ist jetzt dieser Gruppe zugeordnet bzw. Mitglied dieser Gruppe.

   Die Farbe vom Schlüsselsymbol des Modul-Icons schlägt hierbei von grau nach blau um.

3. Selektieren Sie im Inhaltsbereich das SOFTNET Security Client Modul und ziehen Sie es auf "Gruppe1" im Navigationsbereich.

   Das Modul ist jetzt ebenso dieser Gruppe zugeordnet.

4. Speichern Sie dieses Projekt jetzt mit dem folgenden Menübefehl unter einem zweckmäßigen Namen ab:

   Projekt ► Speichern unter…

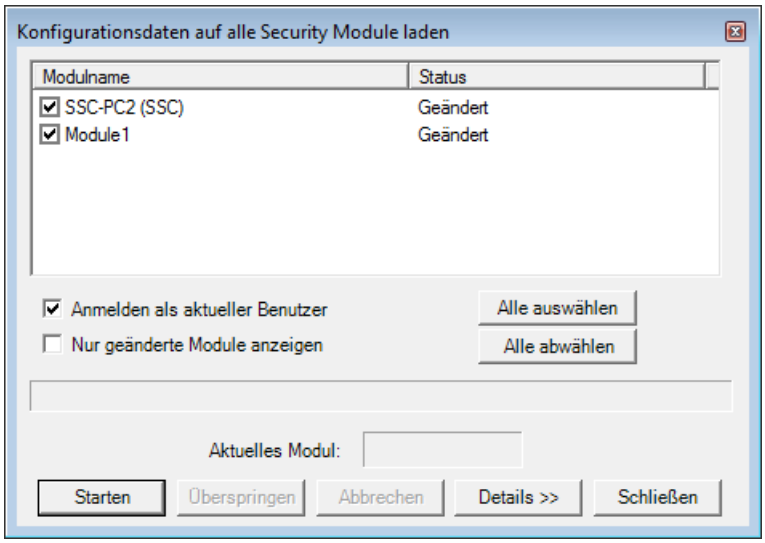
Die Konfiguration der Tunnelverbindung ist damit abgeschlossen.

3.4.6 Konfiguration in SCALANCE S laden und SOFTNET Security Client Konfiguration abspeichern

Gehen Sie wie folgt vor:

1. Rufen Sie mit folgendem Menübefehl den folgenden Dialog auf:

   Übertragen ► An alle Module…



2. Starten Sie den Ladevorgang über die Schaltfläche "Starten".
3. Speichern Sie die Konfigurationsdatei "Projektname.SSC-PC2.dat" in ihr Projektverzeichnis und vergeben Sie ein Passwort für den privaten Schlüssel des Zertifikats.

Wurde der Ladevorgang fehlerfrei abgeschlossen, wird das SCALANCE S automatisch neu gestartet und die neue Konfiguration aktiviert.

Ergebnis: SCALANCE S im Produktivbetrieb

SCALANCE S befindet sich jetzt im Produktivbetrieb. Dieser Betriebszustand wird von der Fault-LED durch grünes Licht signalisiert.

Die Inbetriebsetzung der Konfiguration ist damit abgeschlossen und das SCALANCE S Modul und der SOFTNET Security Client können einen Kommunikationstunnel aufbauen, über den Netzknoten aus dem internen Netzen gesichert mit PC2 kommunizieren können.

Hinweis

Für die Nutzung eines WAN als externes, öffentliches Netzwerk können Sie ein SCALANCE S-Modul mit Werkseinstellung nicht über das WAN konfigurieren. Konfigurieren Sie in diesem Fall das SCALANCE S-Modul aus dem internen Netz heraus.

3.4.7 Tunnelaufbau mit dem SOFTNET Security Client

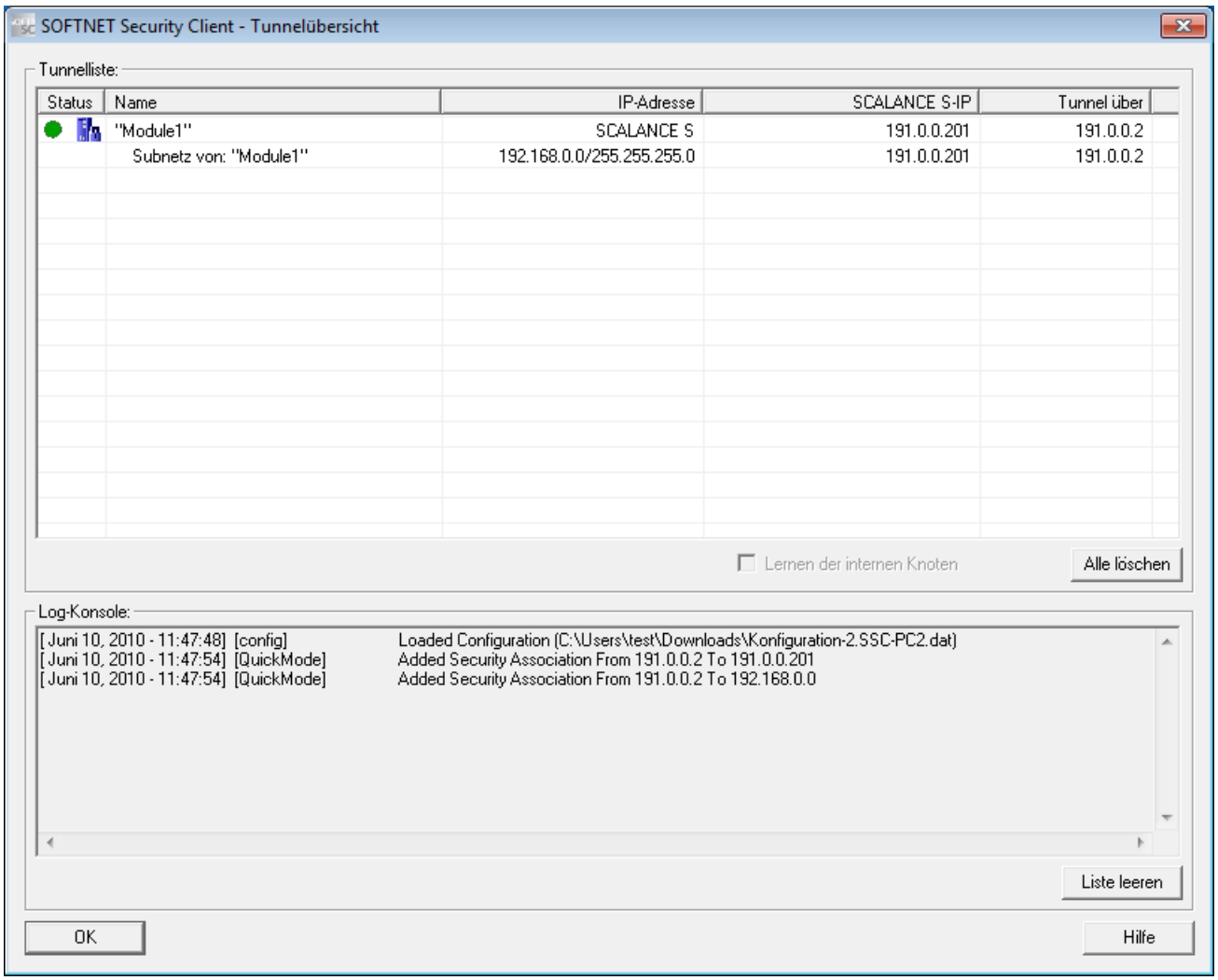
Gehen Sie wie folgt vor:

1. Starten Sie den SOFTNET Security Client auf PC2.
2. Betätigen Sie die Schaltfläche "Konfiguration laden", wechseln Sie in ihr Projektverzeichnis und laden Sie die Konfigurationsdatei "Projektname.SSC-PC2.dat".
3. Geben Sie das Passwort für den privaten Schlüssel des Zertifikats ein und bestätigen Sie mit "Weiter".
4. Bestätigen Sie den Dialog "Alle statisch konfigurierten Teilnehmer aktivieren?" mit "Ja".
5. Betätigen Sie die Schaltfläche "Tunnelübersicht".

Ergebnis: aktive Tunnelverbindung

Der Tunnel zwischen SCALANCE S und SOFTNET Security Client wurde aufgebaut. Dieser Betriebszustand wird durch den grünen Kreis beim Eintrag "Module1" signalisiert.

In der Log-Konsole der Tunnelübersicht des SOFTNET Security Client erhalten Sie einige Rückmeldungen von Ihrem System, wie der Verbindungsversuch abgelaufen ist und ob eine Policy für die Kommunikationsverbindung erstellt wurde.



Die Inbetriebsetzung der Konfiguration ist damit abgeschlossen und das SCALANCE S Modul und der SOFTNET Security Client haben einen Kommunikationstunnel aufgebaut, über den Netzknoten aus dem internen Netz und PC2 gesichert kommunizieren können.

3.4.8 Tunnelfunktion testen (Ping-Test)

Wie können Sie die konfigurierte Funktion testen?

Die Funktionstests können Sie wie nachfolgend beschrieben mit einem Ping-Kommando durchführen.

Alternativ können Sie auch andere Kommunikationsprogramme für den Test der Konfiguration verwenden.

ACHTUNG
Bei Windows kann die Firewall standardmäßig so eingestellt sein, dass PING-Kommandos nicht passieren können. Sie müssen ggf. die ICMP-Dienste vom Typ Request und Response freischalten.

Testabschnitt 1

Testen Sie nun die Funktion der zwischen PC1 und PC2 aufgebauten Tunnelverbindung wie folgt:

1. Rufen Sie auf dem PC2 in der Startleiste den folgenden Menübefehl auf:

   Start ► Alle Programme ► Zubehör ► Eingabeaufforderung

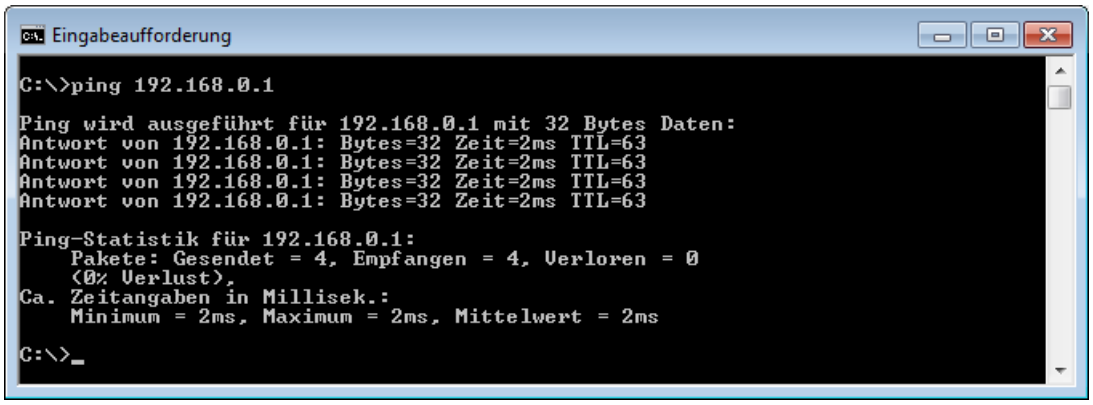
2. Eingabe des Ping-Kommandos von PC2 an den PC1 (IP-Adresse 192.168.0.1).

   Unmittelbar in die Kommandozeile des aufgeblendeten Fensters "Eingabeaufforderung", an der Cursor-Position, geben Sie den Befehl

   ping 192.168.0.1

   ein.

Sie erhalten daraufhin folgende Meldung: (positive Antwort von PC1).



Ergebnis

Wenn die IP-Telegramme PC1 erreicht haben, gibt die "Ping-Statistik" für 192.168.0.1 folgendes aus:

- Gesendet = 4
- Empfangen = 4
- Verloren = 0 (0% Verlust)

Da keine andere Kommunikation zugelassen war, können diese Telegramme nur durch den VPN-Tunnel transportiert worden sein.

Testabschnitt 2

Wiederholen Sie nun den Test, indem Sie ein Ping-Kommando von PC3 aus absetzen.

1. Rufen Sie auf PC3 in der Startleiste den folgenden Menübefehl auf:

   Start ► Alle Programme ► Zubehör ► Eingabeaufforderung

2. Setzen Sie erneut das gleiche Ping-Kommando (**ping 192.168.0.1**) im Fenster der Eingabeaufforderung von PC3 aus ab.

Sie erhalten daraufhin folgende Meldung: (keine Antwort von PC1).

Ergebnis

Die IP-Telegramme von PC3 können PC1 nicht erreichen, da weder eine Tunnel-Kommunikation zwischen diesen Geräten konfiguriert ist, noch normaler IP-Datenverkehr erlaubt ist.

Das wird in der "Ping-Statistik" für 192.168.0.1 folgendermaßen angegeben:

- Gesendet = 4
- Empfangen = 0
- Verloren = 4 (100% Verlust)

3.5 Beispiel 5: Fernzugriff - VPN-Tunnel-Beispiel mit MD741-1 und SOFTNET Security Client

3.5.1 Übersicht

In diesem Beispiel wird die VPN-Tunnelfunktion in der Projektierungssicht "Erweitert-Modus" projektiert. Ein MD741-1 und der SOFTNET Security Client bilden die beiden Tunnelendpunkte für die gesicherte Tunnelverbindung über ein öffentliches Netzwerk.

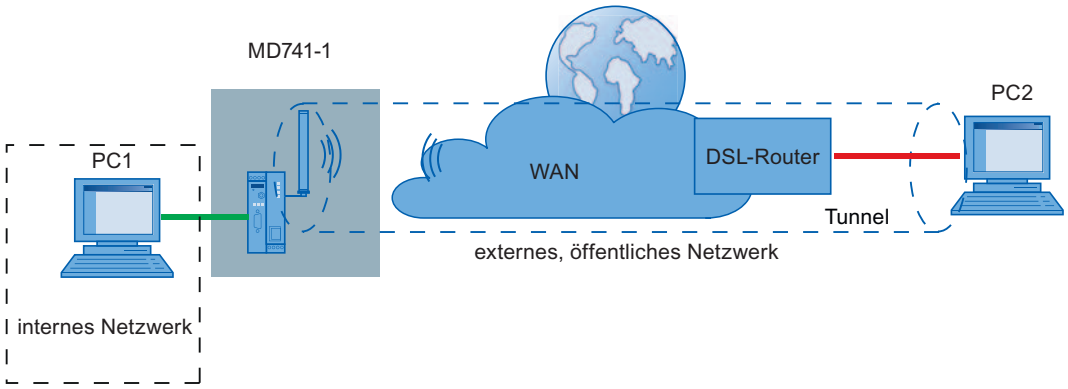
Sie erreichen mit dieser Konfiguration, dass IP-Verkehr nur über die eingerichtete VPN-Tunnelverbindung zwischen autorisierten Partnern möglich ist.

Hinweis

Für die Konfiguration dieses Beispiels ist es zwingend erforderlich, dass Sie für die SIM-Karte des MD741-1 von Ihrem Provider (Mobilfunkanbieter) eine öffentliche, sich nicht ändernde IP-Adresse zur Verfügung gestellt bekommen, welche auch aus dem Internet erreichbar ist.

(Alternativ kann auch mit einer DynDNS-Adresse für das MD741-1 gearbeitet werden.)

Aufbau des Testnetzes:



- Internes Netzwerk - Anschluss an MD741-1 Port X2 ("Netzwerk Intern")

  Im internen Netzwerk wird im Testaufbau ein Netzknoten durch einen PC realisiert, der an den "Internal Network"-Port (Port X2) eines MD741-1 Moduls angeschlossen ist.

  – PC1: repräsentiert einen Teilnehmer des internen Netzwerks

  – MD741-1: MD741-1 Modul für den Schutz des internen Netzwerks

  Externes, öffentliches Netzwerk - Anbindung über MD741-1 Antenne ("Netzwerk Extern")

  Das externe, öffentliche Netzwerk ist ausschließlich ein GSM- oder Mobilfunktnetz, welches vom Anwender beim Provider (Mobilfunkanbieter) gewählt werden kann und wird über die Antenne des MD741-1 Moduls erreicht.

  – PC2: PC mit der Konfigurationssoftware Security Configuration Tool und der Software SOFTNET Security Client für den sicheren VPN-Zugang in das interne Netzwerk

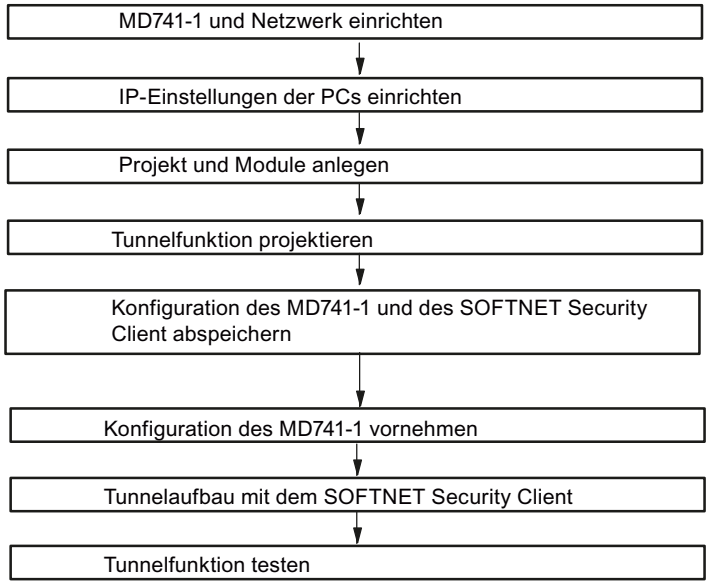
Erforderliche Geräte/Komponenten:

Für den Aufbau verwenden Sie folgende Komponenten:

- 1x MD741-1 Modul mit SIM-Karte, (optional: eine entsprechend montierte Hutschiene mit Montagematerial);
- 1x 24V-Stromversorgung mit Kabelverbindung und Klemmenblockstecker;

- 1x PC auf dem das Projektierungswerkzeug "Security Configuration Tool" und der VPN-Client "SOFTNET Security Client" installiert ist;
- 1x PC im internen Netz, des MD741-1 mit einem Browser für die Projektierung des MD741-1 und den Test der Konfiguration;
- 1x DSL-Router (Verbindung in das Internet für den PC mit dem VPN-Client (ISDN, DSL, UMTS, etc.))
- Die nötigen Netzwerkkabel, TP-Kabel (Twisted Pair) nach dem Standard IE FC RJ45 für Industrial Ethernet.

Die folgenden Schritte in der Übersicht



3.5.2 MD741-1 und Netzwerk einrichten

Gehen Sie wie folgt vor:

1. Packen Sie zunächst das MD741-1 Gerät aus und überprüfen Sie den unbeschädigten Zustand.
2. Folgen Sie der "Schritt für Schritt" Inbetriebnahme des MD741-1 Systemhandbuchs bis zu dem Punkt, an welchem Sie es nach Ihren Anforderungen einrichten sollen. Benutzen Sie dazu PC1, Einrichten des MD741, siehe Kapitel Konfiguration des MD741-1 vornehmen (Seite 98).

3. Stellen Sie jetzt die physikalischen Netzwerkverbindungen her, indem Sie die Stecker der Netzwerkkabel in die dafür vorgesehenen Ports (RJ45-Buchsen) stecken:
   - Verbinden Sie PC1 mit Port X2 ("Netzwerk Intern") vom MD741-1
   - Verbinden Sie PC2 mit dem DSL-Router
4. Schalten Sie jetzt die beteiligten PCs ein.

3.5.3 IP-Einstellungen der PCs einrichten

Die PCs sollten für den Test folgende IP-Adress-Einstellungen erhalten.

PC	IP-Adresse	Subnetzmaske	Standardgateway
PC1	192.168.1.101	255.255.255.0	192.168.1.1
PC2	192.168.2.202	255.255.255.0	192.168.2.1

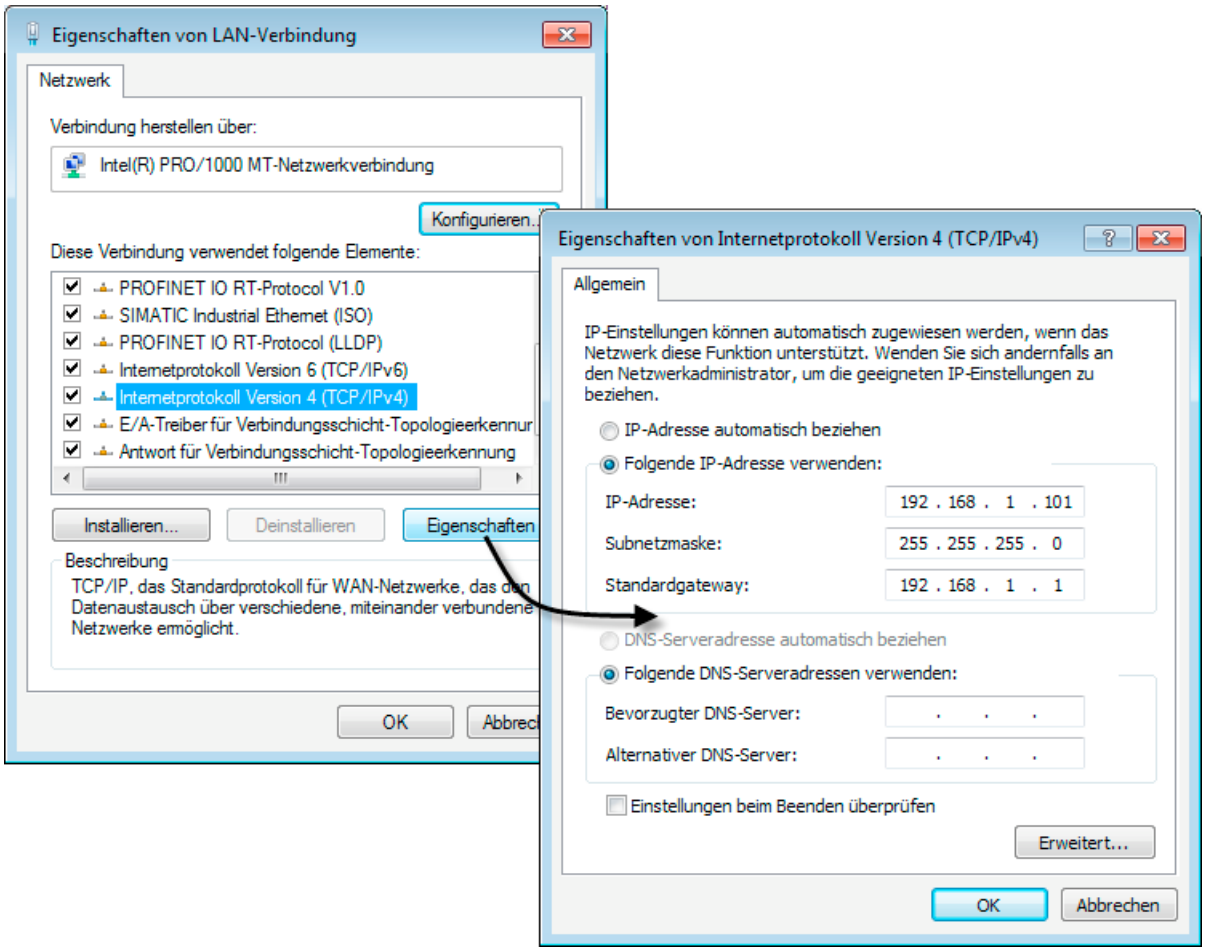
Unter Standardgateway für PC1 ist die IP-Adresse anzugeben, die Sie dem MD741-1 Modul (für die interne Netzwerkschnittstelle) in der nachfolgenden Projektierung zuweisen. Für PC2 geben Sie die IP-Adresse des DSL-Routers (für die interne Netzwerkschnittstelle) an.

Gehen Sie bei PC1 und PC2 jeweils folgendermaßen vor, um auf dem betreffenden PC die Netzwerkverbindungen zu öffnen:

1. Öffnen Sie auf dem betreffenden PC die Systemsteuerung mit folgendem Menübefehl:

   Start ► Systemsteuerung
2. Öffnen Sie das Symbol "Netzwerk und Freigabecenter".

3. Aktivieren Sie im Dialog "Eigenschaften von LAN-Verbindung" das Optionskästchen "Internetprotokoll Version 4 (TCP/IPv4)" und betätigen Sie die Schaltfläche "Eigenschaften".



4. Wählen Sie im Dialog "Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)" das Optionsfeld "Folgende IP-Adresse verwenden:" aus. Geben Sie jetzt die dem PC zugeordneten Werte aus der Tabelle "*IP-Einstellungen der PCs einrichten*" in die dafür vorgesehenen Felder ein.

   Schließen Sie die Dialoge mit "OK" ab und verlassen Sie die Systemsteuerung.

3.5.4 Projekt und Module anlegen

Gehen Sie wie folgt vor:

1. Starten Sie die Projektierungssoftware Security Configuration Tool auf PC2.

2. Erzeugen Sie ein neues Projekt mit folgendem Menübefehl:

   Projekt ► Neu

   Sie werden aufgefordert, einen Benutzernamen und ein Passwort anzugeben. Dem Benutzereintrag, den Sie hierbei festlegen, wird automatisch die Rolle eines Administrators zugewiesen.

3. Geben Sie einen Benutzernamen und ein Passwort ein und bestätigen Sie Ihre Eingabe; damit legen Sie ein neues Projekt an.

   Der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" wird automatisch eingeblendet.

4. Konfigurieren Sie jetzt den Produkttyp "SOFTNET Configuration (SOFTNET Security Client, MD74x)", die Baugruppe "SOFTNET Security Client", das Firmware-Version "V3.0" und vergeben Sie den Modulnamen "SSC-PC2".

5. Schließen Sie den Dialog mit "OK".

6. Erzeugen Sie ein 2. Modul mit folgendem Menübefehl:

   Einfügen ► Modul

   Konfigurieren Sie jetzt den Produkttyp "SOFTNET Configuration (SOFTNET Security Client, MD74x)", die Baugruppe "MD74x" und vergeben Sie den Modulnamen "MD741-1".

7. Klicken Sie jetzt im Bereich "Konfiguration" in das Feld "IP-Adresse (ext.)" und geben Sie diese im vorgegebenen Format ein. Konfigurieren Sie außerdem die dazugehörige externe Subnetzmaske.

   Hinweis

   Für die Konfiguration dieses Beispiels ist es zwingend erforderlich, dass Sie für die SIM-Karte des MD 741-1 von Ihrem Provider (Mobilfunkanbieter) eine öffentliche, sich nicht ändernde IP-Adresse zur Verfügung gestellt bekommen, welche auch aus dem Internet erreichbar ist. Tragen Sie diese IP-Adresse als externe IP-Adresse für Ihr Modul ein.

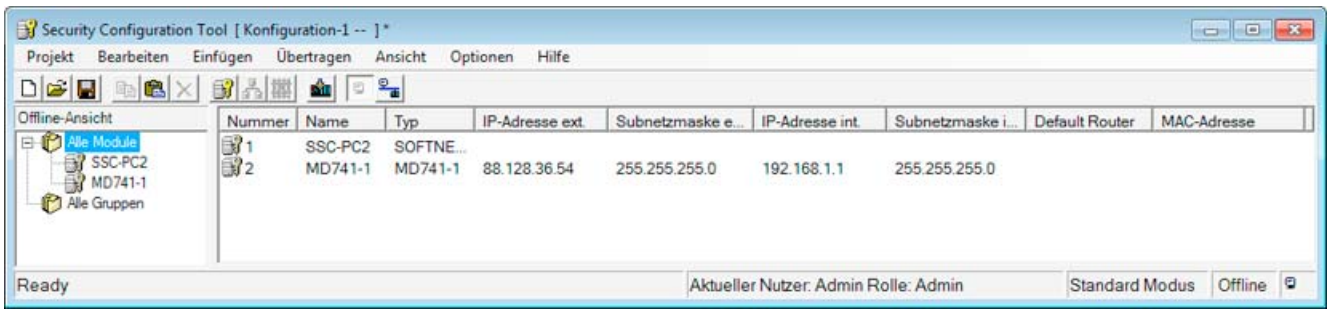
   Wenn Sie mit dynamischen Adressen für das MD741-1 arbeiten, benötigen Sie eine DynDNS-Adresse für das Modul. In diesem Fall brauchen Sie die externe IP-Adresse an dieser Stelle nicht anzupassen. Die eingetragene IP-Adresse dient somit lediglich als Platzhalter.

   Bei der Konfiguration des SOFTNET Security Client vergeben Sie dann später an Stelle einer externen IP-Adresse einen DNS-Namen.

8. Klicken Sie jetzt im Bereich "Konfiguration" in das Feld "IP-Adresse (int.)" und geben Sie diese im vorgegebenen Format ein. (IP-Adresse: 192.168.1.1) Konfigurieren Sie außerdem die dazugehörige interne Subnetzmaske. (Subnetzmaske: 255.255.255.0)

9. Schließen Sie nun den Dialog mit "OK".

Sie erhalten eine Ansicht entsprechend dem folgenden Bild.



3.5.5 Tunnelverbindung projektieren

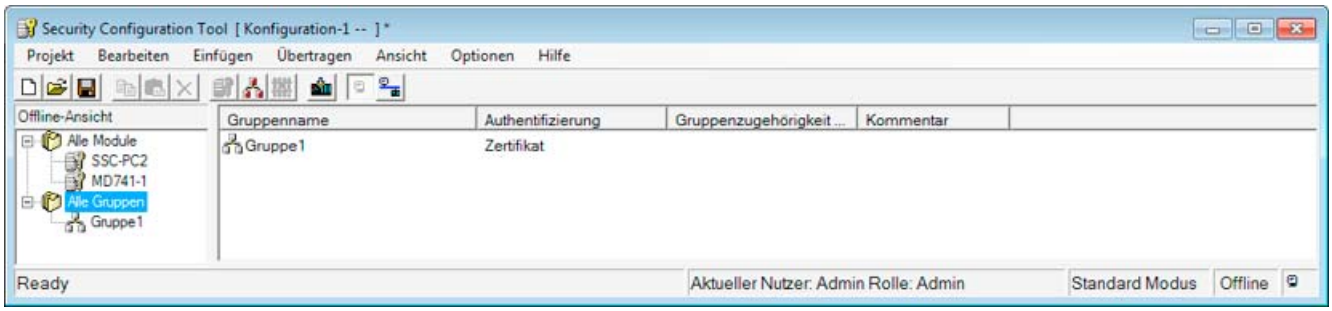
Ein MD741-1 und der SOFTNET Security Client können genau dann einen IPsec-Tunnel für die gesicherte Kommunikation aufbauen, wenn sie im Projekt der gleichen Gruppe zugeordnet sind.

Gehen Sie wie folgt vor:

1. Selektieren Sie im Navigationsbereich "Alle Gruppen" und erzeugen Sie mit folgendem Menübefehl eine neue Gruppe:

   Einfügen ► Gruppe

   Diese Gruppe erhält automatisch den Namen "Gruppe1".



2. Selektieren Sie im Inhaltsbereich das MD741-1 Modul "MD741-1" und ziehen Sie es auf "Gruppe1" im Navigationsbereich.

   Das Modul ist jetzt dieser Gruppe zugeordnet bzw. Mitglied dieser Gruppe.

   Die Farbe vom Schlüsselsymbol des Modul-Icons schlägt hierbei von grau nach blau um. Was aussagt, dass für das Modul eine IPsec-Verbindung projektiert wurde.

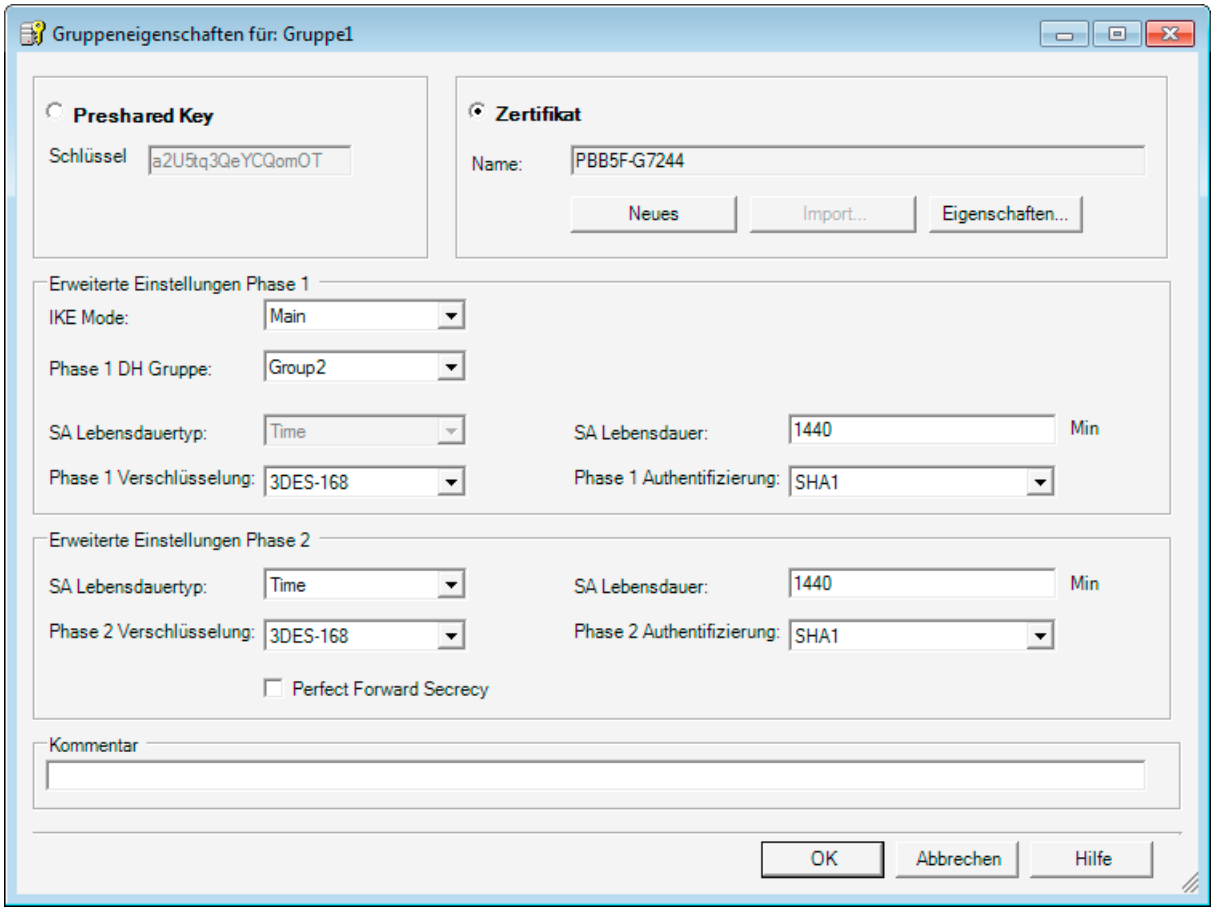
3. Selektieren sie im Inhaltsbereich das SOFTNET Security Client Modul "SSC-PC2" und ziehen Sie es auf "Gruppe1" im Navigationsbereich.

   Das Modul ist jetzt ebenso dieser Gruppe zugeordnet.

4. Versetzen Sie Ihr Projekt jetzt in den "Erweitert-Modus" indem Sie folgendem Menübefehl folgen:

   Ansicht ► Erweitert-Modus

5. Öffnen Sie die Gruppeneigenschaften der Gruppe1 indem Sie im Kontextmenü "Eigenschaften..." auswählen.
6. Ändern Sie die SA Lebensdauer für Phase 1 und Phase 2 auf 1440 Minuten und belassen Sie alle anderen Einstellungen auf Ihren Defaultwerten.



ACHTUNG

Eine erfolgreiche Tunnelverbindung zwischen MD741-1 und SOFTNET Security Client kann nur aufgebaut werden, wenn Sie sich genau an die nachfolgend aufgeführten Parameter halten.

Die Verwendung von abweichenden Parametern kann dazu führen, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen können.

Authentisierungsverfahren: Zertifikat

Erweiterte Einstellungen Phase 1:

- IKE Mode: Main
- Phase 1 DH Gruppe: Group2
- Phase 1 Verschlüsselung: 3DES-168
- SA Lebensdauer (Minuten): 1440
- Phase 1 Authentifizierung: SHA1

Erweiterte Einstellungen Phase 2:

- SA Lebensdauertyp: Time
- Phase 2 Verschlüsselung: 3DES-168
- SA Lebensdauer (Minuten): 1440
- Phase 2 Authentifizierung: SHA1

7. Speichern Sie dieses Projekt jetzt mit dem folgenden Menübefehl unter einem zweckmäßigen Namen ab:

   Projekt ► Speichern unter...

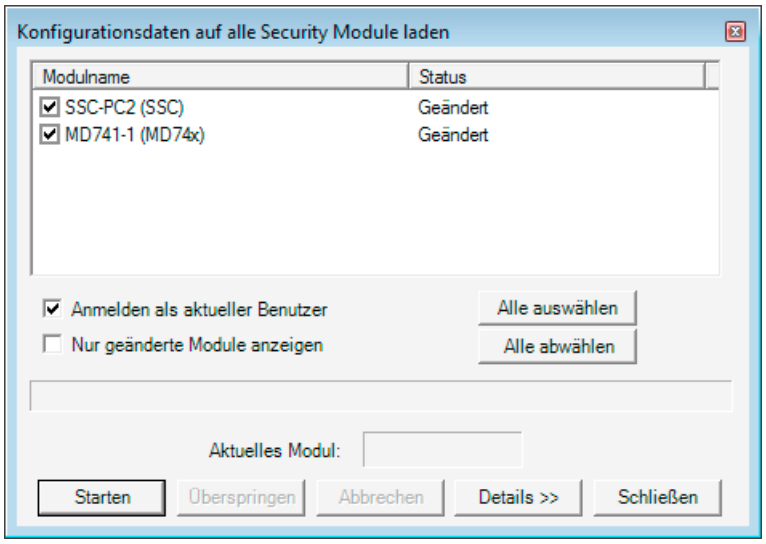
Die Konfiguration der Tunnelverbindung ist damit abgeschlossen.

3.5.6 Konfiguration des MD741-1 und des SOFTNET Security Client abspeichern

Gehen Sie wie folgt vor:

1. Rufen Sie mit folgendem Menübefehl den folgenden Dialog auf:

Übertragen ▸ An alle Module...



2. Starten Sie den Ladevorgang über die Schaltfläche "Starten".
3. Speichern Sie die Konfigurationsdatei "Projektname.SSC-PC2.dat" in Ihr Projektverzeichnis und vergeben Sie ein Passwort für den privaten Schlüssel des Zertifikats. In Ihr Projektverzeichnis werden folgende Dateien abgespeichert:
   - "Projektname.SSC-PC2.dat"
   - "Projektname.Zeichenfolge.SSC-PC2.p12"
   - "Projektname.Gruppe1.cer"
4. Speichern Sie die Konfigurationsdatei "Projektname.MD741-1.txt" in Ihr Projektverzeichnis und vergeben Sie ein Passwort für den privaten Schlüssel des Zertifikats. In Ihr Projektverzeichnis werden folgende Dateien abgespeichert:
   - "Projektname.MD741-1.txt"
   - "Projektname.Zeichenfolge.MD741-1.p12"
   - "Projektname.Gruppe1.MD741-1.cer"

Sie haben nun alle notwendigen Dateien und Zertifikate abgespeichert und können nun den MD741-1 und den SOFTNET Security Client in Betrieb nehmen.

3.5.7 Konfiguration des MD741-1 vornehmen

Mit Hilfe des abgespeicherten Textfiles "Projektname.MD741-1.txt" nehmen Sie anhand des Web Based Management des MD741-1 sehr einfach seine Konfiguration vor. Nachfolgend wird Ihnen anhand dieses Beispiels Schritt für Schritt die Konfiguration des MD741-1 aufgezeigt.

Für die Konfiguration wird Folgendes angenommen:

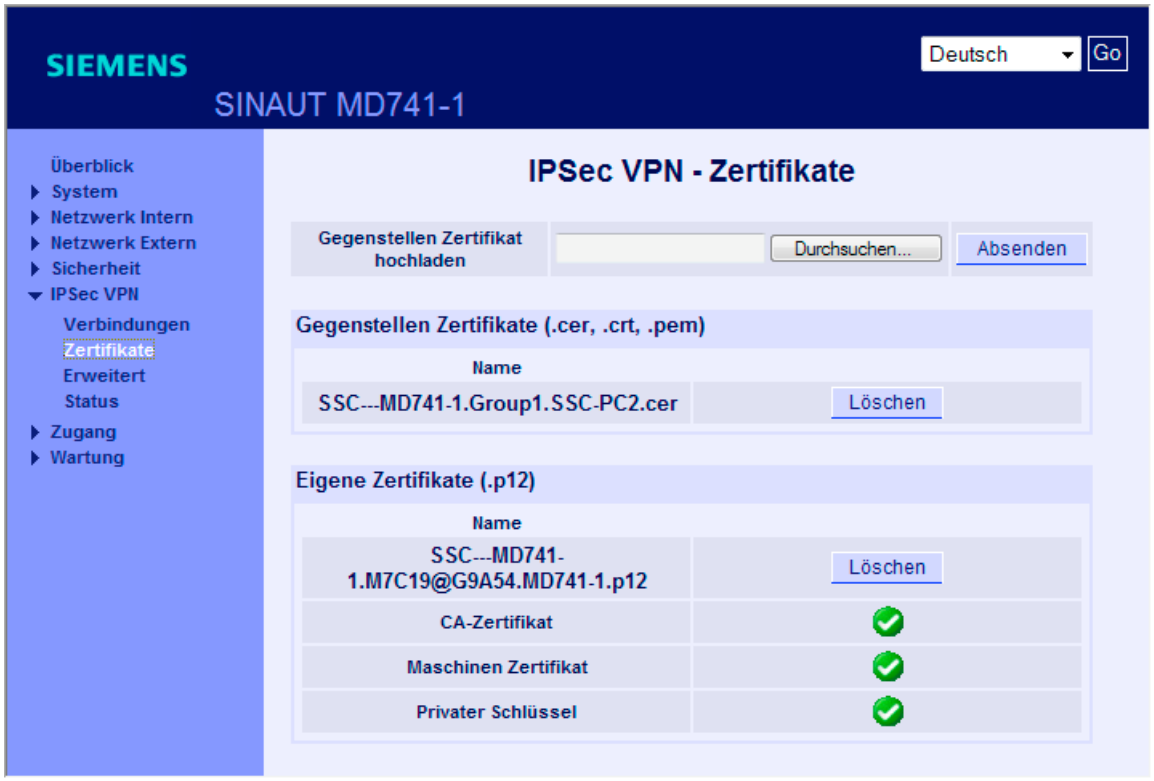
- MD741-1 erhält eine öffentliche, feste IP-Adresse, welche über das Internet erreichbar ist;
- der SOFTNET Security Client erhält eine dynamische IP-Adresse vom Provider zugewiesen.

Parallel wird an den entsprechenden Stellen auch der Hinweis auf die Projektierung eines DynDNS-Namens für den MD741-1 gegeben.

Gehen Sie wie folgt vor:

1. Verbinden Sie sich über PC1 mit der Web-Oberfläche des MD741-1.
   Anmerkung: Befindet sich das MD741-1 in Werkseinstellung, so hat die interne Schnittstelle des Moduls die IP-Adresse 192.168.1.1
2. Navigieren Sie in folgendes Verzeichnis:

   IPSec VPN ► Zertifikate
3. Die benötigten Zertifikate haben Sie im letzten Kapitel auf PC2 abgespeichert und ein Passwort für den privaten Schlüssel vergeben. Übertragen Sie die Zertifikate ("Projektname.Zeichenfolge.MD741-1.p12", "Projektname.Gruppe1.MD741-1.cer") für das MD741-1 zunächst auf PC1.
4. Laden Sie nun das Gegenstellen Zertifikat "Projektname. Gruppe1.MD741-1.cer" sowie die PKCS 12 Datei "Projektname.Zeichenfolge.MD741-1.p12" auf das Modul hoch.



VPN Roadwarrior Modus des MD741-1

Da der SOFTNET Security Client über eine dynamische IP-Adresse verfügt, wird der VPN Roadwarrior Modus des MD741-1 genutzt, um eine gesicherte Verbindung aufzubauen.

- Roadwarrior Modus des MD741-1:
  - Im VPN Roadwarrier Modus kann das SINAUT MD741-1 VPN-Verbindungen von Gegenstellen mit unbekannter Adresse annehmen. Das können zum Beispiel Gegenstellen im mobilen Einsatz sein, die ihre IP-Adresse dynamisch beziehen.
  - Die VPN-Verbindung muss durch die Gegenstelle aufgebaut werden. Es ist nur eine VPN-Verbindung im Roadwarrier Modus möglich. VPN-Verbindungen im Standard Modus können dazu parallel betrieben werden.

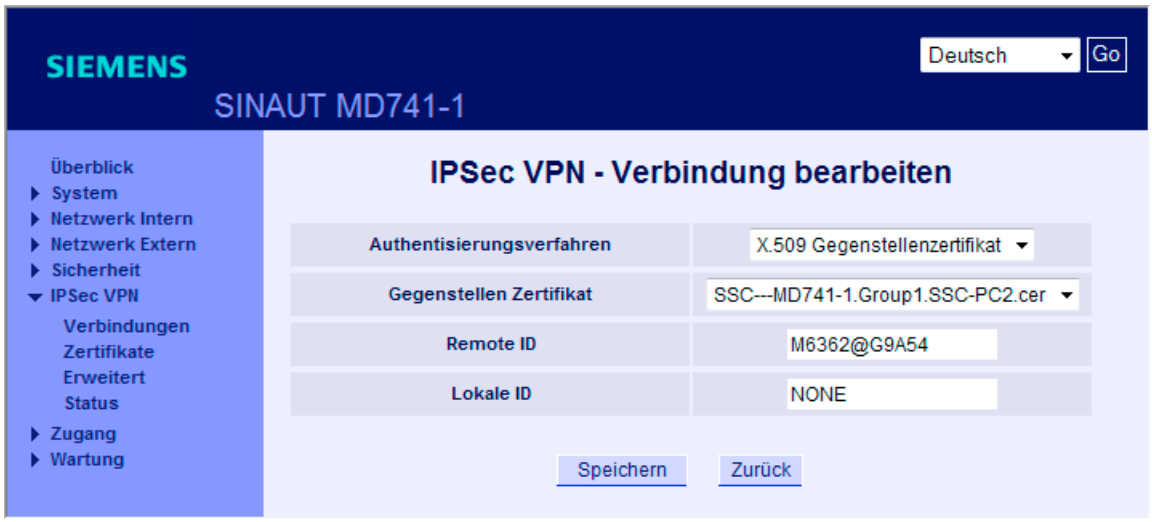
Gehen Sie wie folgt vor:

1. Navigieren Sie in folgendes Verzeichnis:

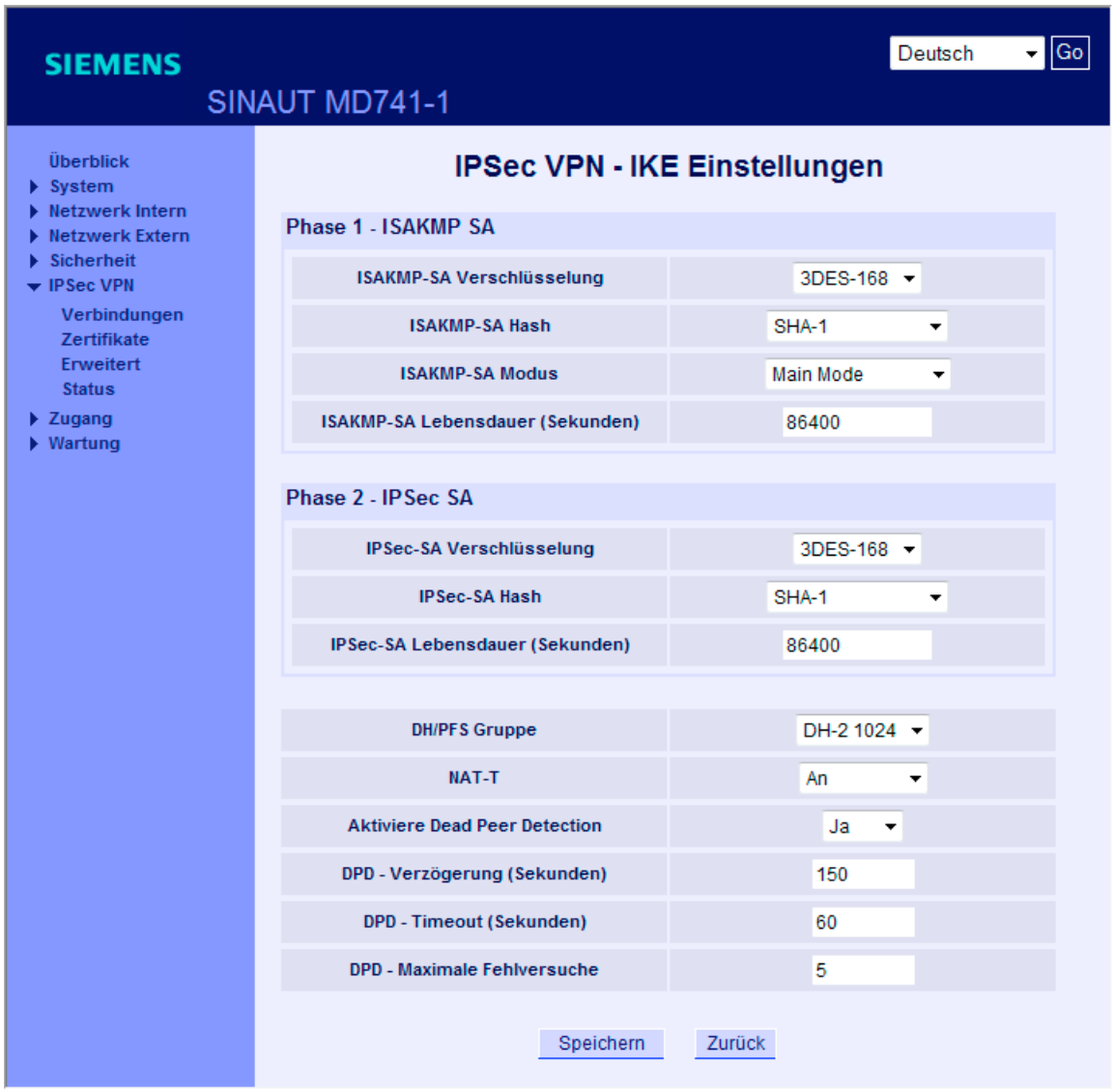
   IPSec VPN ▸ Verbindungen

2. Bearbeiten Sie die Einstellungen des Roadwarrior VPN wie in folgender Abbildung gezeigt und speichern Sie Ihre Eingaben.

   Die "Remote ID" können Sie aus der Textdatei "Projektname.MD741-1.txt" ermitteln. Ein Eintrag der "Remote ID" ist hier optional möglich.



3. Bearbeiten Sie die IKE-Einstellungen des Roadwarrior VPNs wie in folgender Abbildung gezeigt und speichern Sie Ihre Eingaben.



ACHTUNG

Eine erfolgreiche Tunnelverbindung zwischen MD741-1 und SOFTNET Security Client kann nur dann aufgebaut werden, wenn Sie sich genau an die nachfolgend aufgeführten Parameter halten.

Die Verwendung von abweichenden Parametern führt dazu, dass die beiden Tunnelpartner keine VPN-Verbindung miteinander aufbauen. Halten Sie sich daher bitte immer an die im ausgeleiteten Textfile angegebenen Einstellungen (wie nachfolgend zusätzlich aufgeführt).

Authentisierungsverfahren:X.509 Gegenstellenzertifikat

Phase 1 - ISKAMP SA:

- ISAKMP-SA Verschlüsselung:3DES-168
- ISAKMP-SA Hash: SHA-1
- ISAKMP-SA Modus: Main Mode
- ISAKMP-SA Lebensdauer (Sekunden): 86400

Phase 2 - IPSec SA:

- IPSec SA Verschlüsselung: 3DES-168
- IPSec SA Hash: SHA-1
- IPSec SA Lebensdauer (Sekunden): 86400

DH/PFS Gruppe: DH-2 1024

4. Um die Diagnosefunktion des SOFTNET Security Client für erfolgreich aufgebaute VPN-Tunnel in Verbindung mit dem MD741-1 nutzen zu können, müssen Sie einen Ping aus dem externen Netz des MD741-1 zulassen.

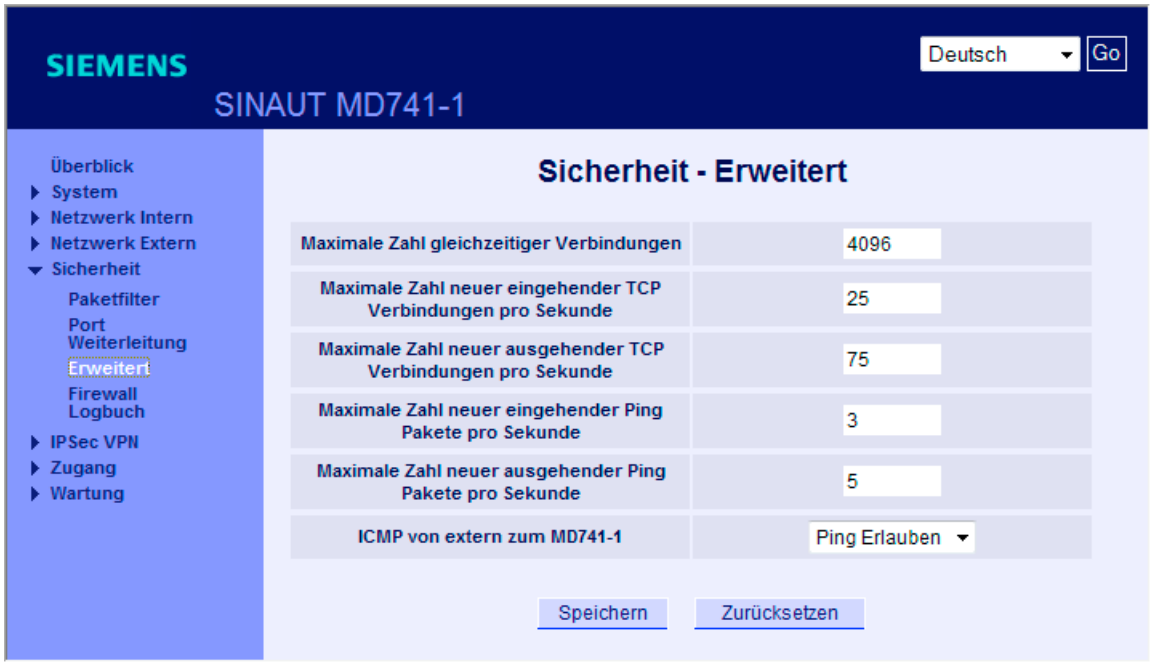
   Navigieren Sie dazu in das Verzeichnis:

   Sicherheit ► Erweitert

   Setzen Sie die Funktion "ICMP von extern zum MD741-1" auf den Wert "Ping Erlauben und speichern Sie Ihre Eingabe. Beachten Sie dazu die nachfolgende Abbildung.

   Hinweis

   Wenn Sie diese Funktion nicht freigeben, dann können Sie die Diagnosefunktion des SOFTNET Security Client für erfolgreich aufgebaute VPN-Tunnel in Verbindung mit dem MD741-1 nicht nutzen. Sie erhalten dann keine Rückmeldung darüber ob der Tunnel erfolgreich aufgebaut wurde, können aber trotzdem sicher über den Tunnel kommunizieren.



5. Damit Sie das Webinterface des MD741-1 Moduls auch über das externe Interface erreichen können, geben Sie den HTTPS-Fernzugang frei.

   Sie haben dadurch die Möglichkeit, das MD741-1 über einen aufgebauten Tunnel aus der Ferne zu konfigurieren und zu diagnostizieren.

