SIEMENS

# SIMATIC NET

# SCALANCE S and SOFTNET Security Client

## Operating Instructions

**Appendix**

**Release 1/2005**
**C79000-G8976-C196-01**

## Classification of Safety-Related Notices

This manual contains notices which you should observe to ensure your own personal safety, as well as to protect the product and connected equipment. These notices are highlighted in the manual by a warning triangle and are marked as follows according to the level of danger:

**Danger**

indicates that death or severe personal injury **will** result if proper precautions are not taken.

**Warning**

indicates that death or severe personal injury **can** result if proper precautions are not taken.

**Caution**

with a warning triangle indicates that minor personal injury can result if proper precautions are not taken.

**Vorsicht**

without a warning triangle indicates that damage to property can result if proper precautions are not taken.

**Notice**

indicates that an undesirable result or status can occur if the relevant notice is ignored.

**Note**

highlights important information on the product, using the product, or part of the documentation that is of particular importance and that will be of benefit to the user.

## Trademarks

SIMATIC®, SIMATIC HMI® and SIMATIC NET® are registered trademarks of SIEMENS AG.

Third parties using for their own purposes any other names in this document which refer to trademarks might infringe upon the rights of the trademark owners.

## Safety instructions regarding your product:

Before you use the product described here, read the safety instructions below thoroughly.

## Qualified personnel

Only **qualified personnel** should be allowed to install and work on this equipment. Qualified persons in the sense of the safety-related notices in this manual are defined as persons who are authorized to commission, to ground, and to tag circuits, equipment, and systems in accordance with established safety practices and standards.

## Correct usage of hardware products

Note the following:

⚠ **Warning**

This device may only be used for the applications described in the catalog or the technical description, and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens.

This product can only function correctly and safely if it is transported, stored, set up, and installed correctly, and operated and maintained as recommended.

Before you use the supplied sample programs or programs you have written yourself, make sure that no injury to persons nor damage to equipment can result in systems in operation.

EU directive: Do not start up until you have established that the machine on which you intend to run this component complies with the directive 89/392/EEC.

## Correct usage of software products

Note the following:

⚠ **Warning**

This software may only be used for the applications described in the catalog or the technical description, and only in connection with software products, devices or components from other manufacturers which have been approved or recommended by Siemens.

Before you use the supplied sample programs or programs you have written yourself, make sure that no injury to persons nor damage to equipment can result in systems in operation.

### Prior to startup

Before putting the product into operation, note the following warning:

**Vorsicht**

Before installation and startup, read the instructions in the corresponding current documentation. For ordering data, please refer to the catalogs or contact your local Siemens representative.

**Disclaimer**

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. We would be thankful for any suggested improvements.

Siemens AG
Automation and Drives
Industrial Communication
Postfach 4848, D90327 Nürnberg

Subject to technical change.

# This manual...

...supports you when commissioning the SCALANCE S612/S613 Security Module and the SOFTNET Security Client. The variants SCALANCE S612/S613 are simply called SCALANCE S in the rest of the manual.

## Validity of this manual

This manual is valid for the following devices and components:

| | |
|---|---|
| • SIMATIC NET SCALANCE S612 | 6GK5 612-0BA00-2AA3 |
| • SIMATIC NET SCALANCE S613 | 6GK5 613-0BA00-2AA3 |
| • SIMATIC NET SOFTNET Security Client | 6GK1 704-1VW01-0AA0 |

## Audience

This manual is intended for personnel involved in the commissioning of the SCALANCE S Security Module and the SOFTNET Security Client in a network.

## Further Documentation

The ”SIMATIC NET Industrial Ethernet Twisted Pair and Fiber Optic Networks“ manual contains additional information on other SIMATIC NET products that you can operate along with the SCALANCE S security module in an Industrial Ethernet network.

You can download this network manual in electronic format from Customer Support at the following address:

http://www4.ad.siemens.de/view/cs/en/1172207

## Standards and Approvals

The SCALANCE S device meets the requirements for the CE mark. For more detailed information, refer to the appendix of this manual.

## Symbols used in this manual

This symbol highlights special tips in the manual.

This symbol indicates specific further reading material.

This symbol indicates that detailed help texts are available in the context help. You can call this with the F1 key or using the ”Help” button in the relevant dialog.

## Further reading /.../

References to other documentation are shown in slashes /.../. Based on these numbers, you can find the title of the documentation in the references at the end of the manual.

# Contents

## Appendix

# 1 Introduction and basics

With SIMATIC NET SCALANCE S and SIMATIC NET SOFTNET Security Client, you have chosen the SIEMENS security concept that meets the exacting requirements of protected communication in industrial automation engineering.

This chapter provides you with an overview of the security functions of the devices and components.

- SCALANCE S Security Module
- SOFTNET Security Client

Tip: To get started quickly with the SCALANCE S, work through Chapter 3 ”Getting started”

## 1.1 Uses of the SCALANCE S and SOFTNET Security Client

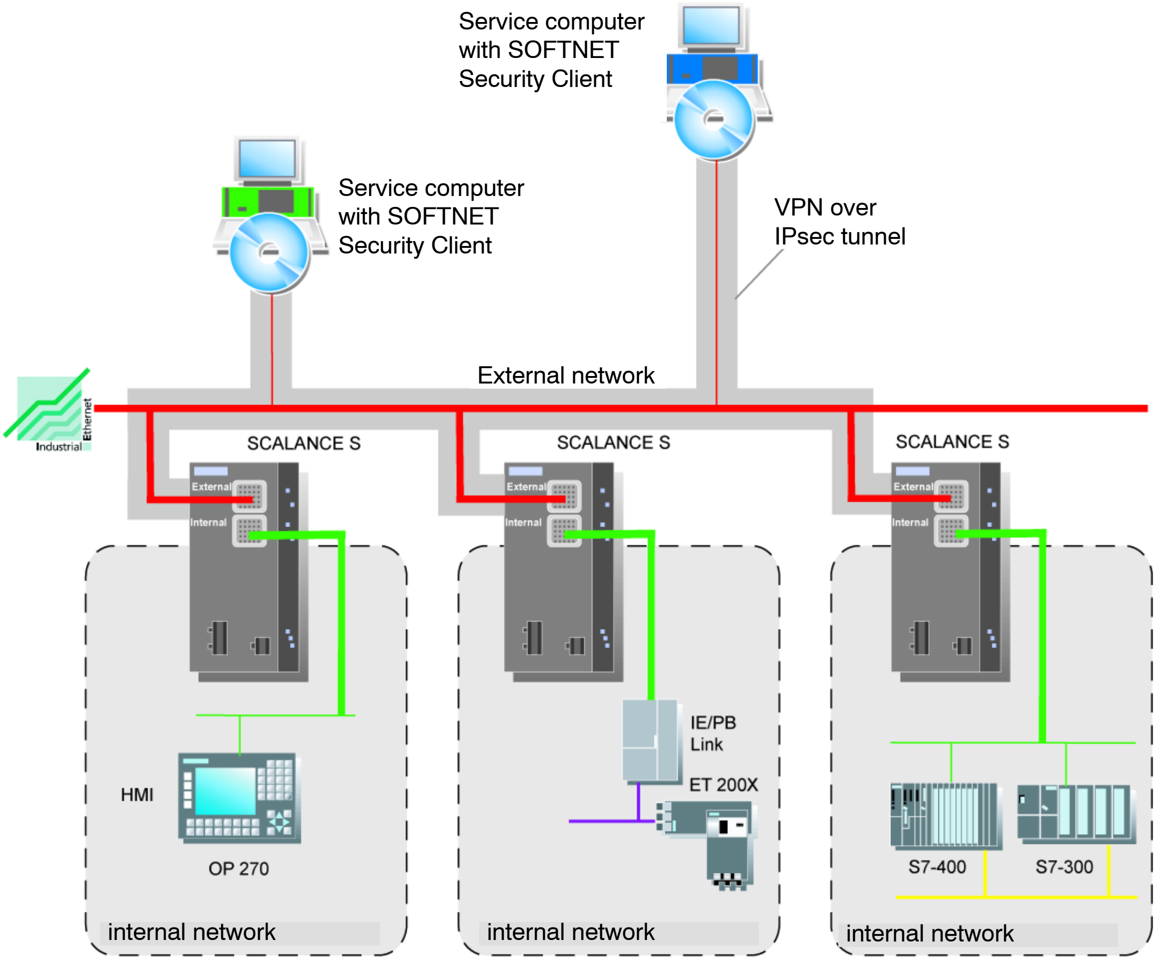
### All-round protection - the job of SCALANCE S

With a combination of different security measures such as firewall and VPN (Virtual Private Network) through an IPsec tunnel, SCALANCE S protects individual devices or even entire automation cells:

- Data espionage;
- Data manipulation;
- Unauthorized access;
- Automated break-in attempts

SCALANCE S allows this protection flexibly, without repercussions, protocol-independent (as of Layer 2 according to IEEE 802.3) and without complicated handling.