   Navigieren Sie dazu in das Verzeichnis:

   Zugang ► HTTPS

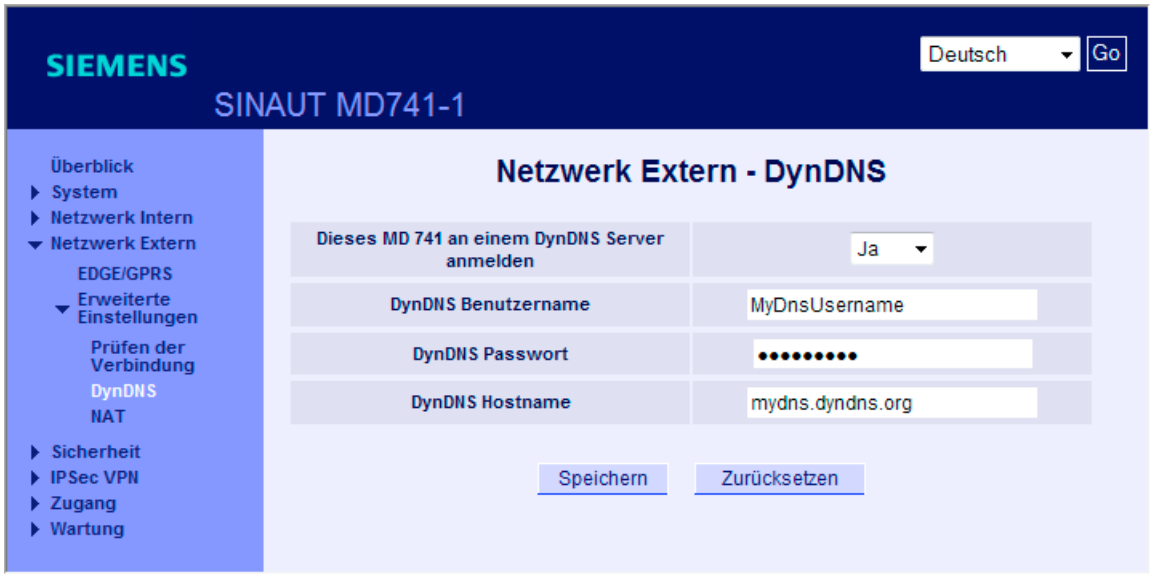
   Setzen Sie die Funktion "HTTPS Fernzugang aktivieren" auf den Wert "Ja", wie in der nachfolgenden Abbildung gezeigt und speichern Sie Ihre Eingabe.

Hinweis

Wenn Sie das MD741-1 über einen DNS-Namen erreichen wollen, parametrieren Sie im folgenden Verzeichnis die DynDNS Server Anbindung:

Netzwerk Extern ▸ Erweiterte Einstellungen ▸DynDNS

1. Ändern Sie die Einstellung "Dieses MD741 an einem DynDNS Server anmelden" auf den Wert "Ja".
2. Geben Sie Ihren Benutzernamen sowie das Passwort Ihres DynDNS Accounts an.
3. Tragen Sie die vollständige DynDNS Adresse in das Feld "DynDNS Hostname" ein. Achten Sie dabei darauf, das Sie auch die Domäne für diese Adresse mit angeben. (Bsp.: "mydns.dyndns.org")



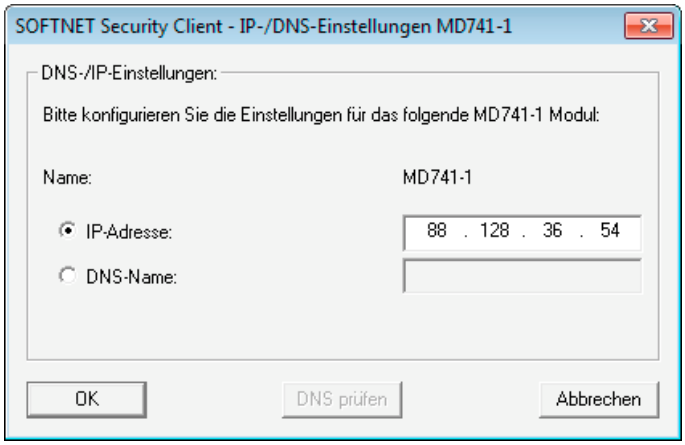
Die Inbetriebsetzung des MD741-1 Moduls ist damit abgeschlossen. Das Modul und der SOFTNET Security Client können einen Kommunikationstunnel aufbauen, über den Netzknoten aus dem internen Netz gesichert mit PC2 kommunizieren können.

3.5.8 Tunnelaufbau mit dem SOFTNET Security Client

Gehen Sie wie folgt vor:

1. Starten Sie den SOFTNET Security Client auf PC2.
2. Betätigen Sie die Schaltfläche "Konfiguration laden", wechseln Sie in Ihr Projektverzeichnis und laden Sie die Konfigurationsdatei "Projektname.SSC-PC2.dat".
3. Für eine MD741-1 Konfiguration öffnet der SOFTNET Security Client den Dialog "IP-/DNS-Einstellungen MD741-1". Geben Sie in diesem Dialog die öffentliche IP-Adresse des MD741-1 Moduls an, welche Sie von Ihrem Provider erhalten haben. Bestätigen Sie den Dialog mit "OK".

   Anmerkung: Wenn Sie mit einem DNS-Namen arbeiten, dann können Sie diesen statt einer IP-Adresse in diesem Dialog konfigurieren.

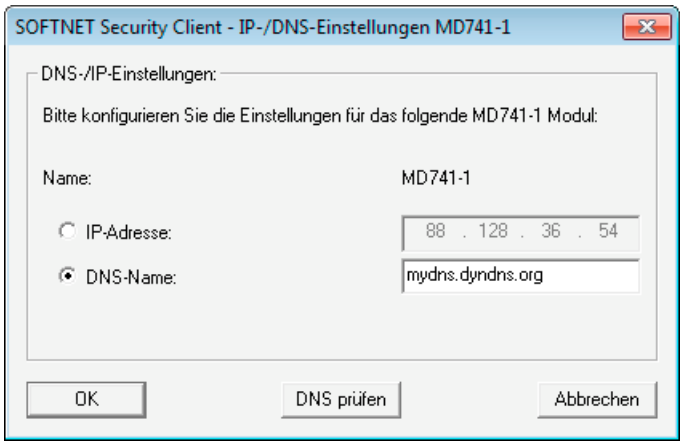


4. Geben Sie das Passwort für das Zertifikat ein und bestätigen Sie mit "Weiter".

5. Bestätigen Sie den Dialog "Alle statisch konfigurierten Teilnehmer aktivieren?" mit "Ja".
6. Betätigen Sie die Schaltfläche "Tunnelübersicht".

Hinweis

Wenn Sie das MD741-1 Modul über einen DNS-Namen erreichen wollen, dann parametrieren Sie bei Schritt 3 die vollständige DynDNS-Adresse im Eingabefeld "DNS-Name". (Bsp.: "mydns.dyndns.org")



Ergebnis: aktive Tunnelverbindung

Der Tunnel zwischen MD741-1 und SOFTNET Security Client wurde aufgebaut.

Anhand des blauen Icons beim Eintrag "MD741-1" erkennen Sie, dass eine Policy für diese Kommunikationsverbindung erstellt wurde.

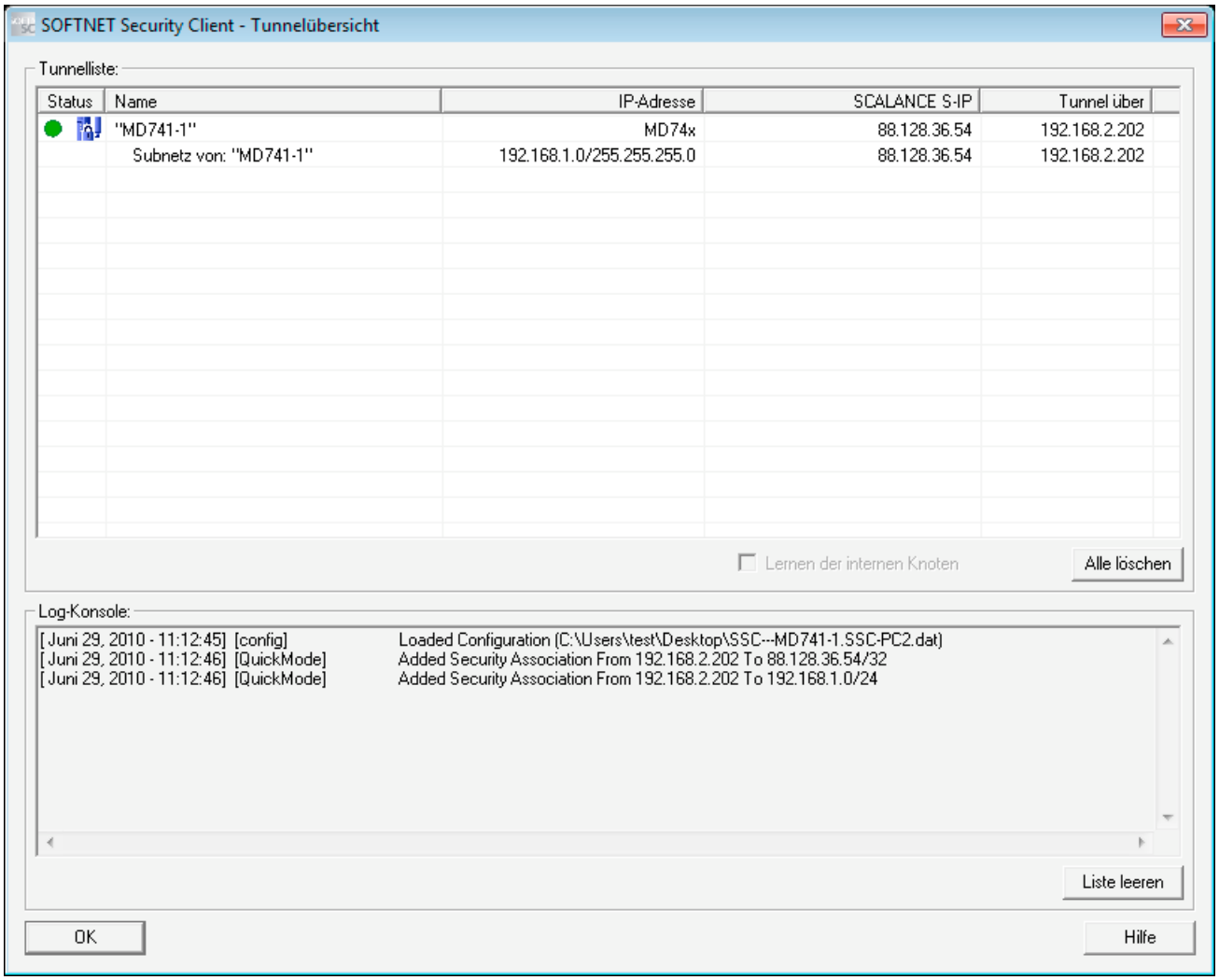
Der Betriebszustand, dass das MD741-1 erreichbar ist, wird durch den "grünen Kreis" beim Eintrag "MD741-1" signalisiert.

Hinweis

Beachten Sie, dass diese Funktion abhängig von der Freigabe der Ping-Funktion auf dem MD741-1 Modul ist.

In der Log-Konsole der Tunnelübersicht des SOFTNET Security Client erhalten Sie zusätzlich einige Rückmeldungen von Ihrem System, denen Sie entnehmen können:

- Wie ist der Verbindungsversuch abgelaufen?
- Wurde die Policy für Ihre Kommunikationsverbindung erstellt?



Die Inbetriebsetzung der Konfiguration ist damit abgeschlossen. Das MD741-1 Modul und der SOFTNET Security Client haben einen Kommunikationstunnel aufgebaut, über den Netzknoten aus dem internen Netz mit PC2 gesichert kommunizieren können.

3.5.9 Tunnelfunktion testen (Ping-Test)

Wie können Sie die konfigurierte Funktion testen?

Die Funktionstests führen Sie wie nachfolgend beschrieben mit einem Ping-Kommando durch.

Alternativ können Sie auch andere Kommunikationsprogramme für den Test der Konfiguration verwenden.

ACHTUNG
Bei Windows kann die Firewall standardmäßig so eingestellt sein, dass Ping-Kommandos nicht passieren. Sie müssen gegebenenfalls die ICMP-Dienste vom Typ Request und Response freischalten.

Testabschnitt

Testen Sie nun die Funktion der zwischen PC1 und PC2 aufgebauten Tunnelverbindung wie folgt:

1. Rufen Sie auf dem PC2 in der Startleiste den folgenden Menübefehl auf:

   Start ► Alle Programme ► Zubehör ► Eingabeaufforderung

2. Eingabe des Ping-Kommandos von PC2 an PC1 (IP-Adresse 192.168.1.101).

   Unmittelbar in die Kommandozeile des aufgeblendeten Fensters "Eingabeaufforderung", an der Cursor-Position, geben Sie den Befehl

   Ping 192.168.1.101

   ein.

Sie erhalten daraufhin folgende Meldung: (positive Antwort von PC1).

Ergebnis

Wenn die IP-Telegramme PC1 erreicht haben, gibt die "Ping-Statistik" für 192.168.1.101 Folgendes aus:

- Gesendet = 4
- Empfangen = 4
- Verloren = 0 (0 % Verlust)

Da keine andere Kommunikation zugelassen war, können diese Telegramme nur durch den VPN-Tunnel transportiert worden sein.

Projektierung mit Security Configuration Tool 4

Das Security Configuration Tool ist das zu SCALANCE S mitgelieferte Projektierwerkzeug.

Das vorliegende Kapitel macht Sie mit der Bedienoberfläche und der Funktionsweise des Projektierwerkzeuges vertraut.

Sie erfahren, wie SCALANCE S-Projekte eingerichtet, bedient und verwaltet werden.

Weitere Informationen

Wie Sie Module und IPsec-Tunnel konfigurieren, wird ausführlich in den Folgekapiteln dieses Handbuches erläutert.

Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe. Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

4.1 Funktionsumfang und Arbeitsweise

Leistungsumfang

Sie verwenden das Projektierwerkzeug Security Configuration Tool für diese Aufgaben:

- Projektierung von SCALANCE S
- Projektierung von SOFTNET Security Client (S612 / S613 / MD 741-1)
- Erstellen von Konfigurations-Daten für MD 740-1 / MD 741-1
- Test- und Diagnosefunktionen, Statusanzeigen

Betriebsarten

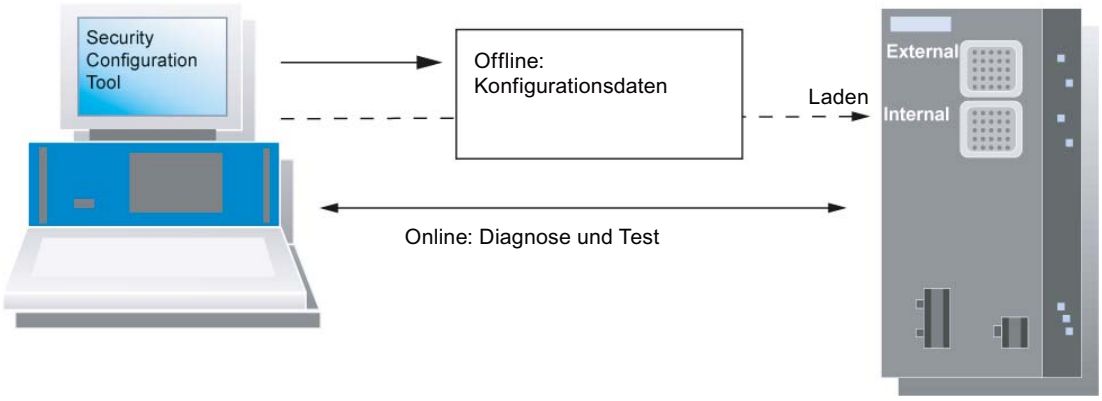
Das Security Configuration Tool verfügt über zwei Betriebsarten:

- Offline - Projektierungssicht

  In der Betriebsart Offline erfolgt die Projektierung der Konfigurationsdaten für die Module SCALANCE S und SOFTNET Security Client. Vor dem Ladevorgang muss hierbei keine Verbindung zu einem SCALANCE S bestehen.

- Online

  Der Online-Modus dient dem Test und der Diagnose eines SCALANCE S.



Zwei Bedienungssichten

In der Betriebsart Offline stellt das Security Configuration Tool zwei Bedienungssichten zur Verfügung:

- Standard-Modus

  Der Standard-Modus ist im Security Configuration Tool voreingestellt. Er bietet eine zügige, unkomplizierte Projektierung für den Betrieb von SCALANCE S.

- Erweitert-Modus

  Im Erweitert-Modus gibt es erweiterte Einstellmöglichkeiten, die eine individuelle Einstellung der Firewall-Regeln und der Sicherheitsfunktionalität zulassen.

Arbeitsweise - Sicherheit und Konsistenz

- Zugriff nur für authorisierte Benutzer

  Jedes Projekt können Sie durch Passwortvergabe vor unberechtigtem Zugriff schützen.

- Konsistente Projektdaten

  Schon während der Eingabe in den einzelnen Dialogen erfolgen Konsistenzprüfungen. Zusätzlich können Sie jederzeit eine dialogübergreifende projektweite Konsistenzprüfung anstoßen.

  Ladbar sind nur konsistente Projektdaten.

- Schutz der Projektdaten durch Verschlüsselung

  Die abgespeicherten Projekt- und Konfigurationsdaten sind sowohl in der Projektdatei als auch auf dem C-Plug durch Verschlüsselung geschützt.

4.2 Installation

Sie installieren das Projektierwerkzeug Security Configuration Tool von der mitgelieferten SCALANCE S CD.

Voraussetzungen

Voraussetzungen für Installation und Betrieb des Security Configuration Tool auf einem PC/PG sind:

- Betriebssystem Windows XP SP2 oder SP3 (nicht Home), Windows 7 (nicht Home);
- PC/PG mit mindestens 128 MByte RAM-Speicher und einer CPU mit einer Taktfrequenz von mindestens 1 GHz.

So gehen Sie vor

ACHTUNG
Vor der Installation des Security Configuration Tool lesen Sie bitte unbedingt die auf der CD mitgelieferte Datei "LIESMICH". In dieser Datei sind ggf. wichtige Hinweise und die letzten Änderungen vermerkt.

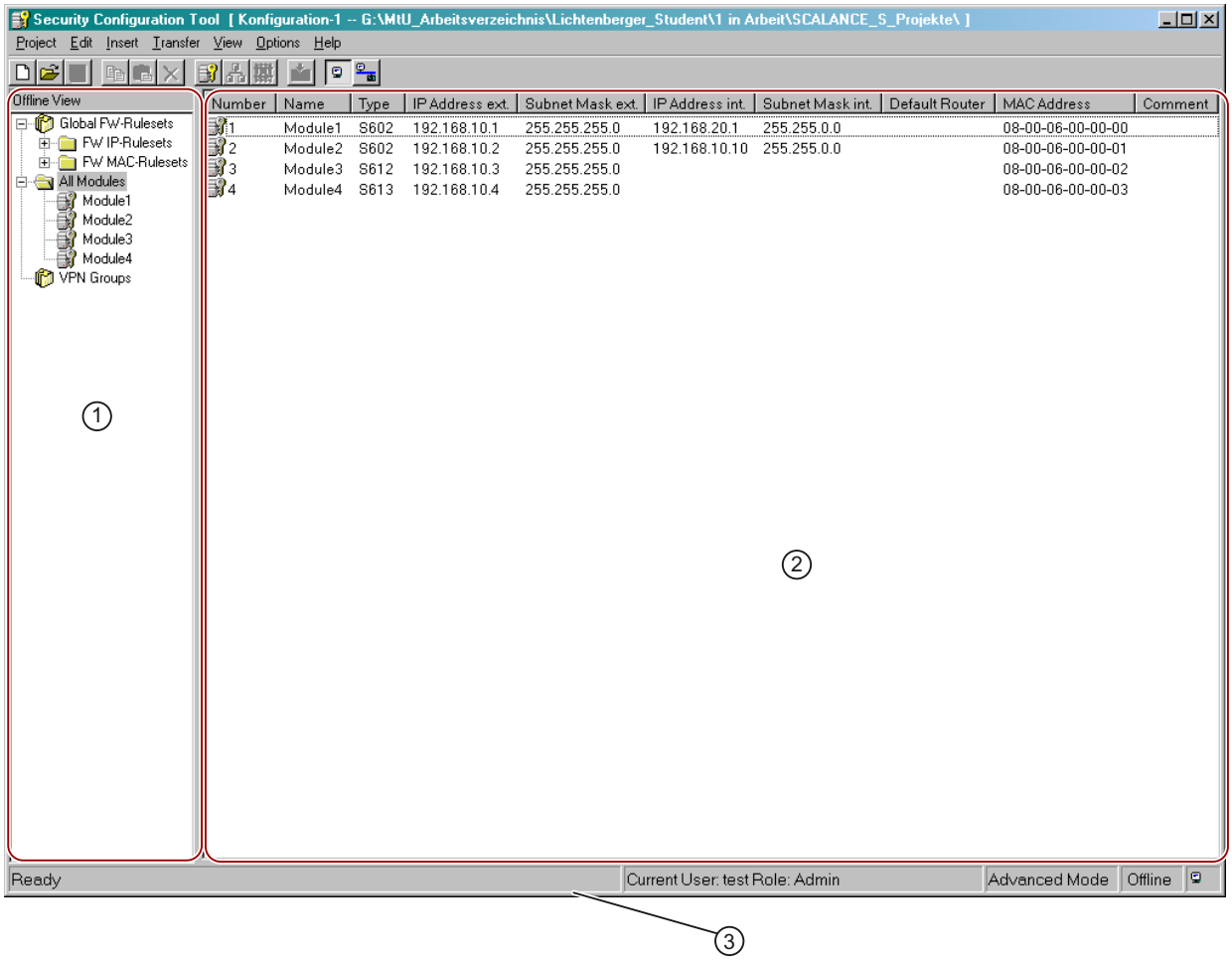
- Legen Sie die SCALANCE S CD in Ihr CD-ROM-Laufwerk; bei eingeschalteter Autorun-Funktion wird die Oberfläche automatisch gestartet, von der aus Sie die Installation durchführen können.

oder

- Starten Sie die auf der mitgelieferten SCALANCE S CD vorhandene Anwendung "start.exe".

4.3 Bedienoberfläche und Menübefehle

Aufbau der Bedienoberfläche



① Der Navigationsbereich fungiert als Projekt-Explorer mit den folgenden Hauptordnern:

- Globale Firewall-Regeln

  Der Knoten enthält die projektierten globalen Firewall-Regelsätze. Weitere Ordner unterscheiden nach:
  - IP-Regelsatz
  - MAC-Regelsatz
- Alle Module

  Der Knoten enthält die projektierten Module SCALANCE S bzw. SOFTNET Security Clients des Projekts.
- Alle Gruppen

  Der Knoten "Alle Gruppen" enthält alle erzeugten VPNs.

Indem Sie ein Objekt im Navigationsbereich anwählen, erhalten Sie im Inhaltsbereich Detailinformationen zu diesem Objekt.

② Inhaltsbereich:
Indem Sie ein Objekt im Navigationsbereich anwählen, erhalten Sie im Inhaltsbereich Detailinformationen zu diesem Objekt.
Einige Parameter können hier eingegeben werden.
Durch Doppelklick auf die Objekte werden Eigenschaftendialoge zur Eingabe weiterer Parameter geöffnet.

③ Statuszeile
Die Statuszeile zeigt Bedienzustände und aktuelle Statusmeldungen an; hierzu gehören:

- Der aktuelle Benutzer und der Benutzertyp
- Die Bedienungssicht - Standard Mode / Advanced Mode
- Die Betriebsart - Online / Offline

Menüleiste

Nachfolgend eine Übersicht der wählbaren Menübefehle und deren Bedeutung.

Menübefehl		Bedeutung / Bemerkungen	Shortcut
Projekt ▸…		Funktionen für die projektspezifischen Einstellungen sowie das Laden und Speichern der Projektdatei.	
	Neu	Neues Projekt anlegen	
	Öffnen…	Bestehendes Projekt öffnen.	
	Speichern	Geöffnetes Projekt unter aktuellem Pfad und Projektnamen speichern.	
	Speichern unter…	Geöffnetes Projekt unter wählbarem Pfad und Projektnamen speichern.	
	Eigenschaften…	Dialog für Projekteigenschaften öffnen.	
	Zuletzt geöffnete Projekte	Direkte Auswahlmöglichkeit der bisher bearbeiteten Projekte.	
	Beenden		
Bearbeiten ▸…		Hinweis: Die hier genannten Funktionen können Sie bei angewähltem Objekt teilweise auch über das Popup-Menü der rechten Maustaste erreichen.	
	Kopieren	Angewähltes Objekt kopieren.	Ctrl+C
	Einfügen	Objekt aus der Zwischenablage holen und einfügen.	Ctrl+V
	Löschen	Angewähltes Objekt löschen.	Del
	Umbenennen	Angewähltes Objekt umbenennen.	F2
	Eigenschaften	Eigenschaftendialog des angewählten Objektes öffnen.	F4
	Online-Diagnose…	Auf die Test- und Diagnosefunktionen zugreifen. Der Menübefehl ist nur in der Online-Ansicht sichtbar.	
Einfügen ▸…		(Menübefehle nur im Offline-Modus)	
	Modul	Neues Modul anlegen. Der Menübefehl ist nur aktiv, wenn ein Modul-Objekt oder eine Gruppe im Navigationsbereich angewählt ist.	Ctrl+M

Menübefehl		Bedeutung / Bemerkungen	Shortcut
	Gruppe	Neue Gruppe anlegen. Der Menübefehl ist nur aktiv, wenn ein Gruppen-Objekt im Navigationsbereich angewählt ist.	Ctrl+G
	Firewall Regelsatz	Einen neuen global gültigen Firewall IP-Regelsatz oder MAC-Regelsatz anlegen. Der Menübefehl ist nur aktiv, wenn ein Firewall-Objekt im Navigationsbereich angewählt ist.	Ctrl+F
Übertragen ▸…			
	An Modul…	Daten in die gewählten Module laden. Anmerkung: Es können nur konsistente Projektdaten geladen werden.	
	An alle Module…	Daten in alle projektierten Module laden. Anmerkung: Es können nur konsistente Projektdaten geladen werden.	
	Konfigurationszustand…	Konfigurationszustand der projektierten Module in einer Liste anzeigen.	
	Firmware übertragen...	Neue Firmware in ausgewähltes SCALANCE S laden.	
Ansicht ▸…			
	Erweitert-Modus	Vom Standard- in den Erweitert-Modus umschalten. Achtung: Sie können eine einmal vorgenommene Umschaltung in den Erweitert-Modus für das aktuelle Projekt nur rückgängig machen, so lange Sie keine Änderungen vorgenommen haben. Voreingestellt ist der Standard-Modus.	Ctrl+E
	Offline	Ist Voreinstellung.	Ctrl+Shift+D
	Online		Ctrl+D
Optionen ▸…			
	IP-Dienst-Definition …	Dialog für Dienst-Definitionen für IP-Firewall-Regeln öffnen. Der Menübefehl ist nur in der Ansicht "Erweitert-Modus" sichtbar.	
	MAC-Dienst-Definition…	Dialog für Dienst-Definitionen für MAC-Firewall-Regeln öffnen. Der Menübefehl ist nur in der Ansicht "Erweitert-Modus" sichtbar.	
	Projekt Passwortänderung…	Funktion zur Änderung des Benutzer-Passwortes.	
	Netzwerkadapter…	Funktion zur Auswahl des lokalen Netzwerk-Adapters, über den eine Verbindung zu SCALANCE S hergestellt werden soll.	
	Log Dateien…	Anzeige von Log-Dateien. Log-Dateien können gelesen und Log-Aufzeichnungen können gestartet werden.	
	Symbolische Namen...	Symbolische Namen für IP-Adressen oder MAC-Adressen vergeben.	
	Konsistenzprüfungen	Konsistenz des gesamten Projektes prüfen. Es wird eine Resultat-Liste ausgegeben.	

Menübefehl		Bedeutung / Bemerkungen	Shortcut
Hilfe ▸…			
	Inhalt …	Hilfe zu den Funktionen und Parametern, die Sie im Security Configuration Tool vorfinden.	Ctrl+Shift+F1
	Index…	Hilfe zu den Funktionen und Parametern, die Sie im Security Configuration Tool vorfinden.	Ctrl+Shift+F2
	Info…	Informationen zum Versions- und Ausgabestand des Security Configuration Tool.	

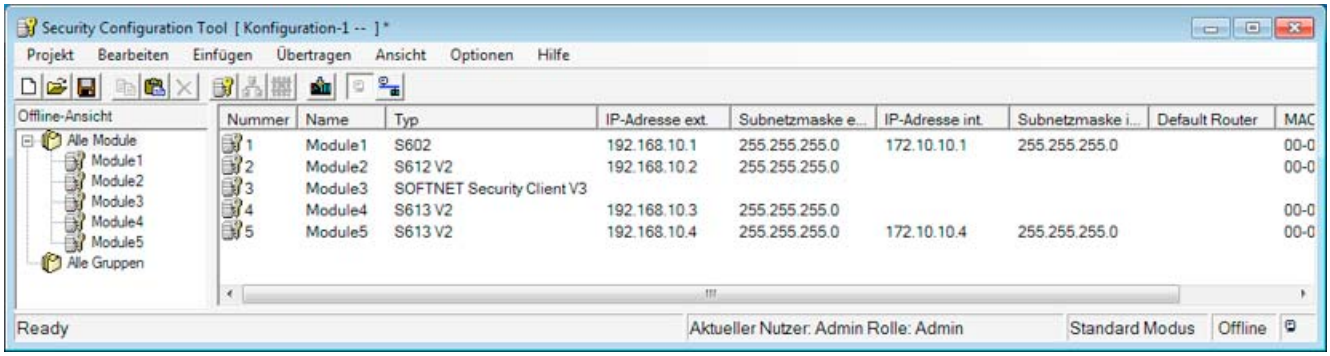
4.4 Projekte verwalten

4.4.1 Übersicht

SCALANCE S Projekt

Ein Projekt im Security Configuration Tool umfasst sämtliche Konfigurations- und Verwaltungsinformationen für ein oder mehrere SCALANCE S Geräte, SOFTNET Security Clients sowie MD74x-Geräte.

Für jedes SCALANCE S Gerät, jeden SOFTNET Security Client und für jedes MD74x-Gerät legen Sie im Projekt ein Modul an.



Allgemein beinhalten die Konfigurationen eines Projektes:

- Projektweit gültige Einstellungen
- Modulspezifische Einstellungen
- Gruppenzuordnungen für IPsec-Tunnel (S612 / S613 / SOFTNET Security Client)

Zusätzlich regelt eine Benutzerverwaltung die Zugriffsberechtigungen auf die Projektdaten und damit auf die SCALANCE S Geräte.

Projektweit gültige Einstellungen

- Projekteigenschaften

  Diese umfassen neben allgemeinen Adress- und Namensangaben Vorgaben für Initialisierungswerte und Authentifizierungseinstellungen.

- globale Firewall-Regelsätze

  Globale Firewall-Regeln können mehreren Modulen gleichzeitig zugewiesen werden. Diese Möglichkeit vereinfacht in vielen Fällen die Projektierung im Gegensatz zur Projektierung von lokalen Firewall-Regelsätzen bei den modulspezifischen Einstellungen.

- Dienst-Definitionen

  Mit Hilfe der IP-Dienst-Definitionen können Sie Firewall-Regeln kompakt und übersichtlich definieren.

Modulspezifische Einstellungen

Die meisten Funktionen werden im Eigenschaftendialog eines Modules konfiguriert. Hier eine Übersicht der angebotenen Register und deren Funktion:

Funktion / Register im Eigenschaftendialog	wird angeboten im Modus ...	
	Standard	Erweitert
Netzwerk Sie können hier ggf. Adressen der in Ihrem Netzwerk befindlichen Router angeben.	X	X
Firewall Im Standard-Modus aktivieren Sie hier die Firewall mit einfachen Standard-Regeln. Zusätzlich können Sie hier Logging-Einstellungen aktivieren. Im Erweitert-Modus können Sie detaillierte Paketfilter-Regeln definieren. Ferner können Sie für jede Paketfilter-Regel explizite Logging-Einstellungen definieren.	X	X
SSL Zertifikate Sie können bei Bedarf - beispielsweise bei kompromittiertem Zertifikat - ein Zertifikat importieren oder ein neues Zertifikat vom Security Configuration Tool erzeugen lassen.		X
Zeitsynchronisierung Legen Sie hier die Synchronisationsart für Datum und Uhrzeit fest.	X	X
Log-Einstellungen Sie können hier genauere Angaben zum Aufzeichnungs- und Speicher-Modus von Logging Ereignissen treffen.		X

Funktion / Register im Eigenschaftendialog	wird angeboten im Modus ...	
	Standard	Erweitert
Knoten Für ein Modul im Bridge-Modus können Sie hier die statischen internen Subnetze sowie die internen IP/MAC-Knoten konfigurieren und das Lernen interner Knoten zulassen oder sperren. Für ein Modul im Routing-Modus können Sie hier die internen Teilnehmer / komplette Subnetze eintragen, welche getunnelt werden sollen.		X
VPN Befindet sich das Modul in einer Gruppe können Sie hier die Dead-Peer-Detection, die Art des Verbindungsaufbaus und die WAN-IP-Adresse konfigurieren.		X
Routing-Modus Im Standard-Modus aktivieren Sie hier die Funktion "Router". Im Erweitert-Modus können Sie zusätzlich die Funktion NAT/NAPT-Router aktivieren und in einer Liste die Adressumsetzung festlegen.	X	X
DHCP-Server Für das interne Netz können Sie das Modul als DHCP-Server aktivieren.		X

Die ausführliche Beschreibung dieser Funktionen finden Sie im Kapitel " Firewall, Router und weitere Moduleigenschaften".

Gruppenzuordnungen für IPsec-Tunnel (S612 / S613 / SOFTNET Security Client)

Diese legen fest, welche SCALANCE S-Module, SOFTNET Security Clients und MD74x-Module miteinander über IPsec-Tunnel kommunizieren dürfen.

Indem Sie SCALANCE S-Module, SOFTNET Security Clients und MD74x-Module einer Gruppe zuordnen, können diese Module über ein VPN (virtual private network) Kommunikationstunnel aufbauen.

Nur Module der gleichen Gruppe können untereinander gesichert über Tunnel kommunizieren, wobei SCALANCE S-Module SOFTNET Security Clients und MD74x-Module mehreren Gruppen gleichzeitig angehören können.

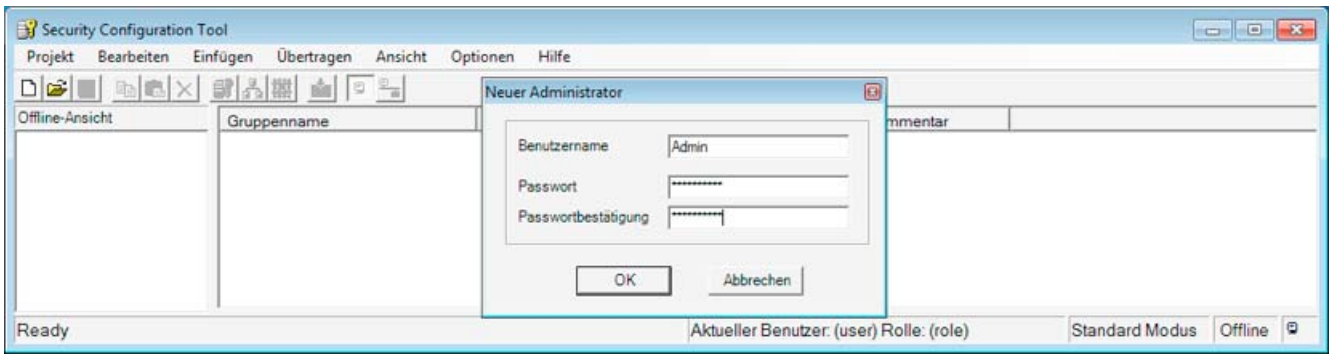
4.4.2 Projekte anlegen und bearbeiten

So legen Sie ein Projekt an

Wählen Sie den Menübefehl

Projekt ▸ Neu…

Sie werden aufgefordert einen Benutzernamen und ein Passwort zu vergeben. Der Benutzer, den Sie hier anlegen, ist vom Typ Administrator.



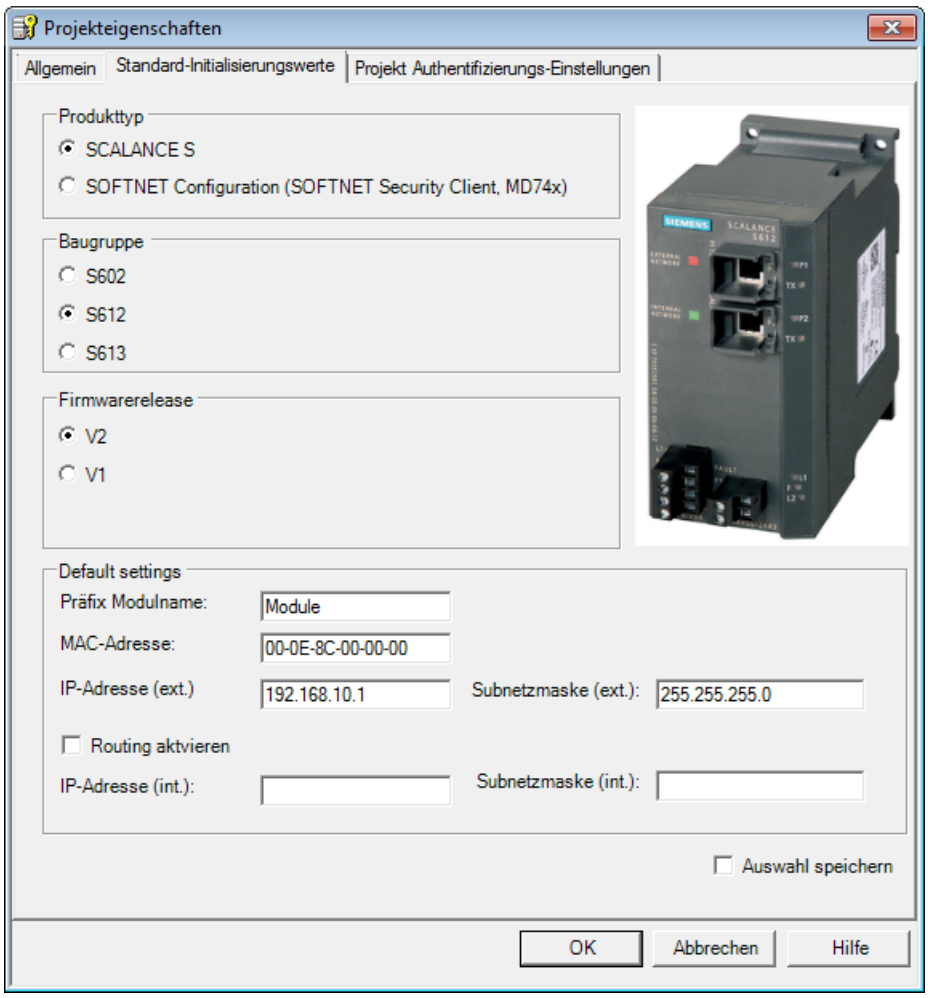
Security Configuration Tool legt daraufhin standardmäßig ein Projekt an und öffnet automatisch den Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration", in welchem Sie Ihr erstes Modul konfigurieren können.

Initialisierungswerte für ein Projekt festlegen

Mit den Initialisierungswerten legen Sie Eigenschaften fest, die beim Anlegen neuer Module automatisch übernommen werden.

Wählen Sie zum Eingeben von Initialisierungswerten folgenden Menübefehl:

Projekt ▸ Eigenschaften…, Register "Standard-Initialisierungswerte"



Schutz der Projektdaten durch Verschlüsselung

Die abgespeicherten Projekt- und Konfigurationsdaten sind sowohl in der Projektdatei als auch auf dem C-Plug durch Verschlüsselung geschützt.

Siehe auch

Firewall, Router und weitere Moduleigenschaften (Seite 131)

4.4.3 Benutzer einrichten

Benutzertypen und Rechte

Der Zugriff auf die Projekte und SCALANCE S-Module wird durch konfigurierbare Benutzereinstellungen verwaltet. SCALANCE S kennt zwei Benutzertypen mit unterschiedlichen Rechten:

- Administratoren

  Mit der Benutzerrolle vom Typ "Administrator" haben Sie uneingeschränkte Zugriffsrechte auf alle Konfigurationsdaten und die SCALANCE S-Module.

- User

  Mit der Benutzerrolle vom Typ "user" haben Sie folgende Zugriffsrechte:

  – Lesender Zugriff auf Konfigurationen; Ausnahme: das Ändern des eigenen Passworts ist erlaubt.

  – Lesender Zugriff auf SCALANCE S in der Betriebsart "Online" für Test und Diagnose.

Benutzer-Authentifizierung

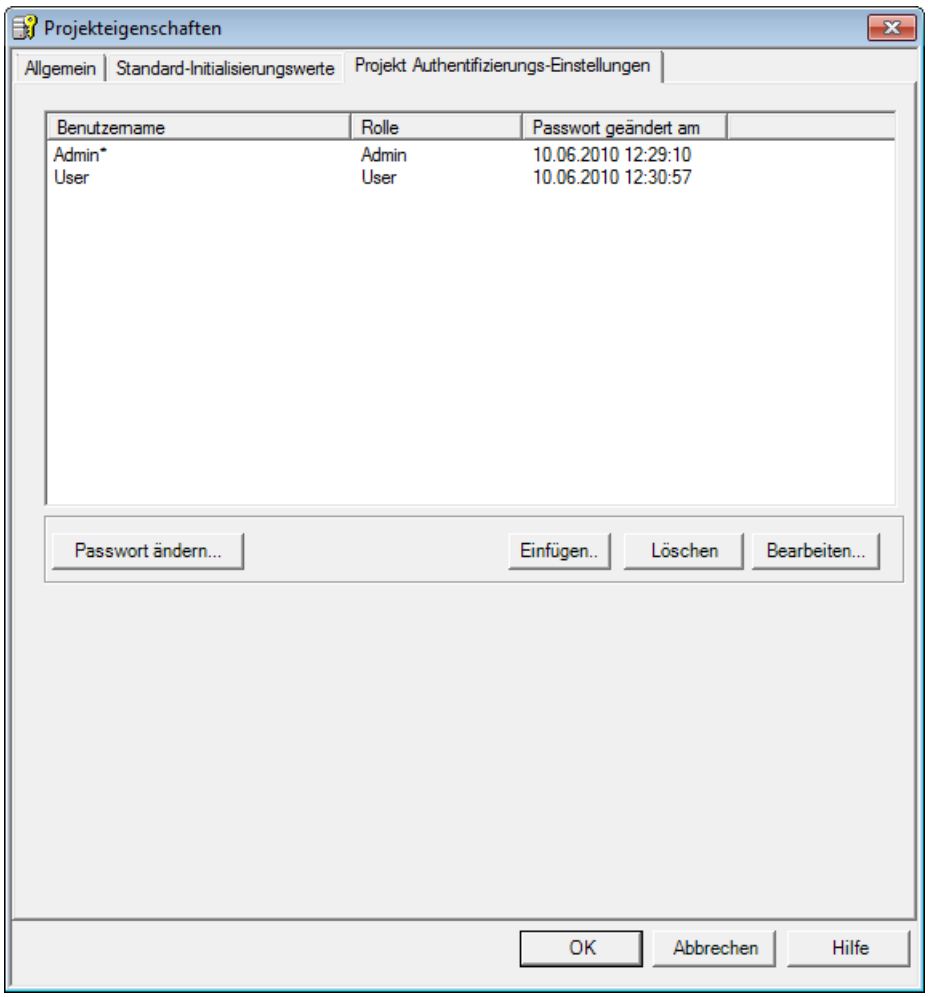
Die Benutzer des Projektes müssen sich beim Zugriff authentifizieren. Für jeden Benutzer können Sie eine Passwort-Authentifizierung festlegen.

ACHTUNG
Sie sollten Ihre Benutzer-Passwörter sicher verwahren. Vergessen Sie Ihre Benutzer-Passworte, haben Sie keinen Zugriff mehr auf das betreffende Projekt und seine Konfigurationen sowie die SCALANCE S-Module. Zugriff auf SCALANCE S-Module können Sie sich dann nur verschaffen, indem Sie ein "Rücksetzen auf Werkseinstellungen" durchführen; man verliert dabei aber die Konfigurationen.

Dialog zum Einrichten von Benutzern

Wählen Sie zum Einrichten von Benutzern folgenden Menübefehl:

Projekt ▸ Eigenschaften…, Register "Authentifizierungseinstellungen".



Schutz vor versehentlichem Zugriffsverlust

Das System stellt sicher, dass im Projekt immer mindestens ein Benutzer vom Typ "Administrator" eingerichtet bleibt. Damit wird verhindert, dass der Zugriff auf ein Projekt durch versehentliche "Selbstlöschung" für immer verloren gehen kann.

ACHTUNG
Werden die Authentisierungseinstellungen geändert, so müssen die SCALANCE S-Module erst neu geladen werden, damit diese Einstellungen (z.B. neue Benutzer, Passwortänderungen) auf den Modulen aktiv werden.

4.4.4 Konsistenzprüfungen

Übersicht

Security Configuration Tool unterscheidet:

- Lokale Konsistenzprüfungen
- Projektweite Konsistenzprüfungen

Auf welche geprüften Regeln Sie bei der Eingabe in den Dialogen achten müssen, darüber informieren die Dialogbeschreibungen im Handbuch unter dem Stichwort "Konsistenzprüfung".

Lokale Konsistenzprüfungen

Eine Konsistenzprüfung heißt lokal, wenn sie direkt innerhalb eines Dialoges durchgeführt werden kann. Bei folgenden Aktionen können Prüfungen ablaufen:

- nach dem Verlassen eines Feldes
- nach dem Verlassen einer Zeile in einer Tabelle
- beim Verlassen des Dialoges mit "OK"

Projektweite Konsistenzprüfungen

Projektweite Konsistenzprüfungen geben Aufschluss über korrekt konfigurierte Module. Da ständige projektweite Konsistenzprüfungen zuviel Zeit kosten, weil während der Erstellung eines Projektes meist inkonsistente Projektdaten konfiguriert werden, erfolgt eine Prüfung lediglich bei folgenden Aktionen automatisch:

- beim Speichern des Projekts
- beim Öffnen des Projekts
- vor dem Laden einer Konfiguration

ACHTUNG
Projektierdaten können Sie nur laden, wenn das Projekt insgesamt konsistent ist.

So veranlassen Sie eine projektweite Konsistenzprüfung

Sie können jederzeit die Konsistenzprüfung für ein geöffnetes Projektes über folgenden Menübefehl anstoßen:

Optionen ▸ Konsistenzprüfungen

Das Prüfergebnis wird in einer Liste ausgegeben. Zusätzlich werden Sie in der Statuszeile auf das Ergebnis der Konsistenzprüfung hingewiesen, wenn das Projekt inkonsistente Daten enthält. Indem Sie den Mauszeiger in die Statuszeile positionieren, können Sie dann durch Klicken die Prüfliste aufblenden.

4.4.5 Symbolische Namen für IP-/MAC-Adressen vergeben

Bedeutung und Vorteil

In einem SCALANCE S-Projekt können Sie stellvertretend für IP-Adressen und MAC-Adressen symbolische Namen in einer Symboltabelle vergeben.

Die Projektierung der einzelnen Dienste kann dadurch einfacher und sicherer erfolgen.

Bei den folgenden Funktionen und deren Projektierung werden symbolische Namen innerhalb des Projektes berücksichtigt:

- Firewall
- NAT/NAPT-Router
- Syslog
- DHCP

Gültigkeit und Eindeutigkeit

Die Gültigkeit der in der Symboltabelle angegebenen symbolischen Namen ist auf die Projektierung innerhalb eines SCALANCE S-Projektes beschränkt.

Innerhalb des Projektes muss jeder symbolische Name eindeutig einer einzigen IP-Adresse oder MAC-Adresse zugeordnet werden.

Automatische Übernahme symbolischer Namen in die Symboltabelle

Sie können symbolische Namen in den genannten Funktionen anstelle von IP-Adressen verwenden - beispielsweise beim Anlegen von Firewall-Regeln -, ohne dass diese in der hier beschriebenen Symboltabelle bereits vergeben sind.

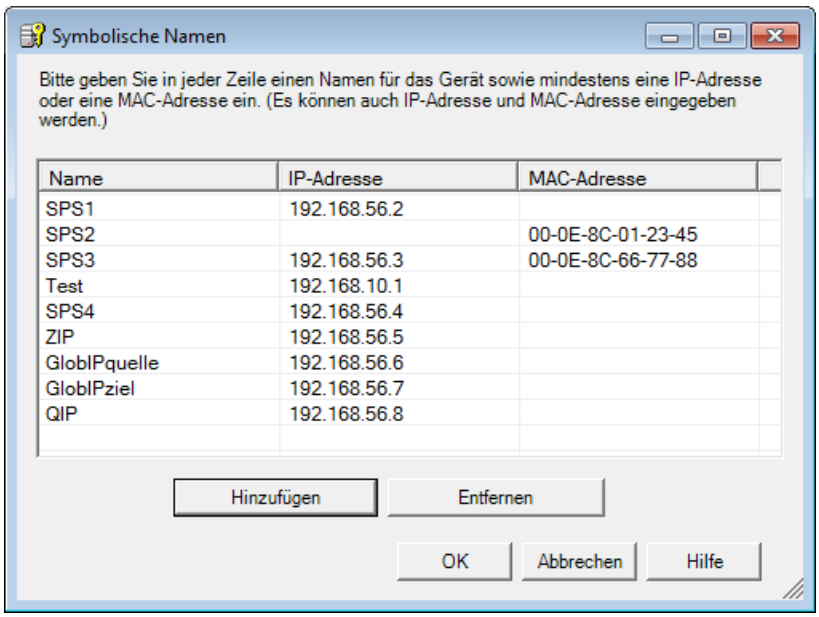
So vergebene symbolische Namen werden automatisch in die Symboltabelle übernommen und können zu einem späteren Zeitpunkt noch zugeordnet werden. Im Rahmen des Konsistenzchecks werden Sie auf fehlende Zuordnungen hingewiesen.

Dialog zum Vergeben symbolischer Namen

Um Inkonsistenzen zwischen einer Zuordnung "IP-Adresse - symbolischer Name" sowie "MAC-Adresse - symbolischer Name" zu vermeiden, werden die symbolischen Namen in einer einzigen Symboltabelle verwaltet.

Wählen Sie folgenden Menübefehl, um diese Symboltabelle zu öffnen:

Optionen ▸ Symbolische Namen..



Gehen Sie so vor, um Einträge in die Symboltabelle aufzunehmen:

- **Neue Einträge**

1. Betätigen Sie die Schaltfläche "Hinzufügen" um einen neuen symbolischen Namen in der nächsten freien Tabellenzeile hinzuzufügen.
2. Geben Sie den symbolischen Namen DNS-konform ein. [1)]
3. Ergänzen Sie den Eintrag mit der IP-Adresse oder der MAC-Adresse. Sie können auch beide Adressen angeben.

Legende:

[1)] DNS-Konformität gemäß RFC1035 beinhaltet folgende Regeln:
- Beschränkung auf 255 Zeichen insgesamt (Buchstaben, Ziffern, Bindestrich oder Punkt);
- der Name muss mit einem Buchstaben beginnen;
- der Name darf nur mit einem Buchstaben oder einer Ziffer enden;
- ein Namensbestandteil innerhalb des Namens, d. h. eine Zeichenkette zwischen zwei Punkten, darf max. 63 Zeichen lang sein;
- keine Sonderzeichen wie Umlaute, Klammern, Unterstrich, Schrägstrich, Blank etc.

- **Automatische Einträge**

Wenn der symbolische Name im Rahmen eines Dienstes bereits angegeben wurde, finden Sie einen entsprechenden Eintrag in der Symboltabelle.

1. Klicken Sie in das Eingabefeld für die IP-Adresse oder für die MAC-Adresse.
2. Ergänzen Sie den Eintrag mit der IP-Adresse oder der MAC-Adresse. Sie können auch beide Adressen angeben.

Falls Sie einen Eintrag in der Symboltabelle löschen, bleiben die in den Diensten verwendeten symbolischen Namen dort bestehen. Die Konsistenzprüfung erkennt in diesem Falle nicht definierte symbolische Namen. Dies gilt sowohl für manuell als auch für automatisch erzeugte Einträge.

Tipp:

Für die hier beschriebene Symboltabelle ist die Anwendung der projektweiten Konsistenzprüfung besonders sinnvoll. Sie können anhand der Liste jede Unstimmigkeit erkennen und korrigieren.

Sie können jederzeit die Konsistenzprüfung für ein geöffnetes Projektes über folgenden Menübefehl anstoßen:

Optionen ▸ Konsistenzprüfungen

Konsistenzprüfung - diese Regeln müssen Sie beachten

Berücksichtigen Sie bei Ihrer Eingabe die nachfolgend aufgeführten Regeln.

Prüfung / Regel	Prüfung erfolgt [1]	
	lokal	projektweit
Die Zuordnung eines symbolischen Namens zu einer IP- oder MAC-Adresse muss in beide Richtungen eindeutig sein.	x	
Die symbolischen Namen müssen DNS-konform sein. [2]	x	
Jede Zeile der Symboltabelle muss einen symbolischen Namen enthalten. Es muss entweder eine IP-Adresse oder eine MAC-Adresse oder beides angegeben sein.	x	
Den IP-Adressen der SCALANCE S-Module dürfen keine symbolischen Namen zugewiesen sein.		x
Im Projekt für IP- oder MAC-Adressen verwendete symbolische Namen müssen in der Symboltabelle enthalten sein. Inkonsistenzen können dadurch entstehen, dass Einträge in der Symboltabelle gelöscht und in den Projektierdialogen nicht entsprechend entfernt oder korrigiert werden.		x

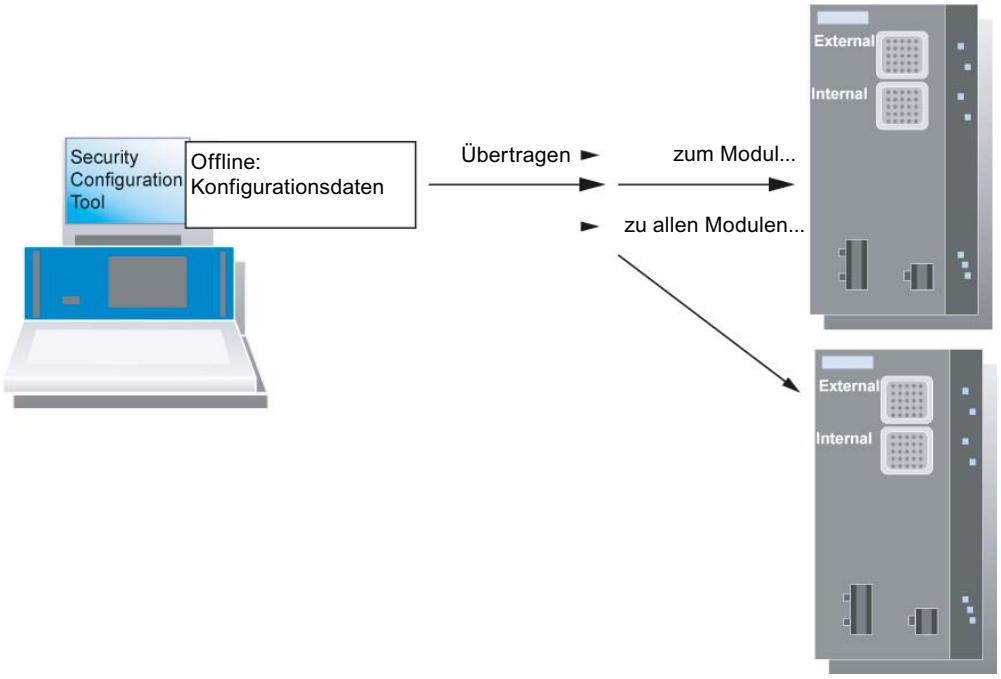
Legende:

[1] Beachten Sie die Erläuterungen im Kapitel "Konsistenzprüfungen".

[2] DNS-Konformität gemäß RFC1035 beinhaltet folgende Regeln:
- Beschränkung auf 255 Zeichen insgesamt (Buchstaben, Ziffern, Bindestrich oder Punkt);
- der Name muss mit einem Buchstaben beginnen;
- der Name darf nur mit einem Buchstaben oder einer Ziffer enden;
- ein Namensbestandteil innerhalb des Namens, d. h. eine Zeichenkette zwischen zwei Punkten, darf max. 63 Zeichen lang sein;
- keine Sonderzeichen wie Umlaute, Klammern, Unterstrich, Schrägstrich, Blank etc.

4.5 Konfiguration in SCALANCE S laden

Die offline erstellten Konfigurationsdaten werden über entsprechende Menübefehle in die im Netz erreichbaren SCALANCE S geladen.



Voraussetzungen

- Anschlüsse

  Prinzipiell können Sie die Konfigurationsdaten sowohl über den Geräte-Port 1 als auch den Geräte-Port 2 laden.

  Konfigurieren Sie die Module einer Gruppe vorzugsweise über das gemeinsame externe Netz dieser Module (Geräte-Port 1).

  Falls sich der Konfigurationsrechner in einem internen Netz befindet, müssen in der Firewall dieses SCALANCE S die IP-Adressen der anderen Module der Gruppe explizit freigeben und dieses Modul als erstes konfigurieren. (Diese Vorgehensweise wird erst unterstützt, wenn allen SCALANCE S Modulen bereits eine IP-Adresse zugewiesen wurde. siehe "Besonderheit bei Erstkonfiguration")

ACHTUNG
Mehrere Netzwerkadapter verwenden bei Erstkonfiguration
Wenn Sie mehrere Netzwerkadapter in Ihrem PC/PG betreiben, wählen Sie bitte vor der Erstkonfiguration zunächst den Netzwerkadapter aus, über den Sie das SCALANCE S Modul erreichen können.
Verwenden Sie hierzu den Menübefehl "**Optionen ▸ Netzwerkadapter…**"

- Betriebszustand

  Konfigurationen können im laufenden Betrieb der SCALANCE S Geräte geladen werden. Nach dem Ladevorgang erfolgt automatisch ein Neustart der Geräte. Nach dem Laden kann es zu einer kurzzeitigen Unterbrechung der Kommunikation zwischen internem und externem Netz kommen.

ACHTUNG
Besonderheit bei Erstkonfiguration
Solange ein Modul noch keine IP-Parameter eingestellt hat - d.h. vor der ersten Konfiguration - darf sich zwischen Modul und Konfigurationsrechner kein Router oder SCALANCE S befinden.

ACHTUNG
PC-Anschluss ändern
Wenn Sie einen PC von der internen auf die externe Schnittstelle des SCALANCE S umstecken, dann werden Zugriffe dieses PCs auf den SCALANCE S für ca. 10 min blockiert (Sicherheitsfunktion zur Abwehr von "ARP-Cache-Spoofing").

ACHTUNG
Projekt muss konsistent sein
Projektierdaten können Sie nur laden, wenn das Projekt insgesamt konsistent ist. Im Falle der Inkonsistenz wird eine detaillierte Prüfliste aufgeblendet.

Sichere Übertragung

Die Daten werden mit einem gesicherten Protokoll übertragen.

So gehen Sie vor

Verwenden Sie für das Laden alternativ die Menübefehle:

- **Übertragen ▸ An Modul…**

  Übertragen Sie hiermit die Konfiguration zu allen angewählten Modulen.

- **Übertragen ▸ An alle Module…**

  Übertragen Sie hiermit die Konfiguration zu allen im Projekt konfigurierten Modulen.

Unterschiedliche Konfiguration abgleichen

Ein Zurückladen von Konfigurationsdaten vom SCALANCE S-Modul in das Projekt ist nicht möglich.

4.6 Konfigurationsdaten für MD 740 / MD 741

Übertragung an ein Modul

Sie können Ihre VPN-Informationen zur Parametrierung eines MD 740-1 / MD 741-1 mit dem Security Configuration Tool generieren. Mit den so generierten Dateien können Sie dann den MD 740-1 / MD 741-1 konfigurieren.

Folgende Dateitypen werden erzeugt:

- Exportdatei mit den Konfigurationsdaten
  - Dateityp: ".txt"-Datei im ASCII-Format
  - Enthält die exportierten Konfigurationsinformationen für den MD 740 / MD 741 einschließlich einer Information über die zusätzlich erzeugten Zertifikate.
- Modul-Zertifikat
  - Dateityp: ".p12"-Datei
  - Die Datei enthält das Modulzertifikat und das Schlüsselmaterial.
  - Der Zugriff ist passwortgeschützt.
- Gruppen-Zertifikat
  - Dateityp: ".cer"-Datei

Die Konfigurationsdateien für das MD 740-1 / MD 741-1 können auch genutzt werden, um weitere VPN-Clienttypen, die nicht in der Modulauswahl enthalten sind, zu konfigurieren. Mindestvoraussetzung für die Verwendung dieser VPN-Clients ist die Unterstützung von IPsec-VPNs im Tunnelmodus.

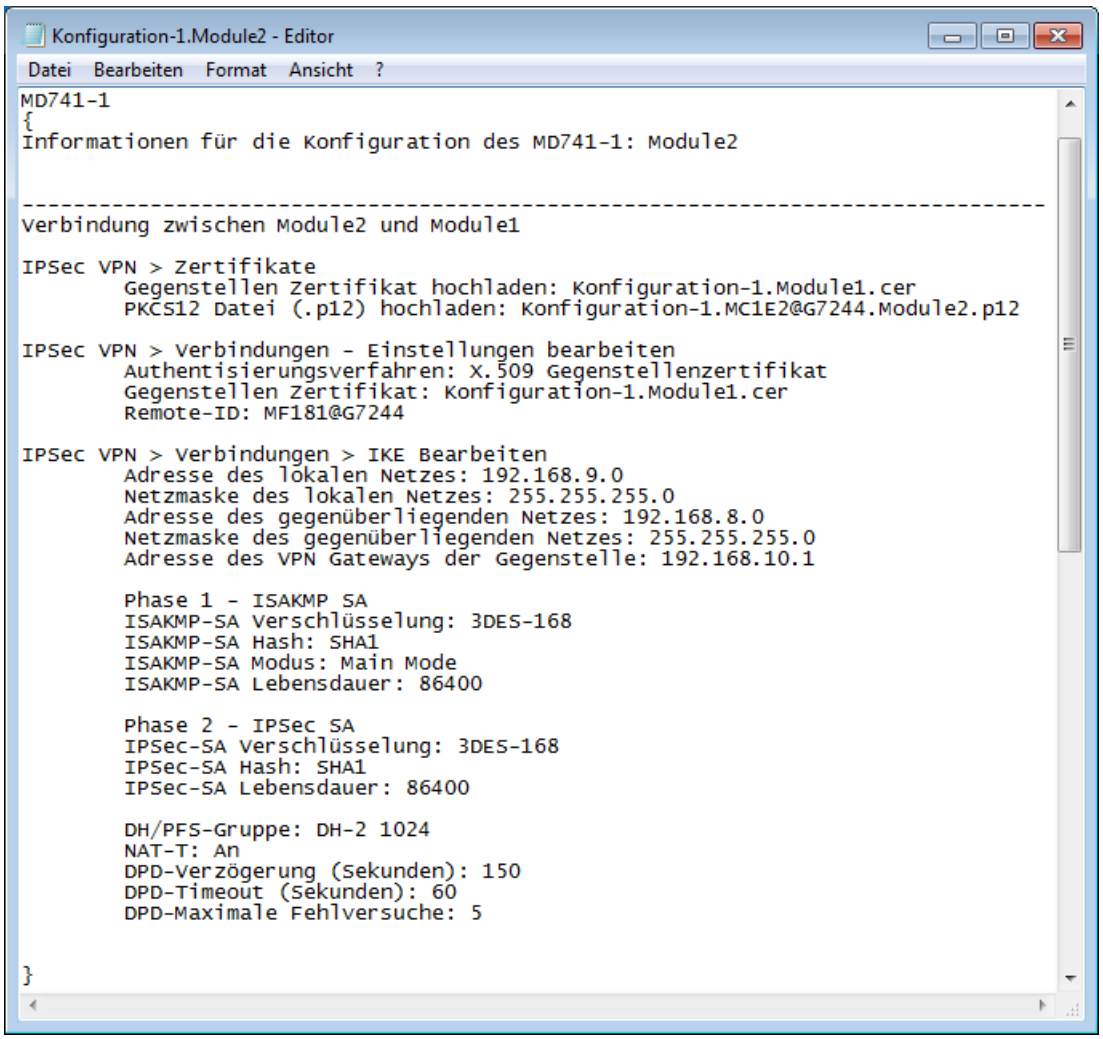


Bild 4-1 Export-Datei für MD 741-1

Hinweis

Es werden keine Konfigurationsdateien an das Modul übertragen. Es wird lediglich eine ASCII-Datei generiert, mit der Sie den MD 740-1 / MD 741-1 konfigurieren können. Dies ist aber nur möglich, wenn sich das Modul in mindestens einer VPN-Gruppe befindet, in der auch ein SCALANCE S-Modul oder ein SOFTNET Security Client V3.0 vorhanden ist.

Gehen Sie so vor

1. Markieren Sie im Inhaltbereich das Modul "MD 740-1" / "MD 741-1" und wählen Sie **Übertragen ▸ An Modul...**

2. Geben Sie im folgenden Speicherdialog den Pfad- und Dateinamen der Konfigurationsdatei an und klicken Sie "Speichern".
3. Im Anschluss werden Sie gefragt, ob Sie für die beiden erstellten Zertifikatdateien ein eigenes Passwort erstellen wollen.

   Wenn Sie "Nein" wählen, wird als Passwort der Name der Projektierung vergeben (z.B. DHCP_ohne_Routing_02), nicht das Projektpasswort.

   Wenn Sie "Ja" wählen (empfohlen), müssen Sie Ihr Passwort im darauf folgenden Dialog eingeben.

   Ergebnis: Die Dateien (und Zertifikate) werden in dem von Ihnen angegebenen Verzeichnis abgespeichert.

Hinweis

Nach dem Speichern werden Sie auf die Abwärts-Inkompatibilität des Projekts hingewiesen. Projekte, die z.B. mit dem Security Configuration Tool V2.1 gespeichert wurden sind nicht mit dem Security Configuration Tool V2 ladbar.

Hinweis

Weitere Informationen zur Konfiguration des MD 740-1 / MD 741-1 finden Sie im Systemhandbuch MD 741-1 / MD 740-1.

Firewall, Router und weitere Moduleigenschaften 5

Das vorliegende Kapitel macht Sie damit vertraut, wie Module angelegt werden und welche Einstellungen für die einzelnen Module in einem Projekt möglich sind. Hierbei spielen die Einstellungen für die Firewall-Funktion und NAT/NAPT-Router-Funktion von SCALANCE S die Hauptrolle.

Hinweis

S612 / S613

Die Firewall-Einstellungen, die Sie für die einzelnen Module vornehmen können, können auch die Kommunikation beeinflussen, die über IPsec-Tunnelverbindungen im internen Netz (VPN) abgewickelt wird.

Weitere Informationen

Wie Sie IPsec-Tunnel konfigurieren, wird ausführlich im nächsten Kapitel dieses Handbuches erläutert.

Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

ACHTUNG
Leistungsmerkmale und Gerätetypen Beachten Sie bitte bei dem von Ihnen verwendeten Gerätetyp, welche Funktionen jeweils unterstützt werden.

Siehe auch

Online Funktionen - Test, Diagnose und Logging (Seite 227)

Hardware-Merkmale und Funktionsübersicht (Seite 17)

5.1 Übersicht / Grundlagen

5.1.1 SCALANCE S als Firewall

Bedeutung

Die Firewall-Funktionalität von SCALANCE S hat die Aufgabe, das interne Netz vor Beeinflussung oder Störung aus dem externen Netz zu schützen. Das bedeutet, dass je nach Konfiguration nur bestimmte, vorher festgelegte Kommunikationsbeziehungen zwischen Netzknoten aus dem internen Netz und Netzknoten aus dem externen Netz erlaubt werden.

Alle Netzknoten, die sich im internen Netzsegment eines SCALANCE S befinden, werden durch dessen Firewall geschützt.

Die Firewall-Funktionalität kann für folgende Protokollebenen konfiguriert werden:

- IP-Firewall mit Stateful Packet Inspection;
- Firewall auch für Ethernet-"Non-IP"-Telegramme gemäß IEEE 802.3; (Layer-2-Telegramme)
- Bandbreitenbegrenzung

Firewall-Regeln

Firewall-Regeln sind Regeln für den Datenverkehr in folgende Richtungen:

- vom internen ins externe Netz und umgekehrt;
- vom internen Netz in einen IPsec-Tunnel und umgekehrt (S612 / S613).

Projektierung

Zu unterscheiden sind die beiden Bedienungssichten:

- Im Standard-Modus wird auf einfache, vordefinierte Regeln zurückgegriffen.
- Im Erweitert-Modus können Sie spezifische Regeln definieren.

  Zusätzlich sind im Erweitert-Modus lokale Firewall-Regeln und globale Firewall-Regelsätze für Module zu unterscheiden:

  – Lokale Firewall-Regeln sind jeweils einem Modul zugewiesen. Sie werden im Eigenschaftendialog der Module projektiert.

  – Globale Firewall-Regeln können mehreren Modulen gleichzeitig zugewiesen werden. Diese Möglichkeit vereinfacht in vielen Fällen die Projektierung.

Zusätzlich haben Sie die Möglichkeit, mit Hilfe von Dienst-Definitionen Firewall-Regeln kompakt und übersichtlich zu definieren. Auf diese Dienst-Definitionen können Sie sich sowohl bei den lokalen Firewall-Regeln als auch bei den globalen Firewall-Regelsätzen beziehen.

5.1.2 SCALANCE S als Router

Bedeutung

Indem Sie SCALANCE S als Router betreiben, verbinden Sie das interne Netz mit dem externen Netz. Das über SCALANCE S verbundene interne Netz wird somit zu einem eigenen Subnetz.

Sie haben folgende Möglichkeiten:

- Routing - einstellbar im Standard-Modus und im Erweitert-Modus
- NAT/NAPT-Routing - einstellbar im Erweitert-Modus

Routing - einstellbar im Standard-Modus und im Erweitert-Modus

Es werden die Telegramme weitergeleitet, die an eine in den jeweiligen Subnetzen (interne oder externe) vorhandene IP-Adresse gerichtet sind. Darüber hinaus gelten die für die jeweilige Übertragungsrichtung getroffenen Firewall-Regeln.

Für diese Betriebsart müssen Sie zusätzlich eine IP-Adresse für das interne Subnetz projektieren.

Hinweis: Im Gegensatz zum Bridge-Betrieb des SCALANCE S gehen im Routing-Modus VLAN-Tags verloren.

NAT/NAPT-Routing - einstellbar im Erweitert-Modus

Bei dieser Betriebsart erfolgt zusätzlich eine Umsetzung der IP-Adressen. Die IP-Adressen der Geräte im internen Subnetz werden auf externe IP-Adressen abgebildet und sind somit am externen Netz nicht "sichtbar".

Für diese Betriebsart projektieren Sie die Adressumsetzung in einer Liste. Sie ordnen jeweils einer internen IP-Adresse eine externe IP-Adresse zu.

Je nachdem, welches Verfahren Sie anwenden möchten, gilt für die Zuordnung:

- NAT (Network Adress Translation)

  Hier gilt: Adresse = IP-Adresse
- NAPT (Network Address Port Translation)

  Hier gilt: Adresse = IP-Adresse + Port-Nummer

5.1.3 SCALANCE S als DHCP-Server

Bedeutung

Sie können SCALANCE S am internen Netz als DHCP-Server betreiben. Damit ist es möglich, den am internen Netz angeschlossenen Geräten automatisch IP-Adressen zuzuweisen.

Die IP-Adressen werden hierbei entweder dynamisch aus einem von Ihnen vergebenen Adressband zugewiesen oder es wird gemäß Ihrer Vorgabe eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

Projektierung

Die Konfiguration als DHCP-Server ist in der Ansicht "Erweitert-Modus" möglich.

5.2 Module anlegen und Netzparameter einstellen

Module anlegen

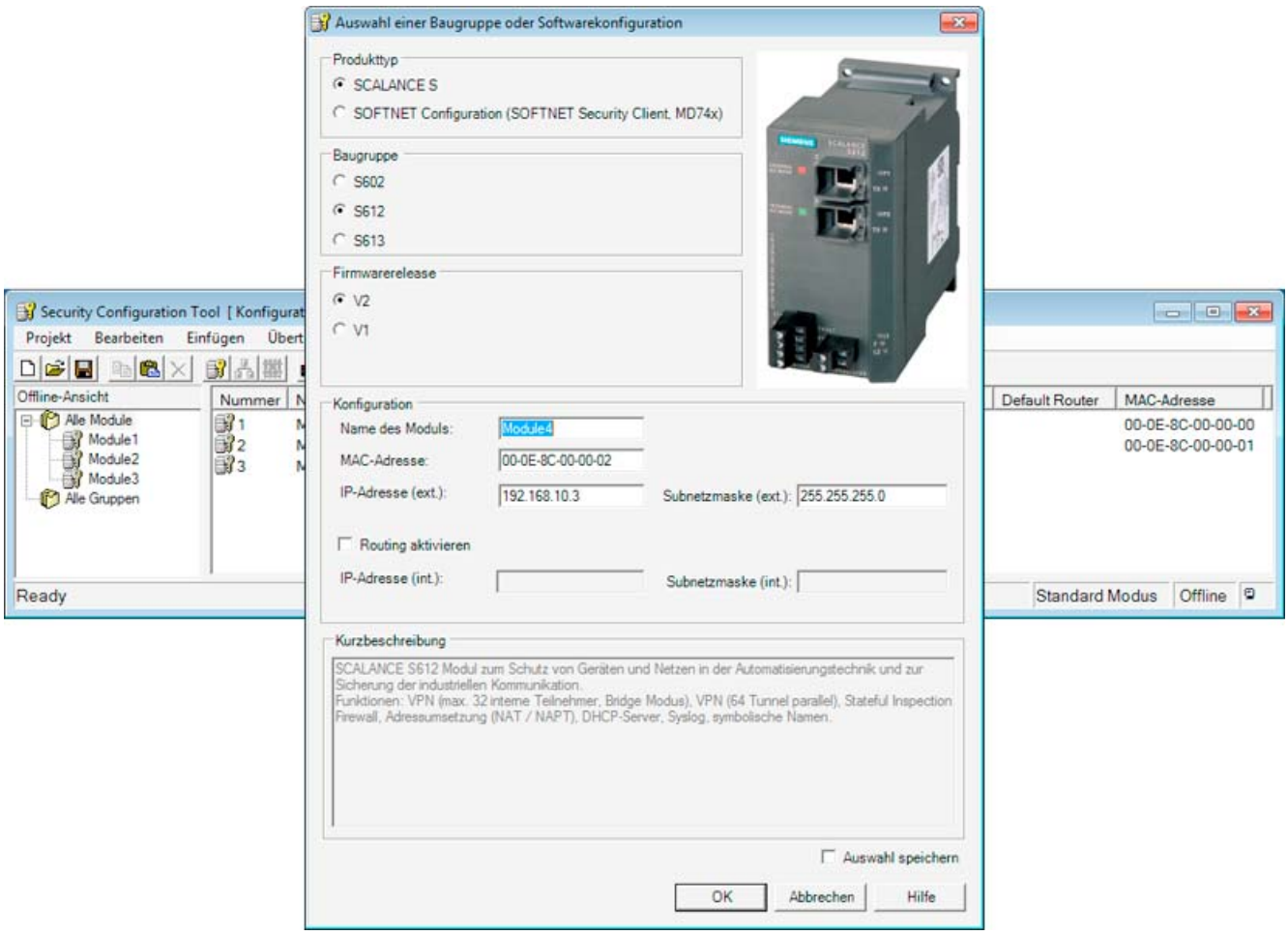
Beim Anlegen eines neuen Projektes wird standardmäßig vom Security Configuration Tool der Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" geöffnet, in welchem Sie Ihr erstes Modul konfigurieren können.

Weitere Module legen Sie über folgenden Menübefehl neu an:

Einfügen ▸ Modul

alternativ: über das Kontextmenü bei angewähltem Objekt "Alle Module".

Wählen Sie im nächsten Schritt in diesem Dialog Ihren Produkttyp, die Baugruppe und das Firmwarerelease aus.



Netzwerkeinstellungen eines Moduls

Die Netzwerkeinstellungen eines Moduls umfassen:

- Adressparameter des Moduls
- Adressen externer Router

Adressparameter

Einige Adressparameter können Sie über den Dialog "Auswahl einer Baugruppe oder Softwarekonfiguration" beim Anlegen eines Moduls konfigurieren.

Die Adressparameter können Sie ebenfalls im Inhaltsbereich eingeben, indem Sie im Navigationsbereich das Objekt "Alle Module" selektieren:

Folgende Eigenschaften der Module werden spaltenweise angezeigt:

Tabelle 5- 1 IP-Parameter - "Alle Module" selektiert

Eigenschaft/Spalte	Bedeutung	Kommentar/Auswahl
Nummer	Fortlaufende Modulnummer	wird automatisch vergeben
Name	Technologisch sinnvolle Modulbenennung.	frei wählbar
IP-Adresse ext.	IP-Adresse, über die das Gerät im externen Netz erreichbar ist, beispielsweise zum Laden der Konfiguration.	Im Netzverbund passende Vergabe.
Subnetzmaske ext.	Subnetzmaske	Im Netzverbund passende Vergabe.
IP-Adresse int.	IP-Adresse, über die das Gerät im internen Netz erreichbar ist, wenn es als Router konfiguriert ist.	Im Netzverbund passende Vergabe. Das Eingabefeld ist nur dann editierbar, wenn in den Moduleigenschaften der Router-Betrieb aktiviert wurde.
Subnetzmaske int.	Subnetzmaske	Im Netzverbund passende Vergabe. Das Eingabefeld ist nur dann editierbar, wenn in den Moduleigenschaften der Router-Betrieb aktiviert wurde.
Default Router	IP-Adresse des Routers im externen Netz.	Im Netzverbund passende Vergabe.
MAC-Adresse	Hardware-Adresse des Moduls	Die MAC-Adresse ist auf dem Modulgehäuse aufgedruckt. • Beachten Sie die zusätzliche MAC-Adresse im Routing-Modus (Angaben im Anschluss an diese Tabelle).
Typ	Gerätetyp	• SCALANCE S602 • SCALANCE S612 V1 • SCALANCE S612 V2 • SCALANCE S613 V1 • SCALANCE S613 V2
		• SOFTNET Security Client 2005 • SOFTNET Security Client 2008 • SOFTNET Security Client V3.0 • MD 74x Für diese Modultypen existiert kein "Eigenschaftendialog". Für MD 74x sind im Inhaltsbereich die IP-Adressen und die Subnetzmasken einstellbar.
Kommentar	Technologisch sinnvolle Information zum Modul und das durch das Modul geschützte Subnetz.	frei wählbar

Zusätzliche MAC-Adresse im Routing-Modus

SCALANCE S verwendet im Routing-Modus an der Schnittstelle zum internen Subnetz eine zusätzliche MAC-Adresse. Diese zweite MAC-Adresse wird aus der auf dem Gerät aufgedruckten MAC-Adresse wie folgt abgeleitet:

- MAC-Adresse (intern) = aufgedruckte MAC-Adresse + 1

Beim Betrieb in flachen Netzen (Bridge-Betrieb) ist immer die aufgedruckte MAC-Adresse sowohl an der internen wie an der externen Schnittstelle gültig.

Im Online-Dialog des Security Configuration Tool werden die aktuell gültigen MAC-Adressen im Register "Zustand" angezeigt.

Dialog "Netzwerk / Externe Router"

Abhängig von der vorliegenden Netzstruktur kann es sein, dass Sie neben dem Standard-Router weitere Router angeben müssen.

Markieren Sie das zu bearbeitende Modul und wählen Sie zum Einrichten externer Router folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften..., Register "Netzwerk".

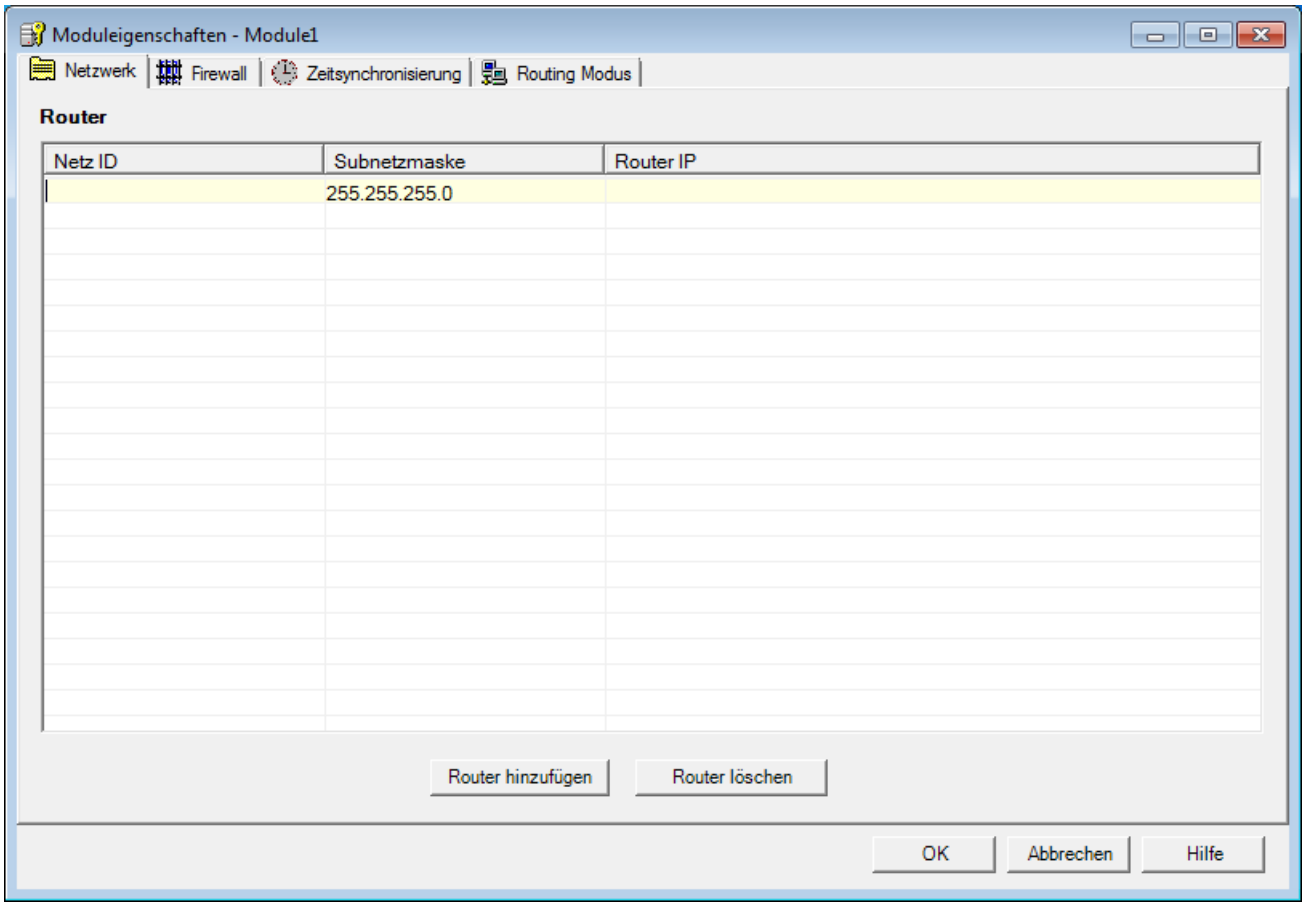


Bild 5-1 Dialog "Netzwerk"

Siehe auch

Funktionsübersicht Online-Dialog (Seite 228)

5.3 Firewall - Moduleigenschaften im Standard-Modus

5.3.1 Firewall projektieren

Schutz vor Störungen aus dem externen Netz

Die Firewall-Funktionalität von SCALANCE S hat die Aufgabe, das interne Netz vor Beeinflussung oder Störung aus dem externen Netz zu schützen. Das bedeutet, dass nur bestimmte, vorher festgelegte Kommunikationsbeziehungen zwischen Netzknoten aus dem internen Netz und Netzknoten aus dem externen Netz erlaubt werden.

Mit Paketfilter-Regeln definieren Sie die Freigabe oder Einschränkung des durchgehenden Datenverkehrs anhand von Eigenschaften der Datenpakete.

Bei SCALANCE S612 / S613 kann die Firewall für den verschlüsselten (IPsec-Tunnel-) und den unverschlüsselten Datenverkehr eingesetzt werden .

Im Standard-Modus können nur Einstellungen für den unverschlüsselten Datenverkehr gemacht werden.

Hinweis

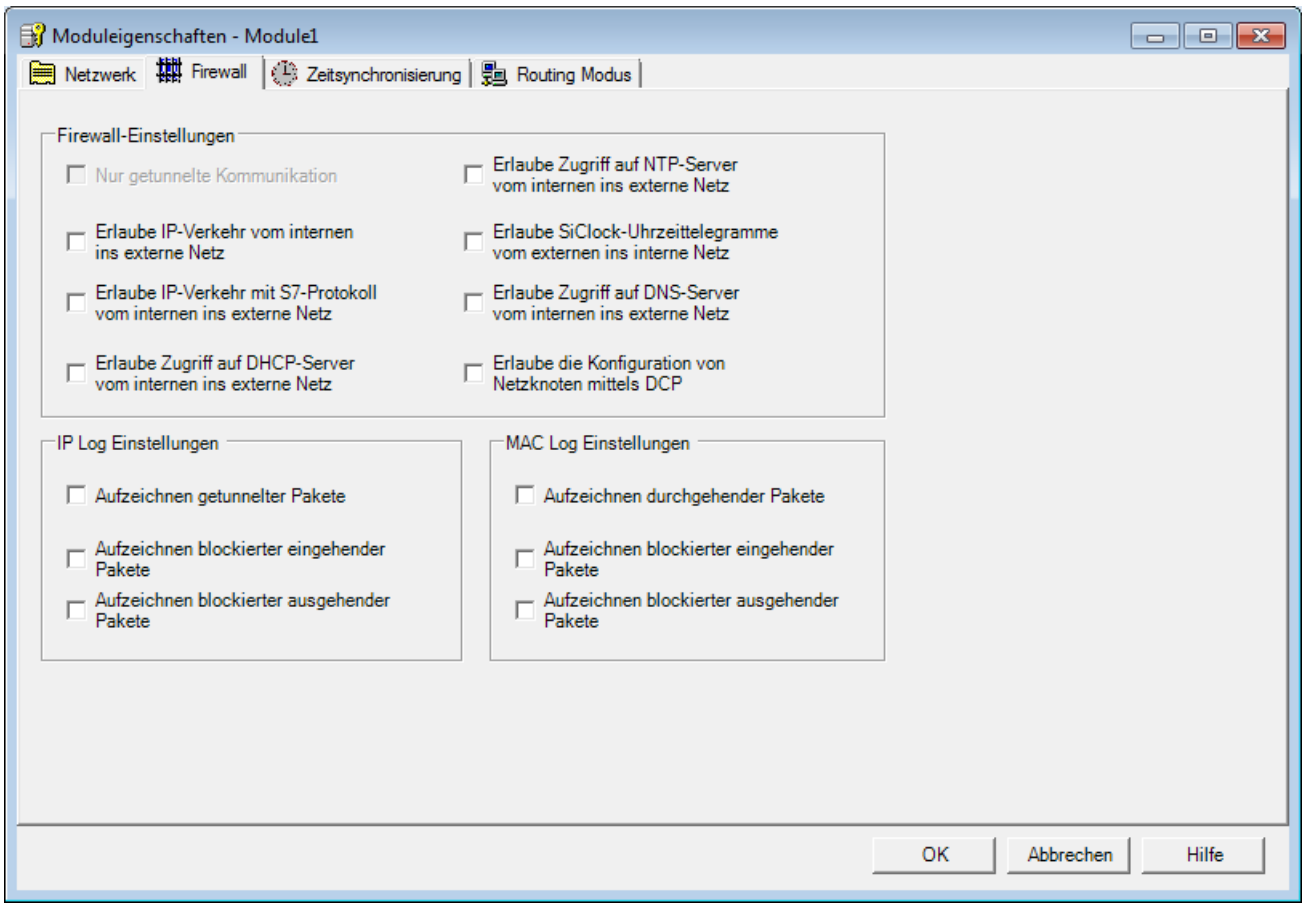
Routing-Modus

Wenn Sie für das SCALANCE S Modul den Routing-Modus aktiviert haben, finden MAC-Regeln keine Anwendung.

Dialog

Markieren Sie das zu bearbeitende Modul und wählen Sie zum Einrichten der Firewall den Menübefehl:

Bearbeiten ▸ Eigenschaften..., Register "Firewall"



Auswahlbereich "Konfiguration" - Vordefinierte Regeln

ACHTUNG
Bedenken Sie bitte, dass das Gefährdungspotenzial umso höher wird, je mehr Optionen Sie freischalten.

Der Standard-Modus beinhaltet für die Firewall folgende vordefinierte Regeln, die Sie im Eingabebereich "Konfiguration" wählen können:

Tabelle 5- 2 Vordefinierte Regeln der einfachen Firewall

Regel/Option	Funktion	Default-Einstellung
Nur getunnelte Kommunikation (S612/ S613) Tunnel Communication only	Das ist die Standardeinstellung. Mit dieser Einstellung wird nur verschlüsselter IPsec-Datentransfer zugelassen; nur Knoten in internen Netzen von SCALANCE S können miteinander kommunizieren. Die Option ist nur dann wählbar, wenn sich das Modul in einer Gruppe befindet. Wenn diese Option abgewählt ist, dann ist die getunnelte Kommunikation und zusätzlich die in den anderen Optionskästchen angewählte Kommunikationsart zugelassen.	Ein
Erlaube IP-Verkehr vom internen ins externe Netz Allow outgoing IP traffic	Interne Knoten können eine Kommunikationsverbindung zu Knoten im externen Netz initiieren. Nur Antworttelegramme aus dem externen Netz werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.	Aus
Erlaube IP-Verkehr mit S7-Protokoll vom internen ins externe Netz. Allow outgoing S7 protocol	Interne Knoten können eine S7-Kommunikationsverbindung (S7-Protokoll - TCP/Port 102) zu Knoten im externen Netz initiieren. Nur Antworttelegramme aus dem externen Netz werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.	Aus
Erlaube Zugriff auf DHCP-Server vom internen ins externe Netz. Allow access to external DHCP server	Interne Knoten können eine Kommunikationsverbindung zu einem DHCP-Server im externen Netz initiieren. Nur die Antworttelegramme des DHCP-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.	Aus
Erlaube Zugriff auf NTP-Server vom internen ins externe Netz. Allow access to external NTP server	Interne Knoten können eine Kommunikationsverbindung zu einem NTP-Server (Network Time Protocol) im externen Netz initiieren. Nur die Antworttelegramme des NTP-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.	Aus
Erlaube SiClock-Uhrzeittelegramme vom externen ins interne Netz. Allow access to external SiClock server	Mit dieser Option werden SiClock-Uhrzeittelegramme vom externen ins interne Netz freigegeben.	Aus (Die Option ist im Routing-Modus nicht bedienbar.)

Regel/Option	Funktion	Default-Einstellung
Erlaube Zugriff auf DNS-Server vom internen ins externe Netz. Allow access to external DNS server	Interne Knoten können eine Kommunikationsverbindung zu einem DNS-Server im externen Netz initiieren. Nur die Antworttelegramme des DNS-Servers werden ins interne Netz weitergeleitet. Vom externen Netz aus kann keine Kommunikationsverbindung zu Knoten im internen Netz initiiert werden.	Aus
Erlaube die Konfiguration von internen Netzknoten mittels DCP vom externen ins interne Netz. Allow access from external or internal nodes via DCP server	Das DCP-Protokoll wird vom PST-Tool verwendet, um bei SIMATIC Net Netzkomponenten die Knotentaufe (Einstellen der IP-Parameter) vorzunehmen. Mit dieser Regel wird Knoten im externen Netz erlaubt, per DCP-Protokoll auf Knoten im internen Netz zuzugreifen.	Aus (Die Option ist im Routing-Modus nicht bedienbar.)

Auswahlbereich "Log" - Aufzeichnung einstellen

Sie können eine Protokollierung über den eingehenden und abgehenden Datenverkehr veranlassen.

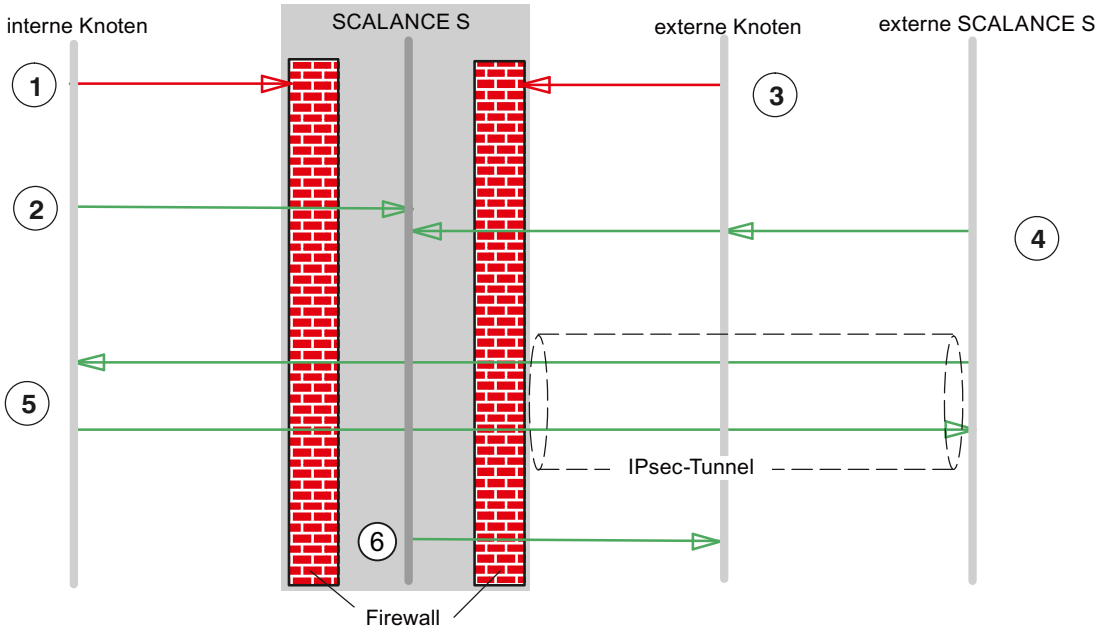
5.3.2 Voreinstellung der Firewall

Verhalten mit Voreinstellung

Die Voreinstellung für die Firewall ist so gewählt, dass kein IP-Datenverkehr möglich ist. Lediglich über ggf. konfigurierte IPsec-Tunnel ist Kommunikation zwischen den Knoten in den internen Netzen von SCALANCE S-Modulen zugelassen.

Die folgenden Diagramme zeigen die Standard-Einstellungen im Detail jeweils für den IP-Paketfilter und den MAC-Paketfilter.

Standard-Einstellung für IP- Paketfilter

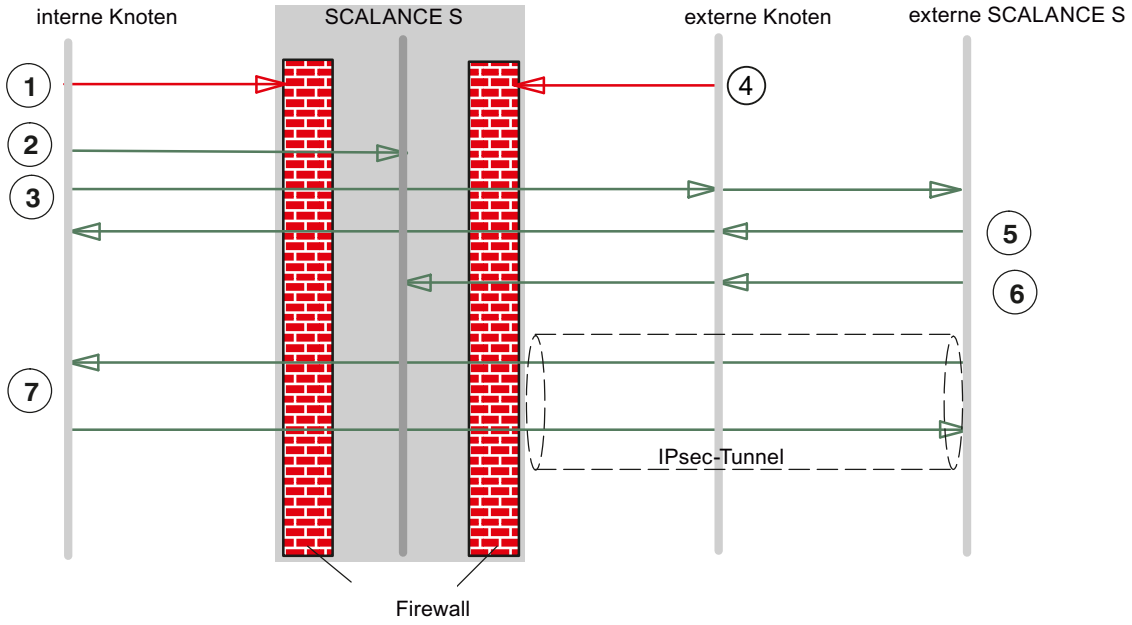


① Alle Telegrammtypen von intern nach extern sind geblockt.
② Alle Telegramme von intern an SCALANCE S sind zugelassen (sinnvoll nur HTTPS).
③ Alle Telegramme von extern nach intern und an SCALANCE S sind geblockt (auch ICMP-Echo-Request).
④ Telegramme von extern (externe Knoten und externe SCALANCE S) an SCALANCE S von folgendem Typ sind zugelassen:

- HTTPS (SSL)
- ESP-Protokoll (Verschlüsselung)
- IKE (Protokoll zum Aufbau der IPsec-Tunnel)
- NAT-Traversal (Protokoll zum Aufbau der IPsec-Tunnel)

⑤ IP-Kommunikation über IPsec-Tunnel ist zugelassen.
⑥ Telegramme vom Typ Syslog und NTP sind von SCALANCE S nach extern zugelassen.

Standard-Einstellung für MAC- Paketfilter



① Alle Telegrammtypen von intern nach extern sind geblockt.
② Alle Telegramme von intern an SCALANCE S sind zugelassen.
③ ARP-Telegramme von intern nach extern sind zugelassen.
④ Alle Telegramme von extern nach intern und an SCALANCE S sind geblockt.
⑤ Telegramme von extern nach intern von folgendem Typ sind zugelassen:
- ARP mit Bandbreitenbegrenzung

⑥ Telegramme von extern an SCALANCE S von folgendem Typ sind zugelassen:
- ARP mit Bandbreitenbegrenzung
- DCP

⑦ MAC-Protokolle, die durch IPsec-Tunnel gesendet werden, sind zugelassen.

5.4 Firewall - Moduleigenschaften im Erweitert-Modus

Im Erweitert-Modus gibt es erweiterte Einstellmöglichkeiten, die eine individuelle Einstellung der Firewall-Regeln und der Sicherheitsfunktionalität zulassen.

In den Erweitert-Modus umschalten

Schalten Sie für alle in diesem Kapitel beschriebenen Funktionen über folgenden Menübefehl die Betriebsart um:

Ansicht ▸ Erweitert-Modus...

Hinweis

Sie können eine einmal vorgenommene Umschaltung in den Erweitert-Modus für das aktuelle Projekt nicht mehr rückgängig machen, sobald Sie die Konfiguration geändert haben.

Symbolische Namen werden unterstützt

Sie können in den nachfolgend beschriebenen Funktionen IP-Adressen oder MAC-Adressen auch als symbolische Namen eingeben.

5.4.1 Firewall projektieren

Im Gegensatz zur Projektierung fest vorgegebener Paketfilter-Regeln im Standard-Modus können Sie im Erweitert-Modus von Security Configuration Tool individuelle Paketfilter-Regeln projektieren.

Die Paketfilter-Regeln stellen Sie in wählbaren Registern für folgende Protokolle ein:

- IP- Protokoll (Schicht/Layer 3)
- MAC-Protokoll (Schicht/Layer 2)

Wenn Sie in den nachfolgend beschriebenen Dialogen keine Regel eintragen, gelten die Standardeinstellungen entsprechend der Beschreibung im Kapitel "Voreinstellung der Firewall".

Hinweis

Routing-Modus

Wenn Sie für das SCALANCE S Modul den Routing-Modus aktiviert haben, finden MAC-Regeln keine Anwendung (Dialoge sind inaktiv).

Globale und lokale Definition möglich

- Globale Firewall-Regeln

  Eine globale Firewall-Regel kann mehreren Modulen gleichzeitig zugewiesen werden. Diese Möglichkeit vereinfacht in vielen Fällen die Projektierung.

- Lokale Firewall-Regeln

  Eine lokale Firewall-Regel ist jeweils einem Modul zugewiesen. Sie wird im Eigenschaftendialog eines Moduls projektiert.

Einem Modul können mehrere lokale Firewall-Regeln und mehrere globale Firewall-Regeln zugewiesen werden.

Die Definition der globalen und der lokalen Regeln erfolgt prinzipiell identisch. Die nachfolgende Beschreibung gilt daher für die beiden genannten Methoden.

5.4.2 Globale Firewall-Regeln

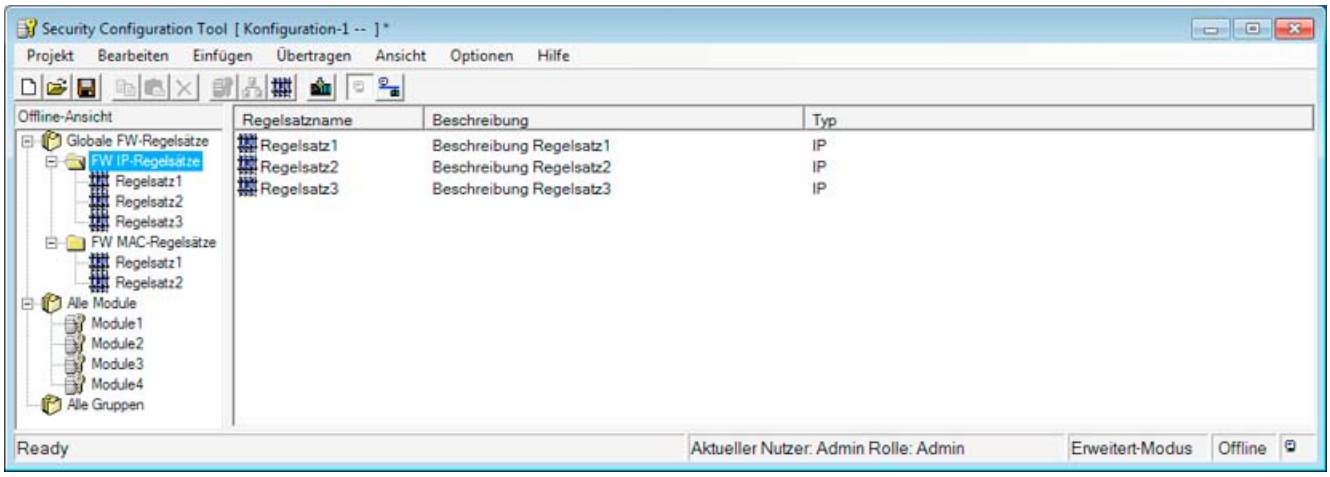
Anwendung

Globale Firewall-Regeln werden außerhalb der Module auf Projektebene projektiert. Sie sind, ähnlich wie die Module, im Navigationsbereich des Security Configuration Tool sichtbar.

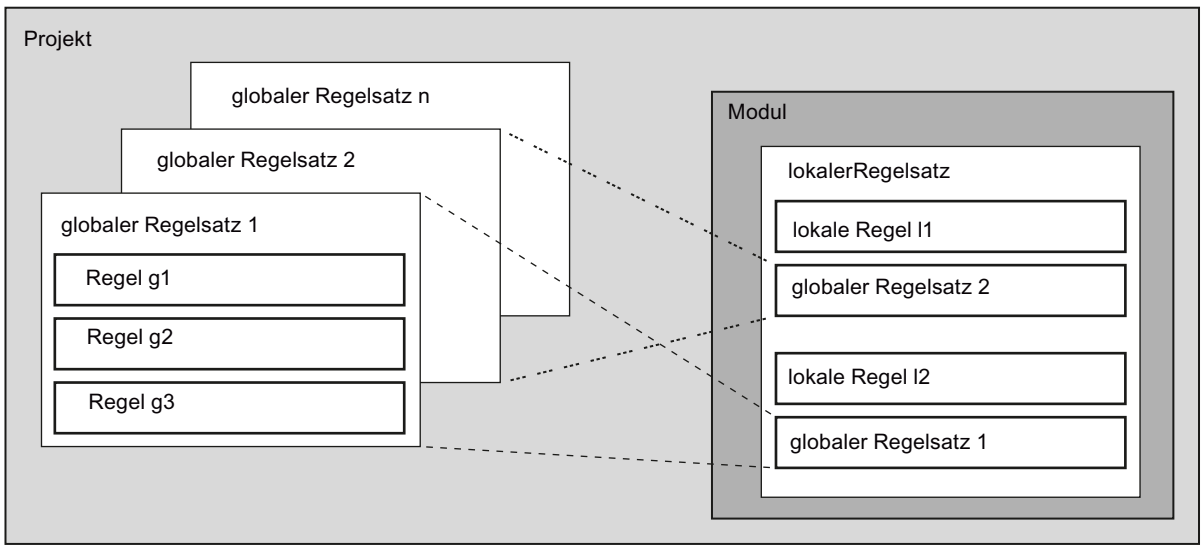
Indem Sie ein projektiertes Modul anwählen und auf die globale Firewall-Regel ziehen (Drag and Drop), ordnen Sie dem Modul diese Firewall-Regel zu. Diese globale Firewall-Regel erscheint dann automatisch in der modulspezifischen Liste der Firewall-Regeln.

Globale Firewall-Regeln können definiert werden für:

- IP-Regelsätze
- MAC-Regelsätze



Die folgende Darstellung verdeutlicht den Zusammenhang zwischen global definierten Regelsätzen und lokal verwendeten Regelsätzen.



Wann sind globale Firewall-Regeln sinnvoll?

Globale Firewall-Regeln sind dann sinnvoll, wenn Sie für mehrere von SCALANCE S-Modulen geschützte Subnetze identische Filterkriterien für die Kommunikation mit dem externen Netz definieren können.

Sie sollten aber beachten, dass diese vereinfachte Projektierung bei fehlerhafter Modulzuordnung zu unerwünschten Ergebnissen führen kann. Sie sollten daher immer die modulspezifischen lokalen Firewall-Regeln im Ergebnis überprüfen. Eine versehentlich erfolgte Regelzuordnung kann im Rahmen der automatischen Konsistenzprüfung nicht erkannt werden!

Globale Firewall-Regeln werden lokal genutzt - Vereinbarungen

Es gelten folgende Vereinbarungen bei der Erstellung eines globalen Firewall-Regelsatzes sowie bei der Zuweisung zu einem Modul:

- Ansicht im Security Configuration Tool

  Globale Firewall-Regeln können nur in der Einstellung des Erweitert-Modus angelegt werden.

- Priorität

  Lokal definierte Regeln haben standardmäßig eine höhere Priorität als globale Regeln; neu zugewiesene globale Regeln werden daher in der lokalen Regelliste zunächst unten angefügt.

  Die Priorität kann durch Verändern der Platzierung in der Regelliste verändert werden.

- Granularität

  Globale Firewall-Regeln können nur als ganzer Regelsatz einem Modul zugeordnet werden.

- Regel eingeben, ändern oder löschen

  Globale Firewall-Regeln sind in der lokalen Regelliste der Firewall-Regeln bei den Moduleigenschaften nicht editierbar. Sie können dort nur angezeigt und gemäß der gewünschten Priorität platziert werden.

  Es kann nicht eine einzelne Regel aus einem zugeordneten Regelsatz gelöscht werden. Es kann nur der Regelsatz als Ganzer aus der lokalen Regelliste genommen werden; die Definition in der globalen Regelliste wird dadurch nicht verändert.

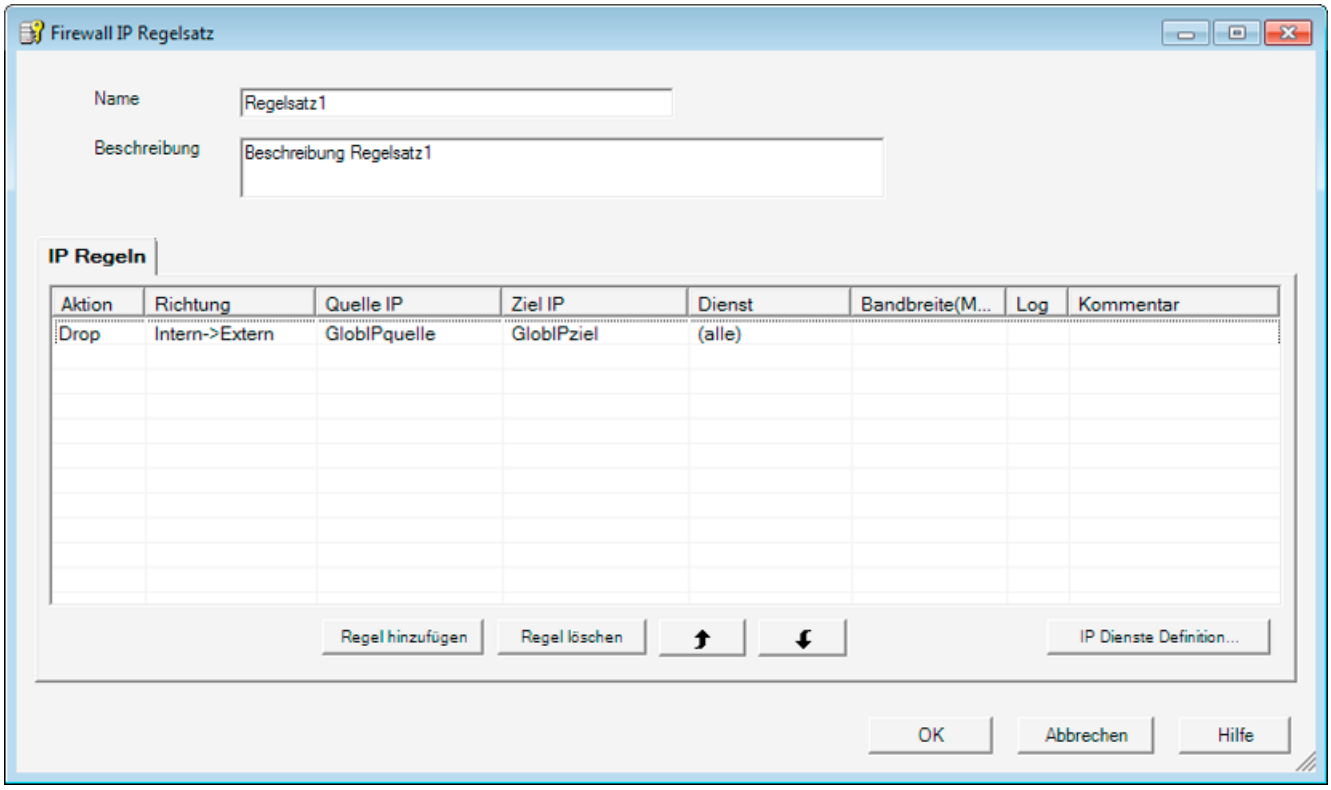
Globale Paketfilter-Regeln einstellen und zuweisen

Falls Sie einen globalen Firewall-Regelsatz definieren und zuordnen möchten, gehen Sie wie folgt vor:

1. Wählen Sie im Navigationsbereich einen der folgenden Ordner:
   - Globale FW-Regelsätze / FW IP-Regelsätze.
   - Globale FW-Regelsätze / FW MAC-Regelsätze.
2. Wählen Sie zum Einrichten eines globalen Regelsatzes den folgenden Menübefehl:

   Einfügen ▸ Firewall Regelsatz

3. Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein; beachten Sie die Beschreibung der Parameter und der Auswertung im Folgekapitel oder in der Online-Hilfe.
4. Ordnen Sie die globale Firewall-Regel denjenigen Modulen zu, in denen diese verwendet werden soll. Wählen Sie hierzu im Navigationsbereich ein Modul an und ziehen Sie dieses auf den passenden globalen Regelsatz im Navigationsbereich (Drag and Drop).