SCALANCE S is configured with the Security Configuration Tool.



## PC/PG communication in the VPN - job of the SOFTNET Security Client

With the SOFTNET Security Client PC software, secure IP-based access is possible from PCs/PGs to automation systems in subnets protected by SCALANCE S.

With the SOFTNET Security Client, a PC/PG is configured automatically so that it can establish secure IPsec tunnel communication in the VPN (Virtual Private Network) with one or more SCALANCE S devices.

PG/PC applications such as NCM Diagnostics or STEP 7 can then access devices or networks in an internal network protected by SCALANCE S over a secure tunnel connection.

The SOFTNET Security Client PC software is also configured with the Security Configuration Tool; ensuring fully integrated configuration without any special security know-how.

## Internal and external network nodes

SCALANCE S device networks into two areas:

- Internal network: Protected areas with the ”internal nodes”

  Internal nodes are all the nodes secured by a SCALANCE S.
- External network: Unprotected areas with the ”external nodes”

  External nodes are all the nodes located outside the protected areas.

**Notice**

The internal network is considered to be secure (trustworthy).

Connect an internal network segment to the external network segments only over SCALANCE S.

There must be no other paths connecting the internal and external network!

## 1.2 Characteristics of SCALANCE S

SCALANCE S has the following essential characteristics:

### Hardware

- Robust housing with degree of protection IP30
- Optional mounting on an S7-300 or DIN 35 mm rail
- Redundant power supply
- Signaling contact
- Extended temperature range (-20 °C to +70 °C SCALANCE S613)

### Security functions

- Firewall
  - IP firewall with stateful packet inspection;
  - Firewall also for Ethernet ”non-IP” frames according to IEEE 802.3 (Layer 2 frames);

  All network nodes located in the internal network segment of a SCALANCE S are protected by its firewall.
- Secure communication through IPsec tunnel (VPN, Virtual Private Network).

  SCALANCE S devices can be configured to form groups. IPsec tunnels are established between all the SCALANCE S devices of a group. All internal nodes of this SCALANCE S can communicate securely with each other through these tunnels.
- Protocol-independent

  Tunneling includes all Ethernet frames according to IEEE 802.3 (Layer 2 frames).

  Both IP and non-IP frames are transmitted through the IPsec tunnel.

- Protection for devices and network segments

  The firewall and VPN protective function can be applied to the operation of single devices, several devices, or entire network segments.

- No repercussions when included in existing networks

  Internal network nodes can be found without configuration. If a SCALANCE S is included in an existing network infrastructure, this does not mean that new settings need to be made for the end devices; in other words, division into IP subnets is not necessary.

## Configuration and administration

- Configuration without expert IT knowledge with the Security Configuration Tool

  With the Security Configuration Tool, a SCALANCE S module can be set by non IT experts. When necessary, more complex settings can be made in an extended mode.

- Secure administrative communication

  The settings on the SCALANCE S are made over an SSL-encrypted channel.

- Access protection in the Security Configuration Tool

  The user administration of the Security Configuration Tool includes access protection for the SCALANCE S devices and the configuration data.

- C-PLUG exchangeable memory medium can be used

  The C-PLUG is a plug-in memory medium on which the encrypted configuration data can be stored. It allows configuration without a PC/PG when replacing a SCALANCE S.

# 2 Product properties and commissioning

This chapter will familiarize you with the handling and all-important properties of the SCALANCE S device.

You will learn how the device can be installed and commissioned in a few simple steps.

## Further information

How to configure the device for standard applications is shown in a condensed form in the Chapter 3 GETTING STARTED.

For details on configuration and the online functions, refer to the reference section starting at Chapter 4 of the manual.

## 2.1 Product Characteristics

**Note**

The specified approvals apply only when the corresponding mark is printed on the product.

### 2.1.1 Components of the Product

**What ships with the SCALANCE S?**

- SCALANCE S device
- 2-pin plug-in terminal block
- 4-pin plug-in terminal block
- Information on the Product
- CD with
  - Manual
  - Security Configuration Tool

### 2.1.2 Unpacking and Checking

**Unpacking, Checking**

1. Make sure that the package is complete
2. Check all the parts for transport damage.

**Warning**

Do not use any parts that show evidence of damage!

### 2.1.3 Attachment to Ethernet

#### Possible attachments

The SCALANCE S has 2 RJ-45 jacks for attachment to Ethernet.

**Note**

TP cords or TP-XP cords with a maximum length of 10 m can be connected at the RJ-45 TP port.

In conjunction with the Industrial Ethernet FastConnect IE FC Standard Cable and IE FC RJ-45 Plug 180, a total cable length of maximum 100 m is possible between two devices.

**Notice**

The Ethernet attachments at port 1 and port 2 are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network.

- Port 1 - external network
  Upper RJ-45 jack, marked red = unprotected network area;
- Port 2 - internal network
  Lower RJ-45 jack, marked green = network protected by SCALANCE S;

If the ports are swapped over, the device loses its protective function.

#### Autonegotiation

SCALANCE S supports autonegotiation.

Autonegotiation means that the connection and transmission parameters are negotiated automatically with the addressed network node.

**Note**

Devices not supporting autonegotiation must be set to 100 Mbps/ half duplex or 10 Mbps half duplex.

## MDI /MDIX autocrossover function

SCALANCE S supports the MDI / MDIX autocrossover function.

The advantage of the MDI /MDIX autocrossover function is that straight-through cables can be used throughout and crossover Ethernet cables are unnecessary. This prevents malfunctions resulting from mismatching send and receive wires. This greatly simplifies installation.

### 2.1.4 Power supply

**Warning**

The SCALANCE S is designed for operation with safety extra-low voltage. This means that only safety extra-low voltages (SELV) complying with IEC950/EN60950/ VDE0805 can be connected to the power supply terminals.

The power supply unit to supply the SCALANCE S must comply with NEC Class 2 (voltage range 18 - 32 V, current requirement 250 mA)

The device may only be supplied by a power unit that meets the requirements of class 2 for power supply units of the ”National Electrical Code, Table 11 (b)”. If the device is connected to a redundant power supply (two separate power supplies), both must meet these requirements.

**Notice**

Never connect the SCALANCE S to AC voltage or to DC voltage higher than 32 V DC.

The power supply is connected using a 4-pin plug-in terminal block. The power supply can be connected redundantly. Both inputs are isolated. There is no distribution of load. When a redundant power supply is used, the power supply unit with the higher output voltage supplies the SCALANCE S alone. The power supply is connected over a high resistance with the enclosure to allow an ungrounded set up.

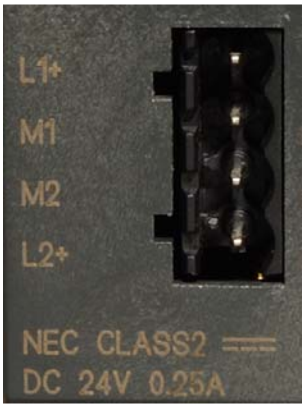


Figure 2-1 Power Supply

### 2.1.5 Signaling contact

**Notice**

The signaling contact can be subjected to a maximum load of 100 mA (safety extra-low voltage (SELV), DC 24 V).

Never connect the SCALANCE S to AC voltage or to DC voltage higher than 32 V DC.

The signaling contact is connected to a 2-pin plug-in terminal block. The signaling contact is a floating switch with which error/fault states can be signaled by breaking the contact.

The following errors/faults can be signaled by the signaling contact:

- Fault in the power supply,
- internal fault.

If a fault occurs or if no power is applied to the SCALANCE S, the signaling contact is opened. In normal operation, it is closed.