Ergebnis:
Der globale Regelsatz wird vom zugewiesenen Modul als lokaler Regelsatz verwendet.

5.4.3 Lokale IP-Paketfilter-Regeln einstellen

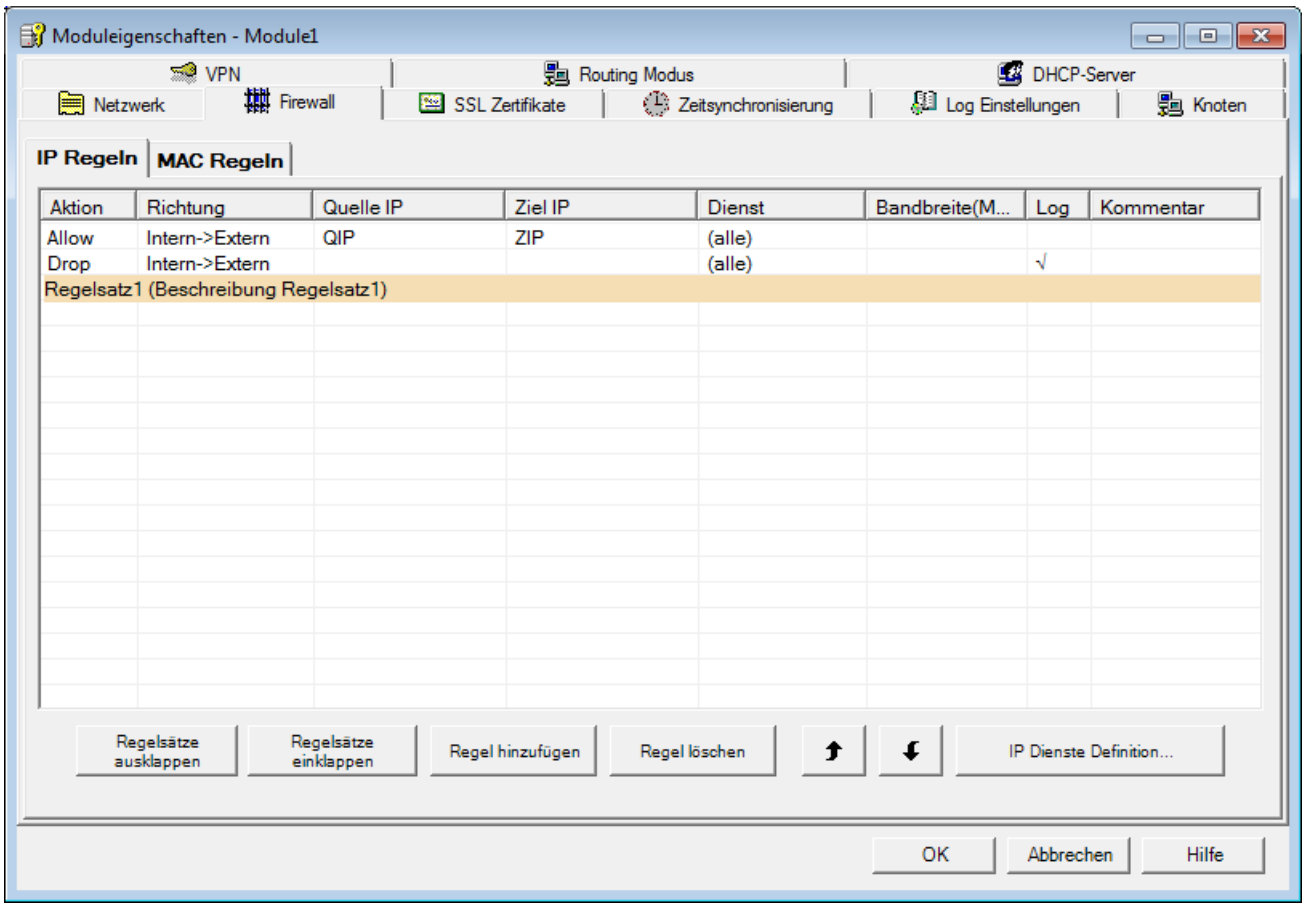
Mittels IP-Paketfilter-Regeln können Sie auf IP-Telegramme wie beispielsweise UDP-, TCP-, ICMP-Telegramme filtern.

Innerhalb einer IP-Paketfilter-Regel können Sie auf Dienst-Definitionen zurückgreifen und damit die Filterkriterien weiter eingrenzen. Wenn Sie keine Dienste angeben, gilt die IP-Paketfilter-Regel für alle Dienste.

Dialog für lokale IP-Paketfilter-Regeln öffnen

Markieren Sie das zu bearbeitende Modul und wählen Sie zum Einrichten der Firewall den Menübefehl:

Bearbeiten ▸ Eigenschaften...



IP-Paketfilter-Regeln eintragen

Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein; beachten Sie die Parameterbeschreibung und die Beispiele im Folgekapitel oder in der Online-Hilfe.

Globale Regelsätze nutzen

Globale Regelsätze, die Sie dem Modul zugewiesen haben, werden automatisch in den lokalen Regelsatz aufgenommen. Diese befinden sich zunächst am Ende der Regelliste, werden also mit der geringsten Priorität bearbeitet. Sie können die Priorität ändern, indem Sie die Position eines lokalen oder globalen Regelsatzes in der Regelliste verändern.

Die Online-Hilfe erläutert Ihnen die Bedeutung der einzelnen Schaltflächen.

5.4.4 IP-Paketfilter-Regeln

Die Bearbeitung von IP-Paketfilter-Regeln erfolgt anhand folgender Auswertungen:

- In der Regel eingetragene Parameter;
- Reihenfolge und der damit verbundenen Priorität der Regel innerhalb des Regelsatzes.

Parameter

Die Projektierung einer IP-Regel beinhaltet folgende Parameter:

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Aktion	Zulassungsfestlegung (Freigabe/Sperre)	• Allow Telegramme gemäß Definition zulassen. • Drop Telegramme gemäß Definition sperren.
Richtung	Gibt die Richtung des Datenverkehrs an ("Tunnel / Any" nur bei S612 / S613)	• Intern → Extern • Intern ← Extern • Tunnel → Intern • Tunnel ← Intern • Intern → Any • Intern ← Any
Quell IP	Quell-IP-Adresse	Siehe unter Abschnitt "IP-Adressen in IP-Paketfilter-Regeln" in diesem Kapitel. Alternativ können Sie symbolische Namen eingeben.
Ziel IP	Ziel-IP-Adresse	
Dienst	Name des verwendeten IP/ICMP-Dienstes oder der Dienstgruppe. Mit Hilfe der Dienst-Definitionen können Sie Paketfilter-Regeln kompakt und übersichtlich definieren Sie wählen hier einen der von Ihnen im Dialog IP-Dienste definierten Dienste: • IP- Dienste oder • ICMP-Dienste Wenn Sie noch keine Dienste definiert haben oder einen weiteren Dienst definieren möchten, betätigen Sie die Schaltfläche "IP/MAC-Dienste-Definition...".	Die Klappliste bietet die projektierten Dienste und Dienstgruppen zur Auswahl an. Keine Angabe bedeutet: es wird kein Dienst geprüft, die Regel gilt für alle Dienste.
Bandbreite (MBit/s)	Einstellmöglichkeit für eine Bandbreiten-Begrenzung. Ein Paket passiert die Firewall, wenn die Pass-Regel zutrifft und die zulässige Bandbreite für diese Regel noch nicht überschritten worden ist.	Wertebereich: 0.001...100 MBit/s

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Log	Ein- bzw. Ausschalten des Logging für diese Regel	
Kommentar	Platz für eigene Erläuterung der Regel	

IP-Adressen in IP-Paketfilter-Regeln

Die IP-Adresse besteht aus 4 Dezimalzahlen aus dem Wertebereich 0 bis 255, die durch einen Punkt voneinander getrennt sind; Beispiel: 141.80.0.16

In der Paketfilter-Regel haben Sie folgende Möglichkeiten, IP-Adressen anzugeben:

- keine Angabe

  Es erfolgt keine Prüfung, die Regel gilt für alle IP-Adressen.

- eine IP-Adresse

  Die Regel gilt genau für die angegebene Adresse.

- Adressband

  Die Regel gilt für alle im Adressband erfassten IP-Adressen.

  Ein Adressband wird definiert, indem die Anzahl der gültigen Bit-Stellen in der IP-Adresse angegeben wird und zwar in der Form:

  [IP-Adresse]/[Anzahl der zu berücksichtigenden Bits]

  – [IP-Adresse]/24 bedeutet demnach, dass nur die höchstwertigen 24 Bit der IP-Adresse in der Filterregel berücksichtigt werden; das sind die ersten drei Stellen der IP-Adresse.

  – [IP-Adresse]/25 bedeutet, dass nur die ersten drei Stellen und das höchstwertige Bit der vierten Stelle der IP-Adresse in der Filterregel berücksichtigt werden.

Tabelle 5- 3 Beispiele für Adressband bei IP-Adressen

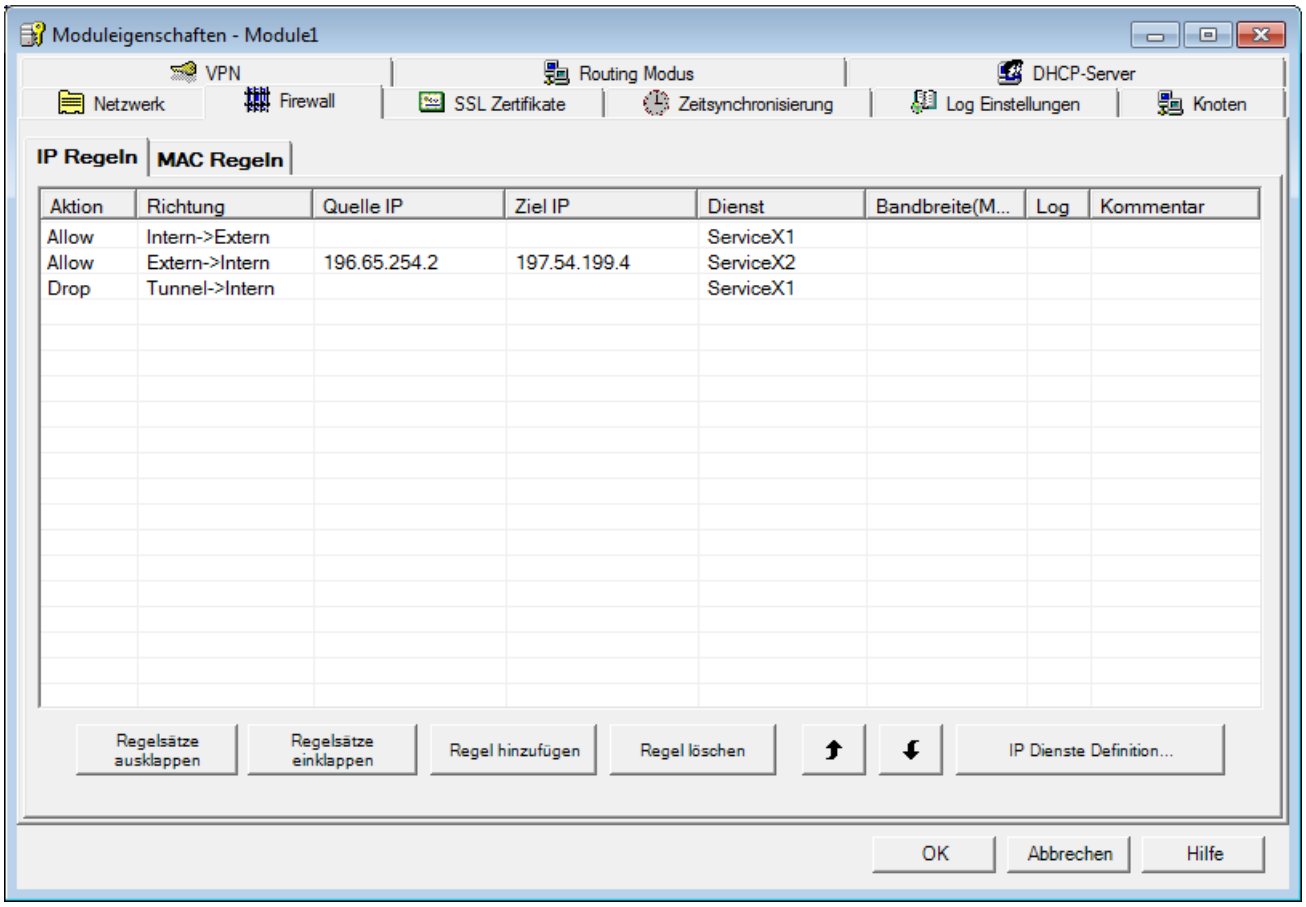
Quell-IP bzw. Ziel-IP	Adressband		Anzahl Adressen *)
	von	bis	
192.168.0.0**/16**	192.168.0.0	192.168.255.255	65.536
192.168.10.0**/24**	192.168.10.0	192.168.10.255	256
192.168.10.0**/25**	192.168.10.0	192.168.10.127	128
192.168.10.0**/26**	192.168.10.0	192.168.10.63	64
192.168.10.0**/27**	192.168.10.0	192.168.10.31	32
192.168.10.0**/28**	192.168.10.0	192.168.10.15	16
192.168.10.0**/29**	192.168.10.0	192.168.10.7	8
192.168.10.0**/30**	192.168.10.0	192.168.10.3	4
*) Hinweis: Beachten Sie, dass die Adresswerte 0 und 255 in der IP-Adresse Sonderfunktionen haben (0 steht für eine Netzwerkadresse, 255 steht für eine Broadcast-Adresse). Die Anzahl der tatsächlich verfügbaren Adressen verringert sich dadurch.			

Reihenfolge bei der Regelauswertung durch SCALANCE S

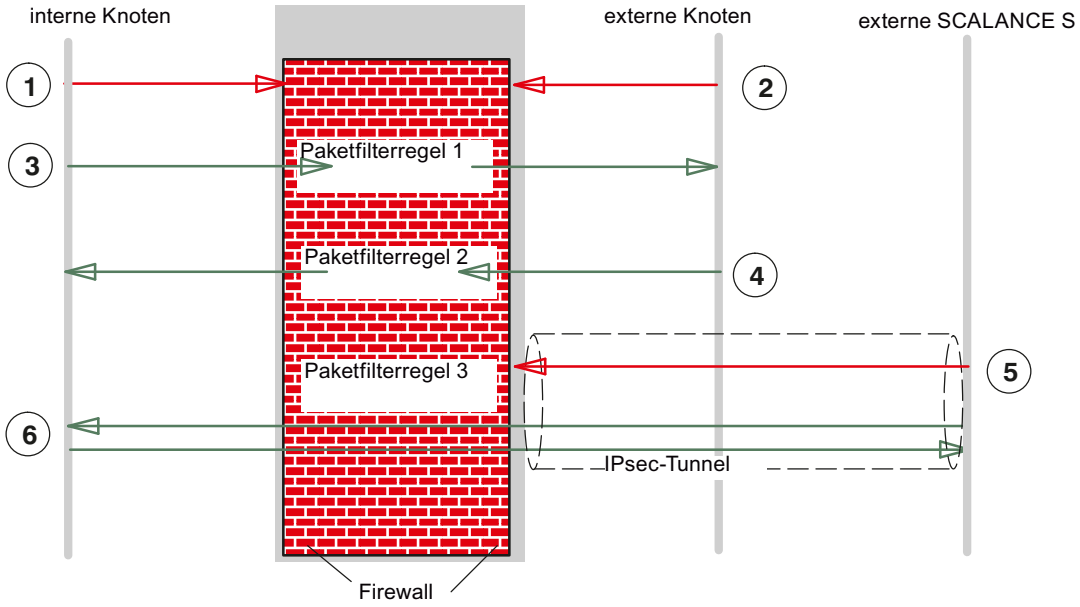
Die Paketfilter-Regeln werden wie folgt von SCALANCE S ausgewertet:

- Die Liste wird von oben nach unten ausgewertet; bei sich widersprechenden Regeln gilt also immer der weiter oben stehende Eintrag.
- Bei Regeln für die Kommunikation zwischen internem und externem Netz gilt die Abschlussregel: alle Telegramme außer den in der Liste explizit zugelassenen Telegrammen sind gesperrt.
- Bei Regeln für die Kommunikation zwischen internem Netz und IPsec-Tunnel gilt die Abschlussregel: alle Telegramme außer den in der Liste explizit gesperrten Telegrammen sind zugelassen.

Beispiel



Die im obigen Dialog beispielhaft dargestellten Paketfilter-Regeln bewirken folgendes Verhalten:



① Alle Telegrammtypen von intern nach extern sind standardmäßig geblockt, außer den explizit zugelassenen.
② Alle Telegrammtypen von extern nach intern sind standardmäßig geblockt, außer den explizit zugelassenen.
③ Die IP-Paketfilter-Regel 1 lässt Telegramme mit der Dienstdefinition "Service X1" von intern nach extern zu.
④ Die IP-Paketfilter-Regel 2 lässt Telegramme von extern nach intern zu, wenn erfüllt ist:

- IP-Adresse des Absenders: 196.65.254.2
- IP-Adresse des Empfängers: 197.54.199.4
- Dienstdefinition: "Service X2"

⑤ Die IP-Paketfilter-Regel 3 blockt Telegramme mit der Dienstdefinition "Service X2" im VPN (IPsec-Tunnel).
⑥ IPsec-Tunnel-Kommunikation standardmäßig ist zugelassen, außer den explizit geblockten Telegrammtypen.

5.4.5 IP-Dienste definieren

Mit Hilfe der IP-Dienst-Definitionen können Sie Firewall-Regeln, die auf bestimmte Dienste angewendet werden, kompakt und übersichtlich definieren. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu.

Zusätzlich können Sie so definierte Dienste wiederum unter einem Gruppennamen zu Gruppen zusammenfassen.

Bei der Projektierung der globalen oder lokalen Paketfilter-Regeln verwenden Sie dann einfach diese Namen.

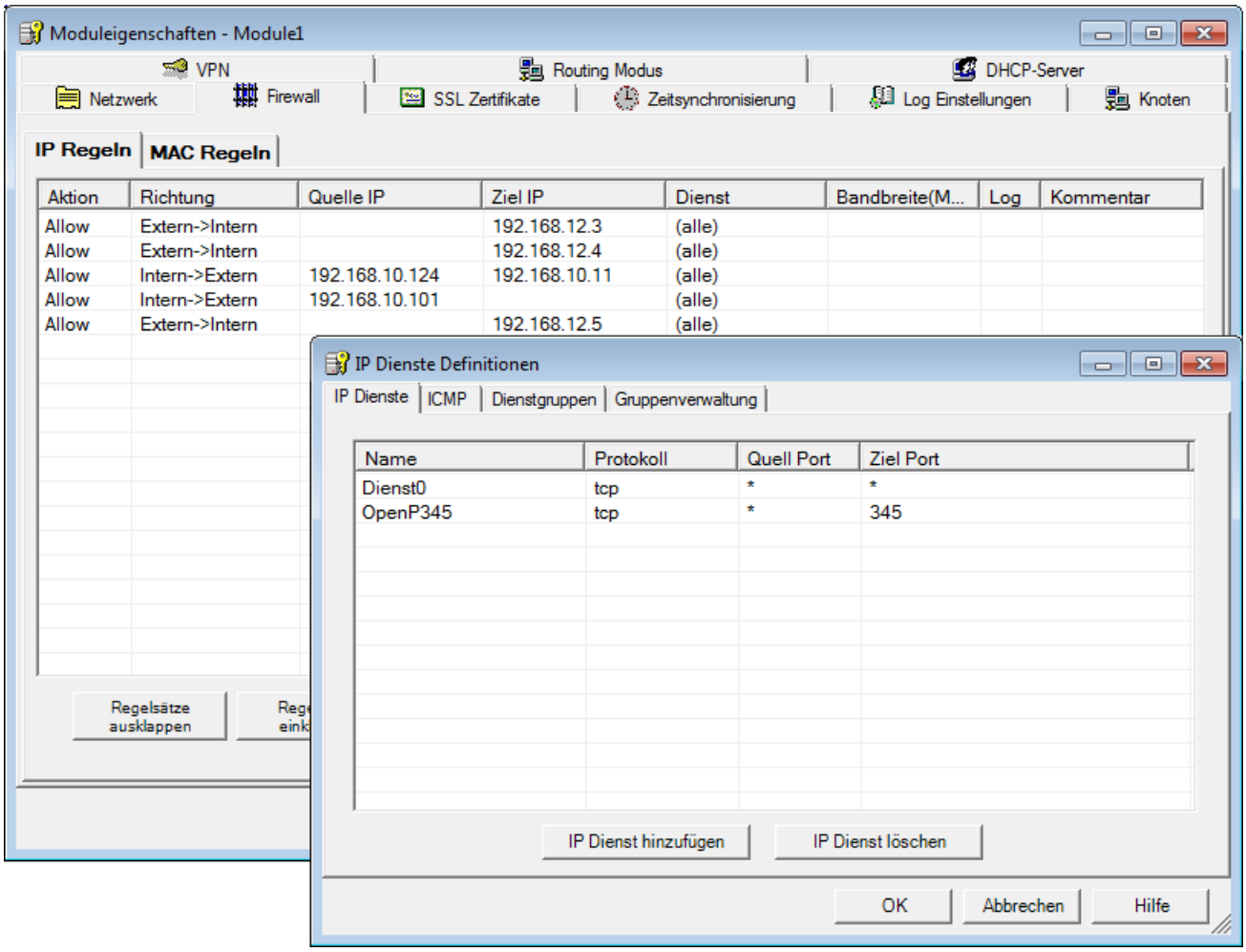
Dialog / Register

Sie öffnen den Dialog wie folgt:

- Über den Menübefehl **Optionen ▸ IP-Dienst-Definition...**

  oder

- Aus dem Register "Firewall/IP-Regeln" über die Schaltfläche "IP-Dienste-Definition...".



Parameter für IP-Dienste

Die Definition der IP-Dienste erfolgt über folgende Parameter:

Tabelle 5- 4 IP-Dienste: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	freie Eingabe

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Protokoll	Name des Protokolltyps	TCP UDP Any (TCP und UDP)
Quell-Port	Es erfolgt Filterung anhand der hier angegebenen Portnummer; diese definiert den Dienstzugang beim Telegrammabsender.	Beispiele: *: Port wird nicht geprüft 20 bzw. 21: FTP-Service
Ziel-Port	Es erfolgt Filterung anhand der hier angegebenen Portnummer; diese definiert den Dienstzugang beim Telegramm-Empfänger.	Beispiele: *: Port wird nicht geprüft 80: Web-HTTP-Service 102: S7-Protokoll - TCP/Port

5.4.6 ICMP-Dienste definieren

Mit Hilfe der ICMP-Dienst-Definitionen können Sie Firewall-Regeln, die auf bestimmte Dienste angewendet werden, kompakt und übersichtlich definieren. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu.

Zusätzlich können Sie so definierte Dienste wiederum unter einem Gruppennamen zu Gruppen zusammenfassen.

Bei der Projektierung der Paketfilter-Regeln verwenden Sie dann einfach diese Namen.

Dialog / Register

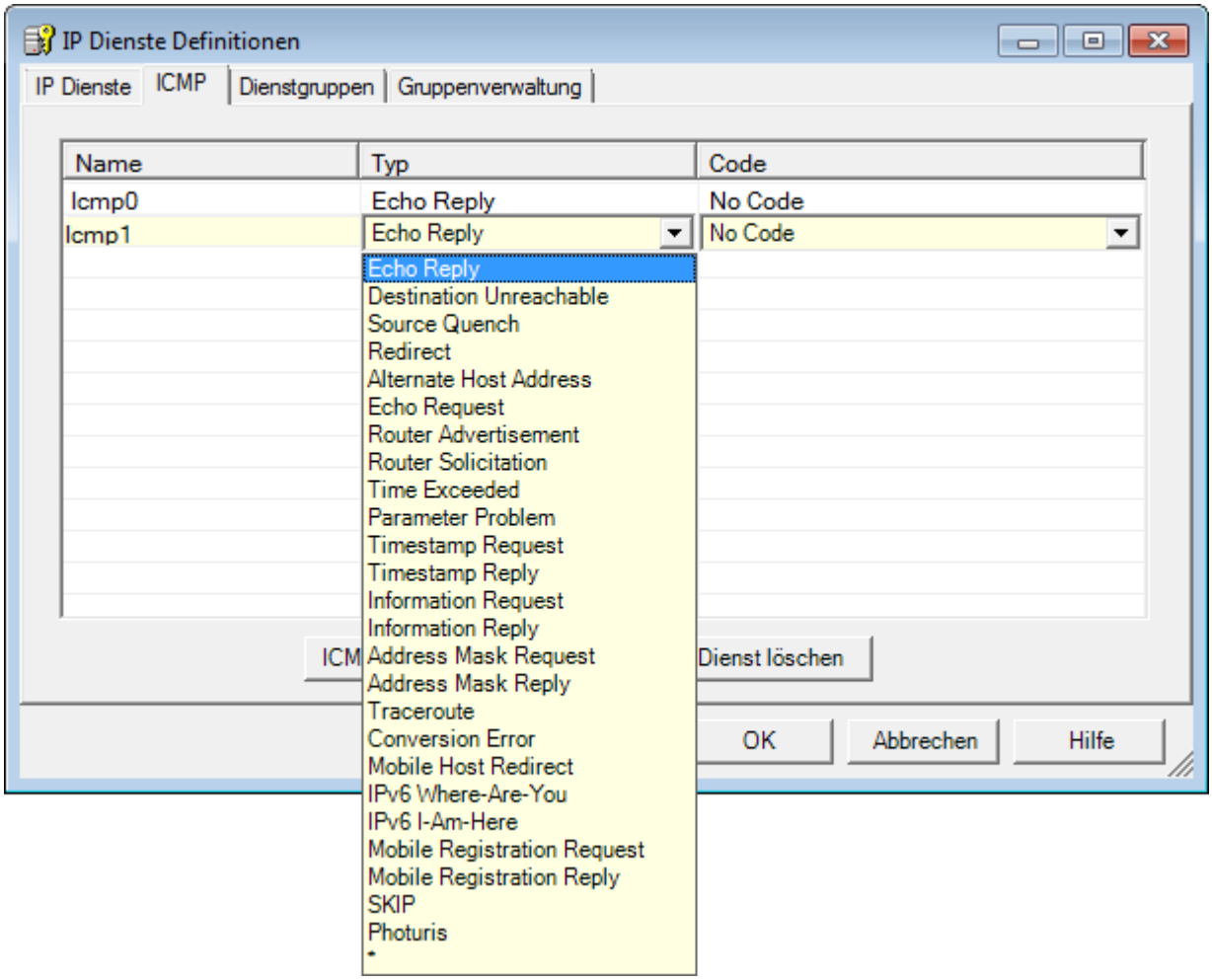
Sie öffnen den Dialog wie folgt:

- Über den Menübefehl

  Optionen ▸ IP-Dienst-Definition...

  oder

- Aus dem Register "Firewall" über die Schaltfläche "IP-Dienste Definition..." .



Parameter für ICMP-Dienste

Die Definition der ICMP-Dienste erfolgt über folgende Parameter:

Tabelle 5- 5 ICMP-Dienste: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	freie Eingabe

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Typ	Typ der ICMP-Message	• siehe Dialog-Darstellung
Code	Codes des ICMP-Types	Werte sind abhängig vom gewählten Typ.

5.4.7 MAC-Paketfilter-Regeln einstellen

Mittels MAC-Paketfilter-Regeln können Sie auf MAC-Telegramme filtern.

Hinweis

Routing-Modus

Wenn Sie für das SCALANCE S Modul den Routing-Modus aktiviert haben, finden MAC-Regeln keine Anwendung (Dialoge sind inaktiv).

Dialog / Register

Markieren Sie das zu bearbeitende Modul und wählen Sie zum Einrichten der Firewall folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften..., Register "Firewall", Tab "MAC-Regeln"

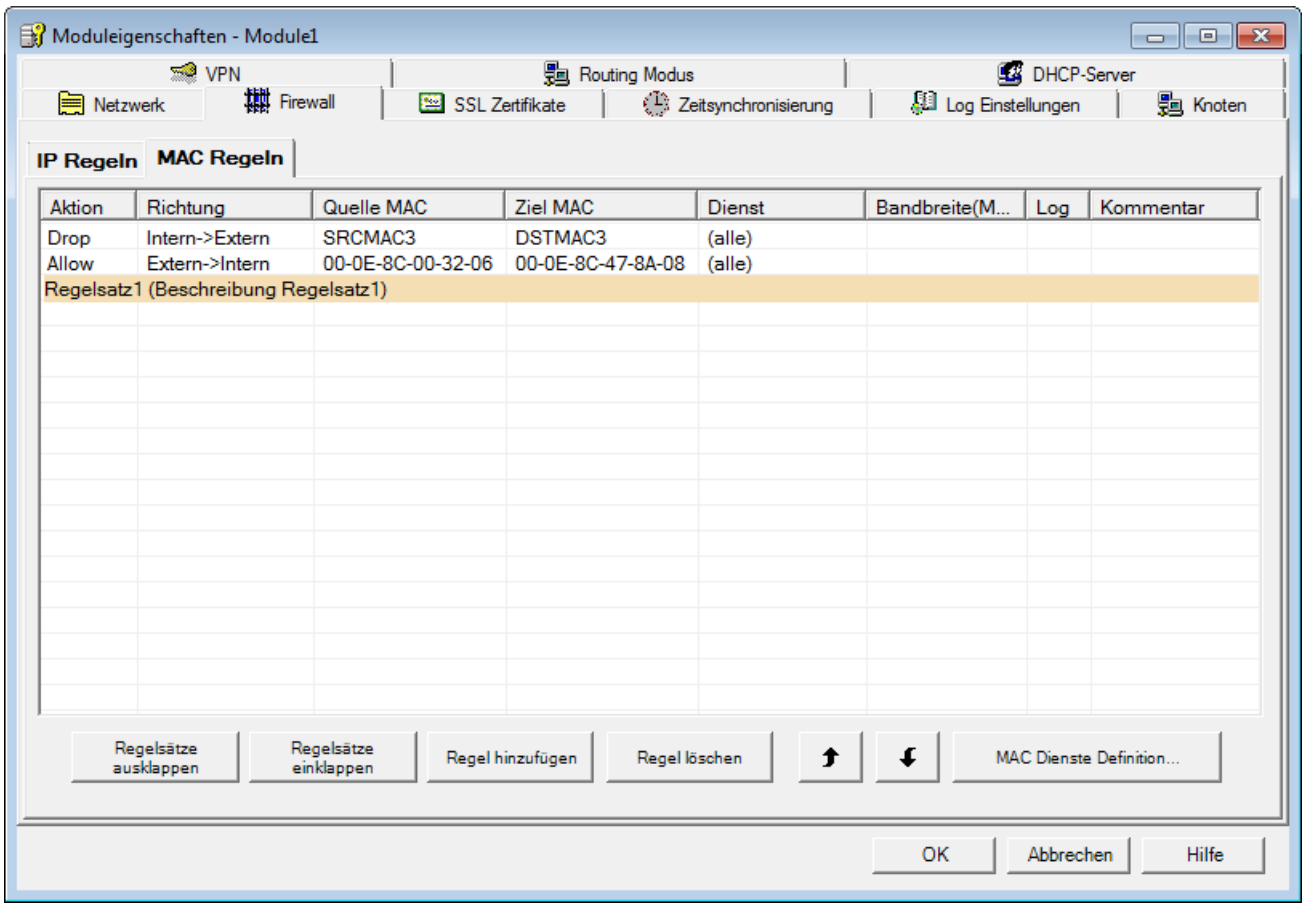


Bild 5-2 Dialog "MAC-Regeln" am Beispiel für SCALANCE S602

Paketfilter-Regeln eintragen

Tragen Sie der Reihe nach die Firewall-Regeln in die Liste ein; beachten Sie die Parameterbeschreibung und die Beispiele im Folgekapitel oder in der Online-Hilfe.

Globale Regelsätze nutzen

Globale Regelsätze, die Sie dem Modul zugewiesen haben, werden automatisch in den lokalen Regelsatz aufgenommen. Diese befinden sich zunächst am Ende der Regelliste, werden also mit der geringsten Priorität bearbeitet. Sie können die Priorität ändern, indem Sie die Position eines lokalen oder globalen Regelsatzes in der Regelliste verändern.

Die Online-Hilfe erläutert Ihnen die Bedeutung der einzelnen Schaltflächen.

5.4.8 MAC-Paketfilter-Regeln

Die Bearbeitung von MAC-Paketfilter-Regeln erfolgt anhand folgender Auswertungen:

- In der Regel eingetragene Parameter;
- Priorität der Regel innerhalb des Regelsatzes.

MAC-Paketfilter-Regeln

Die Projektierung einer MAC-Regel beinhaltet folgende Parameter:

Tabelle 5- 6 MAC-Regeln: Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Aktion	Zulassungsfestlegung (Freigabe/Sperre)	• Allow Telegramme gemäß Definition zulassen. • Drop Telegramme gemäß Definition sperren.
Richtung	Gibt die Richtung und Art des Datenverkehrs an ("Tunnel / Any" nur bei S612 / S613)	• Intern → Extern • Intern ← Extern • Tunnel → Intern • Tunnel ← Intern • Intern → Any • Intern ← Any
Quelle MAC	Quell-MAC-Adresse	Alternativ zu einer MAC-Adressangabe können Sie symbolische Namen eingeben.
Ziel MAC	Ziel-MAC-Adresse	
Dienst	Name des verwendeten MAC-Dienstes oder der Dienstgruppe.	Die Klappliste bietet die projektierten Dienste und Dienstgruppen zur Auswahl an. Keine Angabe bedeutet: es wird kein Dienst geprüft, die Regel gilt für alle Dienste.
Bandbreite (MBit/s)	Einstellmöglichkeit für eine Bandbreiten-Begrenzung. Ein Paket passiert die Firewall, wenn die Pass-Regel zutrifft und die zulässige Bandbreite für diese Regel noch nicht überschritten worden ist.	Wertebereich: 0.001...100 MBit/s
Log	Ein- bzw. Aus-Schalten des Logging für diese Regel	
Kommentar	Platz für eigene Erläuterung der Regel	

Regelauswertung durch SCALANCE S

Die Paketfilter-Regeln werden wie folgt von SCALANCE S ausgewertet:

- Die Liste wird von oben nach unten ausgewertet; bei sich widersprechenden Regeln gilt also immer der weiter oben stehende Eintrag.
- Bei den Regeln für die Kommunikation in Richtung intern->extern und intern<-extern gilt für alle nicht explizit erfassten Telegramme: alle Telegramme sind gesperrt, außer den in der Liste explizit zugelassenen Telegrammen.
- Bei den Regeln für die Kommunikation in Richtung intern-> IPsec-Tunnel und intern <- IPsec-Tunnel gilt für alle nicht explizit erfassten Telegramme: alle Telegramme sind zugelassen, außer den in der Liste explizit gesperrten Telegrammen.

ACHTUNG
Im Bridge-Mode: IP-Regeln greifen für IP-Pakete, MAC-Regeln greifen für Layer-2-Pakete Befindet sich ein Modul im Bridge-Mode so können für die Firewall sowohl IP-Regeln als auch MAC-Regeln definiert werden. Die Bearbeitung in der Firewall ist anhand des Ethertypes des Paketes geregelt. IP-Pakete werden abhängig von den IP-Regeln weitergeleitet bzw. geblockt und Layer-2-Pakete werden abhängig von den MAC-Regeln weitergeleitet bzw. geblockt. Es ist nicht möglich ein IP-Paket mit Hilfe einer MAC-Firewallregel beispielsweise hinsichtlich einer MAC-Adresse zu filtern.

Beispiele

Das Beispiel für den IP-Paketfilter in Kapitel 5.4.3 können Sie sinngemäß auf die MAC-Paketfilter-Regeln anwenden.

5.4.9 MAC-Dienste definieren

Mit Hilfe der MAC-Dienst-Definitionen können Sie Firewall-Regeln, die auf bestimmte Dienste angewendet werden, kompakt und übersichtlich definieren. Sie vergeben hierbei einen Namen und ordnen diesem die Dienstparameter zu.

Zusätzlich können Sie so definierte Dienste wiederum unter einem Gruppennamen zu Gruppen zusammenfassen.

Bei der Projektierung der globalen oder lokalen Paketfilter-Regeln verwenden Sie dann einfach diese Namen.

Dialog

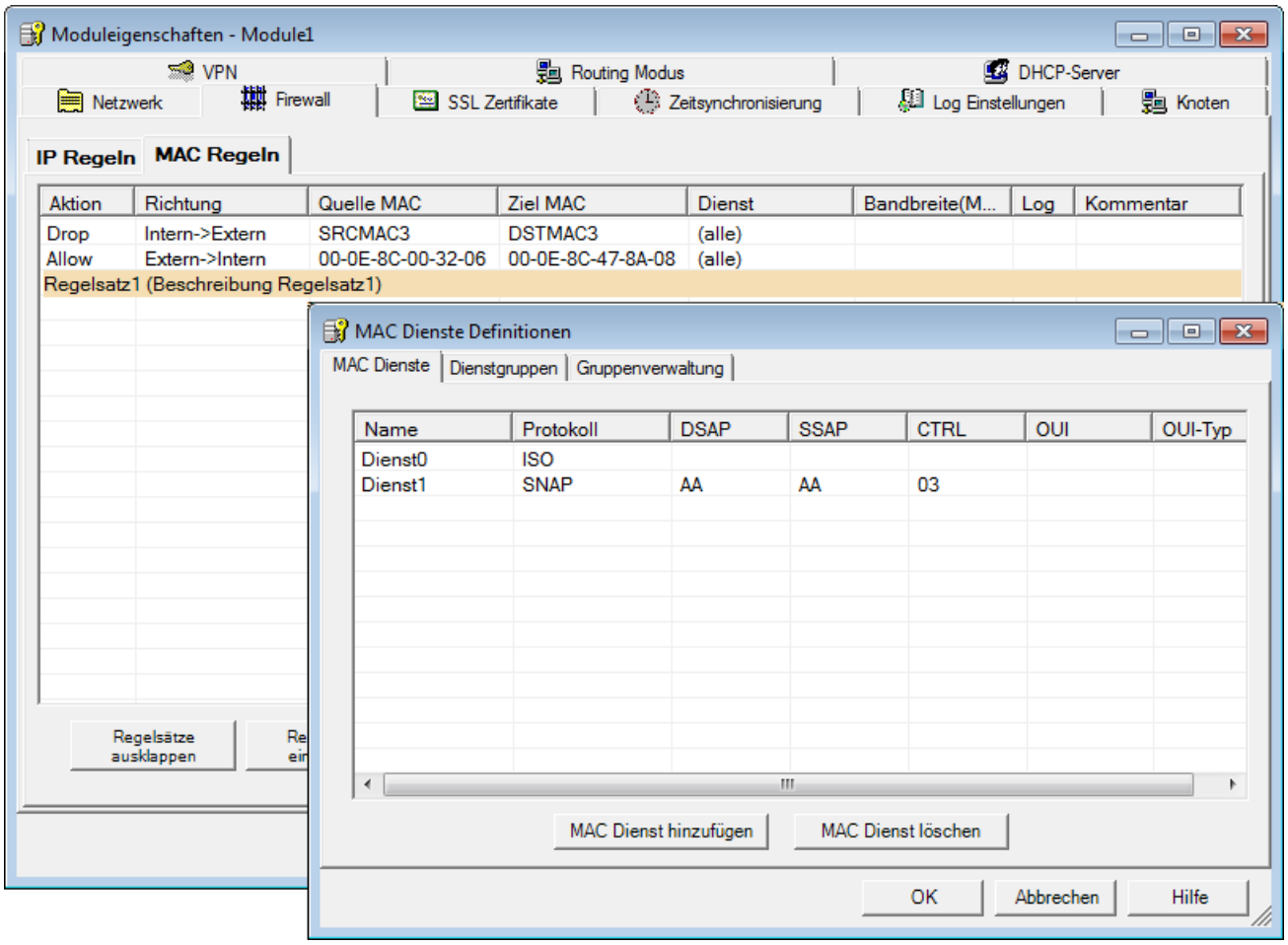
Sie öffnen den Dialog wie folgt:

- Über folgenden Menübefehl:

  Optionen ▸ MAC-Dienst Definition...

  oder

- Aus dem Register "Firewall/MAC-Regeln" über die Schaltfläche "MAC-Dienste-Definition..." .



Parameter für MAC-Dienste

Eine MAC-Dienst Definition beinhaltet eine Kategorie protokoll-spezifischer MAC-Parameter:

Tabelle 5- 7 MAC-Dienste Parameter

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Name	Frei definierbarer Name für den Dienst, der zur Identifikation in der Regeldefinition oder in der Gruppenzusammenfassung verwendet wird.	freie Eingabe

Bezeichnung	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
Protokoll	Name des Protokolltyps: • ISO ISO bezeichnet Telegramme mit folgenden Eigenschaften: Lengthfield <= 05DC (hex), DSAP= userdefined SSAP= userdefined CTRL= userdefined • SNAP SNAP bezeichnet Telegramme mit folgenden Eigenschaften: Lengthfield <= 05DC (hex), DSAP=AA (hex), SSAP=AA (hex), CTRL=03 (hex), OUI=userdefined, OUI-Type=userdefined	• ISO • SNAP • 0x (Code-Eingabe)
DSAP	Destination Service Access Point: LLC-Empfänger-Adresse	
SSAP	Source Service Access Point: LLC-Sender-Adresse	
CTRL	LLC Control Field	
OUI	Organizationally Unique Identifier (die ersten 3 Bytes der MAC Adresse = Hersteller Identifizierung)	
OUI-Type	Protokoll-Typ/Identifizierung	
*) Die Protokolleingaben 0800 (hex) und 0806 (hex) werden nicht akzeptiert, da diese Werte für IP- bzw. ICMP-Telegramme gelten. Diese Telegramme werden mittels der IP-Regeln gefiltert.		

Spezielle Einstellungen für SIMATIC NET Dienste

Verwenden Sie für die Filterung spezieller SIMATIC NET Dienste bitte die folgenden SNAP-Einstellungen:

- DCP (Primary Setup Tool):

  PROFINET

- SiClock:

  OUI= 08 00 06 (hex) , OUI-Type= 01 00 (hex)

5.4.10 Dienstgruppen einrichten

Bildung von Dienstgruppen

Sie können mehrere Dienste durch die Bildung von Dienstgruppen zusammenzufassen. Auf diese Weise können Sie komplexere Dienste aufbauen, die in den Paketfilter-Regeln dann durch einfache Namensauswahl verwendet werden können.

Dialoge / Register

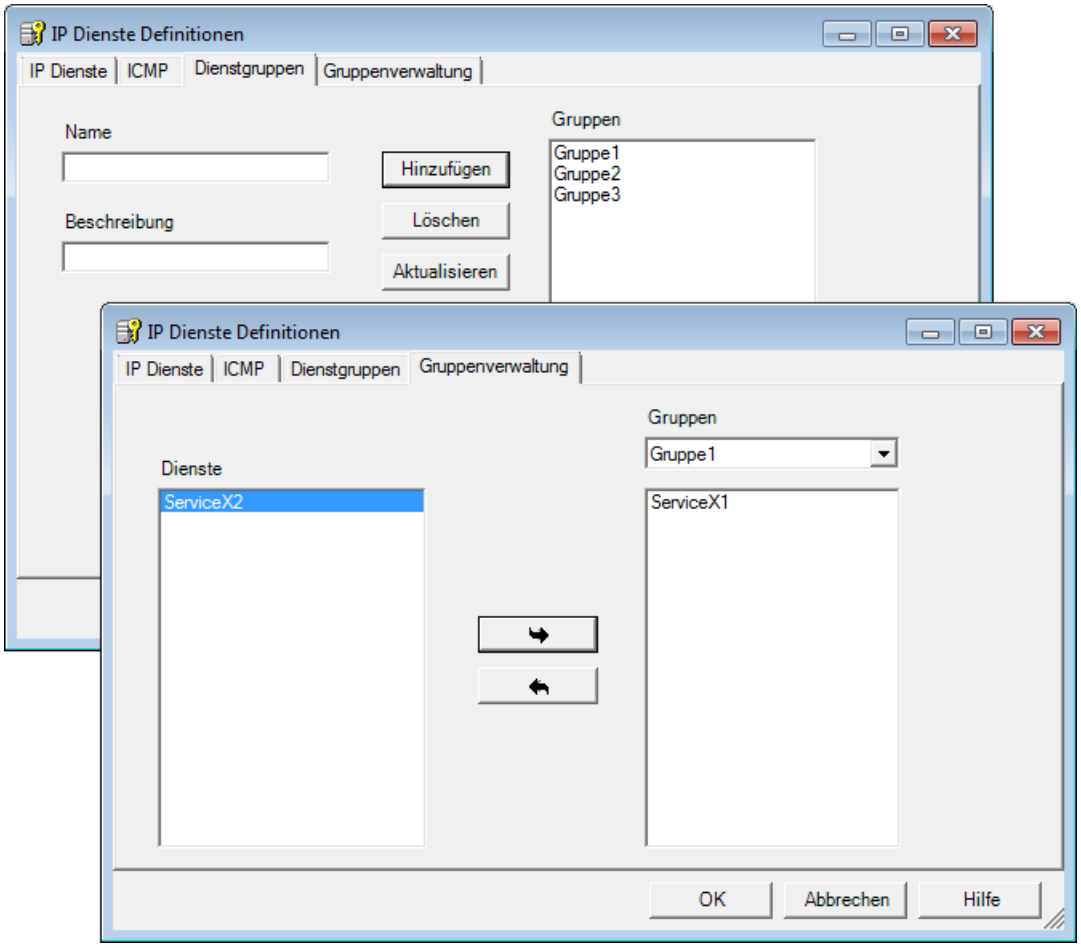
Sie öffnen den Dialog wie folgt:

- Über folgenden Menübefehl:

  Optionen ▸ IP/MAC-Dienst Definition...

  oder

- Aus dem Register "Firewall/IP-Regeln" bzw. "Firewall/MAC-Regeln" über die Schaltfläche "IP/MAC-Dienste-Definition..." .



5.5 Zeitsynchronisierung

Bedeutung

Zur Überprüfung der zeitlichen Gültigkeit eines Zertifikates und für die Zeitstempel von Log-Einträgen, wird auf dem SCALANCE S-Modul Datum und Uhrzeit geführt.

Hinweis

Die Zeitsynchronisation bezieht sich lediglich auf das SCALANCE S-Modul und kann nicht zur Synchronisation von Geräten im internen Netz des SCALANCE S verwendet werden.

Alternativen der Uhrzeitführung

Projektierbar sind folgende Alternativen:

- Lokale PC-Uhr

  Automatisches Stellen der Modul-Uhrzeit mit der PC-Uhrzeit beim Laden einer Konfiguration.

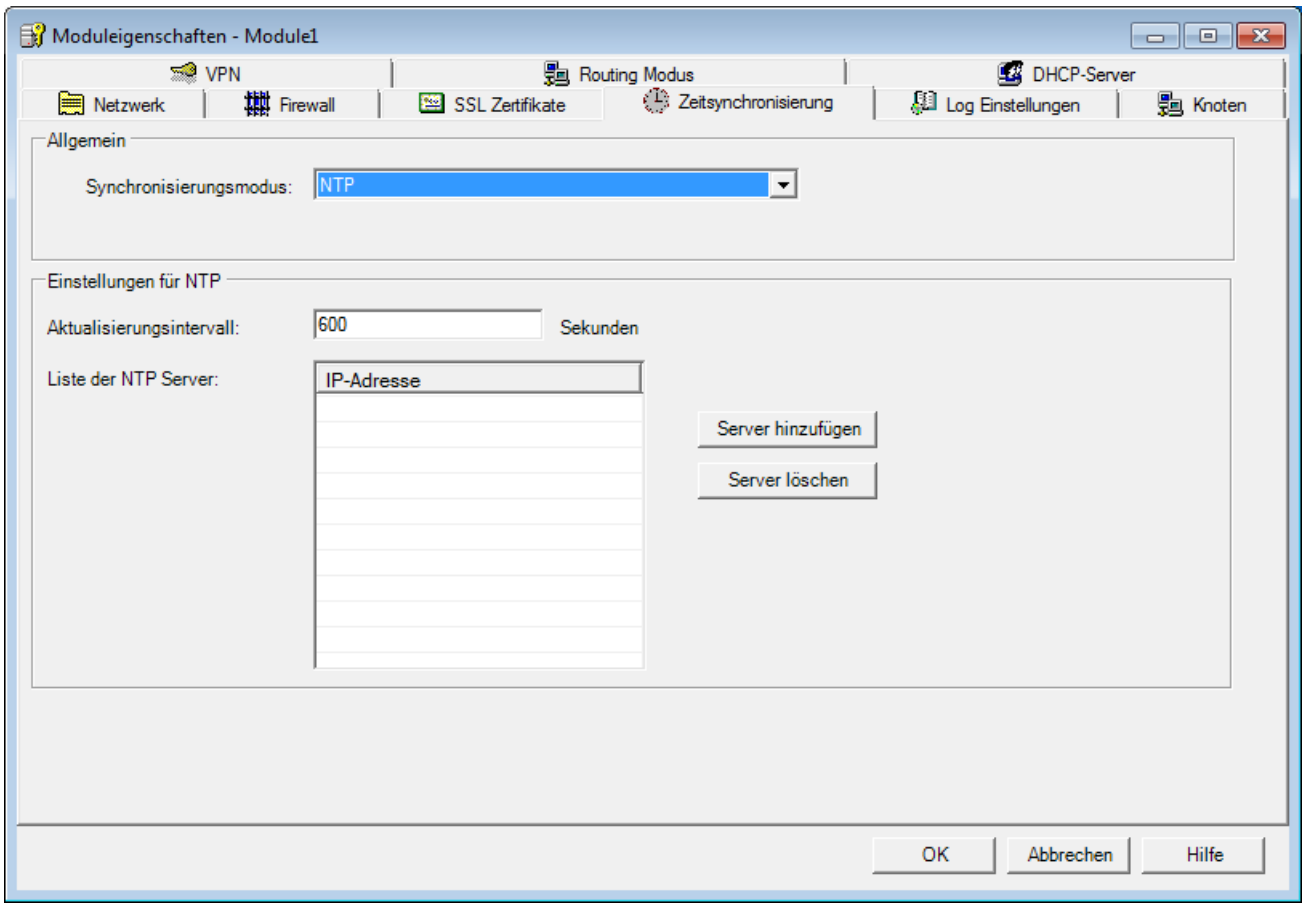
- NTP-Server

  Automatisches Stellen und periodischer Abgleich der Uhrzeit mittels eines NTP- Servers (Network Time Protocol).

Dialog zur Konfiguration der Zeitsynchronisierung öffnen

Markieren Sie das zu bearbeitende Modul und wählen Sie folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften..., Register "Zeitsynchronisierung"



Synchronisierung durch einen NTP-Zeit-Server

Bei der Synchronisierung durch einen NTP-Zeit-Server müssen Sie bei der Konfiguration die beiden folgenden Parameter angeben:

- IP-Adresse des NTP-Servers
- das Updateintervall in Sekunden

ACHTUNG
Wenn der NTP-Server vom Scalance S nicht über eine IPsec-Tunnelverbindung erreichbar ist, müssen Sie die Telegramme des NTP-Servers in der Firewall explizit freigeben (UDP, Port 123).

Externe Zeit-Telegramme

Externe Zeit-Telegramme sind nicht gesichert und können im externen Netz verfälscht werden. Das kann z.B. im internen Netz und bei den SCALANCE S-Modulen zu einer Kompromittierung der lokalen Zeit führen.

Daher sollten NTP-Server möglichst in internen Netzen platziert werden.

5.6 SSL-Zertifikate erzeugen

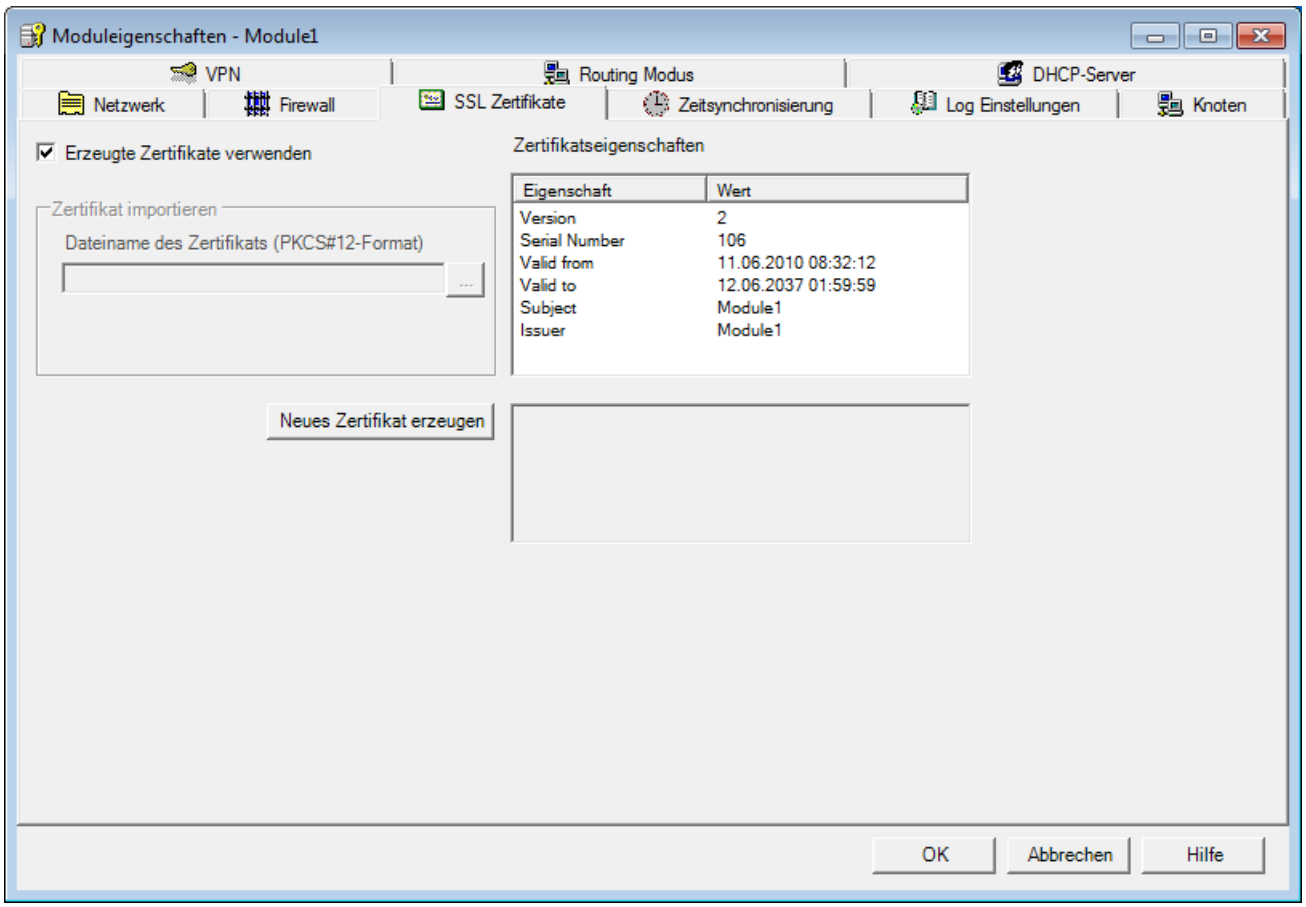
Bedeutung

SSL-Zertifikate werden für die Authentifizierung der Kommunikation zwischen einem Gerät und SCALANCE S bei der Online-Kommunikation herangezogen.

Dialog zur Verwaltung der SSL-Zertifikate öffnen

Markieren Sie das zu bearbeitende Modul und wählen Sie folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften..., Register "SSL-Zertifikate"



5.7 Routing-Modus

5.7.1 Routing

Bedeutung

Wenn Sie den Routing-Modus aktiviert haben, werden die Telegramme weitergeleitet, die an eine in den jeweiligen Subnetzen (interne oder externe) vorhandene IP-Adresse gerichtet sind. Darüberhinaus gelten die für die jeweilige Übertragungsrichtung getroffenen Firewall-Regeln.

Für diese Betriebsart müssen Sie im nachfolgend gezeigten Dialog eine interne IP-Adresse und eine interne Subnetzmaske für die Adressierung des Routers am internen Subnetz projektieren.

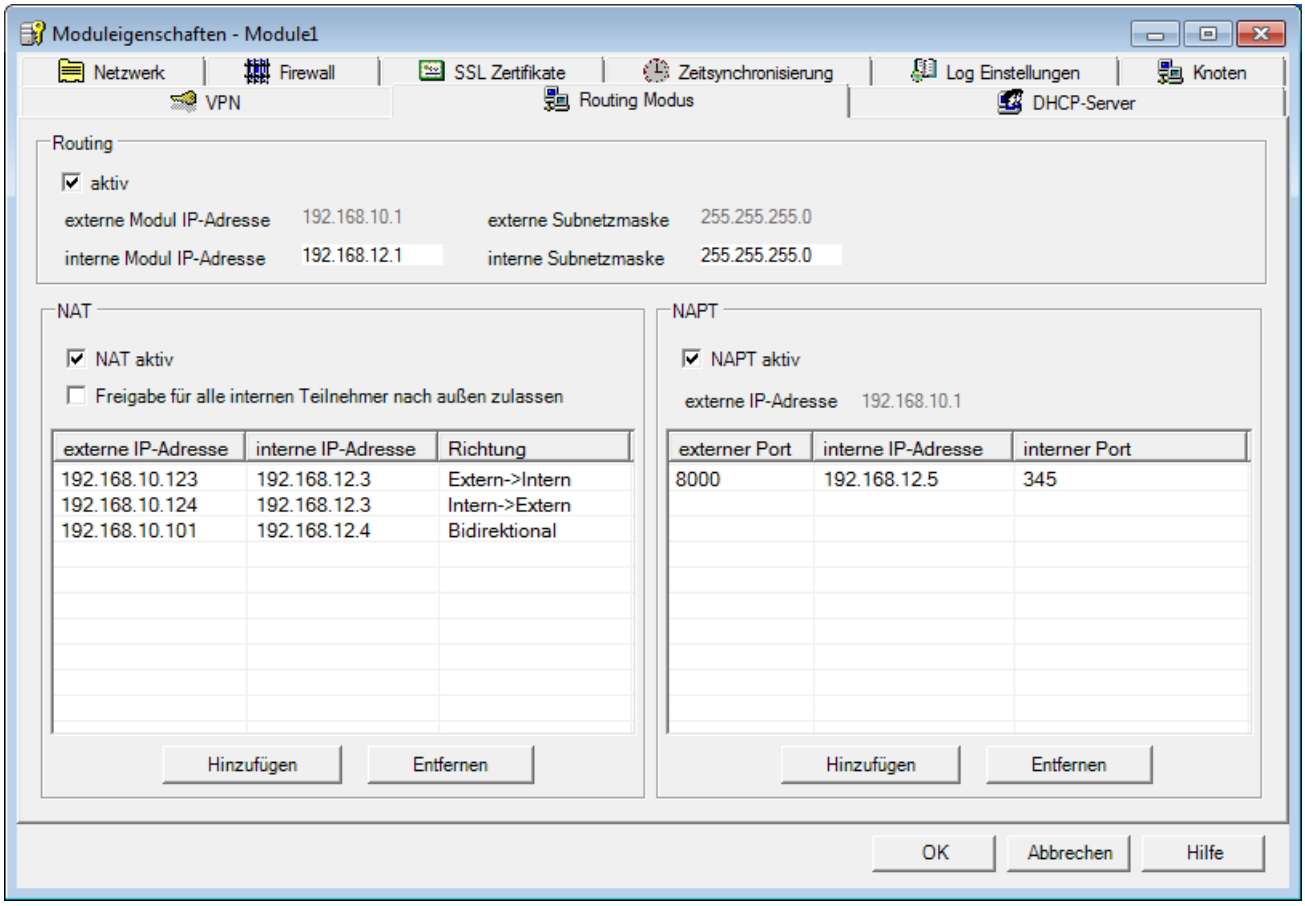
Bedienungssicht

Diese Funktion ist im Standard-Modus und im Erweitert-Modus identisch projektierbar.

Router-Betrieb aktivieren

1. Markieren Sie das zu bearbeitende Modul und wählen Sie folgenden Menübefehl:

   Bearbeiten ▸ Eigenschaften..., Register "Routing-Modus"



2. Wählen Sie die Routingoption "aktiv".
3. Tragen Sie eine interne IP-Adresse und eine interne Subnetzmaske für die Adressierung des Routers am internen Subnetz in die nun aktiven Eingabefelder ein.

5.7.2 NAT/NAPT-Routing

Bedeutung

Indem Sie im Dialog "Routing-Modus" eine Adressumsetzung projektieren, betreiben Sie SCALANCE S als NAT/NAPT-Router. Durch diese Technik erreichen Sie, dass die Adressen der Teilnehmer im internen Subnetz nach außen im externen Netz nicht bekannt werden; die internen Teilnehmer sind im externen Netz nur über die in der Adressumsetzungsliste (NAT-Tabelle und NAPT-Tabelle) definierten externen IP-Adressen sichtbar und damit vor direktem Zugriff geschützt.

- NAT: Network Adress Translation
- NAPT: Network Address Port Translation

Bedienungssicht

Diese Funktion ist im Erweitert-Modus verfügbar.

Schalten Sie für alle in diesem Kapitel beschriebenen Funktionen über folgenden Menübefehl die Betriebsart um:

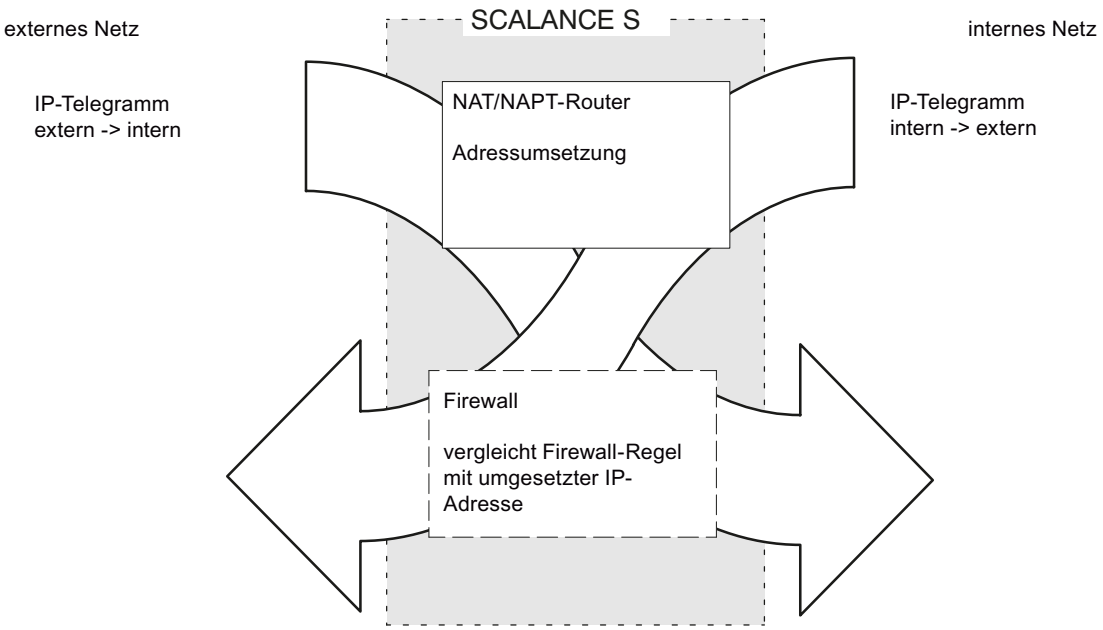
Ansicht ▸ Erweitert-Modus

Die hier beschriebene Betriebsart schließt den Betrieb als Standard-Router ein. Beachten Sie daher die Angaben im Kapitel "Routing".

Zusammenhang zwischen NAT/NAPT-Router und Firewall

Für beide Richtungen gilt, dass Telegramme zunächst die Adressumsetzung im NAT/NAPT-Router und anschließend die Firewall passieren. Die Einstellungen für den NAT/NAPT-Router und die Firewall-Regeln müssen so aufeinander abgestimmt werden, dass Telegramme mit umgesetzter Adresse die Firewall passieren können.

Firewall und NAT/NAPT-Router unterstützen den Mechanismus "Stateful Packet Inspection". Daher können Antworttelegramme den NAT/NAPT-Router und die Firewall passieren, ohne dass deren Adressen in der Firewall-Regel und der NAT/NAPT-Adressumsetzung zusätzlich aufgenommen werden müssen.



Beachten Sie die Beispiele in den nachfolgenden Kapiteln.

Einschränkungen

In der hier beschriebenen Liste erfolgt eine statisch festgelegte Adressumsetzung für die Teilnehmer am internen Netz (Subnetz).

Dialog zur Aktivierung des NAT/NAPT Router-Betrieb bearbeiten

1. Markieren Sie das zu bearbeitende Modul und wählen Sie folgenden Menübefehl:

   Bearbeiten ▸ Eigenschaften..., Register "Routing-Modus"

2. Aktivieren Sie je nach Anforderung eine Adressumsetzung gemäß NAT(Network Adress Translation) oder NAPT (Network Address Port Translation).
3. Projektieren Sie die Adressumsetzung gemäß den folgenden Angaben.

Eingabebereich "NAT" (Network Adress Translation)

Hier gilt: Adresse = IP-Adresse

Tabelle 5- 8 NAT Optionen

Optionskästchen	Bedeutung
NAT aktiv	Der Eingabebereich für NAT wird aktiviert. NAT-Adressumsetzungen werden erst durch die nachfolgend beschriebene Option und Einträge in die Adressumsetzungsliste wirksam. Zusätzlich müssen Sie die Firewall passend konfigurieren (siehe Beispiele).
Freigabe für alle internen Teilnehmer zulassen	Indem Sie diese Option wählen, erfolgt für alle von intern nach extern gehenden Telegramme eine Umsetzung der internen IP-Adresse auf die externe Modul IP-Adresse und einer zusätzlich vom Modul vergebenen Port-Nummer. Dieses Verhalten wird an der in der NAT-Tabelle unten zusätzlich eingeblendeten Zeile sichtbar. Dort wird mit einem Symbol "*" in der Spalte "interne IP-Adresse" angezeigt, dass alle von intern nach extern gerichteten Telegramme umgesetzt werden. Anmerkung: Wegen dieser Auswirkung auf die Adressumsetzungliste ist diese Option trotz der zusätzlichen Zuordnung einer Port-Nummer dem Eingabebereich NAT zugeordnet.

Tabelle 5- 9 NAT-Tabelle

Parameter	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
externe IP-Adresse	• Für Telegrammrichtung "Intern → Extern": neu zugewiesene IP-Adresse • Für Telegrammrichtung "Extern → Intern": erkannte IP-Adresse	Siehe unter Abschnitt "IP-Adressen in IP-Paketfilter-Regeln" in diesem Kapitel. Alternativ können Sie symbolische Namen eingeben.
interne IP-Adresse	• Für Telegrammrichtung " Extern → Intern ": neu zugewiesene IP-Adresse • Für Telegrammrichtung "Intern → Extern": erkannte IP-Adresse	
Richtung	Ordnen Sie hier die Telegrammrichtung zu. Auswirkung am Beispiel "Intern → Extern": Vom internen Subnetz kommende Telegramme werden auf die angegebene interne IP-Adresse geprüft und mit der angegebenen externen IP-Adresse in das externe Netz weitergeleitet.	• Intern → Extern • Extern → Intern • Bidirektional

Eingabebereich "NAPT" (Network Address Port Translation)

Hier gilt: Adresse = IP-Adresse + Port-Nummer

Tabelle 5- 10 NAPT Optionen

Optionskästchen	Bedeutung
NAPT aktiv	Der Eingabebereich für NAPT wird aktiviert. NAPT-Adressumsetzungen werden erst durch Einträge in die Adressumsetzungsliste wirksam. Zusätzlich müssen Sie die Firewall passend konfigurieren (siehe Beispiele).
externe IP-Adresse	Anzeige der IP-Adresse des SCALANCE S Moduls, die von den Teilnehmern am externen Netz als Router-Adresse verwendet wird.

Tabelle 5- 11 NAPT-Tabelle

Parameter	Bedeutung/Kommentar	Auswahlmöglichkeiten / Wertebereiche
externer Port	Ein Teilnehmer im externen Netz kann einem Teilnehmer im internen Subnetz antworten oder ein Telegramm senden, indem er diese Port-Nummer verwendet.	Port oder Portbereiche. Beispiel für die Eingabe eines Portbereiches: • 78:99
interne IP-Adresse	IP-Adresse des angesprochenen Teilnehmers am internen Subnetz.	Siehe unter Abschnitt "IP-Adressen in IP-Paketfilter-Regeln" in diesem Kapitel. Alternativ können Sie symbolische Namen eingeben.
interner Port	Port-Nummer eines Dienstes bei dem am internen Subnetz angesprochenen Teilnehmer.	Port (kein Portbereich)

Konsistenzprüfung - diese Regeln müssen Sie beachten

Beachten Sie für die Adresszuweisung folgende Regeln, um konsistente Einträge zu erhalten:

Prüfung / Regel	Prüfung erfolgt	
	lokal	projektweit
Die Netz-ID des internen Subnetzes muss unterschiedlich sein zur Netz-IDdes externen Subnetzes.		x
Die internen IP-Adressen dürfen nicht identisch sein mit den IP-Adressen des Moduls.		x

Prüfung / Regel	Prüfung erfolgt	
	lokal	projektweit
Übernehmen Sie den durch die Subnetzmaske bestimmten Anteil für die Netz-ID. • Bei der externen IP-Adresse ist der durch die externe Subnetzmaske bestimmte Adressanteil aus der externen SCALANCE S IP-Adresse zu übernehmen. • Bei der internen IP-Adresse ist der durch die interne Subnetzmaske bestimmte Adressanteil aus der internen SCALANCE S IP-Adresse zu übernehmen.		x
Eine IP-Adresse, die in der NAT/NAPT-Adressumsetzungsliste verwendet wird, darf keine Multicast-Adresse und keine Broadcast-Adresse sein.		x
Der Default-Router muss in einem der beiden Subnetze des SCALANCE S liegen, d.h. er muss entweder zur externen oder zur internen IP Adresse passen.		x
Die für die NAPT-Umsetzung vergebenen externen Ports liegen im Bereich > 0 und <= 65535. Port123 (NTP), 443 (HTTPS), 514 (Syslog) und 500+4500 (IPsec; nur für S612 und S613) sind davon ausgeschlossen.	x	
Die externe IP-Adresse des SCALANCE S darf in der NAT-Tabelle nur für die Richtung "Intern → Extern" verwendet werden.	x	
Die interne IP-Adresse des SCALANCE S darf in der NAT-Tabelle und in der NAPT-Tabelle nicht verwendet werden.		x
Duplikatsprüfung in der NAT-Tabelle Eine externe IP-Adresse, die mit Richtung "Extern → Intern" oder "Bidirektional" verwendet wird, darf nur einmal in der NAT-Tabelle erscheinen.	x	
Duplikatsprüfung in der NAPT-Tabelle • Eine externe Portnummer darf nur einmal eingetragen sein. Da immer die IP-Adresse des SCALANCE S als externe IP-Adresse verwendet wird, wäre bei mehrfacher Verwendung keine Eindeutigkeit gegeben. • Die Portnummern bzw. Portbereiche der externen Ports dürfen sich nicht überschneiden.	x	
Sobald der Routing-Modus aktiviert wurde, müssen dem SCALANCE S die zweiten Adressen (IP/Subnetz) zugeordnet werden.		x
Interne NAPT-Ports können im Bereich > 0 und <= 65535 liegen.	x	

Führen Sie nach Abschluss Ihrer Eingaben eine Konsistenzprüfung durch.

Wählen Sie hierzu den Menübefehl:

Optionen ▸ Konsistenzprüfungen

5.7.3 NAT/NAPT-Routing - Beispiele zur Konfiguration Teil 1

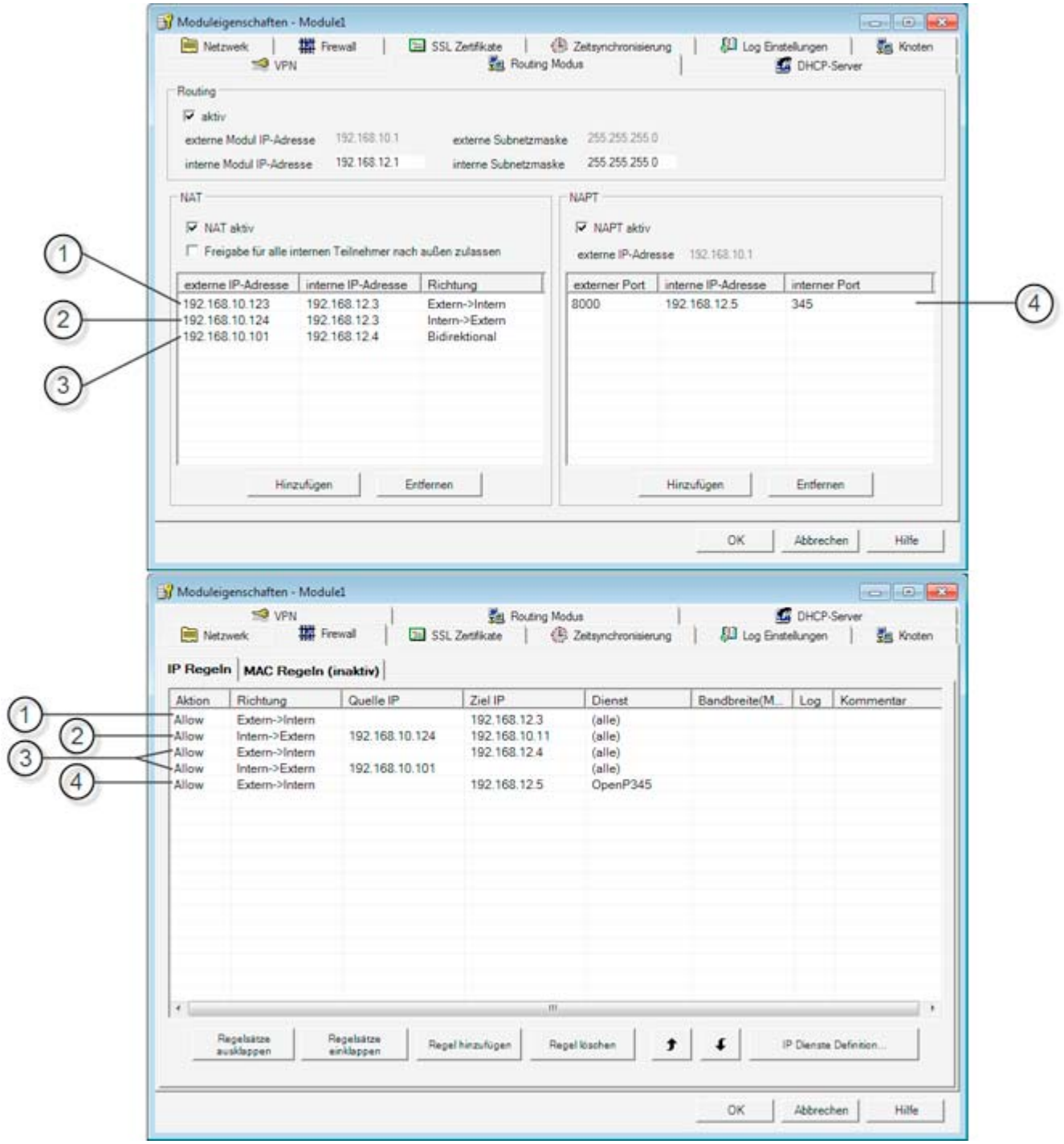
Übersicht

Sie finden in diesem Kapitel folgende Beispiele zur Konfiguration des NAT/NAPT-Routers:

- Beispiel 1: NAT-Adressumsetzung "Extern → Intern"
- Beispiel 2: NAT-Adressumsetzung "Intern → Extern"
- Beispiel 3: NAT-Adressumsetzung "Bidirektional"
- Beispiel 4: NAPT-Adressumsetzung

Projektierung

In der folgenden Routing-Projektierung finden Sie Adresszuweisungen gemäß NAT- und NAPT-Adressumsetzung:



Beschreibung

- **Beispiel 1: NAT-Adressumsetzung "Extern → Intern"**

  Ein Teilnehmer im externen Netz kann dem Teilnehmer mit der internen IP-Adresse 192.168.12.3 im internen Subnetz ein Telegramm senden, indem er die externe IP-Adresse 192.168.10.123 als Zieladresse verwendet.

- **Beispiel 2: NAT-Adressumsetzung "Intern → Extern"**

  Telegramme eines internen Teilnehmers mit der internen IP-Adresse 192.168.12.3 werden in das externe Netz mit der externen IP-Adresse 192.168.10.124 als Quelladresse weitergeleitet. Die Firewall ist im Beispiel so eingestellt, dass Telegramme mit der Quell IP-Adresse 192.168.10.124 von intern nach extern zugelassen sind und dass Teilnehmer mit der IP-Adresse 192.168.10.11 erreicht werden.

- **Beispiel 3: NAT-Adressumsetzung "Bidirektional"**

  In diesem Beispiel wird die Adressumsetzung sowohl bei intern als auch extern eingehenden Telegrammen wie folgt vorgenommen:

  – Ein Teilnehmer im externen Netz kann dem Teilnehmer mit der internen IP-Adresse 192.168.12.4 im internen Subnetz ein Telegramm senden, indem er die externe IP-Adresse 192.168.10.101 als Zieladresse verwendet.

  – Telegramme eines internen Teilnehmers mit der internen IP-Adresse 192.168.12.4 werden am externen Netz mit der externen IP-Adresse 192.168.10.101 als Quelladresse weitergeleitet. Die Firewall ist so eingestellt, dass Telegramme mit der Quell IP-Adresse 192.168.10.101 von intern nach extern zugelassen sind.

- **Beispiel 4: NAPT-Adressumsetzung**

  Adressumsetzungen erfolgen gemäß NAPT so, dass es jeweils zusätzlich Port-Nummern zugewiesen werden. Alle auf dem externen Netz eingehenden TCP- und UDP-Telegramme werden auf ihre Ziel-IP-Adresse und Ziel-Port-Nummer überprüft.

  – Ein Teilnehmer im externen Netz kann dem Teilnehmer mit der IP-Adresse 192.168.12.4 und Port-Numner 345 im internen Subnetz ein Telegramm senden, indem er als Ziel-Adresse die externe Modul-IP-Adresse 192.168.10.1 und die externe Port-Nummer 8000 verwendet.

5.7.4 NAT/NAPT-Routing - Beispiele zur Konfiguration Teil 2

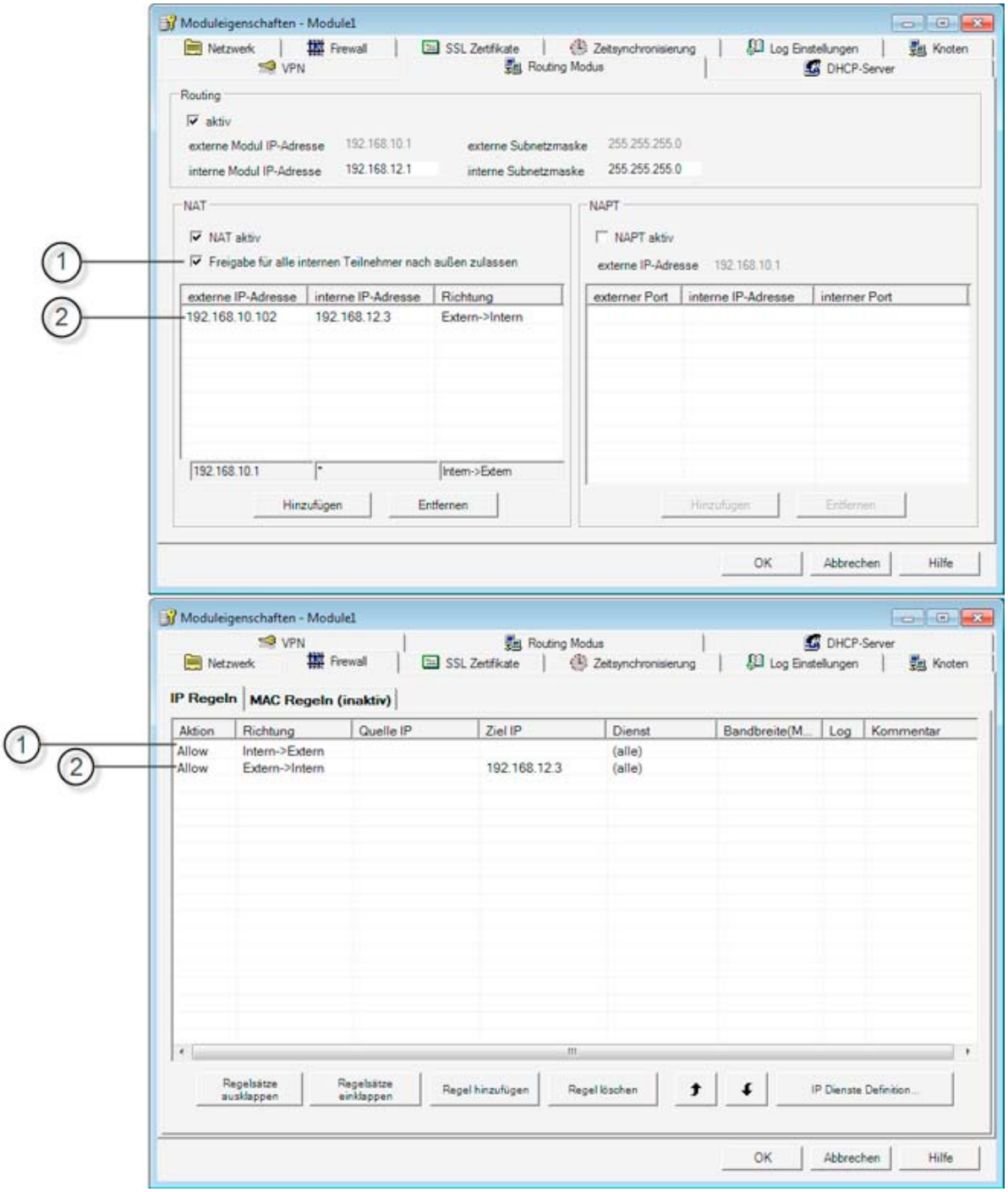
Übersicht

Sie finden in diesem Kapitel folgende Beispiele zur Konfiguration des NAT/NAPT-Routers:

- Beispiel 1: Alle internen Teilnehmer für externe Kommunikation zulassen
- Beispiel 2: Zusätzlich Telegramme zulassen, die von extern nach intern gerichtet sind.

Projektierung

In der folgenden Routing-Projektierung finden Sie Adresszuweisungen gemäß NAT-Adressumsetzung:



Beschreibung

Beispiel 1 - Alle internen Teilnehmer für externe Kommunikation zulassen

Im Dialogbereich "NAT" ist das Optionskästchen "Freigabe für alle internen Teilnehmer nach außen zulassen" aktiviert.

Damit ist die Kommunikation von intern nach extern möglich. Die Adressumsetzung erfolgt hierbei so, dass alle internen Adressen auf die externe IP-Adresse von SCALANCE S und jeweils einer dynamisch vergebenen Port-Nummer umgesetzt werden.

Eine Richtungsangabe in der NAT-Adressumsetzungsliste ist nun nicht mehr relevant. Sämtliche weiteren Angaben beziehen sich auf die Kommunikationsrichtung extern nach intern.

Zusätzlich ist die Firewall so eingestellt, dass die Telegramme von intern nach extern passieren können.

Beispiel 2 - Zusätzlich Telegramme zulassen, die von extern nach intern gerichtet sind.

Um zusätzlich zum Beispiel 1 die Kommunikation von extern nach intern zuzulassen, sind Angaben in der NAT- oder in der NAPT-Adressumsetzungsliste einzutragen. Der Eintrag im Beispiel besagt, dass Telegramme an den Teilnehmer mit der IP-Adresse 192.168.10.102 auf die interne IP-Adresse 192.168.12.3 umgesetzt werden.

Entsprechend muss die Firewall eingestellt werden. Da immer zunächst die NAT/NAPT-Umsetzung erfolgt und erst im zweiten Schritt die umgesetzte Adresse in der Firewall geprüft wird, ist im Beispiel die interne IP-Adresse als Ziel IP-Adresse in der Firewall eingetragen.

5.8 DHCP-Server

Übersicht

Sie können SCALANCE S am internen Netz als DHCP-Server betreiben. Damit ist es möglich, den am internen Netz angeschlossenen Geräten automatisch IP-Adressen zuzuweisen.

Die IP-Adressen werden hierbei entweder dynamisch aus einem von Ihnen vergebenen Adressband zugewiesen oder es wird gemäß Ihrer Vorgabe eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

In den Erweitert-Modus umschalten

Die Konfiguration als DHCP-Server setzt im Security Configuration Tool die Ansicht "Erweitert-Modus" voraus. Schalten Sie über folgenden Menübefehl die Betriebsart um:

Ansicht ▸ Erweitert-Modus

Voraussetzung

Sie müssen die Geräte am internen Netz so konfigurieren, dass diese die IP-Adresse von einem DHCP-Server beziehen.

Je nach Betriebsart übermittelt SCALANCE S den Teilnehmern im Subnetz eine Router IP-Adresse oder Sie müssen den Teilnehmern im Subnetz eine Router IP-Adresse bekannt machen.

- Router IP-Adresse wird übermittelt

  In folgenden Fällen wird durch das DHCP-Protokoll von SCALANCE S eine Router IP-Adresse an den Teilnehmer übermittelt:

  – SCALANCE S ist für den Router-Betrieb konfiguriert;

    SCALANCE S übermittelt in diesem Fall die eigene IP-Adresse als Router IP-Adresse

  – SCALANCE S ist nicht für den Router-Betrieb konfiguriert, es ist aber in der Konfiguration von SCALANCE S ein Default-Router angegeben;

    SCALANCE S übermittelt in diesem Fall die Default-Router IP-Adresse als Router IP-Adresse.

- Router IP-Adresse wird nicht übermittelt

  Tragen Sie in folgenden Fällen die Router IP-Adresse beim Teilnehmer manuell ein:

  – SCALANCE S ist nicht für den Router-Betrieb konfiguriert;

  – In der Konfiguration von SCALANCE S ist kein Default-Router angegeben.

Varianten

Sie haben die beiden folgenden Möglichkeiten zur Konfiguration:

- Statische Adressvergabe

  Geräten mit einer bestimmten MAC-Adresse oder Client-ID werden jeweils vorgegebene IP-Adressen zugeordnet. Tragen Sie hierzu diese Geräte in die Adressliste im Eingabebereich "statische IP-Adressen" ein.

- Dynamische Adressvergabe

  Geräte, deren MAC-Adresse oder deren Client-ID nicht explizit angegeben wurde, erhalten eine beliebige IP-Adresse aus einem vorgegebenen Adressband. Dieses Adressband stellen Sie im Eingabebereich "dynamische IP-Adressen" ein.

ACHTUNG
Dynamische Adressvergabe - Verhalten nach Unterbrechung der Spannungsversorgung Beachten Sie, dass die dynamisch vergebenen IP-Adressen nicht gespeichert werden, wenn die Spannungsversorgung unterbrochen wird. Nach Wiederkehr der Spannungsversorgung müssen Sie daher dafür sorgen, dass die Teilnehmer erneut eine IP-Adresse anfordern. Sie sollten daher die dynamische Adressvergabe nur für folgende Teilnehmer vorsehen: • Teilnehmer, die im Subnetz temporär genutzt werden (wie beispielsweise Service-Geräte); • Teilnehmer, die eine einmal zugewiesene IP-Adresse bei einer erneuten Anforderung an den DHCP-Server als "Vorzugsadresse" übermitteln (wie beispielsweise PC-Stationen). Für die Teilnehmer im dauernden Betrieb ist die statische Adresszuweisung über die Angabe einer Client-ID (empfohlen für S7 CPs wegen des einfacheren Baugruppentauschs) oder der MAC-Adresse vorzuziehen

Symbolische Namen werden unterstützt

Sie können in der hier beschriebenen Funktion IP-Adressen oder MAC-Adressen auch als symbolische Namen eingeben.

Konsistenzprüfung - diese Regeln müssen Sie beachten

Berücksichtigen Sie bei Ihrer Eingabe die nachfolgend aufgeführten Regeln.

Prüfung / Regel	Prüfung erfolgt [1]	
	lokal	Projekt-/Modulweit
Die in der Adressliste im Eingabebereich "statische IP-Adressen" zugewiesenen IP-Adressen dürfen nicht im Bereich der dynamischen IP-Adressen liegen.		x
Symbolische Namen müssen eine numerische Adresszuordnung besitzen. Wenn Sie symbolische Namen hier neu vergeben, müssen Sie die Adresszuordnung im Dialog "Symbolische Namen" noch vornehmen.		x
IP-Adressen, MAC-Adressen und Client-IDs dürfen in der Tabelle "statische IP-Adressen" nur einmal vorkommen (bezogen auf das SCALANCE S-Modul).		x
Sie müssen bei den statisch zugewiesenen IP-Adressen entweder die MAC-Adresse oder die Client-ID (Rechner-Name) angeben.	x	
Die Client-ID ist eine Zeichenfolge mit maximal 63 Zeichen. Es dürfen nur die folgenden Zeichen verwendet werden: a-z, A-Z, 0-9 und - (Bindestrich). Hinweis: Bei SIMATIC S7 kann den Geräten an der Ethernet-Schnittstelle für den Bezug einer IP-Adresse über DHCP eine Client-ID zugewiesen werden. Bei PCs ist die Vorgehensweise abhängig vom verwendeten Betriebssystem; es wird empfohlen, hier die MAC-Adresse für die Zuordnung zu verwenden.	x	
Sie müssen bei den statisch zugewiesenen IP-Adressen die IP Adresse angeben.	x	
Folgende IP Adressen dürfen nicht im Bereich des freien IP Adressbandes (dynamische IP-Adressen) liegen: • alle Router-Adressen im Register "Netzwerk" • NTP-Server • Syslog-Server • Default-Router • SCALANCE S Adresse(n)		x
DHCP wird von SCALANCE S an der Schnittstelle zum internen Subnetz unterstützt. Aus diesem Betriebsverhalten des SCALANCE S ergeben sich weiterhin für IP Adressen im Bereich des freien IP Adressbands (dynamische IP-Adressen) folgende Anforderungen: • Betrieb in flachen Netzen Der Bereich des freien IP-Adressbands muss in dem durch SCALANCE S definierten Netz liegen. • Router-Betrieb Der Bereich des freien IP-Adressbands muss in dem durch SCALANCE S definierten internen Subnetz liegen.		x
Das freie IP-Adressband muss durch die Angabe der Start-IP-Adresse und der End-IP-Adresse vollständig angegeben sein. Die End-IP-Adresse muss größer als die Start-IP-Adresse sein.	x	
Die IP-Adressen, die Sie in die Adressliste im Eingabebereich "statische IP-Adressen" eingeben, müssen im Adressbereich des internen Subnetzes des SCALANCE S-Moduls liegen.		x

Legende:

[1)] Beachten Sie die Erläuterungen im Kapitel "Konsistenzprüfungen".

Gesicherte Kommunikation im VPN über IPsec-Tunnel (S612 / S613)

6

Wie Sie die von SCALANCE S geschützten IP-Subnetze per Drag and Drop zu einem Virtual Private Network verbinden - das ist Thema dieses Kapitels.

Wie bereits in Kapitel 5 bei den Moduleigenschaften beschrieben, können Sie es auch hier bei Standard-Einstellungen belassen, um eine sichere Kommunikation innerhalb Ihrer internen Netze zu betreiben.

Weitere Informationen

Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Siehe auch

Online Funktionen - Test, Diagnose und Logging (Seite 227)

6.1 VPN mit SCALANCE S

Sichere Verbindung durch ungeschütztes Netz

Für die von SCALANCE S geschützten internen Netze stellen IPsec-Tunnel eine gesicherte Datenverbindung durch das unsichere externe Netz zur Verfügung.

Der Datenaustausch der Geräte über die IPsec-Tunnel im VPN hat dadurch folgende Eigenschaften:

- Vertraulichkeit

  Die ausgetauschten Daten sind abhörsicher;

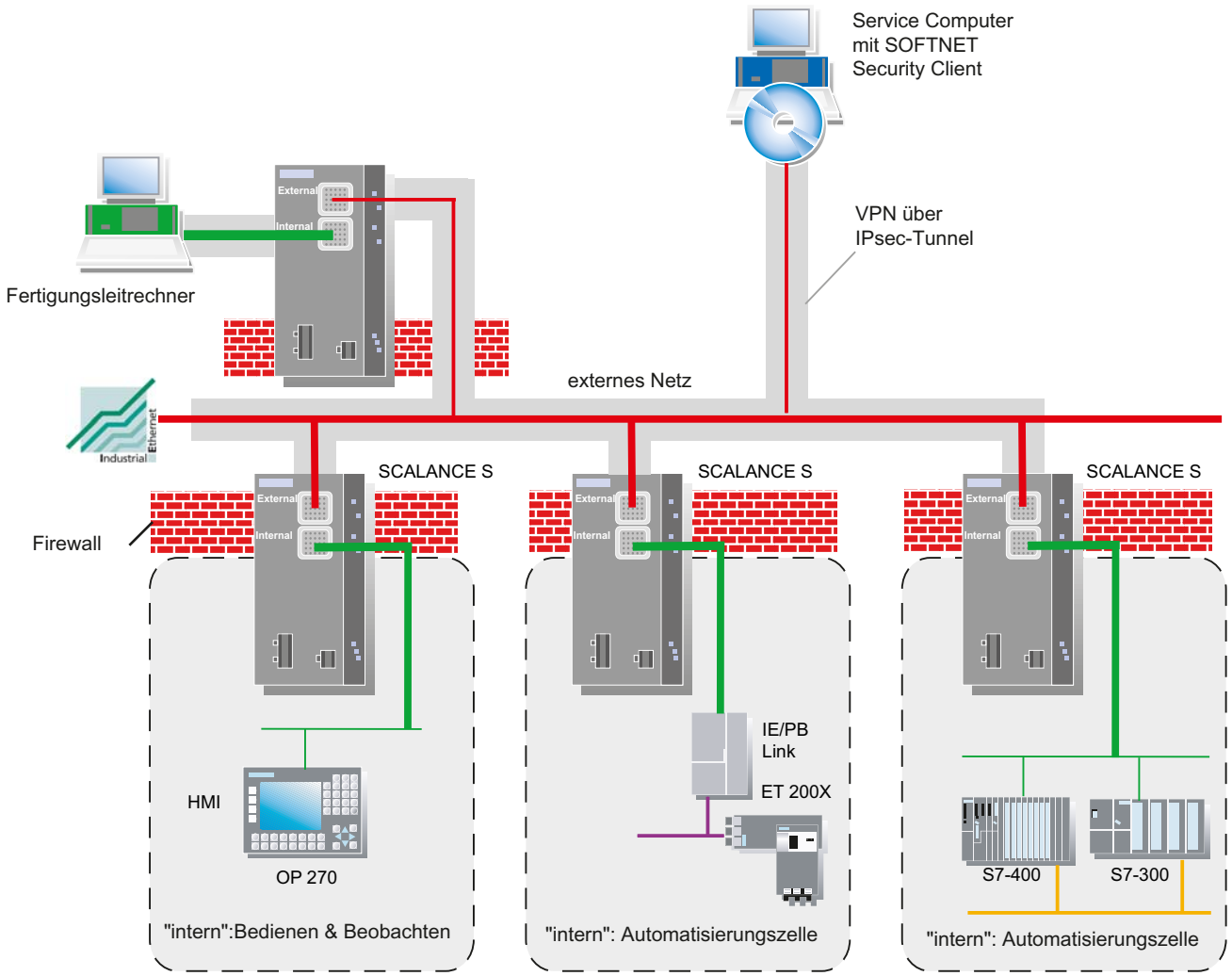
- Integrität

  Die ausgetauschten Daten sind verfälschungssicher;

- Authentizität

  Nur derjenige kann einen Tunnel aufbauen, der die Berechtigung dazu hat.

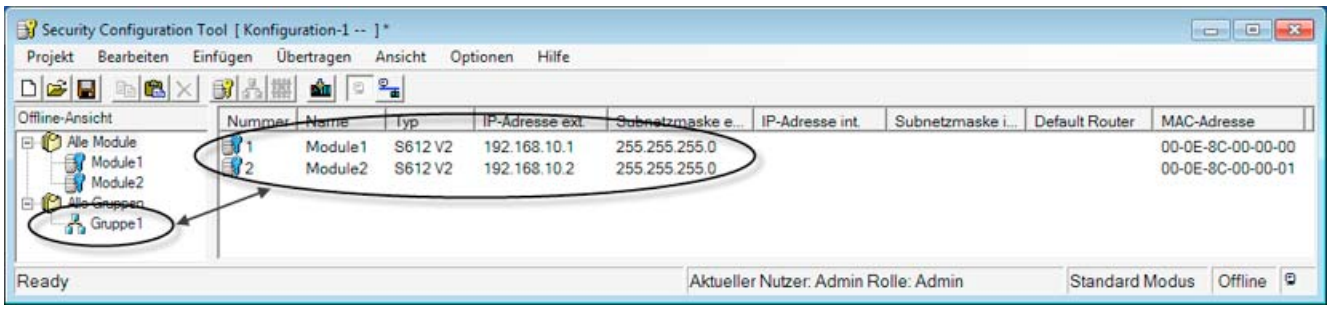
SCALANCE S verwendet für die Tunnelung das IPsec-Protokoll (Tunnelmodus von IPsec).



Tunnelverbindungen bestehen zwischen Modulen der gleichen Gruppe (VPN)

Die Eigenschaften eines VPN werden bei SCALANCE S innerhalb einer Modul-Gruppe für alle IPsec Tunnel zusammengefasst.

IPsec-Tunnel werden automatisch zwischen allen SCALANCE S-Modulen und SOFTNET Security Client-Modulen aufgebaut, die der selben Gruppe angehören.



SCALANCE S-Module können in einem Projekt parallel mehreren verschieden Gruppen angehören.

ACHTUNG

Wird der Name eines SCALANCE S-Moduls geändert, dann müssen alle SCALANCE S-Module derjenigen Gruppen, denen das geänderte SCALANCE S-Modul angehört, neu konfiguriert werden (Menübefehl **Übertragen ▸ An alle Module...)**.

Wird der Name einer Gruppe geändert, dann müssen alle SCALANCE S-Module dieser Gruppe neu konfiguriert werden (Menübefehl **Übertragen ▸ An alle Module...)**.

ACHTUNG

Layer-2-Telegramme werden nur getunnelt, wenn sich zwischen zwei SCALANCE S-Modulen kein Router befindet.

Allgemein gilt: Non-IP-Telegramme werden nur dann durch einen Tunnel übertragen, wenn die Geräte, die die Telegramme senden bzw. empfangen, auch schon vorher, d.h. ohne den Einsatz der SCALANCE S, kommunizieren konnten.

Ob die Netzknoten vor dem Einsatz der SCALANCE S kommunizieren konnten oder nicht wird anhand der IP-Netze bestimmt, in denen sich die SCALANCE S-Geräte befinden. Sind die SCALANCE S im gleichen IP-Subnetz, so wird davon ausgegangen, dass die Endgeräte in den gesicherten Netzen der SCALANCE S auch vor dem Einsatz der SCALANCE S mit Non-IP-Telegrammen kommunizieren konnten. Die Non-IP-Telegramme werden dann getunnelt.

Authentifizierungsmethode

Die Authentifizierungsmethode wird innerhalb einer Gruppe (eines VPNs) festgelegt und bestimmt die Art der verwendeten Authentifizierung.

Es werden schlüsselbasierende oder zertifikatsbasierende Authentifizierungsmethoden unterstützt:

- Preshared Keys

  Der Preshared Key wird an alle in der Gruppe befindlichen Module verteilt.

  Hierzu geben Sie im Dialog "Gruppeneigenschaften" im Feld "Preshared Key" zuvor ein Passwort ein.

- Zertifikat

  Die zertifikat-basierte Authentifizierung "Certificate" ist die Defaulteinstellung, die auch im Standard-Modus eingeschaltet ist. Das Verhalten ist wie folgt:

  – Beim Anlegen einer Gruppe wird automatisch ein Gruppenzertifikat erzeugt (Gruppenzertifikat = CA-Zertifikat).

  – Jedes SCALANCE S, das in der Gruppe ist, erhält ein Zertifikat, das mit dem Schlüssel der Gruppen-CA signiert ist.

  Sämtliche Zertifikate basieren auf dem ITU-Standard X.509v3 (ITU, International Telecommunications Union).

  Die Zertifikate werden von einer im Security Configuration Tool enthaltenen Zertifizierungsstelle erzeugt.

ACHTUNG
Einschränkung bei VLAN-Betrieb Innerhalb eines mit SCALANCE S aufgebauten VPN-Tunnel wird kein VLAN-Tagging übertragen. Begründung: Die in den Telegrammen enthaltenen VLAN-Kennzeichnungen (VLAN-Tags) gehen bei den Unicast-Telegrammen beim Passieren der SCALANCE S verloren, da für die Übertragung der IP-Telegramme IPsec verwendet wird. In einen IPSec-Tunnel werden nur IP-Telegramme (keine Ethernet-Pakete) übertragen, daher geht das VLAN-Tagging verloren. Standardmäßig können mit IPsec keine Broadcast- bzw. Mulitcast-Telegramme übertragen werden. Beim SCALANCE S werden IP-Broadcast genau wie MAC-Pakete in UDP "verpackt" und übertragen und zwar inklusive Ethernet-Header. Daher bleibt bei diesen Paketen auch das VLAN-Tagging erhalten.

6.2 Gruppen

6.2.1 Gruppen anlegen und Module zuordnen

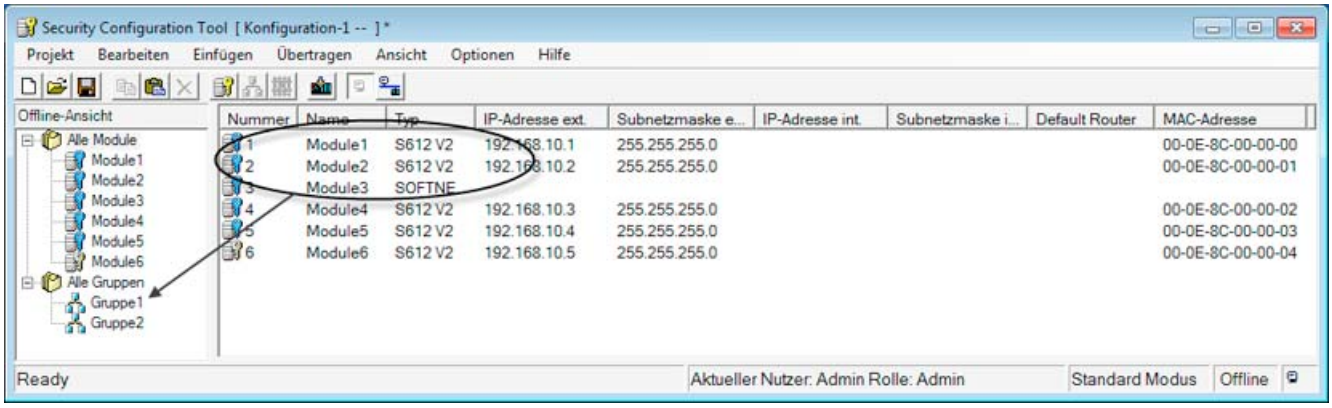
Gehen Sie so vor, um ein VPN zu konfigurieren

Legen Sie über den Menübefehl

Einfügen ▸ Gruppe

eine Gruppe an.

Ordnen Sie der Gruppe die SCALANCE S-Module und SOFTNET Security Client-Module zu, die zu einem internen Netz gehören sollen. Ziehen Sie hierzu mit der Maus das Modul auf die gewünschte Gruppe (Drag and Drop).



Eigenschaften projektieren

Wie bei der Konfiguration von Modulen wirken sich auch bei der Konfiguration von Gruppen die beiden wählbaren Bedienungssichten im Security Configuration Tool aus :

(Menübefehl **Ansicht ▸ Erweitert-Modus**)

- **Standard-Modus**

  Im Standard-Modus belassen Sie es bei den vom System vergebenen Voreinstellungen. Auch als Nicht-IT-Experten können Sie so IPsec-Tunnel konfigurieren und eine sichere Datenkommunikation in Ihren internen Netzen betreiben.

- **Erweitert-Modus**

  Der Erweitert-Modus bietet Ihnen Einstellmöglichkeiten zur spezifischen Konfiguration der Tunnel-Kommunikation.

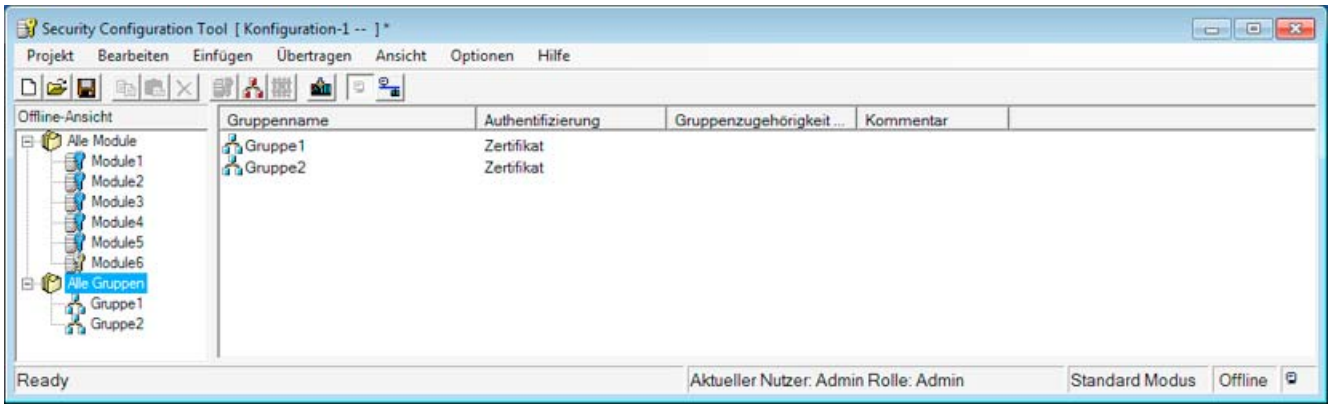
Hinweis

Parametrierung von MD 740 / MD 741 bzw. anderer VPN-Clients

Zur Parametrierung von MD 740 / MD 741 bzw. anderer VPN-Clients müssen sie modulspezifische VPN-Eigenschaften im Erweitert-Modus konfigurieren.

Alle projektierten Gruppen mit ihren Eigenschaften anzeigen

Selektieren Sie im Navigationsbereich "Alle Gruppen"



Folgende Eigenschaften der Gruppen werden spaltenweise angezeigt:

Tabelle 6- 1 Gruppen-Eigenschaften

Eigenschaft/Spalte	Bedeutung	Kommentar/Auswahl
Gruppenname	Gruppenname	frei wählbar
Authentifizierung	Authentifizierungstyp	• Preshared Key • Zertifikat
Gruppenzugehörigkeit bis...	Lebensdauer von Zertifikaten	siehe unten
Kommentar	Kommentar	frei wählbar

Lebensdauer von Zertifikaten einstellen

Öffnen Sie den Dialog, in dem Sie das Ablaufdatum des Zertifikats eingeben können, wie folgt:

- mit Doppelklick auf ein Modul im Eigenschaftsfenster oder über die rechte Maustaste mittels Menübefehl **Eigenschaften**.

ACHTUNG
Nach Ablauf des Zertifikats wird die Kommunikation durch den Tunnel beendet.

6.2.2 Modultypen innerhalb einer Gruppe

Modultypen

Die folgenden Modultypen sind mit dem Security Configuration Tool in Gruppen projektierbar:

- SCALANCE S612
- SCALANCE S613
- SOFTNET Security Client
- MD 74x (steht für MD740-1 oder MD741-1)

Regeln für die Gruppenbildung

Beachten Sie die folgenden Regeln, wenn Sie VPN-Gruppen bilden wollen:

- Das erste in einer VPN-Gruppe zugeordnete Modul bestimmt, welche zusätzlichen Module hinzugefügt werden dürfen.

  Ist das erste hinzugefügte Gerät im Routing-Modus, so können zusätzlich nur Module mit aktiviertem Routing hinzugefügt werden. Ist das erste Gerät im Bridge-Modus, so dürfen zusätzlich nur Module im Bridge-Modus hinzugefügt werden. Soll der "Modus" einer VPN-Gruppe geändert werden, so müssen alle in der Gruppe enthaltenen Module entfernt und neu hinzugefügt werden.

- Es ist nicht möglich, ein MD 740-1/MD 741-1-Modul einer VPN-Gruppe hinzuzufügen, die ein Modul im Bridge-Modus enthält.

Entnehmen Sie der folgenden Tabelle, welche Module zusammen in einer VPN-Gruppe zusammengefasst werden können:

Modul	Modul-Betriebsart …	
	… im Bridge Modus	… im Routing-Modus
S612 V1	x	-
S612 V2 *)	x	x
S613 V1	x	-
S613 V2 *)	x	x
SOFTNET Security Client 2005	x	-
SOFTNET Security Client 2008	x	x
SOFTNET Security Client V3.0	x	x
MD 74x	-	x

6.3 Tunnelkonfiguration im Standard-Modus

Gruppeneigenschaften

Im Standard-Modus gelten folgende Eigenschaften:

- Alle Parameter der IPsec-Tunnel und die Authentifizierungsmethode sind fest vorgegeben.