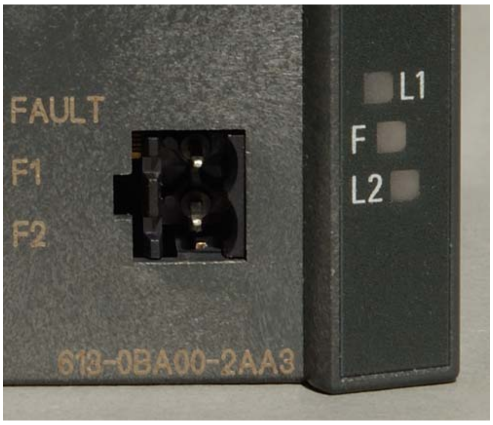


Figure 2-2 Signaling contact

### 2.1.6 Reset button - resets the configuration to factory defaults

SCALANCE S has a reset button. The reset button is located on the rear of the housing below a cover secured with screws immediate beside the C-PLUG.

The reset button is mechanically protected against being activated accidentally.

**Notice**

Make sure that only authorized personnel has access to the SCALANCE S.

#### What does the button do?

Two functions can be triggered with the reset button:

- Restart

  The module is restarted. The loaded configuration is retained.

- Reset to factory settings

  The module is restarted and reset to the status set in the factory. A loaded configuration is deleted.

#### Restart - follow the steps below

| Step | Restart: Procedure |
|---|---|
| 1. | If necessary, remove the SCALANCE S module from its mounting to allow access to the recess. |
| 2. | Remove the M32 plug on the rear of the device.<br>The reset button is in a recess on the rear of the SCALANCE S director beside the slot for the C-PLUG. This recess is protected by a screw plug. The button is located in a narrow hole and is therefore protected from being activated accidentally. |
| 3. | Press the reset button for less than five seconds. |
| 4. | Close the recess with the M32 plug and mount the device again. |

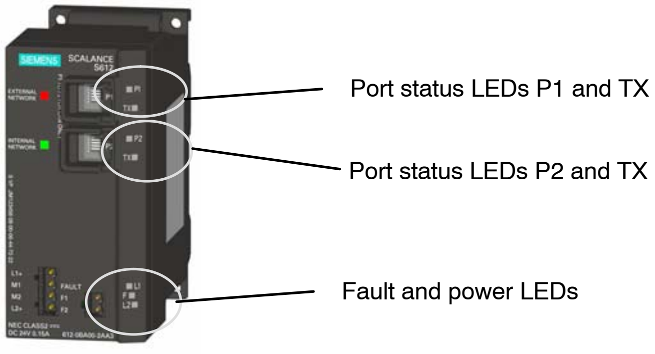
#### Reset to factory settings - follow the steps below

**Notice**

If a C-PLUG is inserted while the factory settings are being restored, the C-PLUG is deleted.

| Step | Reset to factory settings: Procedure |
|---|---|
| 1. | If necessary, remove the SCALANCE S module from its mounting to allow access to the recess. |
| 2. | Remove the M32 plug on the rear of the device.<br>The reset button is in a recess on the rear of the SCALANCE S director beside the slot for the C-PLUG. This recess is protected by a screw plug. The button is located in a narrow hole and is therefore protected from being activated accidentally. |
| 3. | Press the reset button and keep it pressed for longer than 5 seconds until the fault LED flashes yellow/red. |
| 4. | Close the recess with the M32 plug and mount the device again. |

## 2.1.7 Displays



### Fault LED

Mode LED:

| Status | Meaning |
|---|---|
| lit red | Module has identified an error (signaling contact is open)<br>The following errors are identified:<br>• Internal error (e.g. startup unsuccessful)<br>• Invalid C-PLUG (invalid format) |
| lit green | Module in productive operation<br>(Signaling contact closed). |
| NOT lit | Module failure; no power supply<br>(Signaling contact open). |
| Lit yellow (constant) | Module in startup.<br>(Signaling contact open).<br>If no IP address exists, the module remains in this status. |
| Flashes yellow and red alternately | Module resets itself to factory settings.<br>(Signaling contact open). |

### Power LEDs (L1, L2)

The status of the power supply is indicated by two LEDs:

| Status | Meaning |
|---|---|
| lit green | Power supply L1 or L2 is connected. |
| not lit | Power supply L1 or L2 not connected or <14 V (L+). |
| lit red | Power supply L1 or L2 failed during operation or <14 V (L+) |

### Port status LEDs (P1 and TX, P2 and TX)

The status of the interfaces is indicated by 2 LEDs for each of the two ports:

| Status | Meaning |
|---|---|
| **LED P1 / P2** | |
| lit green | TP link exists |
| Flashes / lit yellow | Receiving data at RX |
| Off | No TP link or no data being received |
| **LED TX** | |
| Flashes / lit yellow | Data being sent |
| Off | No data being sent |

## 2.1.8 Technical Specifications

| **Ports** | |
|---|---|
| Attachment of end devices or network components over twisted pair | 2 x RJ-45 sockets with MDI-X pinning<br>10/100 Mbps (half/ full duplex) |
| Connector for power supply | 1 x 4-pin plug-in terminal block |
| Connector for signaling contact | 1 x 2-pin plug-in terminal block |
| **Electrical Data** | |
| Power supply | 24 V DC power supply (18 through 32 V DC)<br>• Implemented redundantly<br>• Safety extra-low voltage (SELV) |
| Power loss at DC 24 V | 3.84 W |
| Current consumption at rated voltage | 250 mA maximum |
| **Permitted Cable Lengths** | |
| Connection over Industrial Ethernet FC TP cables: | |
| 0 -100 m | Industrial Ethernet FC TP standard cable with IE FC RJ-45 Plug 180<br>or<br>Over Industrial Ethernet FC outlet RJ-45 with 0 - 90 m Industrial Ethernet FC TP standard cable + 10 m TP cord |
| 0 - 85 m | Industrial Ethernet FC TP marine/trailing cable with IE FC RJ-45 Plug 180<br>or<br>0 - 75 m Industrial Ethernet FC TP marine/trailing cable + 10 m TP cord |

| **Software quantity structure for VPN** | |
|---|---|
| Number of IPsec tunnels. | |
| SCALANCE S612 | 64 max. |
| SCALANCE S613 | 128 max. |

| **Permitted environmental conditions / EMC** | |
|---|---|
| Operating temperature | |
| SCALANCE S613 | -20 °C to +70 °C |
| SCALANCE S612 | 0 °C to +60 °C |
| Storage/transport temperature | -40 °C to +80 °C |

| | |
|---|---|
| Relative humidity in operation | 95% (no condensation) |
| Operating altitude | Up to 2,000 m above sea level at max. 56 °C ambient temperature<br>Up to 3,000 m above sea level at max. 50 °C ambient temperature |
| RF interference level | EN 50081-2 Class A |
| Noise immunity | EN 50082-2 |
| Degree of protection | IP 30 |
| **Approvals** | |
| c-UL-us | UL 60950 |
| | CSA C22.2 No. 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 | 37.08 years |
| **Construction** | |
| Dimensions (W x H x D) in mm | 60 x 125 x 124 |
| Weight in g | 780 |
| Installation options | • Standard rail<br>• S7-300 standard rail<br>• Wall Mounting |
| **Order Numbers** | |
| SCALANCE S612 | 6GK5612-0BA00-2AA3 |
| SCALANCE S613 | 6GK5613-0BA00-2AA3 |
| ”Industrial Ethernet TP and Fiber Optic Networks” manual | 6GK1970-1BA10-0AA0 |

| Order numbers for accessories | |
|---|---|
| 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 pack of 1 | 6GK1 901-1BB10-2AA0 |
| IE FC RJ-45 Plug 180 pack of 10 | 6GK1 901-1BB10-2AB0 |
| IE FC RJ-45 Plug 180 pack of 50 | 6GK1 901-1BB10-2AE0 |

## 2.2 Installation

**Note**

The requirements of EN61000-4-5, surge test on power supply lines are met only when a Blitzductor VT AD 24V type no. 918 402 is used.

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

**Warning**

When used in hazardous zones (Zone 2), the SCALANCE S product must be installed in an enclosure.

To comply with ATEX 100a (EN 50021), this enclosure must meet the requirements of at least IP54 in compliance with EN 60529.

WARNING
DO NOT CONNECT OR DISCONNECT EQUIPMENT UNLESS AREA IS KNOWN TO BE NONHAZARDOUS.