  Im Eigenschaftendialog für die Gruppe können Sie die eingestellten Standardwerte anzeigen.

- Der Lernmodus ist für alle Module aktiviert.

Dialog zur Anzeige der Standardwerte öffnen

Wählen Sie bei angewählter Gruppe folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften...

Die Anzeige ist identisch zum Dialog im Erweitert-Modus; die Werte sind jedoch nicht änderbar.

6.4 Tunnel-Konfiguration im Erweitert-Modus

Der Erweitert-Modus bietet Ihnen Einstellmöglichkeiten zur spezifischen Konfiguration der Tunnelkommunikation.

In den Erweitert-Modus umschalten

Schalten Sie für alle in diesem Kapitel beschriebenen Funktionen über folgenden Menübefehl die Betriebsart um:

Ansicht ▸ Erweitert-Modus

Hinweis

Sie können eine einmal vorgenommene Umschaltung in den Erweitert-Modus für das aktuelle Projekt nicht mehr rückgängig machen.

Es sei denn, Sie verlassen das Projekt ohne zu speichern und öffnen es erneut.

6.4.1 Gruppeneigenschaften projektieren

Gruppeneigenschaften

In der Bedienungssicht "Erweitert-Modus" sind folgende Gruppeneigenschaften einstellbar:

- Authentifizierungsmethode
- IKE-Einstellungen (Dialogbereich: Erweiterte Einstellungen Phase 1)
- IPsec-Einstellungen (Dialogbereich: Erweiterte Einstellungen Phase 2)

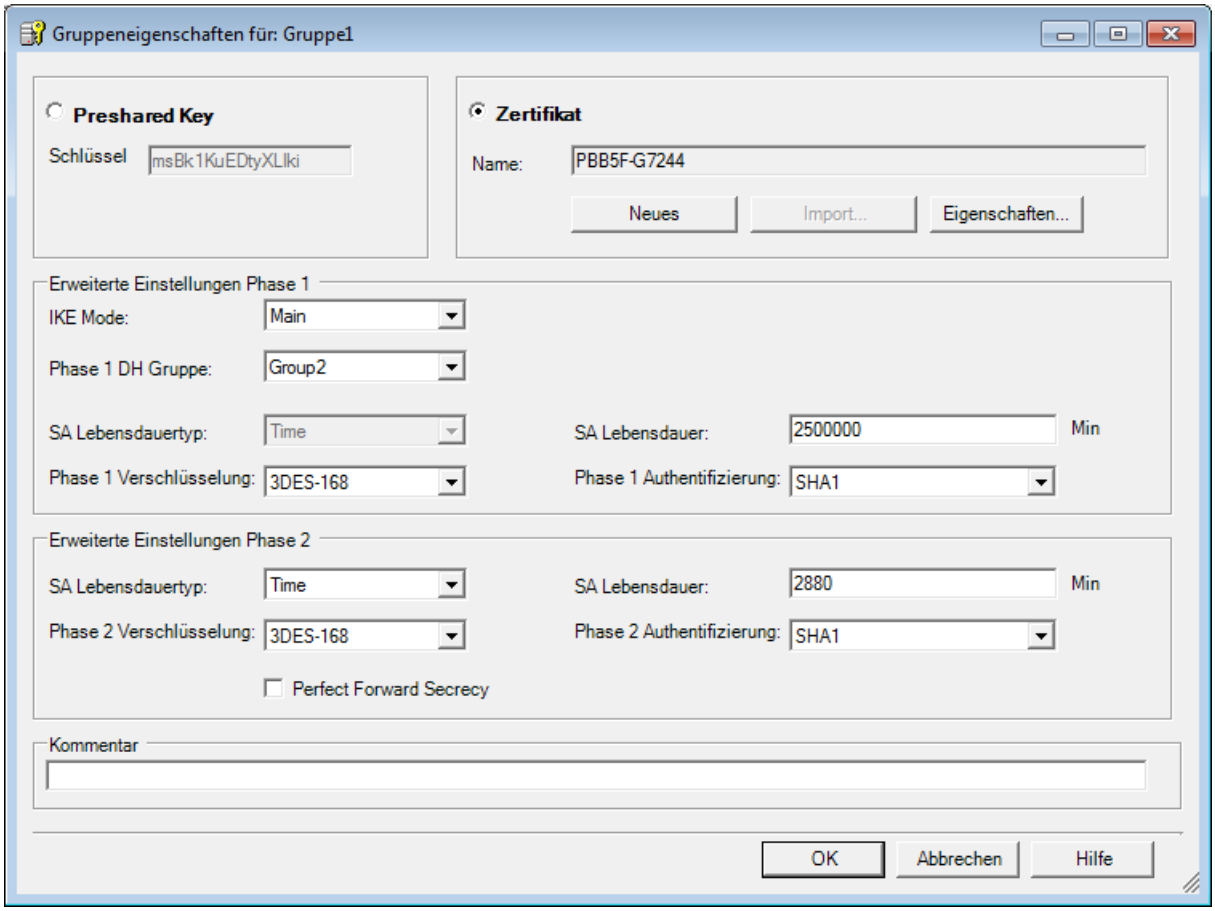
ACHTUNG
Um diese Parameter einstellen zu können, benötigen Sie IPsec-Kenntnisse.

Wenn Sie keine Einstellungen vornehmen bzw. verändern, gelten die Defaulteinstellungen des Standard-Modus.

Dialog zur Eingabe der Gruppeneigenschaften öffnen

- Betätigen Sie bei angewählter Gruppe folgenden Menübefehl:

  Bearbeiten ▸ Eigenschaften...



Parameter für erweiterte Einstellungen Phase 1 - IKE-Einstellungen

Phase 1: Schlüsselaustausch (IKE, Internet Key Exchange):

Hier können Sie Parameter für das Protokoll des IPsec-Schlüsselmanagements einstellen. Der Schlüsselaustausch erfolgt über das standardisierte Verfahren IKE.

Folgende IKE-Protokollparameter können Sie einstellen,

Tabelle 6- 2 IKE-Protokollparameter (Parametergruppe "Erweiterte Einstellungen Phase 1'" im Dialog)

Parameter	Werte/Auswahl	Kommentar
IKE Mode	• Main Mode • Aggressive Mode	Schlüsselaustauschverfahren Der Unterschied zwischen Main- und Aggressive Mode ist die "Identity-Protection", die im Main-Mode verwendet wird. Die Identität wird im Main-Mode verschlüsselt übertragen, im Aggressive-Mode nicht.
Phase 1 DH Gruppe Phase 1 DH Group	• Group 1 • Group 2 • Group 5	Diffie-Hellman-Schlüsselvereinbarung: Diffie-Hellman-Gruppen (wählbare kryptographische Algorithmen im Oakley-Schlüsselaustausch-Protokoll)
SA Lebensdauertyp SA Lifetype	• Time	Phase 1 Security Association (SA) • Zeitbegrenzung (Min., Default: 2500000) Die Nutzdauer für das aktuelle Schlüsselmaterial wird zeitlich begrenzt. Nach Ablauf der Zeit wird das Schlüsselmaterial neu ausgehandelt.
SA Lebensdauer SA Life	Numerischer Wert	("Time"→Min.,) Wertebereich: 1440...2 500 000
Phase 1 Verschlüsselung Phase 1 Encryption	• DES • 3DES-168 • AES-128 • AES-192 • AES-256	Verschlüsselungs-Algorithmus • Data Encryption Standard (56 Bit Schlüssellänge, Modus CBC) • Dreifach-DES (168 Bit Schlüssellänge, Modus CBC) • Advanced Encryption Standard (128 Bit, 192 Bit oder 256 Bit Schlüssellänge, Modus CBC)
Phase 1 Authentifizierung Phase 1 Authentication	• MD5 • SHA1	Authentisierungs-Algorithmus • Message Digest Version 5 • Secure Hash Algorithm 1

Parameter für erweiterte Einstellungen Phase 2 - IPsec-Einstellungen

Phase 2: Datenaustausch (ESP, Encapsulating Security Payload)

Hier können Sie Parameter für das Protokoll des IPsec-Datenaustauschs einstellen. Der Datenaustausch erfolgt über das standardisierte Sicherheitsprotokoll ESP.

Folgende ESP-Protokollparameter können Sie einstellen:

Tabelle 6- 3 IPsec-Protokollparameter (Parametergruppe "Erweiterte Einstellungen Phase 2'" im Dialog)

Parameter	Werte/Auswahl	Kommentar
SA Lebensdauertyp SA Lifetype	• Time	Phase 2 Security Association (SA) • Zeitbegrenzung (Min., Default: 2880) Die Nutzdauer für das aktuelle Schlüsselmaterial wird zeitlich begrenzt. Nach Ablauf der Zeit wird das Schlüsselmaterial neu ausgehandelt.
	• Limit	• Datenvolumen begrenzt (mByte, Default 4000)
SA Lebensdauer SA Life	Numerischer Wert	("Time"→Min., "Limit" → mByte) Wertebereich (Time): 1440...16 666 666 Wertebereich(Limit): 2000...500 000
Phase 2 Verschlüsselung Phase 2 Encryption	• 3DES-168 • DES • AES-128	Verschlüsselungs-Algorithmus • spezieller Dreifach-DES (168 Bit Schlüssellänge, Modus CBC) • Data Encryption Standard (56 Bit Schlüssellänge, Modus CBC) • Advanced Encrypting Standard (128 Bit Schlüssellänge, Modus CBC)
Phase 2 Authentifizierung Phase 2 Authentication	• MD5 • SHA1	Authentisierungs-Algorithmus • Message Digest Version 5 • Secure Hash Algorithm 1
Perfect Forward Secrecy	• On • Off	Vor jedem neuen Aushandeln einer IPsec-SA erfolgt ein erneutes Aushandeln der Schlüssel mit Hilfe des Diffie-Hellman-Verfahrens.

6.4.2 SCALANCE S in konfigurierte Gruppe aufnehmen

Die projektierten Gruppeneigenschaften werden für SCALANCE S, die neu in eine bestehende Gruppe aufgenommen werden, übernommen.

So gehen Sie vor

Je nachdem, ob Sie an den Gruppeneigenschaften etwas geändert haben oder nicht, müssen Sie beim Vorgehen unterscheiden:

- **Fall a:** Wenn Sie die Gruppeneigenschaften nicht geändert haben

1. Fügen Sie die neuen SCALANCE S der Gruppe hinzu.
2. Laden Sie die Konfiguration in die neuen Module.

- **Fall b:** Wenn Sie die Gruppeneigenschaften geändert haben

1. Fügen Sie die neuen SCALANCE S der Gruppe hinzu.
2. Laden Sie die Konfiguration in alle Module, die zur Gruppe gehören.

Vorteil

Bereits vorhandene, in Betrieb genommene SCALANCE S müssen nicht neu projektiert und geladen werden. Es resultiert keine Beeinflussung oder Unterbrechung der laufenden Kommunikation.

6.4.3 SOFTNET Security Client

Kompatible Einstellungen für SOFTNET Security Client

Beachten Sie bitte folgende Besonderheiten, wenn Sie in der projektierten Gruppe Module vom Typ SOFTNET Security Client einbeziehen:

Parameter	Einstellung / Besonderheit
Phase 1 DH Gruppe Phase 1 DH Group	DH Group1 und 5 kann nur für die Kommunikation zwischen den SCALANCE S-Modulen verwendet werden.
Phase 1 Verschlüsselung Phase 1 Encryption	Kein DES, AES-128 und AES-192 möglich.
Phase 1 Authentifizierung Phase 1 Authentication	Kein MD5 möglich.
Phase 1 SA Lebensdauer Phase 1 SA Lifetime	Wertebereich: 1440...2879 (nur SOFTNET Security Client V3.0)
SA Lebensdauertyp SA Lifetype	Muss für beide Phasen identisch gewählt werden.
Phase 2 Verschlüsselung Phase 2 Encryption	Kein AES-128 möglich.
Phase 2 SA Lebensdauer Phase 2 SA Lifetime	Wertebereich: 1440...2879 (nur SOFTNET Security Client V3.0)
Phase 2 Authentifizierung Phase 2 Authentication	Kein MD5 möglich.

ACHTUNG

Die Einstellungen der Parameter für eine SOFTNET Security Client Konfiguration müssen den Default Proposals der SCALANCE S Module entsprechen, da sich ein SOFTNET Security Client meist im mobilen Einsatz befindet und seine IP-Adresse dynamisch bezieht, kann der SCALANCE S eine Verbindung nur über diese Default-Proposals zulassen.

Sorgen Sie also bitte dafür, dass Ihre Phase 1 Einstellungen einem der drei folgenden Vorschläge entspricht, um einen Tunnel mit einem SCALANCE S aufbauen zu können.

Verwenden Sie andere Einstellungen im Security Configuration Tool schlägt beim Versuch einer Ausleitung der Konfiguration der Konsistenzcheck an und Sie können Ihre Konfiguration für den SOFTNET Security Client nicht ausleiten, bis Sie die Einstellungen entsprechend angepasst haben.

Authentifizierung	IKE Mode	DH Gruppe	Verschlüsselung	Hash	Lebensdauer (Min)
Zertifikat	Mainmode	DH-Gruppe 2	3DES-168	SHA1	1440…2879
Preshared Key	Mainmode	DH-Gruppe 2	3DES-168	SHA1	1440…2879
Zertifikat	Mainmode	DH-Gruppe 2	AES256	SHA1	1440…2879

6.4.4 Modulspezifische VPN-Eigenschaften konfigurieren

Für den Datenaustausch über die IPsec-Tunnel im VPN können Sie folgende modulspezifische Eigenschaften konfigurieren:

- Dead-Peer-Detection
- Erlaubnis zur Initiierung des Verbindungsaufbaus
- Öffentliche IP-Adresse zur Kommunikation über Internet Gateways

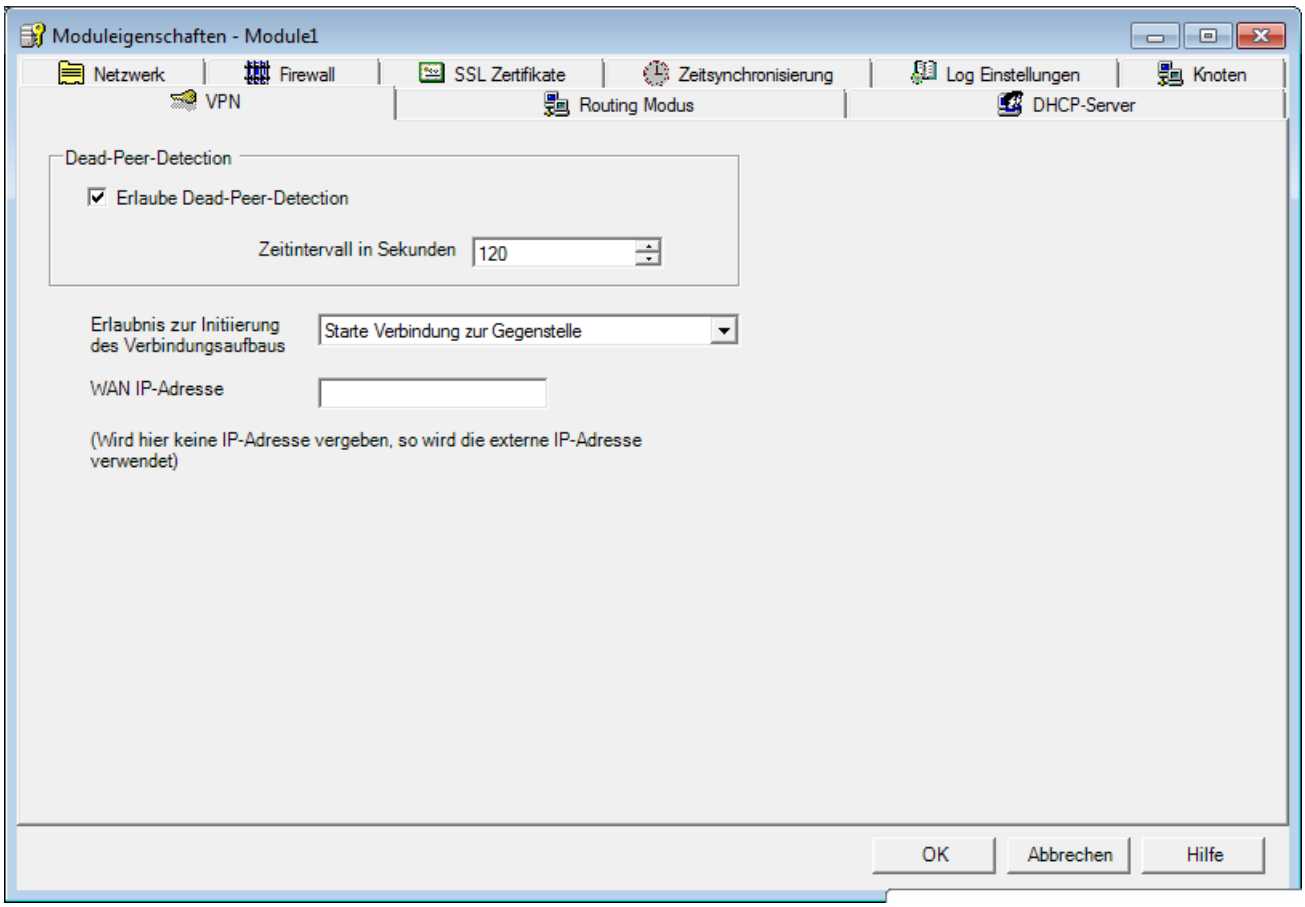
Dialog zur Konfiguration der VPN-Moduleigenschaften öffnen

Markieren Sie das zu bearbeitende Modul und wählen Sie im Erweitert-Modus folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften..., Register "VPN"

Hinweis

Das Register "VPN" ist nur dann wählbar, wenn sich das zu konfigurierende Modul in einer VPN-Gruppe befindet.



Dead-Peer-Detection (DPD)

Bei aktivierter DPD tauschen die Module in einstellbaren Zeitintervallen zusätzliche Nachrichten aus. Hierdurch kann erkannt werden, ob noch eine Verbindung im VPN besteht. Besteht diese nicht mehr, werden die "Security Associations" (SA) vorzeitig beendet. Bei deaktivierter DPD wird die "Security Association" (SA) erst nach Ablauf der SA-Lebensdauer (Einstellung der SA-Lebensdauer: siehe Konfiguration der Gruppeneigenschaften) beendet.

Standardmäßig ist DPD aktiviert.

Erlaubnis zur Initiierung des Verbindungsaufbaus

Sie können die Erlaubnis zur Initiierung des VPN Verbindungsaufbaus auf bestimmte Module im VPN beschränken.

Maßgebend für die Einstellung des hier beschriebenen Parameters ist die Vergabe der IP-Adresse für das Gateway des hier zu projektierenden Moduls. Bei einer statisch vergebenen IP-Adresse kann das Modul von der Gegenstelle gefunden werden. Bei dynamisch vergebener, und daher sich ständig ändernder IP-Adresse, kann die Gegenstelle nicht ohne weiteres eine Verbindung aufbauen.

Modus	Bedeutung
Starte Verbindung zur Gegenstelle (Standard)	Bei dieser Option ist das Modul "aktiv", d.h. es versucht eine Verbindung zur Gegenstelle herzustellen. Diese Option wird empfohlen, wenn Sie von Ihrem Provider für das Gateway des hier zu projektierenden SCALANCE S-Moduls eine dynamische IP-Adresse zugewiesen bekommen. Die Adressierung der Gegenstelle erfolgt über deren projektierte WAN IP-Adresse oder deren externe Modul IP-Adresse.
Warte auf Gegenstelle	Bei dieser Option ist das Modul "passiv", d.h. es wartet bis ein Verbindungsaufbau der Gegenstelle kommt. Diese Option wird empfohlen, wenn Sie von Ihrem Provider für das Gateway des hier zu projektierenden Moduls eine statische IP-Adresse zugewiesen bekommen. Sie erreichen dadurch, dass Verbindungsaufbauversuche nur durch die Gegenstelle erfolgen.

ACHTUNG
Stellen Sie nicht alle Module einer VPN-Gruppe auf "Warte auf Gegenstelle", da sonst keine Verbindung aufgebaut wird.

WAN IP-Adresse - IP-Adressen der Module und Gateways bei einem VPN über Internet

Beim Betrieb eines VPN mit IPsec-Tunnel über das Internet sind in der Regel zusätzliche IP-Adressen für die Internet Gateways wie beispielsweise DSL-Router erforderlich. Den einzelnen SCALANCE S-Modulen oder MD 740-1 / MD 741-1-Modulen müssen die externen IP-Adressen der Partner-Module im VPN bekannt sein.

Hinweis

Wenn Sie einen DSL-Router als Internet Gateway nutzen, müssen an diesem mindestens die folgenden Ports freigeschaltet werden:

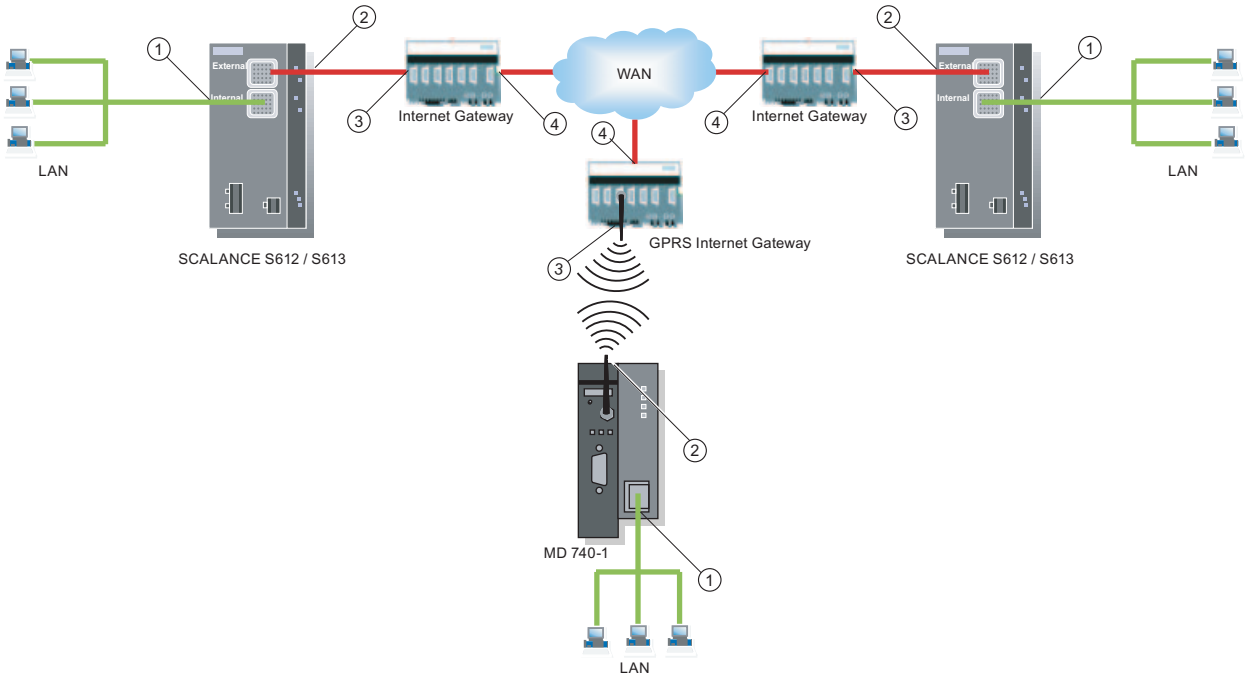
- Port 500 (ISAKMP)
- Port 4500 (NAT-T)

Bei Konfigurations-Downloads (über das WAN ohne aktiven Tunnel) muss zusätzlich der Port 443 (HTTPS) freigeschaltet werden.

Hierzu besteht die Möglichkeit, in der Konfiguration des Moduls diese externe IP-Adresse als "WAN IP-Adresse" zuzuordnen. Beim Laden der Modulkonfiguration werden den Modulen dann diese WAN IP-Adressen der Partner-Module mitgeteilt.

Wenn keine WAN IP-Adresse zugeordnet wird, wird die externe IP-Adresse des Moduls verwendet.

Die folgende Darstellung verdeutlicht den Zusammenhang der IP-Adressen.



① IP-Adresse intern - eines Moduls
② IP-Adresse extern - eines Moduls
③ IP-Adresse intern - eines Internet Gateways (z.B. GPRS-Gateway)
④ IP-Adresse extern (WAN IP-Adresse) - eines Internet Gateways (z.B. DSL-Router)

6.5 Interne Netzknoten konfigurieren

Um den Tunnelpartnern seine eigenen internen Knoten bekannt machen zu können muss ein SCALANCE S seine eigenen internen Knoten kennen. Zudem muss er auch die internen Knoten der SCALANCE S kennen mit denen er zusammen in einer Gruppe ist. Diese Information wird auf einem SCALANCE S dazu verwendet zu bestimmen, welches Datenpaket in welchem Tunnel übertragen werden soll.

SCALANCE S bietet in flachen Netzen die Möglichkeit, die Netzknoten automatisch zu erlernen oder statisch zu konfigurieren.

Im Routing-Modus werden komplette Subnetze getunnelt; dort ist das Lernen und die statische Konfiguration der Netzknoten nicht notwendig.

6.5.1 Arbeitsweise des Lernmodus

Teilnehmer für die Tunnelkommunikation automatisch finden (nur Bridge-Modus)

Ein großer Vorteil für die Konfiguration und den Betrieb der Tunnelkommunikation ist, dass SCALANCE S Teilnehmer in internen Netzen selbsttätig auffinden kann.

Neue Teilnehmer werden von SCALANCE S im laufenden Betrieb erkannt. Die erkannten Teilnehmer werden an die SCALANCE S Module, die zur selben Gruppe gehören, gemeldet. Dadurch ist der Datenaustausch innerhalb der Tunnel einer Gruppe jederzeit in beide Richtungen gewährleistet.

Voraussetzungen

Erkannt werden folgende Teilnehmer:

- IP-fähige Netzknoten

  IP-fähige Netzknoten werden gefunden, wenn Sie eine ICMP-Antwort auf den ICMP-Subnetz-Broadcast senden.

  IP-Knoten hinter Routern sind auffindbar, wenn die Router ICMP-Broadcasts weiterleiten.

- ISO-Netzknoten

  Netzknoten, die zwar nicht IP-fähig sind, jedoch über ISO-Protokolle ansprechbar sind, können ebenfalls gelernt werden.

  Voraussetzung ist, dass sie auf XID- bzw. TEST-Telegramme antworten. TEST und XID (Exchange Identification) sind Hilfsprotokolle zum Informationsaustausch auf der Layer 2-Ebene. Durch das Versenden dieser Telegramme mit einer Broadcast-Adresse können diese Netzknoten ausfindig gemacht werden.

- PROFINET-Knoten

  Mit Hilfe von DCP (Discovery and basic Configuration Protocol) werden PROFINET-Knoten gefunden.

Netzknoten, die diese Bedingungen nicht erfüllen, müssen Sie konfigurieren.

Subnetze

Konfiguriert werden müssen auch Subnetze, die sich hinter internen Routern befinden.

Lernmodus ein-/ausschalten

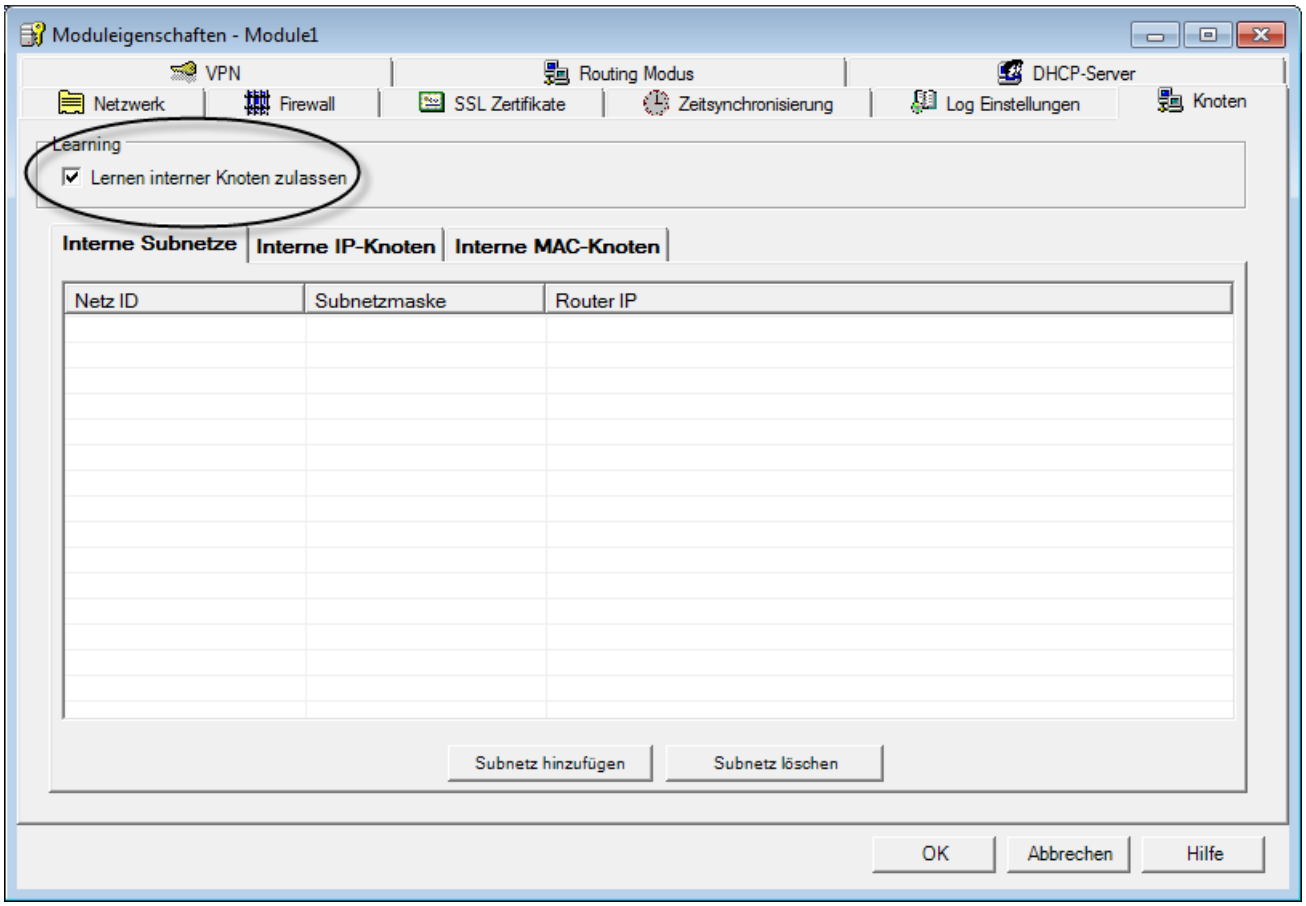
Die Lernfunktion ist in der Konfiguration durch die Projektierungssoftware Security Configuration Tool standardmäßig für jedes SCALANCE S-Modul eingeschaltet.

Das Lernen kann auch völlig abgeschaltet werden. Dann müssen Sie alle internen Knoten, die an der Tunnelkommunikation teilnehmen sollen, manuell konfigurieren.

Den Dialog, in dem Sie die Option wählen können, öffnen Sie wie folgt:

- Bei angewähltem Modul über den Menübefehl

  Bearbeiten ▸ Eigenschaften..., Register "Knoten".



Wann ist es sinnvoll, den automatischen Lernmodus auszuschalten?

Die Standardeinstellungen für SCALANCE S gehen davon aus, dass interne Netze stets "sicher" sind; das heißt auch, dass im Normalfall keine Netzknoten in das interne Netz zugeschaltet werden, die nicht vertrauenswürdig sind.

Das Ausschalten des Lernmodus kann sinnvoll sein, wenn das interne Netz statisch ist, d.h. wenn sich die Anzahl der internen Knoten und deren Adressen sich nicht ändern.

Mit Ausschalten des Lernmodus entfällt im internen Netz die Belastung des Mediums und der Knoten durch die Lerntelegramme. Auch SCALANCE S wird etwas leistungsfähiger, da er nicht durch die Bearbeitung der Lerntelegramme belastet wird.

Anmerkung: Im Lernmodus werden alle Knoten im internen Netz erfasst. Die Angaben zum Mengengerüst zu VPN beziehen sich nur auf die Knoten, die im internen Netz über VPN kommunizieren.

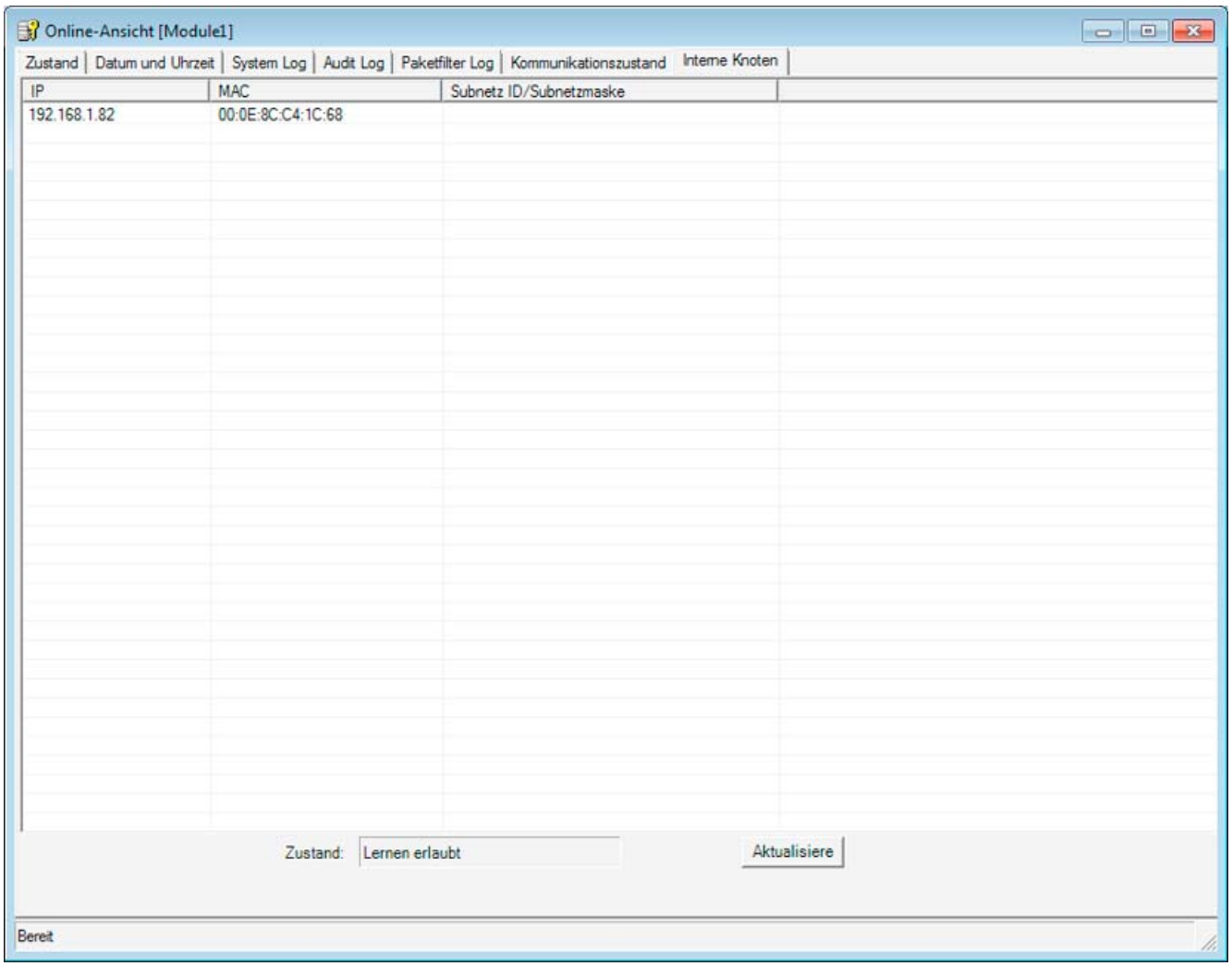
ACHTUNG
Werden im internen Netz mehr als 64 (bei SCALANCE S613) bzw. 32 (bei SCALANCE S612) interne Knoten betrieben, wird damit das zulässige Mengengerüst überschritten und ein nicht erlaubter Betriebszustand erzeugt. Aufgrund der Dynamik im Netzwerkverkehr kommt es dann dazu, dass interne Knoten, die bereits gelernt wurden, wieder durch neue, bis jetzt noch nicht bekannte interne Knoten ersetzt werden.

6.5.2 Anzeige der gefundenen internen Netzknoten

Alle gefundenen Netzknoten lassen sich in Security Configuration Tool, in der Betriebsart "Online", im Register "Internal Nodes" anzeigen.

Rufen Sie folgenden Menübefehl auf:

Bearbeiten ▸ Online Diagnose..



6.5.3 Netzknoten manuell konfigurieren

Nicht-lernbare Netzknoten

Es gibt Teilnehmer im internen Netz, die nicht gelernt werden können. Diese Teilnehmer müssen Sie konfigurieren. Hierzu müssen Sie im Security Configuration Tool den Erweitert-Modus einschalten.

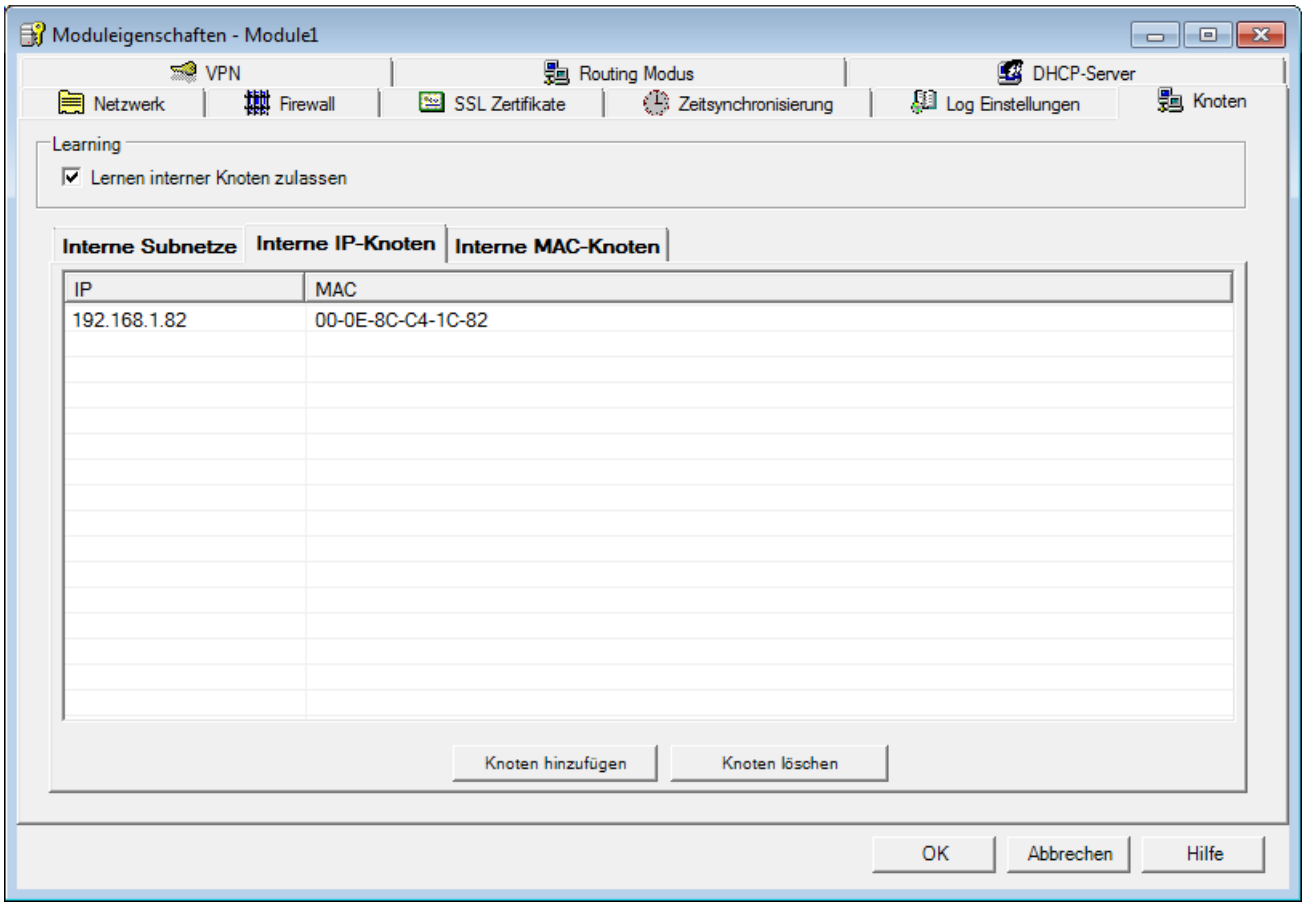
Sie müssen auch Subnetze konfigurieren, die sich im internen Netz des SCALANCE S befinden.

Dialog / Register

Den Dialog, in dem Sie die Netzknoten konfigurieren können, öffnen Sie wie folgt:

- Bei angewähltem Modul über den Menübefehl

  Bearbeiten ▸ Eigenschaften..., Register "Knoten".



Geben Sie in den hier wählbaren Registern die jeweils erforderlichen Adressparameter zu allen Netzknoten an, die vom gewählten SCALANCE S-Modul geschützt werden sollen.

Register "interne IP-Knoten" (nur im Bridge-Modus)

Projektierbare Parameter: IP-Adresse und optional die MAC Adresse;

Register "interne MAC-Knoten" (nur im Bridge-Modus)

Projektierbarer Parameter: MAC-Adresse

Register "Interne Subnetze"

Im Falle eines internen Subnetzes (ein Router im internen Netz) müssen Sie die folgenden Adressparameter angeben:

Parameter	Funktion	Beispiel-Wert
Netz ID	Netz-ID des Subnetzes: Anhand der Netz-ID erkennt der Router, ob eine Ziel-Adresse im Subnetz oder außerhalb liegt.	196.80.96.0
Subnetzmaske	Subnetzmaske: Die Subnetzmaske strukturiert das Netz und dient zur Bildung der Sub-Netz-ID.	255.255.255.0
Router IP	IP-Adresse des Routers	196.80.96.1

Auswirkung beim Einsatz des SOFTNET Security Client

Wenn Sie beim Einsatz von SCALANCE S612 / S613 Teilnehmer wie oben beschrieben statisch konfigurieren, müssen Sie auch die Konfiguration für einen in der VPN-Gruppe genutzten SOFTNET Security Client neu laden.

SOFTNET Security Client (S612 / S613) 7

Mit der PC-Software SOFTNET Security Client sind gesicherte Fernzugriffe vom PC/PG auf Automatisierungsgeräte, die durch SCALANCE S geschützt sind, über öffentliche Netze hinweg, möglich.

Wie Sie den SOFTNET Security Client im Security Configuration Tool projektieren und anschließend auf dem PC/PG in Betrieb nehmen, ist Gegenstand dieses Kapitels.

Weitere Informationen

Detailinformationen zu den Dialogen und den einstellbaren Parametern gibt Ihnen auch die Online-Hilfe des SOFTNET Security Client.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Siehe auch

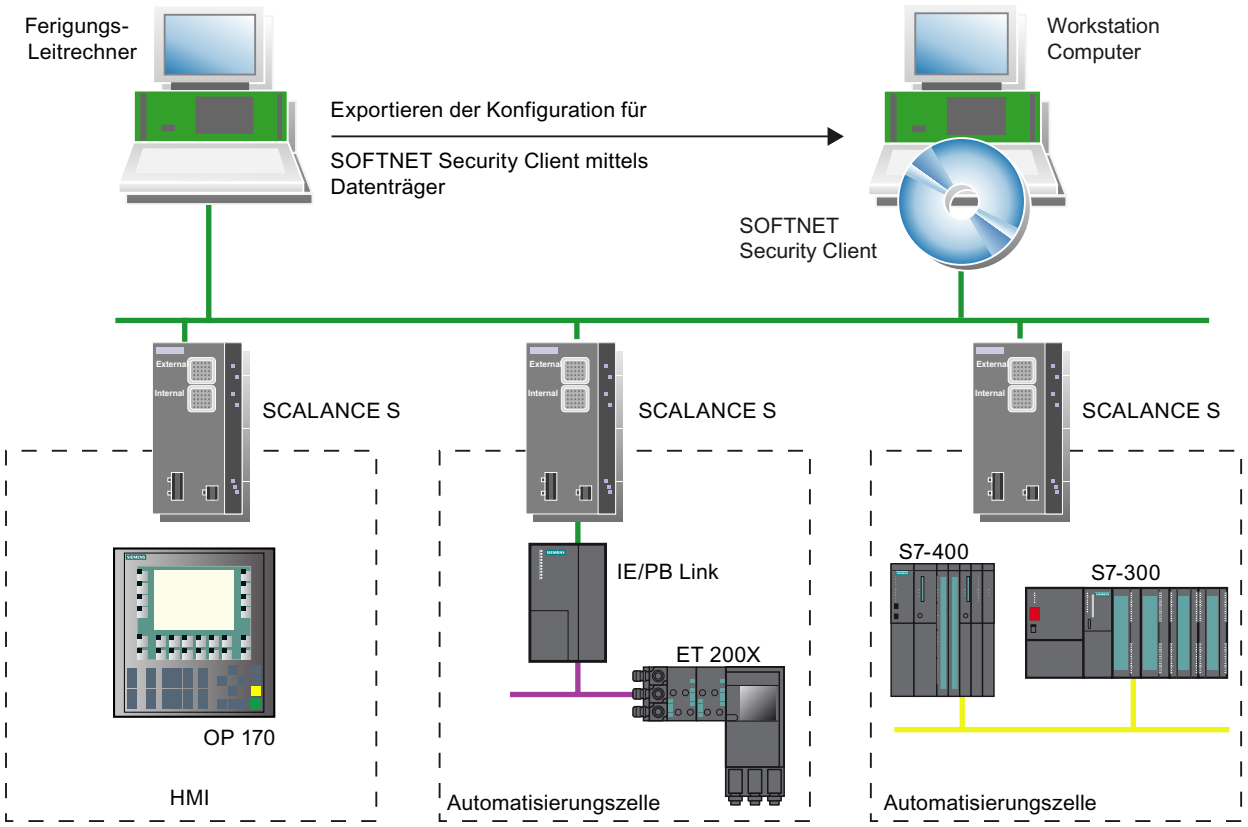
Gesicherte Kommunikation im VPN über IPsec-Tunnel (S612 / S613) (Seite 183)

7.1 Einsatz des SOFTNET Security Client

Einsatzbereich - Zugriff über VPN

Mittels des SOFTNET Security Client wird ein PC/PG automatisch so konfiguriert, dass er eine gesicherte IPsec Tunnelkommunikation im VPN (Virtual Private Network) zu einem oder mehreren SCALANCE S aufbauen kann.

PG/PC-Applikationen wie NCM Diagnose oder STEP7 können so über eine gesicherte Tunnelverbindung auf Geräte oder Netzwerke zuzugreifen, die sich in einem durch SCALANCE S geschützten internen Netz befinden.



Automatische Kommunikation über VPN

Wichtig für Ihre Anwendung ist, dass der SOFTNET Security Client selbsttätig erkennt, wenn ein Zugriff auf die IP-Adresse eines VPN-Teilnehmers erfolgt. Sie adressieren den Teilnehmer einfach so über die IP-Adresse, als würde sich dieser im lokalen Subnetz befinden, an dem auch der PC/PG mit der Applikation angeschlossen ist.

ACHTUNG
Beachten Sie bitte, dass über den IPsec-Tunnel nur IP-basierte Kommunikation zwischen SOFTNET Security Client und SCALANCE S erfolgen kann.

Bedienung

Die PC-Software SOFTNET Security Client besitzt eine einfach zu bedienende Oberfläche zur Konfiguration der Security Eigenschaften, welche zur Kommunikation mit durch SCALANCE S geschützten Geräten notwendig sind. Nach der Konfiguration läuft der SOFTNET Security Client im Hintergrund ab - sichtbar durch ein Ikon im SYSTRAY auf Ihrem PG/PC.

Details in der Online-Hilfe

Detaillierte Informationen zu den Dialogen und Eingabefeldern finden Sie auch in der Online-Hilfe der Bedienoberfläche des SOFTNET Security Client.

Sie erreichen die Online-Hilfe über die Schaltfläche "Hilfe" oder über die F1-Taste.

Wie funktioniert der SOFTNET Security Client ?

Der SOFTNET Security Client liest die vom Projektierwerkzeug Security Configuration Tool erstellte Konfiguration ein und ermittelt aus der Datei die zu importierenden Zertifikate.

Das Root-Certificate und die Private Keys werden importiert und im lokalen PG/PC abgelegt.

Anschließend werden mit den Daten aus der Konfiguration Security-Einstellungen vorgenommen, damit Applikationen auf IP-Adressen hinter SCALANCE-S Modulen zugreifen können.

Ist der Lernmodus für die internen Teilnehmer bzw. Automatisierungsgeräte aktiviert, stellt das Konfigurationsmodul zunächst eine Sicherheitsrichtlinie für den gesicherten Zugriff auf SCALANCE S-Module ein. Danach spricht SOFTNET Security Client die SCALANCE S-Module an um die IP-Adressen der jeweils internen Teilnehmer zu ermitteln.

SOFTNET Security Client trägt diese IP-Adressen in spezielle Filterlisten dieser Sicherheitsrichtlinie ein. Anschließend können Applikationen wie z.B. STEP 7 mit den Automatisierungsgeräten über VPN kommunizieren.

ACHTUNG
Auf einem Windows-System sind die IP-Sicherheitsrichtlinien benutzerspezifisch hinterlegt. Unter einem Benutzer kann jeweils nur eine IP-Sicherheitsrichtlinie gültig sein. Wenn eine vorhandene IP-Sicherheitsrichtlinie durch die Installation des SOFTNET Security Client nicht überschrieben werden soll, sollten Sie daher die Installation und Nutzung des SOFTNET Security Client unter einem eigens dafür eingerichteten Benutzer vornehmen.

Einsatzumgebung

Der SOFTNET Security Client ist für den Einsatz unter den Betriebssystemen Windows XP SP2 und SP3 (nicht "Home-Edition") und Windows 7 (nicht "Home-Edition") vorgesehen.

Verhalten bei Störungen

Bei auftretenden Störungen auf Ihrem PG/PC verhält sich SOFTNET Security Client wie folgt:

- Eingerichtete Sicherheitsrichtlinien bleiben über das Aus- und Einschalten Ihres PG/PC erhalten;
- Bei fehlerhafter Konfiguration werden Meldungen ausgegeben.

7.2 Installation und Inbetriebnahme des SOFTNET Security Client

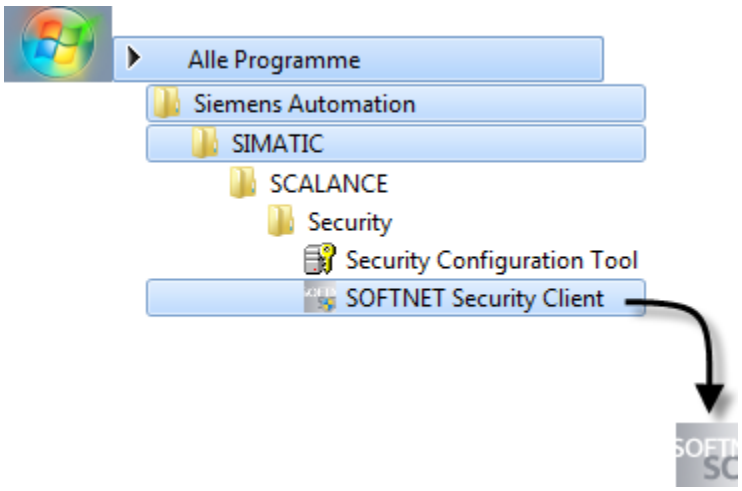
7.2.1 SOFTNET Security Client installieren und starten

Sie installieren die PC-Software SOFTNET Security Client von der SCALANCE S CD.

1. Lesen Sie zunächst die Angaben in der LIESMICH-Datei Ihrer SCALANCE S CD und beachten Sie ggf. zusätzliche Installationshinweise.
2. Führen Sie das Setup-Programm aus;

   Öffnen Sie hierzu am einfachsten die Inhaltsübersicht Ihrer SCALANCE S CD → wird beim CD-Einlegen automatisch gestartet oder kann über die Datei start.exe geöffnet werden. Wählen Sie dann direkt den Eintrag "Installation SOFTNET Security Client"

Nach der Installation und dem Start des SOFTNET Security Client erscheint das Ikon für den SOFTNET Security Client in der Windows Taskleiste:



SOFTNET Security Client einrichten

Einmal aktiviert, laufen die wichtigsten Funktionen im Hintergrund auf Ihrem PG/PC ab.

Die Projektierung des SOFTNET Security Client erfolgt in 2 Schritten:

- Exportieren einer Security-Konfiguration aus dem SCALANCE S Projektierwerkzeug Security Configuration Tool.
- Import der Security-Konfiguration in der eigenen Oberfläche, wie im nächsten Unterkapitel beschrieben.

Anlaufverhalten

Für eine maximale Projektierung benötigt der SOFTNET Security Client systembedingt bis zu 15 Minuten zum Laden der Sicherheitsregeln. Die CPU Ihres PG/PC wird in dieser Zeitspanne bis zu 100% ausgelastet.

SOFTNET Security Client beenden - Auswirkungen

Wird der SOFTNET Security Client beendet wird auch die Sicherheitsrichtlinie deaktiviert.

So können Sie den SOFTNET Security Client beenden:

- über den Menübefehl im SYSTRAY von Windows; wählen Sie mittels rechter Maustaste das Ikon des SOFTNET Security Client an und wählen Sie die Option "Beende SOFTNET Security Client".
- bei geöffneter Oberfläche über die Schaltfläche "Beenden".

7.2.2 SOFTNET Security Client deinstallieren

Bei der Deinstallation werden die vom SOFTNET Security Client eingestellten Security-Eigenschaften zurückgesetzt.

7.3 Konfigurationsdatei mit Projektierwerkzeug Security Configuration Tool erstellen

SOFTNET Security Client-Modul im Projekt konfigurieren

Der SOFTNET Security Client wird im Projekt als Modul angelegt. Im Gegensatz zu den SCALANCE S-Modulen sind keine weiteren Eigenschaften zu projektieren.

Sie weisen das SOFTNET Security Client-Modul lediglich der oder den Modul-Gruppen zu, in denen IPsec-Tunnel zum PC/PG eingerichtet werden sollen.

Maßgeblich sind dann die Gruppeneigenschaften, die Sie für diese Gruppen projektiert haben.

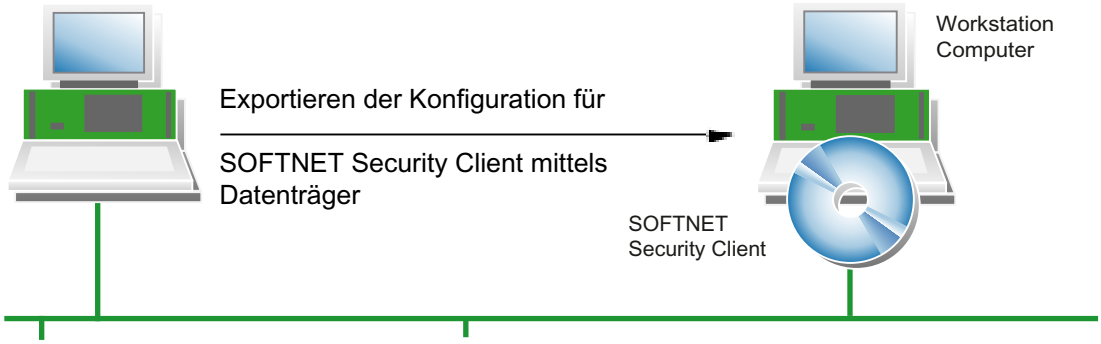
ACHTUNG
Beachten Sie bitte die Angaben zu den Parametern, die im Kapitel 6.4 im Abschnitt "Kompatible Einstellungen für SOFTNET Security Client" beschrieben werden.