### Types of Installation

The SCALANCE S can be installed in various ways:

- Installation on a 35 mm DIN rail
- Installation on a SIMATIC S7-300 standard rail
- Wall mounting

**Note**

When installing and operating the device, keep to the installation instructions and safety-related notices as described here and in the manual SIMATIC NET Industrial Ethernet Twisted Pair and Fiber Optic Networks /2/.

**Notice**

We recommend that you provide suitable shade to protect the device from direct sunlight.

This avoids unwanted warming of the device and prevents premature aging of the device and cabling.

## 2.2.1 Installation on a DIN rail

### Installation

Install the SCALANCE S on a 35 mm DIN rail complying with DIN EN 50022.

| Step | Procedure |
|---|---|
| 1. | Place the upper catch of the device over the top of the rail and then push in the lower part of the device against the rail until it clips into place. |
| 2. | Install the electrical connecting cables and the terminal block for the signaling contact. |

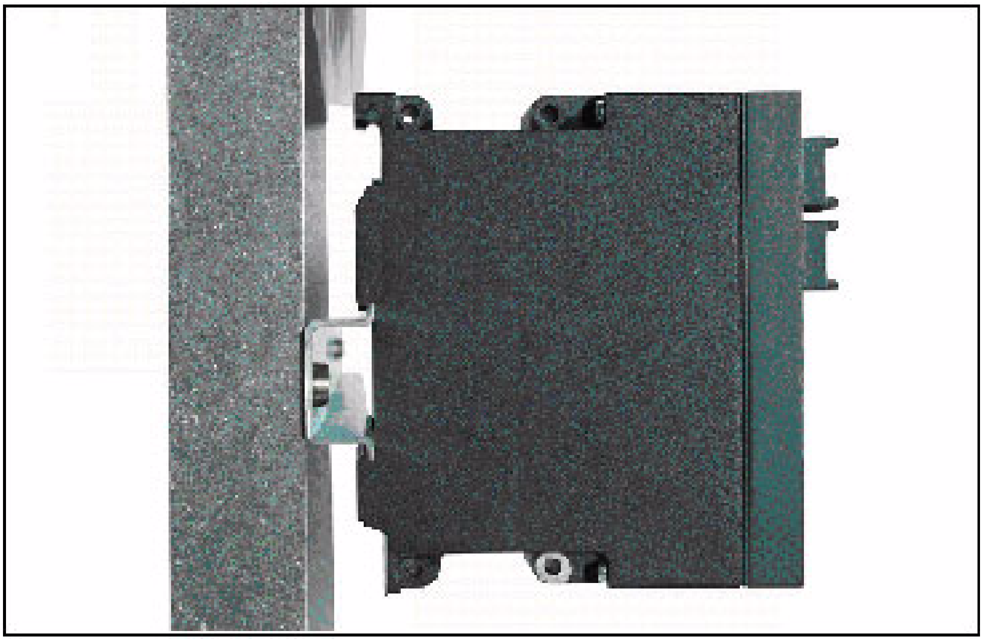


Figure 2-3 SCALANCE S installation on a DIN rail (35 mm)

## Uninstalling

To remove the SCALANCE S from the rail:

| Step | Procedure |
|---|---|
| 1. | First disconnect the TP cables and pull out the terminal blocks for the power supply and the signaling contact. |
| 2. | Use a screwdriver to release the lower rail catch of the device and pull the lower part of the device away from the rail. |

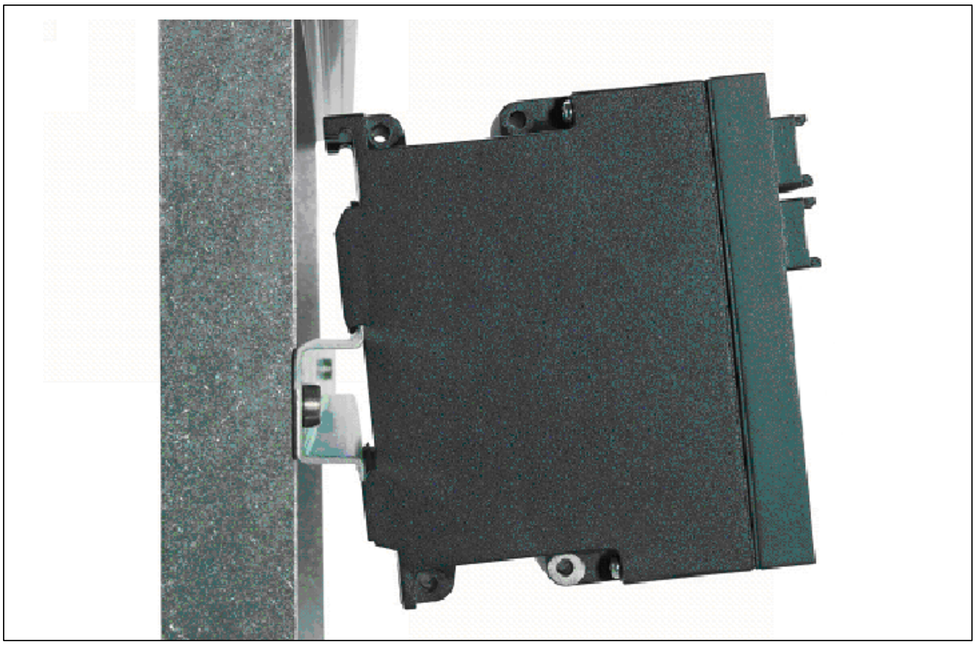


Figure 2-4 SCALANCE S uninstalling from a DIN rail (35 mm)

## 2.2.2 Installation on a standard rail

### Installation on a SIMATIC S7-300 Standard Rail

| Step | Procedure |
|---|---|
| 1. | Place the upper guide at the top of the SCALANCE housing in the S7 standard rail. |
| 2. | Screw the SCALANCE S device to the lower part of the standard rail. |

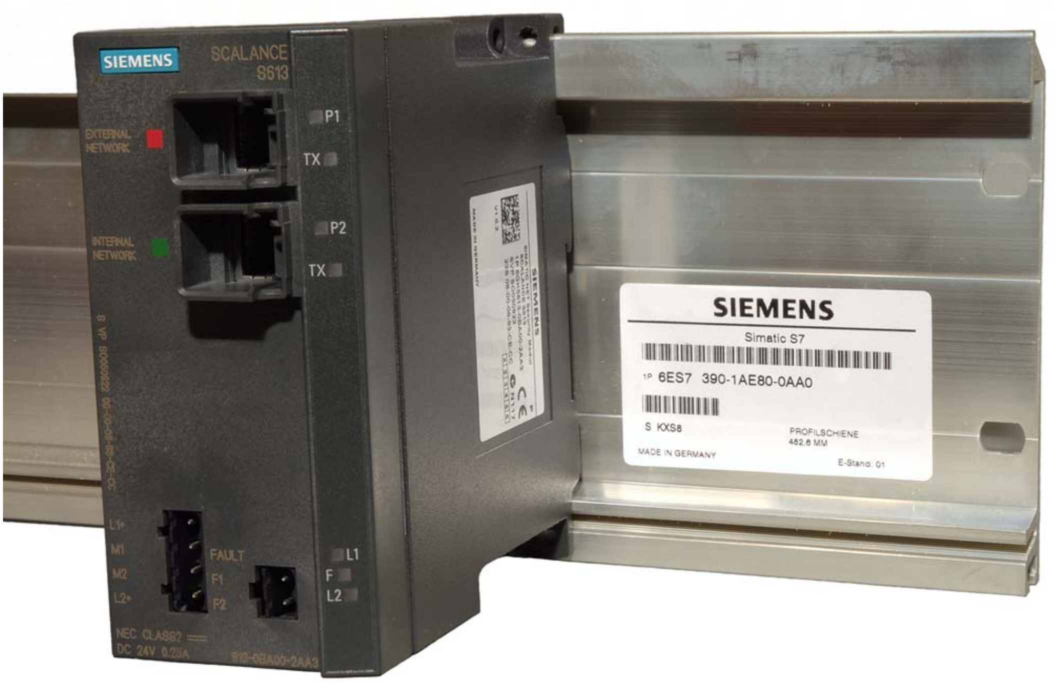


Figure 2-5 SCALANCE S installation on a SIMATIC S7-300 standard rail

### 2.2.3 Wall mounting

#### Installation fittings

Use the following fittings, for example when mounting on a concrete wall:

- 4 wall plugs, 6 mm in diameter and 30 mm long;
- Screws 3.5 mm in diameter and 40 mm long.

**Note**

The wall mounting must be capable of supporting at least four times the weight of the device.

### 2.2.4 Grounding

#### Installation on a DIN Rail

The device is grounded over the DIN rail.

#### S7 Standard Rail

The device is grounded over its rear panel and the neck of the screw.

#### Wall Mounting

The device is grounded by the securing screw in the unpainted hole.

**Notice**

Please note that the SCALANCE S must be grounded over one securing screw with minimum resistance.

## 2.3 Commissioning

**Notice**

Before putting the device into operation, make sure that you read the information in Sections 2.1 and 2.2 carefully and follow the instructions there, particularly those in the safety notices.

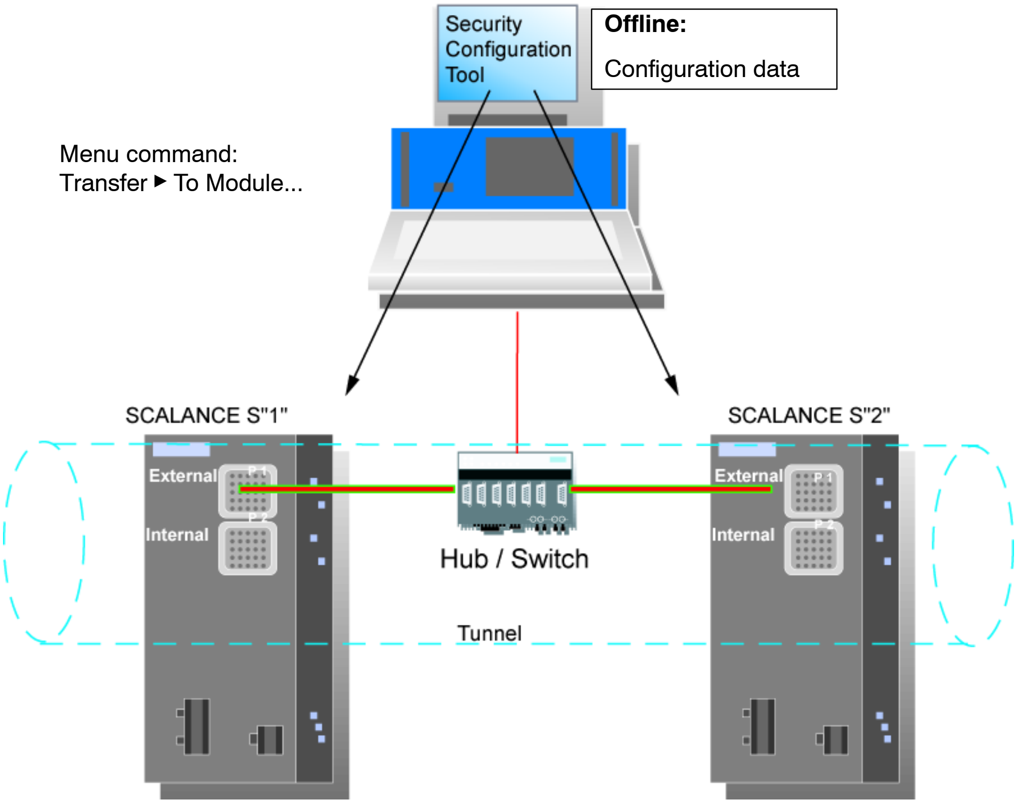
### Principle

To operate the SCALANCE S, you must download a configuration created with the Security Configuration Tool. This procedure is described below.

A SCALANCE S configuration includes the IP parameters and the setting for firewall rules and, if applicable, the setting for IPsec tunnels.

Before putting the device into operation, you can first create the entire configuration offline and then download it. For the first configuration (device with address settings), use the MAC address printed on the device.

Depending on the application, you will download the configuration to one or more modules during the commissioning phase.



## Factory defaults

With the factory defaults (settings as supplied or after resetting to factory defaults), the SCALANCE S behaves as follows after turning on the power supply:

- IP communication is not possible since the IP settings are missing; the SCALANCE S itself does not yet have an IP address.

  As soon as the SCALANCE S module is assigned a valid IP address by the configuration, the module is accessible even over routers (IP communication is then possible).

- The device has a fixed, default MAC address; the MAC address is printed on the device and must be used during configuration.
- The firewall is preconfigured with the following basic firewall rules:
  - Unsecured data traffic from internal port to external port and vice versa (external <-> internal) is **not** possible;

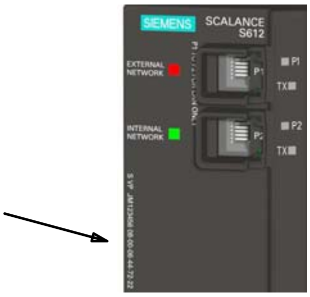
The unconfigured status can be recognized when the F LED is lit yellow.

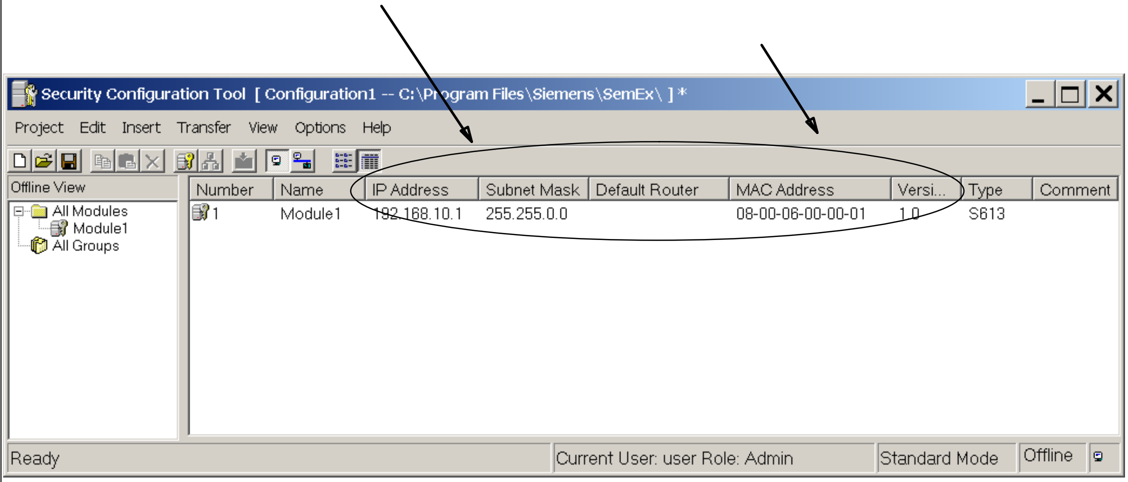
## Follow the steps below when commissioning:

**Note**

Working with the Security Configuration Tool is described in Chapter 4.

| Step | Set up SCALANCE S and the network - procedure |
|---|---|
| 1. | First unpack the SCALANCE S and check that it is undamaged. |
| 2. | Connect the power supply to the SCALANCE S modules.<br>Result: After connecting the power, the Fault LED (F) is lit yellow. |
| 3. | Now establish the physical network connections by plugging the network cable connectors into the ports being used (RJ-45 jacks).<br>• Connect port 1 with the external network to which the configuration PC/PG is connected.<br>• Connect port 2 with the internal network.<br>Note:<br>During commissioning, you can, in principle, initially connect the configuration PC/PG to port 1 or port 2 and do without a connection to other network nodes until the device has been supplied with a configuration. If you connect to port 2, however, you must configure each individual SCALANCE S module separately! |
| 4. | Start the supplied Security Configuration Tool. |