Hinweis

Wenn Sie mehrere SOFTNET Security Clients innerhalb einer Gruppe anlegen, werden keine Tunnel zwischen diesen Clients aufgebaut, sondern nur vom jeweiligen Client zu den SCALANCE S-Modulen!

Konfigurationsdateien für den SOFTNET Security Client

Die Schnittstelle zwischen dem Projektierwerkzeug Security Configuration Tool und dem SOFTNET Security Client wird über Konfigurationsdateien bedient.



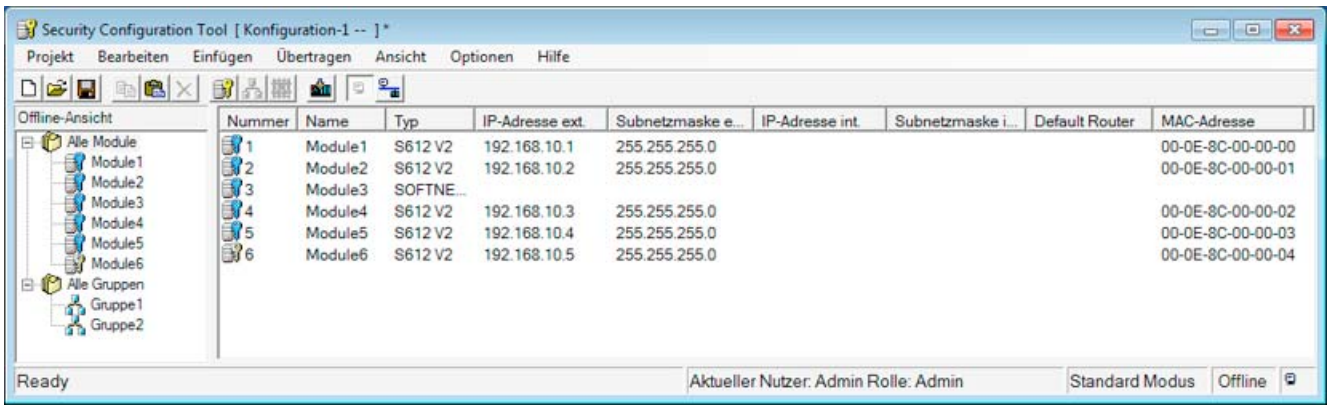
Die Konfiguration wird in folgenden 3 Dateitypen hinterlegt:

- *.dat
- *.p12
- *.cer

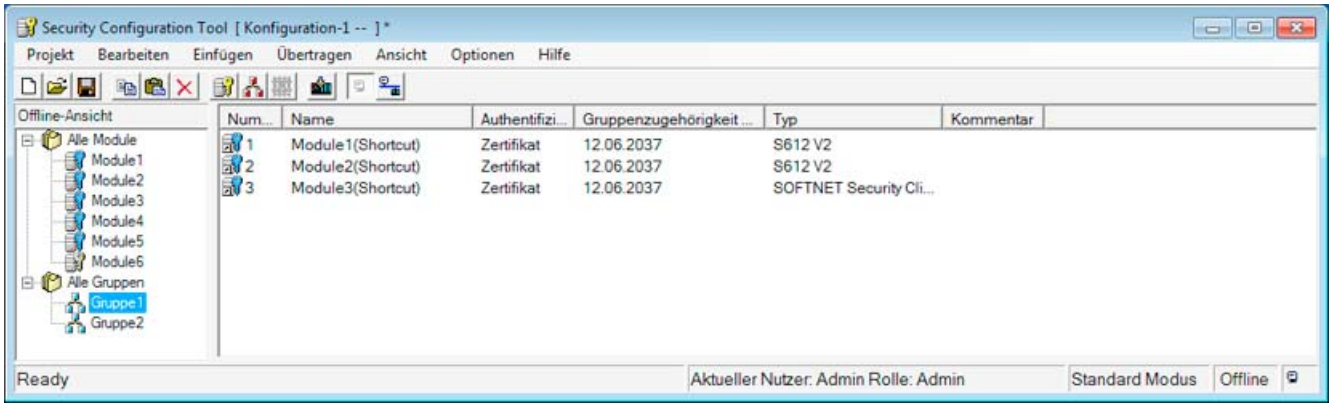
Vorgehensweise

Führen Sie im Projektierwerkzeug Security Configuration Tool folgende Schritte aus, um die Konfigurationsdateien zu erzeugen:

1. Legen Sie in Ihrem Projekt zunächst ein Modul vom Typ SOFTNET Security Client an.



2. Ordnen Sie das Modul den Modul-Gruppen zu, in denen der PC/PG über IPsec-Tunnel kommunizieren soll.



3. Wählen Sie den gewünschten SOFTNET Security Client mit der rechten Maustaste und wählen Sie folgenden Menübefehl:

   Übertragen ▸ An Modul...

4. Wählen Sie im aufgeblendeten Dialog den Speicherort für die Konfigurationsdatei.
5. Wenn Sie als Authentifizierungsmethode Zertifikat gewählt haben werden Sie im nächsten Schritt aufgefordert, ein Passwort für das Zertifikat der VPN-Konfiguration anzugeben. Sie haben hier die Möglichkeit, ein eigenes Passwort zu vergeben. Vergeben Sie kein Passwort wird der Projektname als Passwort übernommen.

   Die Eingabe des Passworts erfolgt wie üblich mit Wiederholung.

   Damit ist der Export der Konfigurationsdateien abgeschlossen.
6. Übernehmen Sie die Dateien vom Typ *.dat, *.p12, *.cer auf den PC/PG, auf dem Sie den SOFTNET Security Client betreiben möchten.

7.4 SOFTNET Security Client bedienen

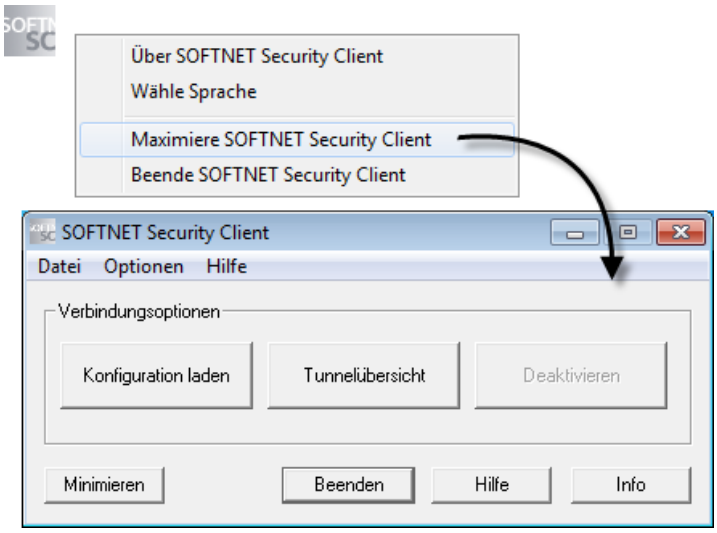
Konfigurierbare Eigenschaften

Im Einzelnen können Sie folgende Dienste nutzen:

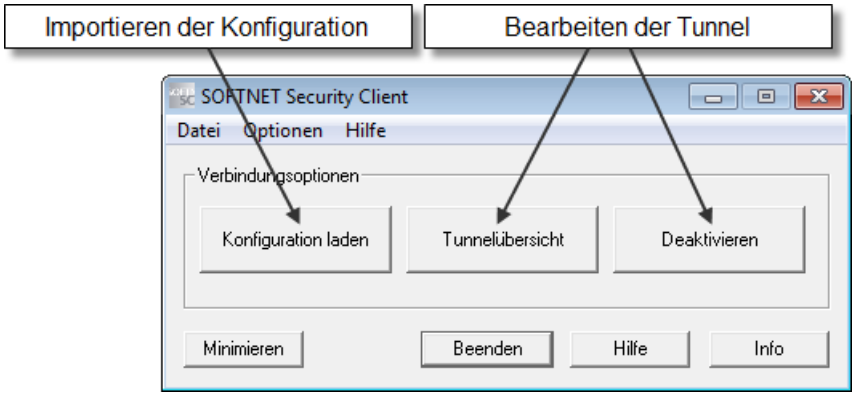
- Einrichten von sicherer IPsec-Tunnelkommunikation (VPN) zwischen dem PC/PG und allen SCALANCE S-Modulen eines Projektes oder einzelnen SCALANCE S-Modulen. Über diese IPsec-Tunnel kann der PC/PG auf die internen Knoten des VPN zugreifen.
- Aus- und Einschalten von bereits eingerichteten sicheren Verbindungen;
- Verbindungen einrichten bei nachträglich hinzugefügten Endgeräten; (hierzu muss der Lernmodus aktiviert sein)
- Überprüfen einer Konfiguration, d.h. welche Verbindungen sind eingerichtet oder möglich.

So rufen Sie SOFTNET Security Client für die Konfiguration auf

Öffnen Sie die Bedienoberfläche des SOFTNET Security Client, indem Sie auf das Ikon im SYSTRAY doppelklicken oder über die rechte Maustaste den Menüpunkt "Öffne SOFTNET Security Client" wählen:



Über die Schaltflächen erreichen Sie folgende Funktionen:



Schaltfläche	Bedeutung
Konfigurationsdaten einlesen	Import der Konfiguration Sie öffnen hiermit einen Dateidialog für die Selektion einer Konfigurationsdatei. Nach dem Schließen des Dialogs wird die Konfiguration eingelesen und ein Passwort für jede Konfigurationsdatei abgefragt. Im Dialog wird abgefragt, ob die Tunnel für alle SCALANCE S sofort eingerichtet werden sollen. Falls in der Konfiguration IP-Adressen von SCALANCE S eingetragen sind oder der Lernmodus aktiv ist, werden die Tunnel für alle konfigurierten oder ermittelten Adressen eingerichtet. Diese Vorgehensweise ist besonders bei kleinen Konfigurationen schnell und effizient. Optional können Sie im Dialog für "Tunnelübersicht" alle Tunnel einrichten. Anmerkung: Sie können nacheinander die Konfigurationsdateien aus mehreren im Security Configuration Tool erstellten Projekten importieren (siehe auch nachfolgende Erläuterung zur Vorgehensweise).
Tunnelübersicht	Dialog für das Einrichten und Bearbeiten der Tunnel. Über diesen Dialog nehmen Sie die eigentliche Konfiguration des SOFTNET Security Client vor. In diesem Dialog finden Sie eine Liste für die eingerichteten gesicherten Tunnel vor. Dort können die IP-Adressen für die SCALANCE S Module angezeigt/geprüft werden. Falls auf Ihrem PG/PC mehrere Netzwerkadapter vorhanden sind wählt der SOFTNET Security Client automatisch einen aus über den ein Tunnelaufbau versucht wird. Gegebenenfalls konnte der SOFTNET Security Client jedoch keinen zu ihrem Teilnehmer passenden finden und hat einen beliebigen eingetragen. In diesem Fall müssen Sie die Netzwerkadaptereinstellung über den Dialog "Netzwerkadapter" im Kontextmenü der Teilnehmer und SCALANCE S-Module manuell anpassen
Deaktivieren	Alle gesicherten Tunnel deaktivieren. Anwendungsfall: Wenn die Konfiguration eines SCALANCE S612 / S613-Moduls geändert und neu geladen wird, sollten Sie den Tunnel zum SOFTNET Security Client deaktivieren. Der erneute Tunnelaufbau wird dadurch beschleunigt.
Minimieren	Die Bedienoberfläche des SOFTNET Security Client wird geschlossen. Das Ikon für den SOFTNET Security Client befindet sich weiterhin in der Windows Taskleiste.
Beenden	Konfiguration abbrechen; SOFTNET Security Client wird beendet; alle Tunnel werden deaktiviert.

Schaltfläche	Bedeutung
Hilfe	Online-Hilfe aufrufen.
Info	Informationen zum Ausgabestand des SOFTNET Security Client Details: Liste aller für die Funktion des SOFTNET Security Client benötigten Dateien mit Rückmeldung ob diese auf dem System gefunden werden konnten

7.5 Tunnel einrichten und bearbeiten

Einrichten von sicheren Verbindungen zu allen SCALANCE S

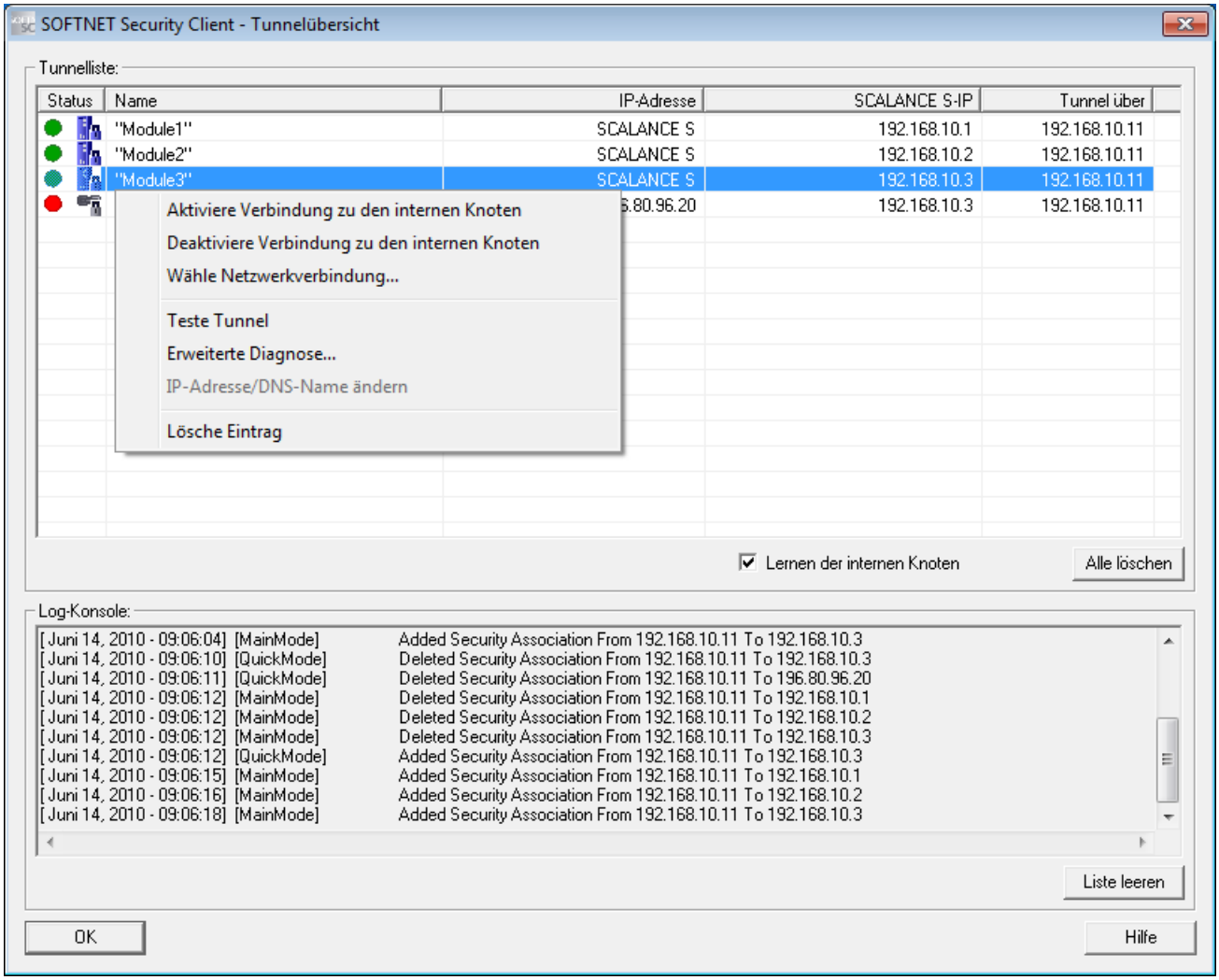
Im Dialog für den Konfigurationsimport können Sie wählen, ob die Tunnel für alle SCALANCE S sofort eingerichtet werden sollen. Dadurch ergeben sich die folgenden Möglichkeiten:

- Tunnel automatisch aktivieren

  Falls in der Konfiguration IP-Adressen von SCALANCE S eingetragen sind oder der Lernmodus aktiv ist, werden die Tunnel für alle konfigurierten oder ermittelten Adressen eingerichtet.

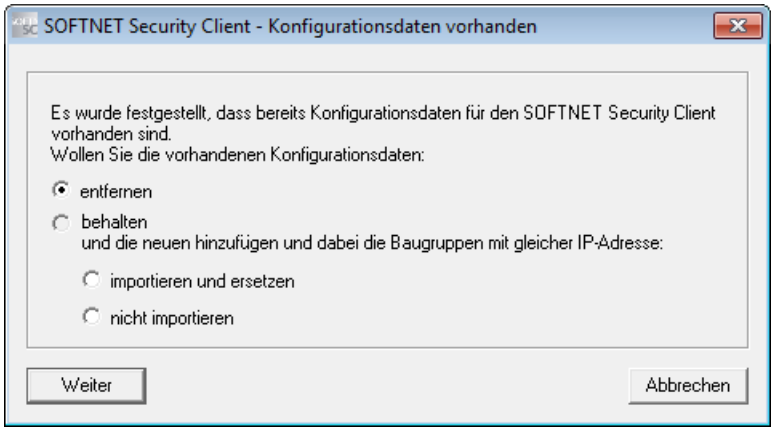
- Tunnelkonfiguration nur einlesen

  Optional können Sie die konfigurierten Tunnel nur einlesen und anschließend im Dialog für das Einrichten der Tunnel einzel aktivieren.



So richten Sie die Tunnelverbindungen ein

1. Öffnen Sie über die Schaltfläche "Konfigurationsdaten einlesen" den Dialog zum Import der Konfigurationsdatei.
2. Wählen Sie die mit dem Security Configuration Tool erstellte Konfigurationsdatei aus.
3. Falls im SOFTNET Security Client bereits Konfigurationsdaten vorliegen, werden Sie nun aufgefordert, über die Handhabung der neu zu übernehmenden Konfigurationsdaten zu entscheiden. Wählen Sie aus den angebotenen Optionen:



Hinweise zu diesem Dialog:

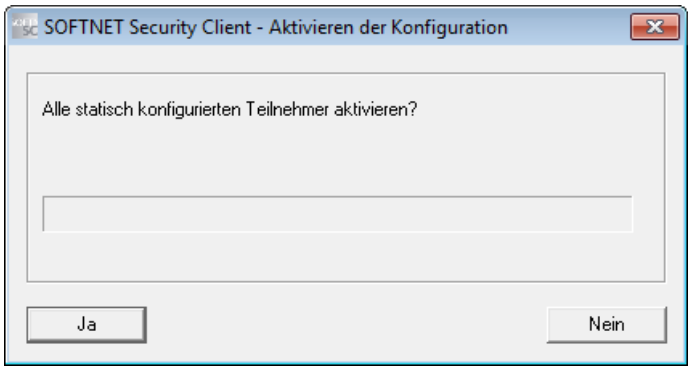
Grundsätzlich können die Konfigurationsdaten aus mehreren Projekten eingelesen werden. Mit diesem Dialog wird den Randbedingungen bei mehreren Projekten Rechnung getragen werden. Entsprechend haben die Optionen folgende **Auswirkung:**

- Bei "entfernen" sind nur noch die zuletzt geladenen Konfigurationsdaten vorhanden.
- Der zweite Auswahlpunkt "importieren und ersetzen" ist bei geänderten Konfigurationsdaten sinnvoll, beispielsweise nur die Konfiguration im Projekt a ist geändert, Projekt b und c bleiben erhalten.
- Der dritte Auswahlpunkt "nicht importieren" ist sinnvoll, wenn in einem Projekt ein Scalance S hinzugefügt wurde, ohne dass bereits gelernte interne Knoten verloren gehen.

4. Falls Sie bei der Konfiguration im Security Configuration Tool als Authentifizierungsmethode Zertifikat gewählt haben werden Sie nun aufgefordert Ihr Passwort einzugeben.

5. Wählen Sie nun aus, ob für die in der Konfiguration projektierten Teilnehmer (statisch konfigurierte Teilnehmer) die Tunnelverbindungen aktiviert werden sollen.

   Falls Sie die Aktivierung hier noch nicht anstoßen, können Sie dies jederzeit im nachfolgend beschriebenen Tunnel-Dialog durchführen.

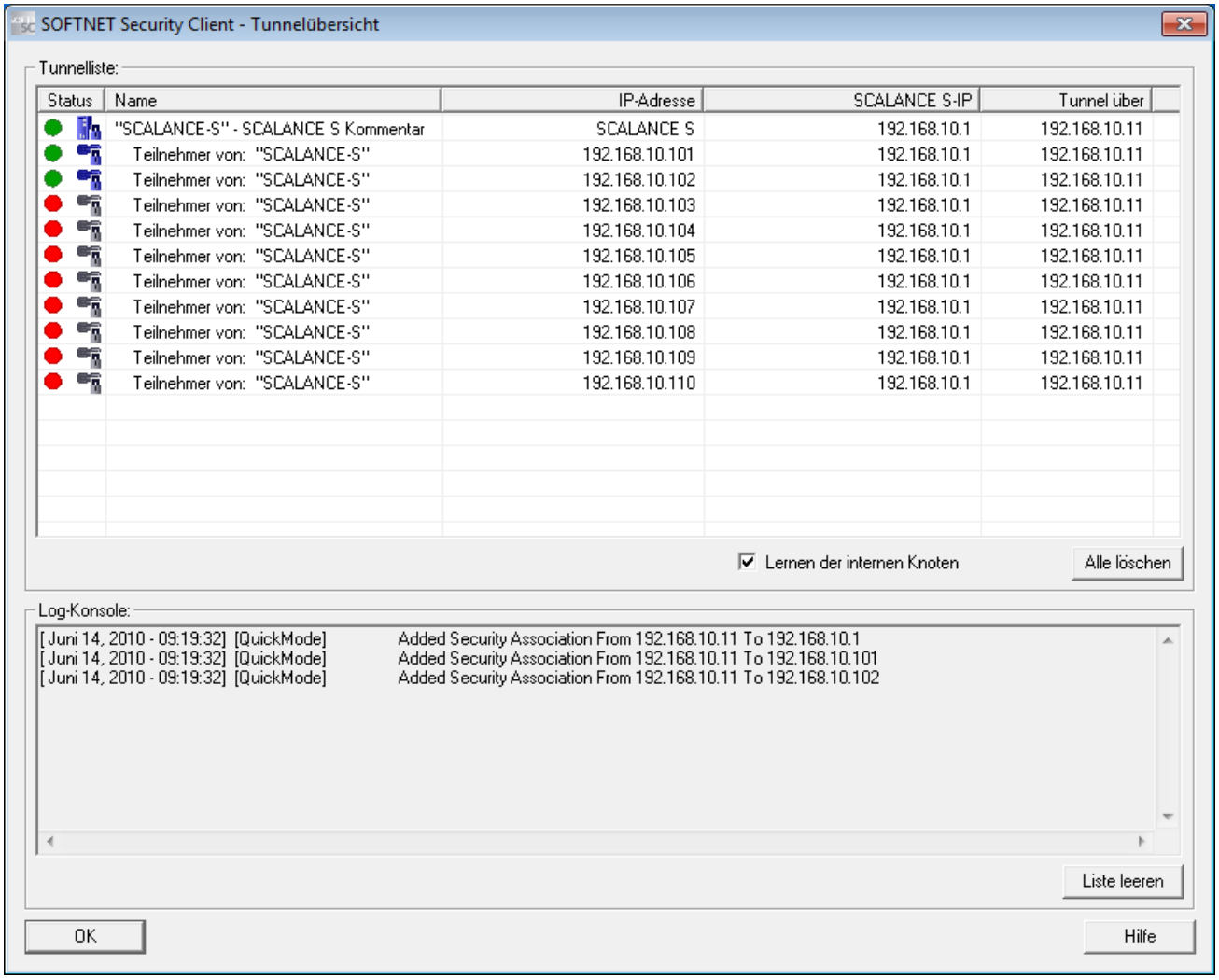


   Wenn Sie die Aktivierung der Tunnelverbindungen gewählt haben, werden nun die Tunnelverbindungen zwischen dem SOFTNET Security Client und den SCALANCE S-Modulen aufgebaut.

   Dies kann mehrere Sekunden dauern.

6. Öffnen Sie nun den Dialog "Tunnelübersicht".

   Sie sehen in der aufgeblendeten Tabelle die Module und Teilnehmer mit Statusinformationen über die Tunnelverbindungen.



7. Falls Sie nun feststellen, dass gewünschte Knoten bzw. Teilnehmer in der Tabelle nicht angezeigt werden, gehen Sie bitte so vor:

   Setzen Sie über die Kommandozeile ein PING-Kommando an den gewünschten Knoten ab.

   Sie veranlassen dadurch, dass der Knoten vom SCALANCE S gelernt wird und an den SOFTNET Security Client weitergegeben wird.

   Anmerkung:

   Falls der Dialog nicht geöffnet ist während ein Teilnehmer erfasst wird, wird der Dialog automatisch aufgeblendet.

   Hinweis

   Statisch konfigurierte Teilnehmer und Subnetze

   Wenn Sie beim Einsatz von SCALANCE S612 / S613 Teilnehmer oder Subnetze statisch konfigurieren, müssen Sie auch die Konfiguration für einen in der VPN-Gruppe genutzten SOFTNET Security Client neu laden.

8. Aktivieren Sie die Teilnehmer, bei denen die Statusanzeige anzeigt, dass noch keine Tunnelverbindung aufgebaut ist.

   Nach erfolgreichem Verbindungsaufbau können Sie nun Ihre Applikation - beispielsweise STEP 7 - starten und eine Kommunikationsverbindung zu einem der Teilnehmer aufbauen.

ACHTUNG
Falls auf Ihrem PG/PC mehrere Netzwerkadapter vorhanden sind wählt der SOFTNET Security Client automatisch einen aus über den ein Tunnelaufbau versucht wird. Gegebenenfalls konnte der SOFTNET Security Client jedoch keinen zu ihrem Projekt passenden finden und hat einen beliebigen eingetragen. In diesem Fall müssen Sie die Netzwerkadaptereinstellung über das Kontextmenü der Teilnehmer und SCALANCE S-Module manuell anpassen.

Bedeutung der Parameter

Tabelle 7- 1 Parameter im Dialogfeld "Tunnelübersicht"

Parameter	Bedeutung / Wertebereich
Status	mögliche Statusanzeigen finden Sie in Tabelle 7–2
Name	Aus der Konfiguration mit Security Configuration Tool übernommener Name des Moduls oder des Teilnehmers.
Int. Teilnehmer-IP / Subnetz	IP-Adresse des internen Knotens, bzw. Netz ID des internen Subnetzes, wenn interne Teilnehmer / Subnetze vorhanden
Tunnelendpunkt-IP	IP-Adresse des zugeordneten SCALANCE S-Moduls oder MD741-1 Moduls
Tunnel über..	Falls Sie in Ihrem PC mehrere Netzwerkkarten betreiben, wird hier die zugeordnete IP-Adresse angezeigt.

Tabelle 7- 2 Statusanzeigen

Symbol	Bedeutung
	Es besteht keine Verbindung zum Modul oder Teilnehmer.
	Es sind weitere Teilnehmer vorhanden, die nicht angezeigt werden. Doppelklicken Sie auf das Symbol, um weitere Teilnehmer anzuzeigen.
	Der Teilnehmer ist nicht aktiviert.
	Der Teilnehmer ist aktiviert.
	Deaktiviertes SCALANCE S-Modul.
	Aktiviertes SCALANCE S-Modul.
	Deaktiviertes MD741-1 Modul.
	Aktiviertes MD741-1 Modul.
	Modul / Teilnehmer ist nicht erreichbar.
	Modul / Teilnehmer ist erreichbar.

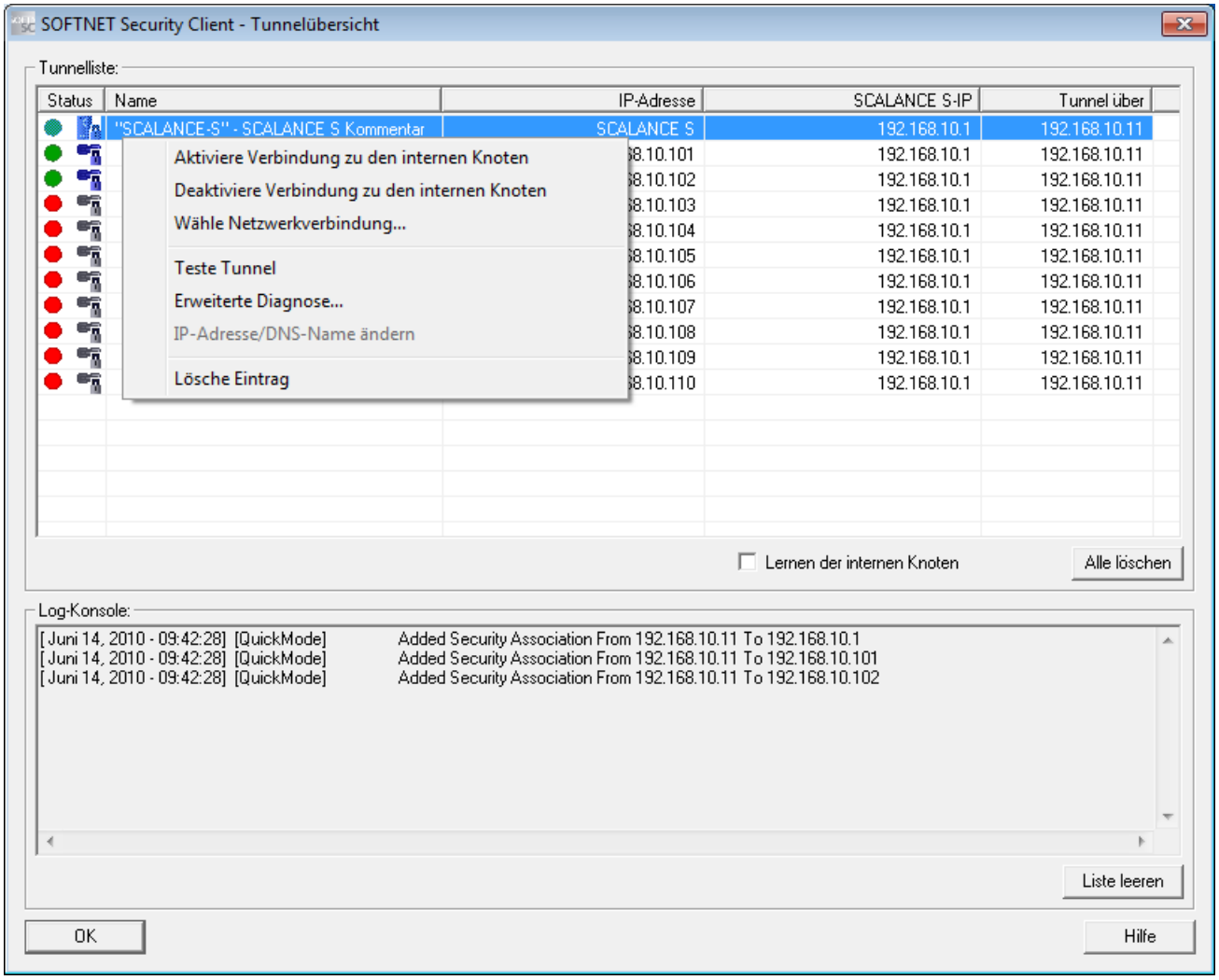
Optionskästchen "Lernen der internen Knoten"

Wenn in der Konfiguration der SCALANCE S Module der Lernmodus aktiviert ist, können Sie auch den Lernmodus für den SOFTNET Security Client nutzen; Sie erhalten dadurch automatisch die Informationen von den SCALANCE S Modulen.

Ansonsten wird das Auswahlfeld "Activate learning mode" inaktiv und gegraut dargestellt.

Tunnel-Eintrag selektieren und bedienen

Im Dialog "Tunnel" können Sie einen Eintrag selektieren und weitere Menübefehle über die rechte Maustaste aufschlagen.



ACHTUNG
Wenn für einen Netzwerkadapter mehrere IP-Adressen verwendet werden, müssen Sie gegebenenfalls die jeweils zu verwendende IP-Adresse im Dialog "Tunnel" für jeden einzelnen Eintrag zuweisen.

Schaltfläche "Alle löschen"

Sie löschen hiermit die IP-Sicherheitsrichtlinie vollständig - einschließlich zusätzlicher, nicht vom SOFTNET Security Client eingerichteter Einträge.

Aus- und Einschalten von bereits eingerichteten sicheren Verbindungen

Sie können eingerichtete sichere Verbindungen mit der Schaltfläche "Deaktivieren" ausschalten. Wurde die Schaltfläche angeklickt, ändert sich der Text in der Schaltfläche auf "Aktivieren" und das Symbol in der Statusleiste wird ersetzt.

Auf dem PC ist jetzt die Security Policy deaktiviert.

Mit einem erneuten Klick auf die Schaltfläche können Sie die obige Änderung wieder rückgängig machen und die eingerichteten Tunnel sind wieder aktiv.

Log-Konsole

Die Log-Konsole befindet sich im unteren Teil des Dialogs "Tunnelübersicht" und liefert Diagnoseinformationen zum Verbindungsaufbau mit den konfigurierten SCALANCE S- / MD741-1 - Modulen und internen Teilnehmern / Subnetzen.

Mit Datums und Zeitstempel können die Zeitpunkte der entsprechenden Ereignisse erfasst werden.

Es wird das Auf- und Abbauen einer Security Association angezeigt. Ebenso wird das Ergebnis eines Testpings (Erreichbarkeitstest) zu den konfigurierten Teilnehmern angezeigt, wenn es negativ ist.

Welche Ausgaben angezeigt werden sollen können Sie im Dialog "Einstellungen" konfigurieren.

Schaltfläche "Liste leeren"

Sie löschen bei Betätigung die Einträge aus der Log-Konsole der Tunnelübersicht.

Globale Einstellungen für den SOFTNET Security Client

Öffnen Sie im Hauptdialog des SOFTNET Security Client den Menüpunkt:

Optionen ▸ Einstellungen

Hier können Sie globale Einstellungen machen, welche nach dem Beenden und Öffnen des SOFTNET Security Client erhalten bleiben.

Die Funktionen entnehmen Sie aus der folgenden Tabelle.

Funktion	Beschreibung / Optionen
Log-File Größe (Log-Konsole)	Log-File Größe der Quelldatei, welche die Meldungen enthält die gefiltert und auf eine bestimmte Anzahl begrenzt in der Log-Konsole ausgegeben werden
Anzahl anzuzeigender Meldungen in Log-Konsole der Tunnelübersicht	Anzahl der Meldungen, welche aus dem Log-File der Quelldatei extrahiert und in der Log-Konsole angezeigt werden

Folgende Log-Meldungen in Log-Konsole der Tunnelübersicht ausgeben: • Anzeige des negativen Erreichbarkeitstest (Ping) • Anlegen / Löschen von Security Associations (Quick Modes) • Anlegen / Löschen von Main Modes • Laden von Konfigurationsdateien • Lernen interner Teilnehmer	Meldungen, welche in der Log-Konsole optional angezeigt werden, können hier an und ausgeschaltet werden
Logfile-Größe (Debug-Logfiles)	Log-File Größe der Quelldateien für Debug-Meldungen des SOFTNET Security Client (können vom Customer Support angefordert werden, um Analysen zu erleichtern)
Erreichbarkeitstest, Wartezeit auf Rückantwort	Einstellbare Wartezeit für den Ping, welcher die Erreichbarkeit eines Tunnelpartners angeben soll. Vor allem wichtig einzustellen bei Tunneln über langsame Übertragungswege (UMTS, GPRS, etc.), bei denen die Laufzeit der Datenpakete deutlich höher ist. Beeinflusst somit direkt die Anzeige der Erreichbarkeit in der Tunnelübersicht. **Hinweis** Wählen Sie bei Funknetzen eine Wartezeit von mind. 1500 ms aus.
Erreichbarkeitstest global deaktivieren	Wenn Sie diese Funktion aktivieren, wird der Erreichbarkeitstest global für alle enthaltenen Konfigurationen im SOFTNET Security Client deaktiviert. Dies hat den Vorteil, dass keine zusätzlichen Pakete Datenvolumen erzeugen und den Nachteil, dass Sie in der Tunnelübersicht keine Rückmeldung mehr darüber erhalten, ob ein Tunnelpartner erreichbar ist oder nicht.

Erweiterte Moduldiagnose

Öffnen Sie im Hauptdialog des SOFTNET Security Client den Menüpunkt:

Optionen ▸ Erweiterte Moduldiagnose

Hier können Sie den aktuellen Status Ihres Systems im Zusammenhang mit einem konfigurierten Modul ermitteln. Diese Ansicht dient rein der Diagnose Ihres Systemzustands und kann bei Customer Support Anfragen helfen.

- SCALANCE S / MD741-1 Modul
  Hier wählen Sie das Modul aus für das Sie den aktuellen Systemstatus diagnostizieren möchten.
- Routingeinstellungen (Modulspezifische Parameter)
  Hier werden Ihnen die aus der Konfiguration ermittelten Einstellungen des Moduls hinsichtlich seiner Schnittstellen und internen Knoten / Subnetze aufgezeigt.

- Aktive Main Modes / Aktive Quick Modes
  Hier werden Ihnen die aktiven Main Modes bzw. Quick Modes im Detail angezeigt, sobald diese für das ausgewählte Modul auf dem PG/PC eingerichtet worden sind. Zusätzlich haben Sie eine Anzeige darüber, wie viele Main Modes bzw. Quick Modes passend zu dem ausgewählten Modul auf dem System gefunden wurden.
- Routingeinstellungen (Netzwerkeinstellungen des Rechners)
  Hier werden Ihnen die aktuellen Routingeinstellungen Ihres Rechners angezeigt. Mit der Option "Alle Routingeinstellungen anzeigen" können Sie die aus Gründen der Übersichtlichkeit ausgeblendeten Routingeinstellungen einblenden.
- Zugewiesene IP-Adressen
  Hier haben Sie eine Liste über Ihre dem Rechner bekannten Netzwerkschnittstellen in Verbindung mit den konfigurierten bzw. zugewiesenen IP-Adressen.

Online Funktionen - Test, Diagnose und Logging

8

Zu Test- und Überwachungszwecken verfügt SCALANCE S über Diagnose- und Logging-Funktionen.

- Diagnosefunktionen

  Hierunter sind verschiedene System- und Statusfunktionen zu verstehen, die Sie im Online-Mode anwenden können.

- Logging-Funktionen

  Hierbei geht es um die Aufzeichnung von System- und Sicherheits-Ereignissen.

Die Aufzeichnung der Ereignisse erfolgt in Pufferbereiche des SCALANCE S oder eines Servers. Die Parametrierung und Auswertung dieser Funktionen setzt eine Netzwerkverbindung auf das ausgewählte SCALANCE S-Modul voraus.

Ereignisse mit Logging-Funktionen aufzeichnen

Welche Ereignisse aufgezeichnet werden sollen, legen Sie mit den Log-Einstellungen zum jeweiligen SCALANCE S-Modul fest.

Dabei können Sie für die Aufzeichnung wiederum folgende Varianten konfigurieren:

- Lokaler Log

  Bei dieser Variante zeichnen Sie die Ereignisse in lokalen Puffern des SCALANCE S-Moduls auf. Im Online-Dialog des Security Configuration Tool können Sie dann auf diese Aufzeichnungen zugreifen, diese sichtbar machen und in der Service-Station archivieren.

- Netzwerk Syslog

  Beim Netzwerk Syslog nutzen Sie einen im Netz vorhanden Syslog-Server. Dieser zeichnet die Ereignisse entsprechend der Konfiguration in den Log-Einstellungen zum jeweiligen SCALANCE S-Modul auf.

Weitere Informationen

Detailinformationen zu den Dialogen und den in der Diagnose und dem Logging aufgezeichneten Parametern entnehmen Sie bitte der Online-Hilfe von Security Configuration Tool.

Sie erreichen diese über die F1-Taste oder über die Schaltfläche "Hilfe" im jeweiligen Dialog.

Siehe auch

Funktionsübersicht Online-Dialog (Seite 228)

8.1 Funktionsübersicht Online-Dialog

SCALANCE S bietet im Security Configuration Tool folgende Funktionen im Online-Dialog:

Tabelle 8- 1 Funktionen und Logging in der Online-Diagnose

Funktion / Register im Online-Dialog	Bedeutung
System- und Statusfunktionen	
Zustand	Anzeige des Geräte-Status des im Projekt angewählten SCALANCE S-Moduls.
Kommunikations-zustand (S612 / S613)	Anzeige des Kommunikations-Status und der internen Netzknoten zu weiteren der VPN-Gruppe zugehörenden SCALANCE S-Modulen.
Datum und Uhrzeit	Einstellung von Datum und Uhrzeit.
Interne Knoten (S612 / S613)	Anzeige der internen Netzknoten des SCALANCE S-Moduls.
Logging-Funktionen	
System Log	Anzeige von geloggten System-Ereignissen.
Audit Log	Anzeige von geloggten Sicherheits-Ereignissen.
Paketfilter Log	Anzeige von geloggten Daten-Paketen, sowie Starten und Stoppen des Paket-Logging.

Anmerkung: Bitte beachten Sie die Hinweise zu den Gerätetypen.

Zugriffsvoraussetzungen

Damit Sie Online an einem SCALANCE S-Modul die Online-Funktionen durchführen können, müssen folgende Voraussetzungen erfüllt sein:

- die Online-Betriebsart im Security Configuration Tool ist eingeschaltet
- eine Netzwerkverbindung zum ausgewählten Modul besteht
- das zugehörige Projekt, mit dem das Modul konfiguriert wurde, ist geöffnet

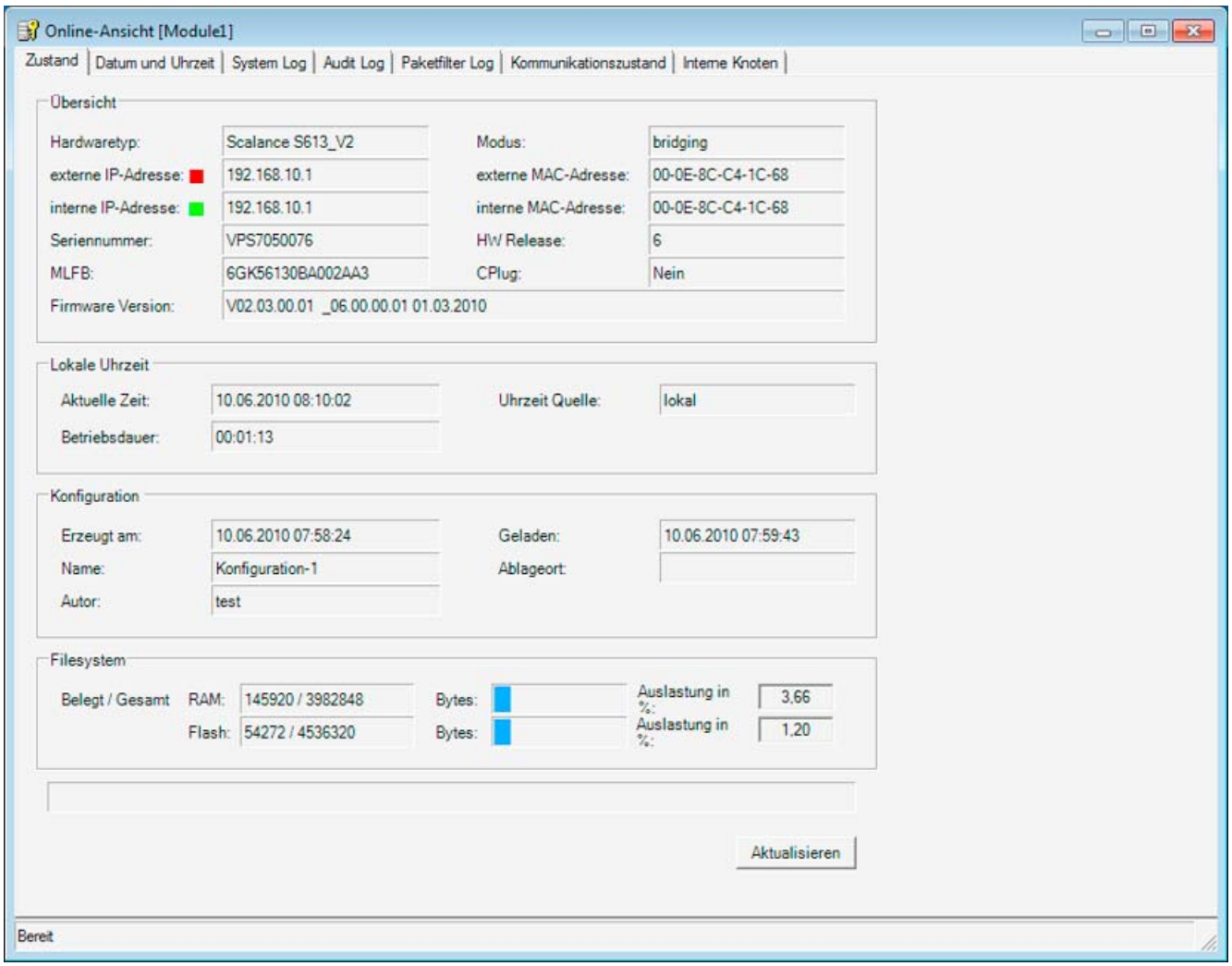
Online-Dialog öffnen

Schalten Sie über folgenden Menübefehl die Betriebsart von Security Configuration Tool um:

Ansicht ▸ Online

Markieren Sie das zu bearbeitende Modul und wählen Sie zum Öffnen des Online-Dialoges den Menübefehl

Bearbeiten ▸ Online Diagnose...



Warnmeldung bei nicht-aktueller Konfiguration oder Fremdprojekt

Wenn Sie den Online-Dialog aufrufen, wird geprüft, ob die aktuelle Konfiguration auf dem SCALANCE S-Modul und die Konfiguration des geladenen Projekts übereinstimmen. Unterscheiden sich die beiden Konfigurationen, so wird eine Warnmeldung ausgegeben. Dadurch wird signalisiert, dass Sie entweder die Konfiguration (noch) nicht aktualisiert haben, oder das falsche Projekt verwenden.

Online-Einstellungen werden nicht in der Konfiguration gespeichert

Einstellungen, die Sie in der Online-Betriebsart vornehmen, werden nicht in der Konfiguration auf dem SCALANCE S-Modul gespeichert. Nach einem Modul-Neuanlauf sind deshalb immer die Einstellungen in der Konfiguration wirksam.

8.2 Ereignisse aufzeichnen (Logging)

Übersicht

Ereignisse auf dem SCALANCE S können aufgezeichnet werden. Die Aufzeichnung erfolgt je nach Ereignistyp in flüchtige oder dauerhafte lokale Pufferbereiche. Alternativ kann auch eine Aufzeichnung in einem Netzwerk-Server erfolgen.

Konfiguration im Standard- und im Erweitert-Modus

Die Auswahlmöglichkeiten im Security Configuration Tool hängen auch beim Logging von der gewählten Ansicht ab:

- Standard-Modus

  Lokaler Log ist im Standard-Modus standardmäßig aktiviert; Paketfilter-Ereignisse können global im Register "Firewall" aktiviert werden. Netzwerk Syslog ist in dieser Ansicht nicht möglich.

- Erweitert-Modus

  Sämtliche Logging-Funktionen können gezielt aktiviert oder deaktiviert werden; Paketfilter-Ereignisse müssen selektiv im Register "Firewall" (lokale oder globale Regeln) aktiviert werden.

Aufzeichnungsverfahren und Ereignisklassen

Sie können in der Konfiguration festlegen, welche Daten aufgezeichnet werden sollen. Dadurch aktivieren Sie die Aufzeichnung bereits mit dem Laden der Konfiguration in das SCALANCE S-Modul.

Außerdem wählen Sie in der Konfiguration eine oder beide der möglichen Aufzeichnungsverfahren:

- Lokaler Log
- Netzwerk Syslog

Das SCALANCE S kennt für beide Aufzeichnungsverfahren jeweils die drei folgenden Arten von Ereignissen:

Tabelle 8- 2 Logging - Übersicht über wählbare Ereignisse

Funktion / Register im Online-Dialog	Funktionsweise
Paketfilter-Ereignisse (Firewall) / Packet Filter Log	Der Paket Filter Log zeichnet bestimmte Pakete des Datenverkehrs auf. Es werden nur solche Datenpakete geloggt, auf die eine projektierte Paket-Filter-Regel (Firewall) zutrifft, oder auf die der Basisschutz reagiert (korrupte bzw. ungültige Pakete). Voraussetzung ist, dass die Aufzeichnung für die Paket-Filter-Regel aktiviert ist.
Audit-Ereignisse / Audit Log	Der Audit Log zeichnet automatisch fortlaufend sicherheits-relevante Ereignisse auf. Beispielsweise Benutzeraktionen wie das Ein- oder Ausschalten des Paket-Logging oder Aktionen, bei denen sich ein Benutzer nicht korrekt über Passwort authentisiert hat.
Systemereignisse / System Log	Das System Log zeichnet automatisch fortlaufend System-Ereignisse, wie z.B. den Start eines Prozesses, auf. Anhand von Ereignisklassen ist die Aufzeichnung skalierbar. Zusätzlich ist eine Leitungsdiagnose projektierbar. Die Leitungsdiagnose liefert Meldungen, sobald die Anzahl fehlerhafter Telegrammpakete einen einstellbaren Grenzwert überschritten hat.

Speicherverfahren für die Datenaufzeichnung beim lokalen Logging

Die Speicherung bei der Datenaufzeichnung erfolgt nach zwei wählbaren Verfahren:

- **Ring Buffer**

Bei Erreichen des Pufferendes wird die Aufzeichnung am Pufferanfang mit dem Überschreiben der ältesten Einträge fortgesetzt.

- **One Shot Buffer**

Die Aufzeichnung stoppt, wenn der Puffer voll ist.

Ein- bzw. Ausschalten des Logging

In der Betriebsart Offline können Sie über die Log Einstellungen das Lokale Logging für die Ereignisklassen aktivieren und das Speicherverfahren festlegen. Diese Log-Einstellungen werden mit der Konfiguration in das Modul geladen und werden mit dem Start des SCALANCE S wirksam.

Sie können das lokale Logging für Paketfilter-Ereignisse und Systemereignisse in den Online-Funktionen bei Bedarf ebenfalls aktivieren oder deaktivieren. Die Einstellungen in der Projektkonfiguration werden dadurch nicht verändert.

8.2.1 Lokaler Log - Einstellungen in der Konfiguration

In der Betriebsart Offline können Sie über die Log Einstellungen die Ereignisklassen aktivieren und das Speicherverfahren festlegen. Diese Log-Einstellungen werden mit der Konfiguration in das Modul geladen und werden mit dem Start des SCALANCE S wirksam.

Sie können diese projektierten Log-Einstellungen in den Online-Funktionen bei Bedarf ändern. Die Einstellungen in der Projekt-Konfiguration werden dadurch nicht verändert.

Log-Einstellungen im Standard-Modus

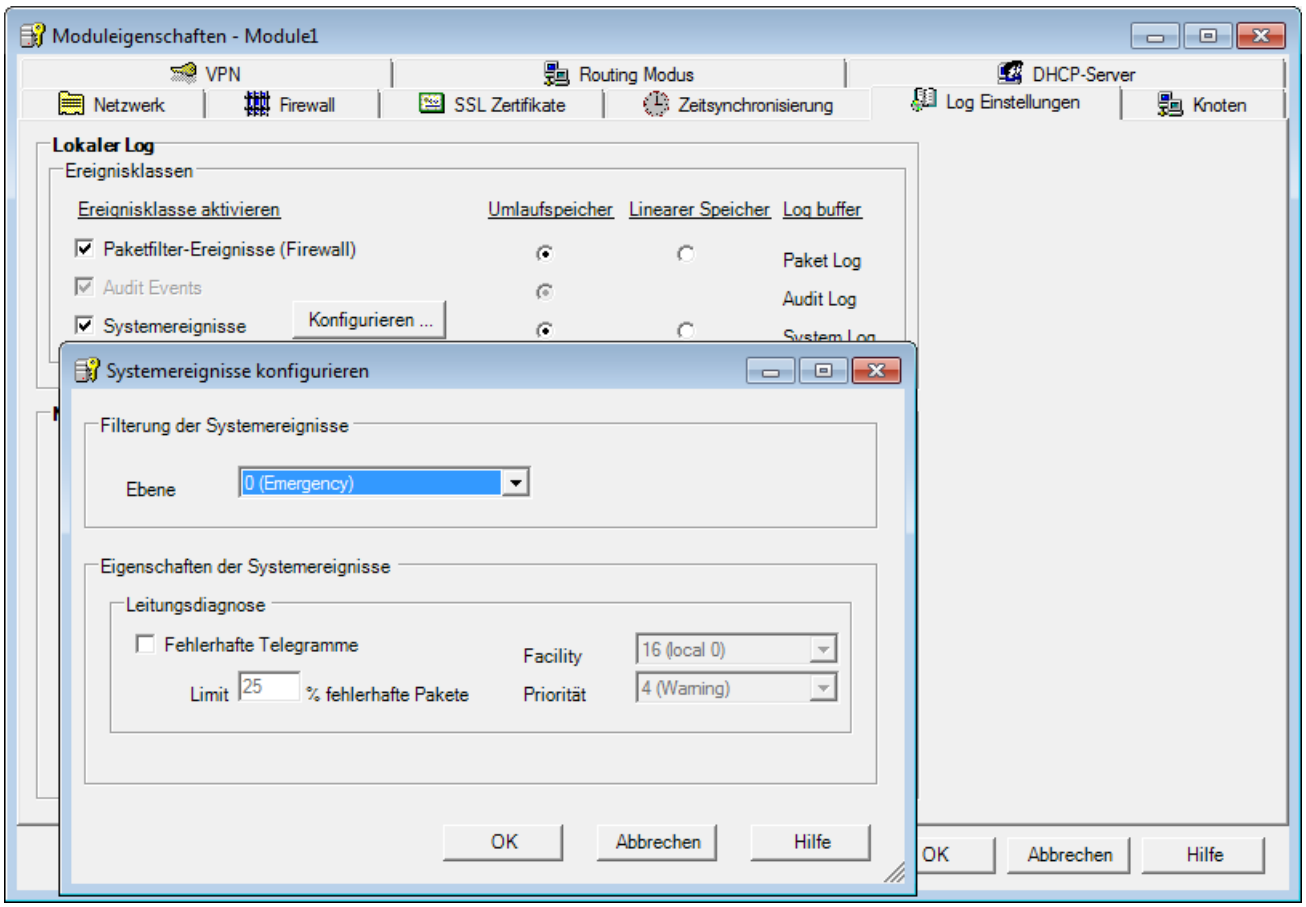
Die Log-Einstellungen im Standard-Modus entsprechen den Voreinstellungen im Erweitert-Modus. Im Standard-Modus können Sie die Einstellungen jedoch nicht verändern.

Log-Einstellungen im Erweitert-Modus

Markieren Sie das zu bearbeitende Modul und wählen Sie folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften..., Register "Log Einstellungen".