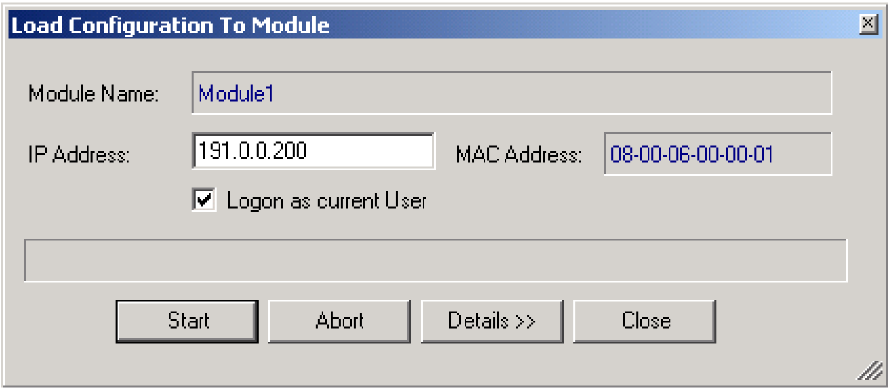
| Step | Set up SCALANCE S and the network - procedure |
|---|---|
| 5. | Select the menu command **Project ▸ New..**<br>You will be prompted to enter a user name and a password. The user entry you specify here will be assigned the role of an administrator. |
| 6. | Enter a user name and a password and confirm your entries to create a new project. |
| 7. | Now select the ”Module 1” object and click in the ”MAC Address” column. |
| 8. | Enter the MAC address printed on the module housing in the ”MAC Address” column you have just activated.<br> SIEMENS<br>SCALANCE S612<br>EXTERNAL NETWORK<br>INTERNAL NETWORK<br>P1<br>TX<br>P2<br>TX |
| 9. | Enter the IP address, the subnet mask and, if applicable, the IP address of the default router. |


Security Configuration Tool [ Configuration1 -- C:\Program Files\Siemens\SemEx\ ] *
Project
Edit
Insert
Transfer
View
Options
Help
Offline View
All Modules
Module1
All Groups

| Number | Name | IP Address | Subnet Mask | Default Router | MAC Address | Versi... | Type | Comment |
|---|---|---|---|---|---|---|---|---|
| 1 | Module1 | 192.168.10.1 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 | |

Ready | Current User: user Role: Admin | Standard Mode | Offline

| | |
|---|---|
| Optional: | Configure any other properties of the module and module groups if required.<br>How to configure firewall rules and IPsec tunnels is described in detail in Chapters 5 and 6. |
| 10. | Save the project under a suitable name with the following menu command:<br>**Project ▸Save As...** |
| 11. | Select the following menu command**:**<br>**Transfer ▸ To Module**<br>**Transfer ▸ To Module**<br>The following transfer dialog opens. |

| Step | Set up SCALANCE S and the network - procedure |
|---|---|
| | <br>Load Configuration To Module<br>Module Name: Module1<br>IP Address: 191.0.0.200<br>MAC Address: 08-00-06-00-00-01<br>☑ Logon as current User<br> |
| 12. | If you click on the ”Start” button, you transfer the configuration to the SCALANCE S module. |
| | Result: The SCALANCE S module is now configured and can communicate at the IP level. This mode is indicated by the Fault LED being lit green. |

## 2.4 C-PLUG (Configuration Plug)

### Area of Application

The C-PLUG is an exchangeable medium for storage of the configuration and project engineering data of the basic device (SCALANCE S). This means that the configuration data remains available if the basic device is replaced.

### How It Works

Power is supplied by the end device. The C-PLUG retains all data permanently when the power is turned off.

### Inserting in the C-PLUG Slot

The slot for the C-PLUG is located on the back of the device.

To insert the C-PLUG, remove the M48 screw cover. The C-PLUG is inserted in the receptacle. The screw cover must then be closed correctly.

**Notice**

The C-PLUG may only be inserted or removed when the power is off!

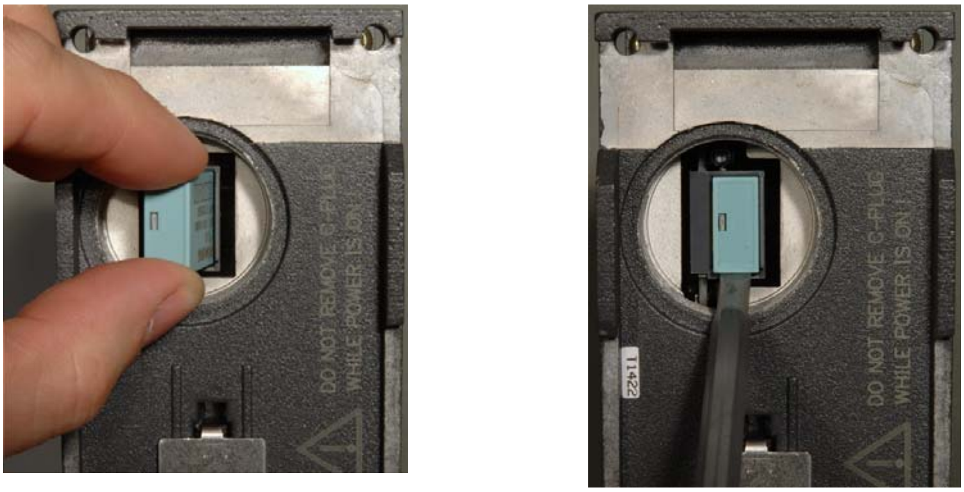


Figure 2-6 Inserting the C-PLUG in the device and removing the C-PLUG from the device with a screwdriver

## Function

If an empty C-PLUG (factory settings) is inserted, all configuration data of the SCALANCE S is saved to it when the device starts up. Changes to the configuration during operation are also saved on the C-PLUG without any operator intervention being necessary.

A basic device with an inserted C-PLUG automatically uses the configuration data of the C-PLUG when it starts up. This is, however, only possible when the data was written by a compatible device type.

This allows fast and simple replacement of the basic device. If a device is replaced, the C-PLUG is taken from the failed component and inserted in the replacement. After it has started up, the replacement device has the same device configuration as the failed device.

**Notice**

When you replace the C-PLUG, you must adapt the MAC address stored on the C-PLUG to the MAC address printed on your SCALANCE S.

**Notice**

If a C-PLUG is inserted while the factory settings are being restored, the C-PLUG is deleted.

## Using a Previously Written C-PLUG

Use only C-PLUGs that are formatted for SCALANCE S. C-PLUGs that have already been used in other device types and formatted for these device types must not be used for SCALANCE S.

## Removing the C-PLUG

It is only necessary to remove the C-PLUG if the basic device develops a fault (see Figure 2-6).

**Notice**

The C-PLUG may only be removed when the power is off!

## Diagnostics

Inserting a C-PLUG that does not contain the configuration of a compatible device type, inadvertently removing the C-PLUG, or general malfunctions of the C-PLUG are indicated by the diagnostic mechanisms of the end device (F-LED red).

## 2.5 Firmware update

You can download new firmware versions to the SCALANCE S modules using the Security Configuration Tool.

### Prerequisites

To transfer new firmware to a SCALANCE S module, the following conditions must be met:

- You must have administrator permissions;
- SCALANCE S must have been configured with an IP address.

### The transfer is secure

The firmware is transferred over a secure connection and can therefore also be transferred from the unprotected network.

The firmware itself is signed and encrypted. This ensures that only authentic firmware can be downloaded to the SCALANCE S module.

### The transfer can take place during operation

The firmware can be transferred while a SCALANCE S module is in operation. Newly downloaded firmware only becomes active after the SCALANCE S module has been restarted. If the transfer is disturbed and aborted, the module starts up again with the old firmware version.

### How to make the transfer

Select the following menu command:

**Transfer ▸ Firmware Update**

# 3 GETTING STARTED

## Getting results fast with GETTING STARTED

Based on a simple test network, this chapter shows you how to work with SCALANCE S and the Security Configuration Tool. You will soon see that you can implement the protective functions of SCALANCE S in the network without any great project engineering effort.

Working through the chapter, you will be able to implement two different security examples - the two basic functions of SCALANCE S.

- Configuring a VPN with SCALANCE S modules as IPsec tunnel endpoints.
- Configuring SCALANCE S as a firewall;

## If you want to know more

You will find more detailed information in the next chapters of this manual. They describe the entire functionality in detail.

**Note**

The IP settings in the examples are freely selected and do not cause any conflicts in the isolated test network.

In a real network, you would need to adapt these IP settings to avoid possible address conflicts.