Der folgende Dialog zeigt die Standard-Einstellungen für SCALANCE S; zusätzlich ist der Dialog zur Konfiguration der Aufzeichnung von Systemereignissen geöffnet:



Ereignisklassen konfigurieren

Tabelle 8- 3 Lokaler Log - Funktionsübersicht

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Paketfilter-Ereignisse (Firewall) / Packet Filter Log (projektierbar)	Die Aktivierung erfolgt über Optionskästchen. Die Auswahl des Speicherverfahrens erfolgt über Optionsfelder.	• Paketfilter-Log-Daten sind nicht remanent Die Daten werden in einem flüchtigen Speicher von SCALANCE S abgelegt, und stehen deshalb nach einem Ausschalten der Spannungsversorgung nicht mehr zur Verfügung.
Audit-Ereignisse / Audit Log (immer eingeschaltet)	Logging ist immer aktiviert. Die Speicherung erfolgt immer im Umlaufpuffer.	• Audit Log-Daten sind remanent Die Audit Log-Daten werden in einem remanenten Speicher von SCALANCE S abgelegt. Die Daten des Audit Log stehen deshalb auch nach einem Ausschalten der Spannungsversorgung noch zur Verfügung.

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
System-Ereignisse / System Log (projektierbar)	Die Aktivierung erfolgt über Optionskästchen. Die Auswahl des Speicherverfahrens erfolgt über Optionsfelder. Zur Konfiguration des Ereignisfilters und der Leitungsdiagnose öffnen Sie über die Schaltfläche "Konfigurieren..." einen weiteren Dialog. Sie stellen in diesem Sub-Dialog für die Systemereignisse eine Filterebene ein. Standardmäßig ist die höchste Ebene eingestellt, so dass nur kritische Ereignisse aufgezeichnet werden. Die Leitungsdiagnose erzeugt ein spezielles Systemereignis. Dabei wird bei einem von Ihnen einstellbaren Prozentsatz fehlerhafter Telegramme ein Systemereignis erzeugt. Diesem Systemereignis wird die in diesem Sub-Dialog einstellbare Priorität und Bedeutung (Facility) zugewiesen.	• System Log-Daten sind nicht remanent Die System Log-Daten werden in einem flüchtigen Speicher von SCALANCE S abgelegt. Diese Daten stehen deshalb nach einem Ausschalten der Spannungsversorgung nicht mehr zur Verfügung. • Filterung der Systemereignisse Wählen Sie als Filterebene "Error" oder einen höheren Wert, um die Aufzeichnung von allgemeinen, nicht kritischen Ereignissen zu unterbinden. • Priorität der Systemereignisse der Leitungsdiagnose Achten Sie darauf, dass Sie den Systemereignissen der Leitungsdiagnose keine geringere Priorität zuweisen, als Sie für den Filter eingestellt haben. Bei geringerer Priorität würden diese Ereignisse den Filter nicht passieren und nicht aufgezeichnet werden.

8.2.2 Netzwerk Syslog - Einstellungen in der Konfiguration

Sie können SCALANCE S so konfigurieren, dass es als Client Syslog-Informationen an einen Syslog-Server sendet. Der Syslog-Server kann sich im internen oder im externen Subnetz befinden. Die Implementierung entspricht RFC 3164.

Hinweis

Firewall - Syslog-Server im externen Netz nicht aktiv

Wenn der Syslog-Server auf dem adressierten Rechner nicht aktiv ist, sendet dieser Rechner in der Regel ICMP-Antworttelegramme "port not reachable" zurück. Wenn aufgrund der Firewall-Konfiguration diese Antworttelegramme als Systemereignisse aufgezeichnet werden und an den Syslog-Server gesendet werden, kann sich dieser Vorgang endlos fortsetzen (Ereignis-Lawine).

Abhilfen:

- Syslog-Server starten;
- Firewall-Regeln ändern;
- Rechner mit deaktiviertem Syslog-Server vom Netz nehmen;

In den Erweitert-Modus umschalten

Die Konfiguration des Syslog-Servers setzt im Security Configuration Tool die Ansicht "Erweitert-Modus" voraus. Schalten Sie über folgenden Menübefehl die Betriebsart um:

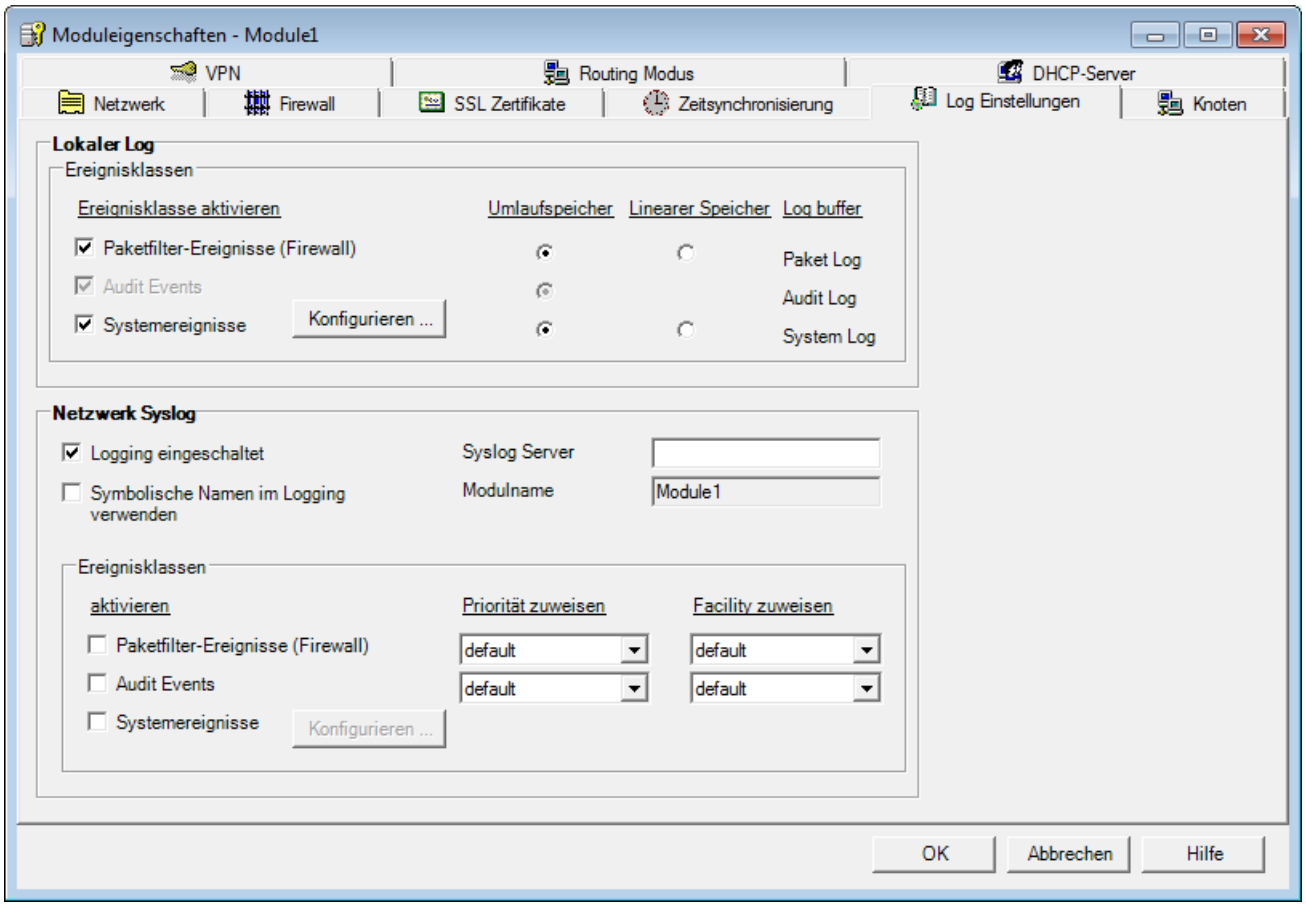
Ansicht ▸ Erweitert-Modus

Log-Einstellungen vornehmen

Markieren Sie das zu bearbeitende Modul und wählen Sie folgenden Menübefehl:

Bearbeiten ▸ Eigenschaften... , Register "Log Einstellungen".

Der folgende Dialog zeigt die Standard-Einstellungen für SCALANCE S bei aktiviertem Logging für das Netzwerk Syslog.:



Verbindung zum Syslog-Server herstellen

SCALANCE S verwendet den projektierten Modulnamen als Hostnamen gegenüber dem Syslog-Server. Die IP-Adresse des Syslog-Servers müssen Sie angeben. Sie können die IP-Adresse alternativ als symbolischen Namen oder numerisch eingeben.

Der Syslog-Server muss von SCALANCE S aus über die angegebene IP-Adresse erreichbar sein, ggf. über die Router-Projektierung im Register "Netzwerk". Wenn der Syslog-Server nicht erreichbar ist, wird das Versenden der Syslog-Informationen abgeschaltet. Sie können diesen Betriebszustand anhand entsprechender Systemmeldungen erkennen. Um das Versenden der Syslog-Informationen erneut zu aktivieren, müssen Sie ggf. die Routing-Informationen aktualisieren und einen Neustart des SCALANCE S veranlassen.

Symbolische Namen im Logging verwenden

Sie können die Adressangaben in den an den Syslog-Server übermittelten Log-Telegrammen durch symbolische Namen ersetzen. SCALANCE S prüft bei eingeschalteter Option, ob entsprechende symbolische Namen projektiert sind und trägt diese in das Log-Telegramm ein. Beachten Sie, dass dies die Bearbeitungszeit im SCALANCE S-Modul erhöht.

Für die IP-Adressen der SCALANCE S-Module werden automatisch die Modulnamen als symbolische Namen verwendet. Im Routing-Modus werden diese Namen mit einer Port-Bezeichnung wie folgt erweitert: "Modulname-P1", "Modulname-P2" usw.

Ereignisklassen konfigurieren

Tabelle 8- 4 Netzwerk Syslog - Funktionsübersicht

Funktion / Register im Online-Dialog	Projektierung	Bemerkungen
Paketfilter-Ereignisse (Firewall) / Packet Filter Log (projektierbar)	Die Aktivierung erfolgt über Optionskästchen. Die Zuordnung der Priorität und Bedeutung (Facility) erfolgt über Klapplisten. Jedem Ereignis wird die Priorität und die Bedeutung (Facility) zugewiesen, die Sie hier einstellen.	Welchen Wert Sie hier für Priorität und Bedeutung (Facility) wählen, hängt von der Auswertung im Syslog-Server ab. Damit können Sie eine Anpassung an die Erfordernisse im Syslog-Server vornehmen. Defaulteinstellungen: Facility: 10 (security/auth) Prio: 5 (Notice)
Audit-Ereignisse / Audit Log (immer eingeschaltet)	Die Aktivierung erfolgt über Optionskästchen. Die Zuordnung der Priorität und Bedeutung (Facility) erfolgt über Klapplisten. Jedem Ereignis wird die Priorität und die Bedeutung (Facility) zugewiesen, die Sie hier einstellen.	Welchen Wert Sie hier für Priorität und Bedeutung (Facility) wählen, hängt von der Auswertung im Syslog-Server ab. Damit können Sie eine Anpassung an die Erfordernisse im Syslog-Server vornehmen. Defaulteinstellungen: Facility: 13 (log audit) Prio: 6 (Informational)
Systemereignisse / System Log (projektierbar)	Die Aktivierung erfolgt über Optionskästchen. Zur Konfiguration des Ereignisfilters und der Leitungsdiagnose öffnen Sie über die Schaltfläche "Konfigurieren..." einen weiteren Dialog. Sie stellen in diesem Sub-Dialog für die Systemereignisse eine Filterebene ein. Standardmäßig ist die höchste Ebene eingestellt, so dass nur kritische Ereignisse aufgezeichnet werden. Die Leitungsdiagnose erzeugt ein spezielles Systemereignis. Dabei wird bei einem von Ihnen einstellbaren Prozentsatz fehlerhafter Telegramme ein Systemereignis erzeugt. Diesem Systemereignis wird die in diesem Sub-Dialog einstellbare Priorität und Bedeutung (Facility) zugewiesen.	• Filterung der Systemereignisse Wählen Sie als Filterebene "Error" oder einen höheren Wert, um die Aufzeichnung von allgemeinen, nicht kritischen Ereignissen zu unterbinden. • Priorität der Systemereignisse der Leitungsdiagnose Über die Priorität gewichten Sie die Systemereignisse der Leitungsdiagnose im Verhältnis zur Priorität der übrigen Systemereignisse. Achten Sie darauf, dass Sie den Systemereignissen der Leitungsdiagnose keine geringere Priorität zuweisen, als Sie für den Filter eingestellt haben. Bei geringerer Priorität würden diese Ereignisse den Filter nicht passieren und nicht zum Syslog-Server gelangen.

8.2.3 Die Projektierung des Paket-Logging

Der Paket Filter Log zeichnet die Datenpakete auf, für die Sie das Logging in einer Paket-Filter-Regel (Firewall) in der Konfiguration aktiviert haben. Diese Aktivierung muss also projektiert werden.

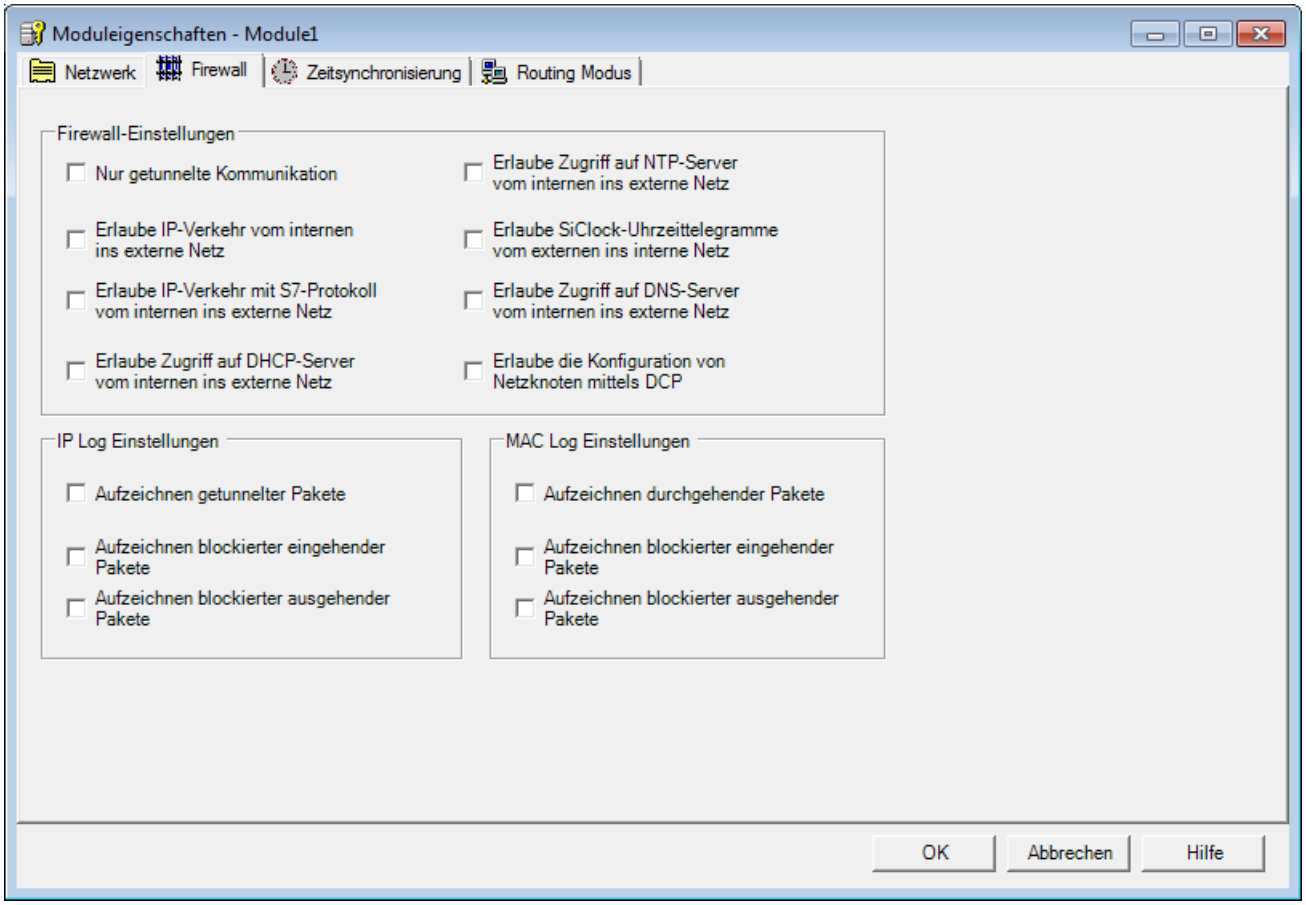
Je nach eingestellter Bedienungssicht unterscheidet sich die Projektierung. Während im Standard-Modus das Logging nur für einige vordefinierte Regelsätze pauschal eingeschaltet werden kann, kann es im Erweitert-Modus für jede einzelne Paket-Filter-Regel aktiviert werden.

Projektierung im Standard-Modus

Im Standard-Modus gibt es folgende Regelsätze für IP- und MAC-Log-Einstellungen, für die das Logging aktiviert werden kann:

Tabelle 8- 5 IP und MAC Log Einstellungen

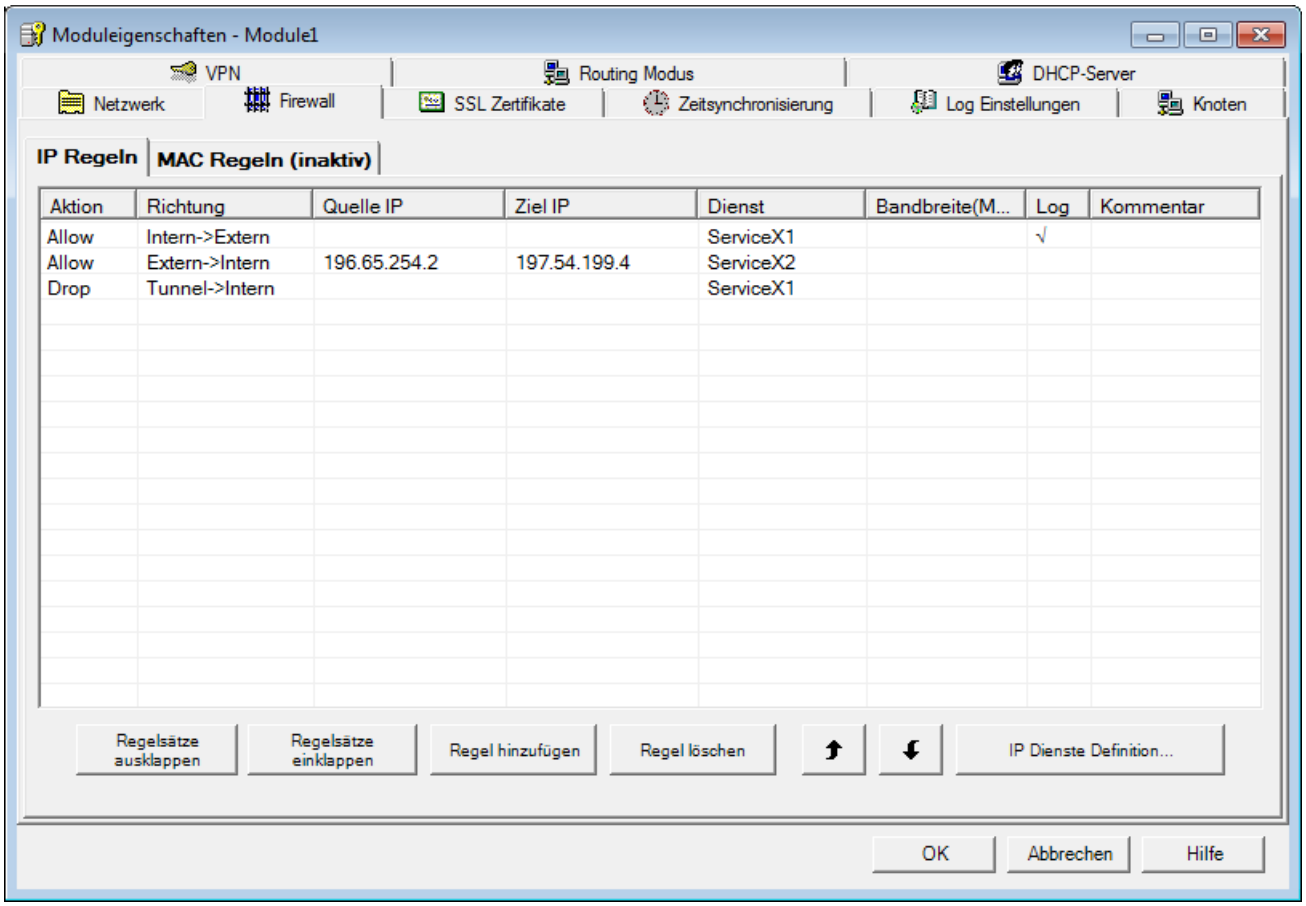
Regelsatz	Aktion bei Aktivierung
Aufzeichnen durchgehender Pakete	Alle MAC-Pakete, die weitergeleitet wurden, werden geloggt.
Aufzeichnen blockierter einkommender Pakete	Alle eintreffenden IP / MAC-Pakete, die verworfen wurden, werden geloggt.
Aufzeichnen blockierter abgehender Pakete	Alle abgehenden IP / MAC-Pakete, die verworfen wurden, werden geloggt.
Aufzeichnen getunnelter Pakete	Alle IP-Pakete, die über den Tunnel weitergeleitet wurden, werden geloggt.



Projektierung im Erweitert-Modus

Die Aktivierung des Logging ist für beide Regel-Typen (IP oder MAC) und alle Regeln identisch.

Um Datenpakete bestimmter Paket-Filter-Regeln aufzuzeichnen, setzen Sie im Register "Firewall" in der Spalte "Log" einen Auswahlhaken.



Tipps und Hilfestellung

A

A.1 SCALANCE S-Modul bootet nicht korrekt

Wenn die Fault-Anzeige des SCALANCE S-Moduls nach dem Hochlauf des Moduls rot leuchtet, sollten Sie das Modul zunächst vollständig zurücksetzen. Drücken Sie den Reset-Taster, bis die Fault-Anzeige gelb-rot zu blinken beginnt. Das Modul ist dann auf die Werkseinstellungen zurückgesetzt. Für den Produktivbetrieb müssen Sie anschließend die Konfiguration neu auf das Modul laden.

Sollte die Fault-Anzeige des SCALANCE S-Modul jedoch weiter rot leuchten, kann das Modul nur im Werk repariert werden.

A.2 SCALANCE S-Modul ist nicht erreichbar

Wenn das SCALANCE S-Modul nicht erreichbar ist prüfen bzw. beachten Sie folgende Punkte:

- Befindet sich Ihr Rechner im gleichen Netzwerk wie die Baugruppe?
- Der Reset einer Baugruppe kann bis zu einigen Minuten dauern.

A.3 Austausch eines SCALANCE S-Moduls

Der Austausch eines SCALANCE S-Moduls kann ohne PC erfolgen (ohne die Konfiguration auf das neue Modul laden zu müssen). Der C-PLUG des auszutauschenden Moduls wird einfach auf das neue Modul gesteckt, das in Betrieb genommen werden soll.

ACHTUNG
Der C-PLUG darf nur im spannungslosen Zustand gesteckt oder gezogen werden!

A.4 SCALANCE S-Modul ist kompromittiert

Ein SCALANCE S-Modul ist kompromittiert, wenn

- der zum Server-Zertifikat gehörige private Schlüssel,
- der private Schlüssel der CA oder
- das Passwort eines Benutzers bekannt geworden ist.

Privater Schlüssel des Server-Zertifikats bekannt

Ist der zum Server-Zertifikat gehörige private Schlüssel bekannt geworden, so muss das Server-Zertifikat auf dem SCALANCE S-Modul ausgetauscht werden. Die im SCALANCE S-Modul gespeicherten Benutzernamen müssen hierbei nicht geändert werden.

Gehen Sie so vor:

1. Markieren Sie das zu bearbeitende Modul und wählen Sie den Menübefehl

   Bearbeiten ▸ Eigenschaften..., Register "Zertifikate".
2. Erzeugen Sie ein neues Zertifikat.
3. Laden Sie die Konfiguration in das SCALANCE S-Modul.

Der private Schlüssel der CA bekannt

Ist der private Schlüssel der CA bekannt geworden, so muss auf dem SCALANCE S-Modul das Zertifikat der CA ausgetauscht werden. Die Benutzernamen können unverändert bleiben. Allerdings benötigen die Benutzer neue Zertifikate, die von der neuen CA ausgestellt sind.

Gehen Sie so vor:

1. Markieren Sie die zu bearbeitende Gruppe und wählen Sie den Menübefehl

   Bearbeiten ▸ Eigenschaften....
2. Erzeugen Sie ein neues Zertifikat.
3. Laden Sie die Konfiguration in alle zur Gruppe gehörenden SCALANCE S-Module.

Passwort eines Benutzers aus der User-Gruppe bekannt

Ist das Passwort eines Benutzers aus der User-Gruppe bekannt geworden, so muss das Passwort dieses Benutzers geändert werden.

Passwort eines Benutzers aus der Administrator-Gruppe bekannt

Handelt es sich um einen Benutzer aus der Administratoren-Gruppe, so sollte das Server-Zertifikat des SCALANCE S-Moduls ebenfalls geändert werden.

A.5 Schlüssel aus den Projektierungsdaten kompromittiert oder verloren

Schlüssel kompromittiert

Wurde ein privater Schlüssel, aus den Projektierungsdaten des SCALANCE S-Moduls kompromittiert, so muss der Schlüssel über das Projektierungswerkzeug des SCALANCE S-Moduls geändert werden.

Verlust des Schlüssels

Ging der private Schlüssel, der den Zugriff auf die Projektierungsdaten autorisiert, verloren, so kann mit dem Projektierungstool nicht mehr auf das SCALANCE S-Modul zugegriffen werden. Die einzige Möglichkeit wieder Zugriff zu bekommen besteht darin die Projektierungsdaten und damit auch die Schlüssel zu löschen. Das Löschen kann durch Drücken des Reset-Tasters ausgelöst werden. Daraufhin muss das SCALANCE S-Modul wieder neu in Betrieb genommen werden.

A.6 Allgemeines Betriebsverhalten

Anpassen der MTU (Maximum Transmission Unit)

Die MTU legt die zulässige Größe eines Datenpaketes für die Übertragung im Netzwerk fest. Wenn diese Datenpakete nun von SCALANCE S über den IPsec Tunnel übertragen werden, wird das ursprüngliche Datenpaket durch die zusätzlichen Header-Informationen größer und muss unter Umständen für die weitere Übertragung segmentiert werden. Dies ist abhängig von den MTU-Vorgaben im angeschlossenen Netzwerk. Eine erforderliche Segmentierung kann aber zu merklichen Performanceverlusten oder zum Abbruch der Datenübertragung führen.

Vermeiden können Sie dies, indem Sie das MTU-Format anpassen, d.h. so reduzieren, dass die beim SCALANCE S eintreffenden Datenpakete mit den benötigten Zusatzinformationen ergänzt werden können, ohne dass eine anschließende Segmentierung erforderlich ist. Eine sinnvolle Größe liegt im Bereich zwischen 1000 und 1400 Byte.

Hinweise zur CE-Kennzeichnung

B

Produktbezeichnung

SIMATIC NET	SCALANCE S602	6GK5602-0BA00-2AA3
SIMATIC NET	SCALANCE S612	6GK5612-0BA00-2AA3
SIMATIC NET	SCALANCE S613	6GK5613-0BA00-2AA3

EMV-Richtlinie

Richtlinie 89/336/EWG "Elektromagnetische Verträglichkeit"

Einsatzbereich

Das Produkt ist ausgelegt für den Einsatz im Industriebereich:

Einsatzbereich	Anforderungen an	
	Störaussendung	Störfestigkeit
Industriebetrieb	EN 61000-6-4 : 2001	EN 61000-6-2 : 2001

Aufbaurichtlinien beachten

Das Produkt erfüllt die Anforderungen, wenn Sie bei Installation und Betrieb die Aufbaurichtlinien und Sicherheitshinweise einhalten, die in dieser Beschreibung sowie im Handbuch "SIMATIC NET Industrial Ethernet TP- und Fiber Optic Netze" /1/ beschrieben sind.

Konformitätserklärung

Die EG-Konformitätserklärung wird gemäß den obengenannten EG-Richtlinien für die zuständigen Behörden zur Verfügung gehalten bei:

Siemens Aktiengesellschaft
Bereich Automatisierungs- und Antriebstechnik
Industrielle Kommunikation (A&D SC IC)
Postfach 4848
D-90327 Nürnberg

Hinweise für Hersteller von Maschinen

Das Produkt ist keine Maschine im Sinne der EG-Richtlinie Maschinen. Es gibt deshalb für dieses Produkt keine Konformitätserklärung bezüglich der EG-Richtlinie Maschinen 89/392/EWK.

Ist das Produkt Teil der Ausrüstung einer Maschine, muss es vom Maschinenhersteller in das Verfahren zur Konformitätserklärung einbezogen werden.

Literaturverzeichnis

C

/1/

SIMATIC NET Industrial Twisted Pair- and Fiber Optic Netze, Ausgabe 05/2001

Bestellnummern:
6GK1970-1BA10-0AA0 deutsch
6GK1970-1BA10-0AA1 englisch
6GK1970-1BA10-0AA2 französisch
6GK1970-1BA10-0AA4 italienisch

/2/

Das GPRS/GSM-Modem SINAUT MD740-1 Systemhandbuch ist verfügbar unter:

http://support.automation.siemens.com/WW/view/de/23940893

Maßzeichnung

D

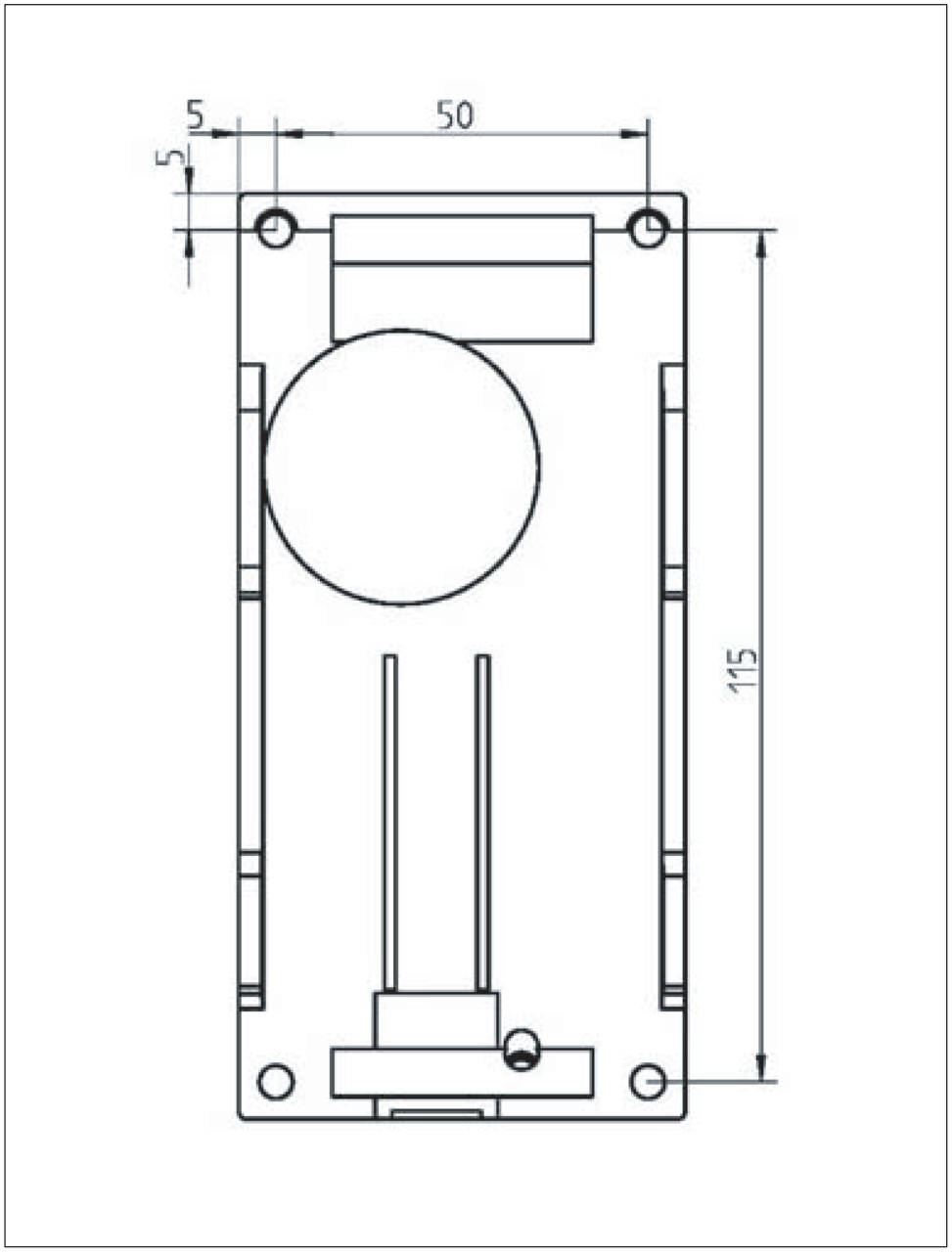


Bild D-1 Bohrschablone

Dokument-Historie

E

E.1 Dokument-Historie

Das war neu in Ausgabe 02 dieses Handbuchs

- **neues Modul SCALANCE S602**

  Mit SCALANCE S602 steht ein weiteres Modul in der Palette skalierbarer Sicherheitsfunktionalität zur Verfügung. SCALANCE S602 schützt mit Stateful Inspection Firewall, NAT/NAPT-Routing, DHCP-Server und Syslog.

Das war neu in Ausgabe 03 dieses Handbuchs

- **Routing-Modus bei SCALANCE S612 / S613**

  Die SCALANCE S-Module S612 und S613 stehen mit erweiterter Funktionalität zur Verfügung; unterstützt werden jetzt zusätzlich NAT/NAPT-Routing, DHCP-Server und Syslog.

- **Security Configuration Tool V2.1**

  Mit der neuen Version des Projektierwerkzeuges können Sie die Module S612 / S613 mit ihren neuen Funktionen projektieren.

- **Konfigurations-Daten für MD 740-1**

  Um einen externen MD 740-1 zu konfigurieren, können Sie mit der neuen Version des Security Configuration Tools Konfigurationsdaten erzeugen.

Das war neu in Ausgabe 04 dieses Handbuchs

- Ausgabe wurde nicht publiziert -

Das war neu in Ausgabe 05 dieses Handbuchs

In dieser Ausgabe wurden unter anderem folgende neue Funktionen berücksichtigt:

- **Security Configuration Tool V2.2**

  Ein SOFTNET Security Client kann zusammen mit einem SCALANCE S im Routing Modus konfiguriert werden. (GETTING STARTED Beispiel – Fernzugriff)

  Neben dem direkten internen Subnetz, welches am SCALANCE S anliegt, können im Routing-Modus weitere Subnetze konfiguriert und somit erreicht werden.

- **SOFTNET Security Client V2.0**

  In der Tunnelübersicht ist ein Textfeld mit Diagnoseinformationen zum Verbindungsaufbau hinzugekommen.

  Die Netzwerkadaptereinstellung wurde durch einen Automatismus vereinfacht. Der SOFTNET Security Client versucht beim Start automatisch eine passende Netzwerkadaptereinstellung zu finden.

- **Konfigurationsdaten für Modul MD 741-1**

  Um einen externen MD 741-1 zu konfigurieren, können Sie mit der neuen Version des Security Configuration Tools Konfigurationsdaten erzeugen.

Das war neu in Ausgabe 06 dieses Handbuchs

- **SOFTNET Security Client V3.0**

  Neben den Betriebssystemen Windows XP SP2 und Windows XP SP3 wird das Betriebssystem Windows 7 unterstützt (nicht die Home-Version).

Glossar / Abkürzungsverzeichnis

AAA

AAA steht für die Zusammenfassung eines Sicherheitskonzeptes unter dem die Begriffe Authentication, Authorization und Accounting fallen.

AES

Advanced Encryption Standard

Eine symmetrische Blockchiffre. Sie kann beim SCALANCE S zum Verschlüsseln der Daten ausgewählt werden.

ARP

Address Resolution Protocol

Ein Protokoll, das zur Adressauflösung dient. Es erfüllt die Aufgabe, zu einer gegebenen Protokoll-Adresse die korrespondierende Netzwerk-Hardware-Adresse (MAC-Adresse) herauszufinden. Auf Hosts, auf denen die Internet-Protokoll-Familie benutzt wird, ist oft auch eine ARP-Protokoll-Implementation anzutreffen. Durch IP wird ein virtuelles Netzwerk mit Hilfe der IP-Adressen gebildet. Diese müssen beim Transport der Daten auf die gegebenen Hardware-Adressen abgebildet werden. Um diese Abbildung vorzunehmen, wird oft das ARP-Protokoll benutzt.

Bandbreite

Maximaler Durchsatz einer Verbindungsleitung (Angabe normalerweise in bps).

BDC

Backup Domain Controller

Die Backup Domain Controller halten eine Sicherheitskopie der User- und Anmeldedaten, die in regelmäßigen Abständen aktualisiert werden.

BRI

Basic Rate Interface

Standard-Netzanschluss an das ISDN.

CA

Certification Authority

Zertifizierungsstelle, die der Authentifizierung sowie zur Verschlüsselung und Entschlüsselung vertraulicher Daten dient, die über das Internet und andere Netze verbreitet werden, indem sie beispielsweise digitale Zertifikate herausgibt und diese signiert.

CA-Zertifikat

Eine Zertifizierungsstelle (englisch Certificate Authority, kurz CA) ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist bei der Kommunikation in Computernetzen das Äquivalent zu einem Personalausweis. Eine Zertifizierungsstelle vergibt Zertifikate an Netzwerksteilnehmer und beglaubigt diese.

Beim SCALANCE S wird jeweils für eine Gruppe ein CA-Zertifikat erzeugt. Die Gruppe vergibt Zertifikate an die Gruppenmitglieder und beglaubigt diese mit dem Gruppenzertifikat (Gruppenzertifikat = CA-Zertifikat).

CHAP

Challenge Handshake Authentication Protocol

Authentifizierungsprotokoll, das im Rahmen von Point-to-Point Protocol (PPP) eingesetzt wird. PPP ist auf der Sicherungsschicht in der Internetprotokollfamilie angesiedelt.

Client

Unter Client wird ein Gerät, oder allgemein ein Objekt verstanden, das einen -> Server auffordert, einen Dienst zu erbringen.

CTRL

Das Control-Feld (CTRL) enthält Steuerinformation für das LLC Protokoll .Logical Link Control (LLC) ist die Bezeichnung für ein Netzwerkprotokoll das vom IEEE standardisiert wurde. Es ist ein Protokoll, dessen Hauptzweck in der Datensicherung auf der Verbindungsebene liegt, und gehört daher zur Schicht 2 des OSI-Modells.

Data Encryption Standard

Methode zum Verschlüsseln von Daten (56-Bit-Verschlüsselung)

DCP

Discovery and basic Configuration Protocol

Ein Protokoll, das geeignet ist, Adressparameter von PROFINET-Komponenten zu ermitteln.

DES

Data Encryption Standard

Ein symmetrischer Verschlüsselungsalgorithmus

DES3

Data Encryption Standard

Ein symmetrisches Verschlüsselungsverfahren, d. h. zur Verschlüsselung und zur Entschlüsselung der Daten wird der gleiche Schlüssel verwendet. DES3 bedeutet, dass der Algorithmus dreimal angewendet wird, um die Sicherheit zu erhöhen.

DHCP

Dynamic Host Configuration Protocol

Sie können SCALANCE S am internen Netz als DHCP-Server betreiben. Damit ist es möglich, den am internen Netz angeschlossenen Geräten automatisch IP-Adressen zuzuweisen. Die IP-Adressen werden hierbei entweder dynamisch aus einem von Ihnen vergebenen Adressband zugewiesen oder es wird gemäß Ihrer Vorgabe eine bestimmte IP-Adresse einem bestimmten Gerät zugewiesen.

Dienste

Angebotene Leistungen eines Kommunikationsprotokolls.

Diffie-Hellmann-Gruppen

wählbare kryptographische Algorithmen im Oakley-Schlüsselaustausch-Protokoll

Diffie-Hellmann-Schlüsselvereinbarung

Verfahren zum sicheren Austausch von geheimen Schlüsseln über eine unsichere Leitung.

DMZ

Demilitarized Zone

Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.

Encapsulating Security Payload

Protokoll für sichere Datenübertragung

ESP

Encapsulating Security Payload

Das ESP-Protokoll stellt sicher, dass übertragene Daten authentisch, integer und vertraulich sind. ESP erlaubt es auch, dass nur die Authentizität von Daten geprüft wird oder nur Daten verschlüsselt werden. Beim SCALANCE S wird ESP immer mit Authentizitätsprüfung und Verschlüsselung verwendet.

HTTPS

Secure Hypertext Transfer Protocol bzw. HyperText Transfer Protocol Secured Socket Layer (SSL)

Protokoll für die Übertragung verschlüsselter Daten. Erweiterung von HTTP für die geschützte Übertragung von vertraulichen Daten mit Hilfe von SSL.

ICMP

Internet Control Message Protocol

ist ein Hilfs-Protokoll der IP-Protokoll-Familie und baut auf dem IP-Protokoll auf. Es dient zum Austausch von Informations- und Fehlermeldungen.

ICMP-Echo-Request

Ausgehendes Ping-Paket zur Überprüfung der Erreichbarkeit eines Netzwerkteilnehmers.

ICMP-Subnetz-Broadcast

Um die IP-Knoten im internen Netz zu finden, sendet SCALANCE S ein ICMP-Echo-Request mit der IP-Subnetz-Broadcast-Adresse, d.h. einer Adresse, die sich an alle IP-Knoten im internen Subnetz des SCALANCE S wendet.

Identity-Protection

Der Unterschied zwischen Main- und Aggressive Mode ist die "Identity-Protection", die im Main Mode verwendet wird. Die Identität wird im Main Mode verschlüsselt übertragen, im Aggressive Mode nicht.

IKE

Internet Key Exchange

Protokoll für die automatische Schlüsselverwaltung für IPsec. IKE arbeitet in zwei Phasen. In der ersten Phase authentifizieren sich die beiden Teilnehmer, die gesichert miteinander kommunizieren. Die Authentifizierung kann entweder über Zertifiakte oder über vorher ausgetauschte Schlüssel (Pre Shared Keys) erfolgen. In der zweiten Phase werden die Schlüssel für die Datenkommunikation ausgetauscht und die Verschlüsselungsalgorithmen ausgewählt.

Internet Key Exchange (IKE)

Protokoll zum Aufbau der IPsec-Tunnel. Hier können Sie Parameter für das Protokoll des IPSec-Schlüssel-Managements einstellen. Der Schlüsselaustausch erfolgt über das standardisierte Verfahren IKE. (IKE-Einstellungen)

IP Subnet ID

Netz-ID des Subnetzes: Anhand der Netz-ID erkennt der Router, ob eine Ziel -Adresse im Subnetz oder außerhalb liegt.

IP/MAC-Dienst Definition

Mithilfe der IP-Dienst-Definitionen können Sie Firewall-Regeln kompakt und übersichtlich definieren. Sie vergeben hierbei einen Namen und ordnen diesem die Dienst-Parameter zu.

Zusätzlich können Sie so definierte Dienste wiederum unter einem Gruppennamen zu Gruppen zusammenfassen. Bei der Projektierung der Paketfilter-Regel verwenden Sie dann einfach diese Namen.

IP-Verkehr

Bezeichnet die Kommunikation in Computernetzwerken, die das IP-Protokoll als Netzwerkprotokoll verwendet.

ISAKMP

Internet Security Association and Key Management Protocol

Protokoll zum Aufbau von Security Associations (SA) und Austausch von kryptographischen Schlüsseln im Internet.

ISO-Netzknoten

Netzknoten, die zwar nicht IP-fähig sind, jedoch über ISO-Protokolle ansprechbar sind.

ISP

Internet Service Provider

Anbieter für Internet-Dienste

L2F

Layer 2 Forwarding

Netzwerkprotokoll (ähnlich PPTP), das verschiedene Protokolle und mehrere unabhängige Tunnel unterstützt.

L2TP

Layer 2 Tunneling Protocol

Netzwerkprotokoll, das Frames von Protokollen der Sicherungsschicht (Schicht 2) des OSI-Modells zwischen zwei Netzwerken über das Internet tunnelt um ein virtuelles privates Netzwerk (VPN) herzustellen.

Logging

Ereignisse können aufgezeichnet werden. Die Aufzeichnung erfolgt in sogenannte Log-Files (kurz Log genannt). Sie können bereits in der Konfiguration festlegen, welche Daten aufgezeichnet werden sollen und ob die Aufzeichnung bereits mit dem Laden der Konfiguration eingeschaltet werden soll.

MAC-Paketfilter-Regel

Mittels MAC-Paketfilter -Regeln können Sie auf MAC-Telegramme filtern.

MAC-Protokoll

Zugriffssteuerung auf ein Übertragungsmedium

Maximum Transmission Unit

MTU

Legt die zulässige Größe eines Datenpaketes für die Übertragung im Netzwerk fest.

MD

Message Digest

Bezeichnet eine Gruppe kryptografischer Protokolle.

MD5

Message Digest Version 5

Eine weit verbreitete kryptographische Hashfunktion. MD5 wird von einer Vielzahl von Sicherheitsanwendungen eingesetzt, um die Integrität von Daten zu verifizieren. Beim SCALANCE S kann MD5 für die Integritätsprüfung der Daten, die in einem Tunnel übertragen werden, ausgewählt werden.

MDI/MDI-X Autocrossing Funktion

Die MDI/MDI-X Autocrossing Funktion bietet den Vorteil einer durchgängigen Verkabelung, ohne dass externe, gekreuzte Ethernet-Kabel erforderlich sind. Fehlfunktionen bei vertauschten Send- und Empfangsleitungen werden dadurch verhindert. Die Installation wird dadurch für den Anwender wesentlich vereinfacht.

NAPT

Network Address Port Translation

ein Verfahren, bei dem in einem Router eine IP-Adresse durch eine andere IP-Adresse und zusätzlich die Port-Nummer durch eine andere Port-Nummer in einem Telegramm ersetzt wird.

NAT

Network Address Translation

ein Verfahren, bei dem in einem Router eine IP-Adresse in einem Telegramm durch eine andere ersetzt wird.

NAT/NAPT-Router

Durch diese Technik erreichen Sie, dass die Adressen der Teilnehmer im internen Subnetz nach außen im externen Netz nicht bekannt werden; sie sind im externen Netz nur über die in der Umsetzungsliste definierten externen IP-Adressen sichtbar.

NAT-Traversal

Ist ein Verfahren, bei dem IPsec-Daten ermöglicht wird NAT-Geräte zu passieren.

Oakley Schlüsselaustausch-Protokoll

Das OAKLEY Key Determination Protocol beschreibt die Erzeugung von geheimen Schlüsselmaterial. Es ist Teil des Internet-Key-Exchange-Protocols (IKE).

One Shot Buffer

Die Aufzeichnung stoppt, wenn der Puffer voll ist.

Organizationally Unique Identifier

Bezeichnet die ersten 3 Bytes der MAC Adresse = Hersteller-Identifizierung.

OUI

Organizationally Unique Identifier

24-Bit Zahl, die von der IEEE Registration Authority an Firmen vergeben wird. Firmen verwenden die OUI für verschiedene Hardware-Produkte unter Anderem als die ersten 24 Bit der MAC-Adresse.

Paketfilter-Regel

Mit Paketfilter-Regeln definieren Sie, ob ein Datenpaket den Paketfilter passieren kann oder nicht. Die Entscheidung, ob ein Paket passieren darf oder nicht, wird anhand von Protokollfeldern getroffen. Beipiele für Protokollfelder sind die IP-Quell- bzw. die IP-Ziel-Adresse. Auf dem SCALANCE S können Filterregeln für MAC- oder für IP-Protokolle angegeben werden.

PAP

Password Authentication Protocol

Passwort-Authentifizierungsprotokoll

PEM

Privacy Enhanced Mail; Privacy Enhanced Mail

ist ein Standard für die Verschlüsselung von E-Mails im Internet

Perfect Forward Secrecy

Perfect Forward Secrecy

versichert, dass neue Schlüssel-Aushandlungen nicht mit vorhergehenden Schlüsseln in Verbindung stehen. Ausschalten dieser Option gestattet schnellere, aber weniger sichere Verschlüsselung.

PGP

Pretty Good Privacy

ist ein Programm zur Verschlüsselung und zum Unterschreiben von Daten.

Ping

Bezeichnet ein Testprotokoll der IP-Protokoll-Familie. Dieses Protokoll ist auf jedem MS-Windows-Rechner unter dem gleichen Namen als Konsolen-Anwendung (Kommandozeilen-Ebene) vorhanden. Mit "Ping" können Sie von einem IP-Netzknoten innerhalb des Netzverbundes eine Antwort (Lebenszeichen) anfordern, sofern Sie dessen IP-Adresse kennen. So können Sie feststellen, ob dieser Netzknoten auf IP-Ebene erreichbar ist und damit die Wirksamkeit der konfigurierten SCALANCE S-Funktionalität überprüfen.

PKCS

Public Key Cryptography Standards

sind Spezifikationen zu kryptographischen Schlüsseln, die von RSA Security und Anderen entwickelt wurden. Ein Zertifikat verknüpft Daten eines kryptographischen Schlüssels (oder Schlüsselpaars, bestehend aus öffentlichem und privatem Schlüssel) mit Daten des Inhabers und einer Zertifizierungsstelle.

PKCS#12-Format

Dieser Standard legt ein PKCS-Format fest, das für den Austausch des öffentlichen Schlüssels sowie zusätzlich des kennwortgeschützten privaten Schlüssels geeignet ist.

PKI

Public Key Infrastructure

bezeichnet in der Kryptologie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.

PoP

Point of Presence

Einwahlknoten eines Internet Providers

PPP

Point-to-Point Protocol - Punkt-zu-Punkt-Protokoll

PPTP

Point-to-Point Tunneling Protocol

ist ein Protokoll zum Aufbau eines Virtual Private Network (VPN). Es ermöglicht das Tunneln des PPP durch ein IP-Netzwerk.

Preshared Keys

Bezeichnet ein symmetrisches Schlüssel-Verfahren. Der Schlüssel muss beiden Seiten vor der Kommunikation bekannt gemacht werden. Dieser Schlüssel wird beim Anlegen einer Gruppe ebenfalls automatisch erzeugt. Jedoch müssen im Security Configuration Tool-Dialog "Group Properties" im Feld "Key" zuvor ein Passwort eingeben haben, aus dem dieser Schlüssel generiert wird.

PST (-Tool)

Primary Setup Tool

Mit dem Primary Setup Tool (PST) können Sie SIMATIC NET-Netzwerkkomponenten, SIMATIC NET Ethernet-CPs und Netzwerkübergängen eine Adresse zuweisen (z.B. IP-Adresse).

PSTN

Public Switched Telephone Network

öffentliches Kommunikationssystem für den Sprechverkehr zwischen entfernten Teilnehmern.

Public Key-Verfahren

Der Sinn von Verschlüsselungsverfahren mit öffentlichem Schlüssel besteht darin, daß das Sicherheitsrisiko beim gegenseitigen Schlüsselaustausch gänzlich vermieden wird. Jeder hat ein Schlüsselpaar mit einem öffentlichen und einem geheimen Schlüssel. Zum Verschlüsseln einer Nachricht benutzt man den öffentlichen Schlüssel des Empfängers, und nur dieser kann sie mit seinem geheimen Schlüssel wieder entschlüsseln.

RAS

Remote-Access Service

Mit dem Remote Access Service haben Sie die Möglichkeit, Clients über eine Modem-, ISDN- oder X.25-Verbindung mit dem lokalen Netzwerk zu verbinden. Dabei werden nicht nur unterschiedliche Clients unterstützt, sondern es besteht auch eine große Flexibilität in der Auswahl und Kombinationsmöglichkeit der verwendeten Netzwerkprotokolle.

RSA

Rivest, Shamir & Adleman Algorithm

ist ein asymmetrisches Kryptosystem, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann. Es verwendet ein Schlüsselpaar bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nicht oder nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

Secure Hash Algorithm 1

Algorithmus zur Verifizierung von Daten

Security Configuration Tool

SCT

Projektierwerkzeug für SCALANCE S Produkte.

Server

Ein Server ist ein Gerät, oder allgemein ein Objekt, das bestimmte Dienste erbringen kann; aufgrund der Anforderung durch einen -> Client wird der Dienst erbracht.

SHA1

Secure Hash Algorithm 1

Weit verbreitete kryptographische Hashfunktion. Beim SCALANCE S kann SHA1 für die Integritätsprüfung der Daten, die in einem Tunnel übertragen werden, ausgewählt werden.

SIMATIC NET

Siemens SIMATIC Network and Communication. Produktbezeichnung für Netze und Netzkomponenten bei Siemens. (bisher SINEC)

SNAP

Subnetwork Access Protocol

Mechanismus um in Netzwerken, die IEEE 802.2 LLC verwenden, Protokolle zu multiplexen.

SOHO

Small Office, Home Office

SSL-Verbindung

Das SSL-Protokoll ist zwischen dem TCP (OSI-Layer 4) und den Übertragungsdiensten (wie z.B. HTTP, FTP, IMAP etc.) angesiedelt und dient einer gesicherten Transaktion. SSL sorgt hierbei dafür, dass der Anwender eindeutig mit dem gewünschten Server verbunden ist (Authentisierung) und dass die sensiblen Daten über eine gesicherte (verschlüsselte) Verbindung übertragen werden.

SSL-Zertifikat

SSL-Zertifikate werden für die Authentifizierung der Kommunikation zwischen

PG/PC und SCALANCE S beim Laden der Konfiguration sowie beim Logging herangezogen.

SSN = DMZ

Secure Server Net = Demilitarized Zone

Stateful Packet Inspection

Stateful Inspection (auch Stateful Packet Filter oder Dynamic Packet Filter) ist eine Firewall-Technologie und arbeitet sowohl auf der Netz- als auch auf der Anwendungsschicht. Die IP-Pakete werden auf der Netzschicht entgegengenommen, von einem Analysemodul zustandsabhängig inspiziert und gegenüber einer Zustandstabelle abgeglichen. Für die Kommunikationspartner stellt sich eine Firewall mit Stateful Inspection als eine direkte Leitung dar, die nur für eine den Regeln entsprechende Kommunikation durchlässig ist.

Syslog

Ein Dienst, der auf einem Server (Syslog-Server) System-Meldungen entgegennimmt und beispielsweise in Log-Dateien aufzeichnet.

TACACS

Terminal Access Controller Access Control System; Das Terminal Access Controller Access Control System (TACACS) ist ein AAA-Protokoll. Es dient der Client-Server-Kommunikation zwischen AAA-Servern und einem Network Access Server (NAS). TACACS-Server stellen eine zentrale Authentifizierungsinstanz für entfernte Benutzer zur Verfügung, die eine IP-Verbindung mit einem NAS herstellen möchten.

Tunnel

Tunnel bzw. Tunneling bezeichnet den Gebrauch des Kommunikationsprotokolls eines Netzwerkdienstes als Transportmittel für Daten, die nicht zu diesem Dienst gehören.

VLAN-Kennzeichnung

Ein Ethernet-Paket hat eine VLAN-Kennzeichnung, wenn das Feld EtherType im Ethernet-Paket-Header einen bestimmten Wert hat. Der Ethernet-Paket-Header enthält in diesem Fall Informationen zu virtuellen LAN und unter Umständen auch eine Paket-Priorität.

Index

I

K

L

M

N

O

P

R

S

T

U

V

W

Z