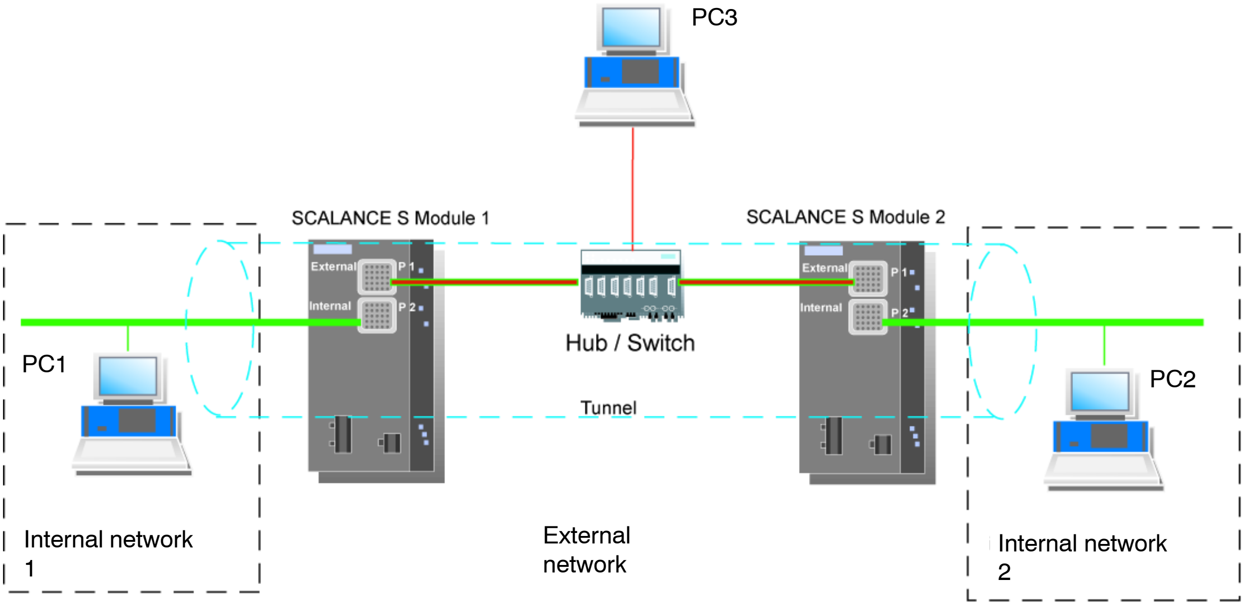
# 3.1 Example 1: Tunnel example with SCALANCE S

## 3.1.1 Overview

In this example, the tunnel function is configured in the ”standard mode” project engineering view. SCALANCE S module 1 and module 2 are the two tunnel endpoints for the secure tunnel connection in this example.

With this configuration, IP traffic is possible only over the established tunnel connections with authorized partners.

### Setup of the test network



- Internal network - attachment to SCALANCE S port 2

  In the test setup in the internal networks, the network node is implemented in each case by one PC connected to the ”internal port” (port 2, green) of a SCALANCE S module.

  - PC1: Represents internal network 1
  - PC2: Represents internal network 2
  - SCALANCE S Module 1: SCALANCE S module for internal network 1
  - SCALANCE S Module 2: SCALANCE S module for internal network 2

- External network - attachment to SCALANCE S port 1

  The unprotected network (”external network”) is attached to the ”external port” (port 1, red) of a SCALANCE S module.

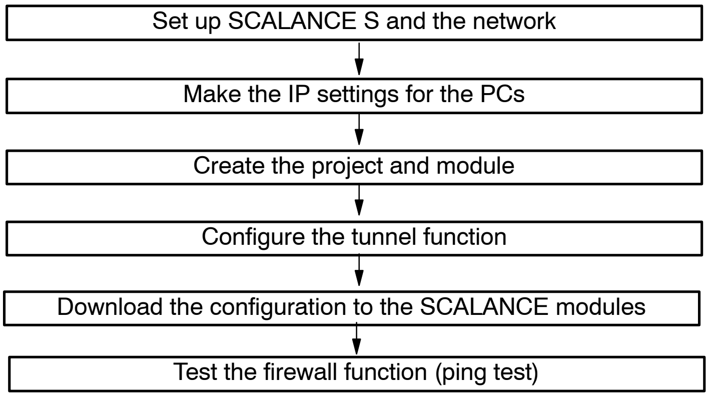
- PC3: PC with the Security Configuration Tool

### Required devices/components:

Use the following components to set up to the network:

- 2 SCALANCE S modules, (optional: 1 or 2 suitably installed standard rails with fittings);
- 1 or 2 24 V power supplies with cable connections and terminal block plugs (both modules can also be operated from a common power supply);
- 1 PC on which the "Security Configuration Tool" is installed;
- 2 PCs in the internal networks to test the configuration;
- 1 network hub or switch to set up the Ethernet network with the two SCALANCE S modules and the PCs/PGs;
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

### Overview of the next steps:


Set up SCALANCE S and the network
Make the IP settings for the PCs
Create the project and module
Configure the tunnel function
Download the configuration to the SCALANCE modules
Test the firewall function (ping test)

### 3.1.2 Set up SCALANCE S and the network

**Follow the steps outlined below:**

| Step | Set up SCALANCE S and the network - procedure |
|---|---|
| 1. | First unpack the SCALANCE S devices and check that they are undamaged. |
| 2. | Connect the power supply to the SCALANCE S modules. |

Result: After connecting the power, the Fault LED (F) is lit yellow.

**Warning**

The SCALANCE S is designed for operation with safety extra-low voltage. This means that only safety extra-low voltages (SELV) complying with IEC950/EN60950/ VDE0805 can be connected to the power supply terminals.

The power supply unit to supply the SCALANCE S must comply with NEC Class 2 (voltage range 18 - 32 V, current requirement approx. 250 mA)

When installing and connecting the SCALANCE S modules, refer to the section 2 ”Hardware description of the SCALANCE S”.

| Step | Set up SCALANCE S and the network - procedure |
|---|---|
| 3. | Now establish the physical network connections by plugging the network cable connectors into the ports being used (RJ-45 jacks):<br>- Connect PC1 with port 2 of module 1 and PC2 with port 2 of module 2.<br>- Connect port 1 of module 1 and port 1 of module 2 with the hub/switch.<br>- Connect PC3 to the hub/switch as well. |
| 4. | Now turn on the PCs. |

**Notice**

The Ethernet attachments at port 1 and port 2 are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network.

- Port 1 - external network

  Upper RJ-45 jack, marked red = unprotected network area;
- Port 2 - internal network

  Lower RJ-45 jack, marked green = network protected by SCALANCE S;

If the ports are swapped over, the device loses its protective function.

## 3.1.3 Make the IP settings for the PCs

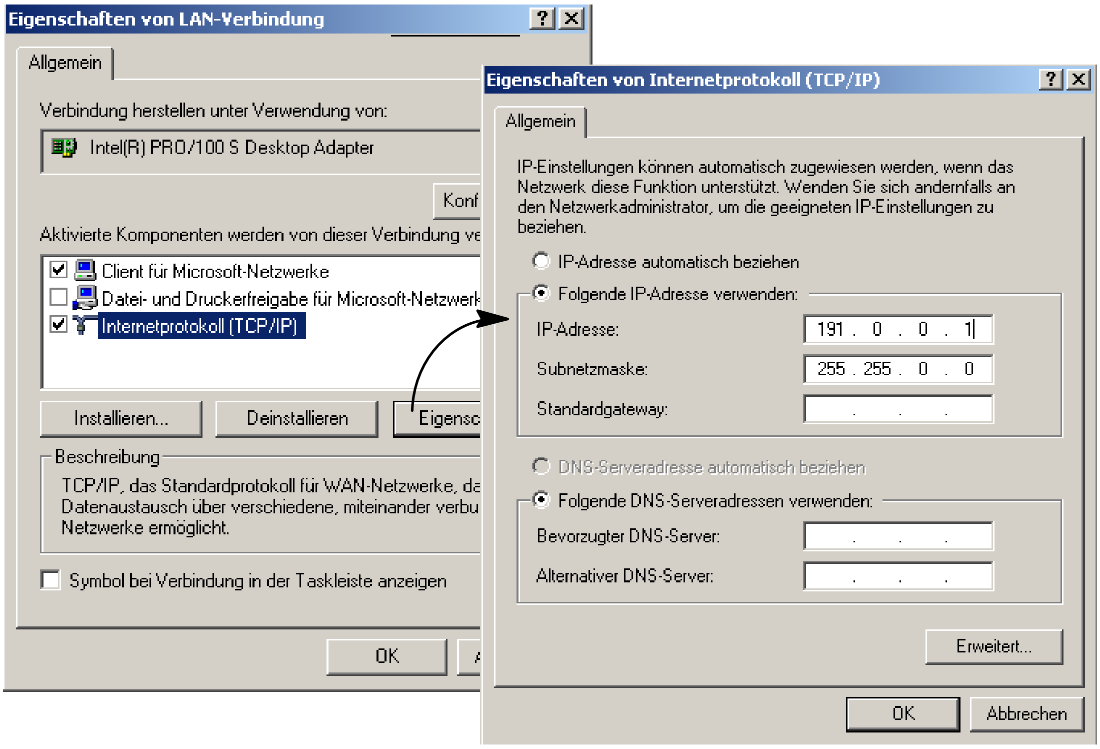
For the test, the PCs should be given the following IP address settings:

Table 3-1

| PC | IP address | Subnet mask |
|---|---|---|
| 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 |

### Follow the steps below for PC1, PC, and PC3:

| Step | Make the IP settings for the PCs - procedure |
|---|---|
| 1. | On the relevant PC, open the Control Panel with the following menu command:<br>**Start ▸ Settings ▸ Control Panel**. |
| 2. | Open the ”Network and Dial-up Connections” Icon |
| 3. | In the ”Local Area Connection Properties” dialog, enable the ”Internet Protocol (TCP/IP)” check box and click the ”Properties” button. |



Eigenschaften von LAN-Verbindung

Verbindung herstellen unter Verwendung von:

Intel(R) PRO/100 S Desktop Adapter

Aktivierte Komponenten werden von dieser Verbindung ve

☑ Client für Microsoft-Netzwerke

□ Datei- und Druckerfreigabe für Microsoft-Netzwerk

☑ Internetprotokoll (TCP/IP)

Beschreibung

TCP/IP, das Standardprotokoll für WAN-Netzwerke, da Datenaustausch über verschiedene, miteinander verbu Netzwerke ermöglicht.

□ Symbol bei Verbindung in der Taskleiste anzeigen

Eigenschaften von Internetprotokoll (TCP/IP)

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

○ IP-Adresse automatisch beziehen

● Folgende IP-Adresse verwenden:

IP-Adresse: 191 . 0 . 0 . 1

Subnetzmaske: 255 . 255 . 0 . 0

Standardgateway: . . .

○ DNS-Serveradresse automatisch beziehen

● Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server: . . .

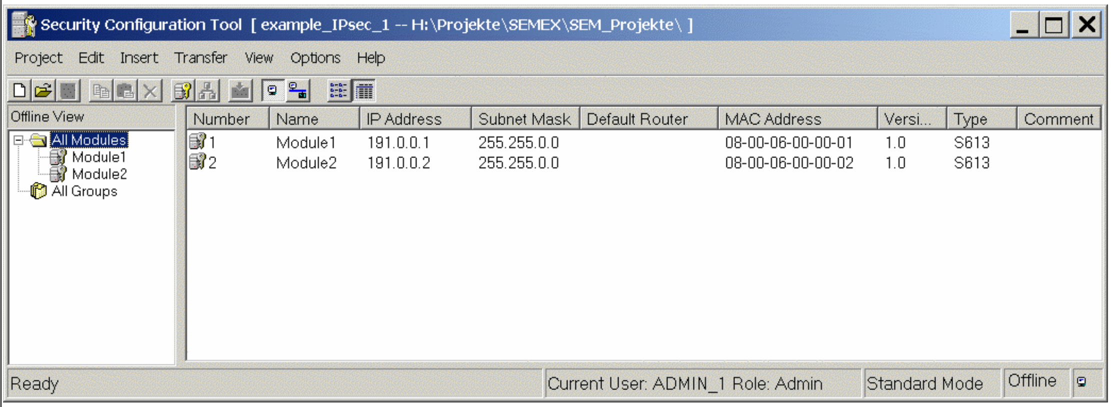
Alternativer DNS-Server: . . .

| Step | Make the IP settings for the PCs - procedure |
|---|---|
| 4. | In the ”Internet Protocol (TCP/IP) Properties” dialog, select the ”Use the following IP address:” option button and enter the values for the PC from the table 3-2 in the relevant boxes.<br>Close the dialogs with ”OK” and exit the Control Panel. |

## 3.1.4 Create the project and modules

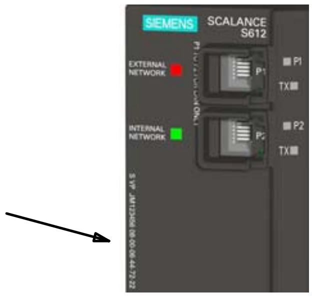
### Follow the steps below:

| Step | Create the project and modules - procedure |
|---|---|
| 1. | Start the Security Configuration Tool on PC1. |
| 2. | Create a new project with the following menu command:<br>**Project ▸ New**.<br>You will be prompted to enter a user name and a password. The user entry you specify here will be assigned the role of an administrator. |
| 3. | Enter a user name and a password and confirm your entries to create a new project. |
| 4. | Now click on ”All Modules”. |
| 5. | Create a second module with the following menu command:<br>**Insert ▸ Module**<br>This module is automatically given a name according to the defaults for the project along with default parameter values. The IP address is incremented from ”module 1” and is therefore different. |

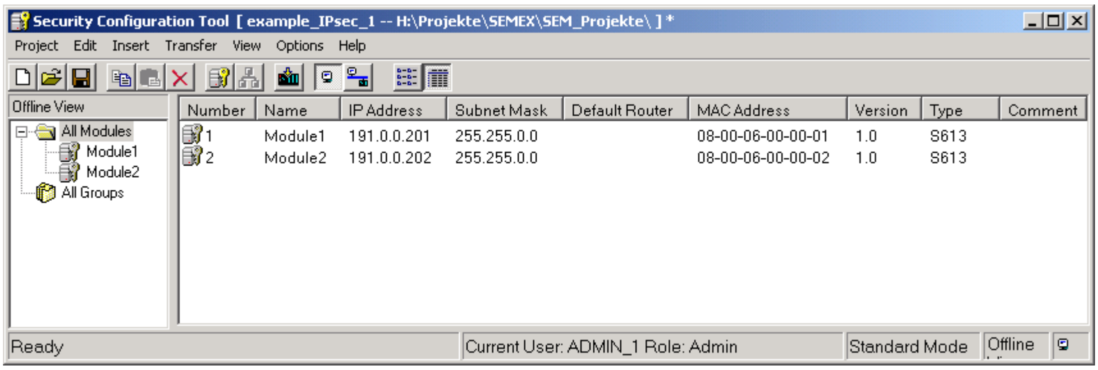

Security Configuration Tool [ example_IPsec_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ]
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
All Groups

| Number | Name | IP Address | Subnet Mask | Default Router | MAC Address | Versi... | Type | Comment |
|---|---|---|---|---|---|---|---|---|
| 1 | Module1 | 191.0.0.1 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 | |
| 2 | Module2 | 191.0.0.2 | 255.255.0.0 | | 08-00-06-00-00-02 | 1.0 | S613 | |

Ready | Current User: ADMIN_1 Role: Admin | Standard Mode | Offline

| | |
|---|---|
| 6. | In the navigation area, click on ”All Modules” and then on the row with ”Module 1” in the content area. |
| 7. | Click on the ”Type” column and select the type of module you are using. |
| 8. | Now click on the ”MAC Address” column and enter the MAC address in the specified format.<br>You will find this address on the front panel of the SCALANCE S module (see picture)<br> SIEMENS SCALANCE S612 EXTERNAL NETWORK INTERNAL NETWORK P1 TX P2 TX |

| Step | Create the project and modules - procedure |
|---|---|
| 9. | Now click on the ”IP Address” column and enter the IP address in the specified format.<br>For module 1: 191.0.0.201<br>For module 2: 191.0.0.202 |


Security Configuration Tool [ example_IPsec_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
All Groups

| Number | Name | IP Address | Subnet Mask | Default Router | MAC Address | Version | Type | Comment |
|---|---|---|---|---|---|---|---|---|
| 1 | Module1 | 191.0.0.201 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 | |
| 2 | Module2 | 191.0.0.202 | 255.255.0.0 | | 08-00-06-00-00-02 | 1.0 | S613 | |

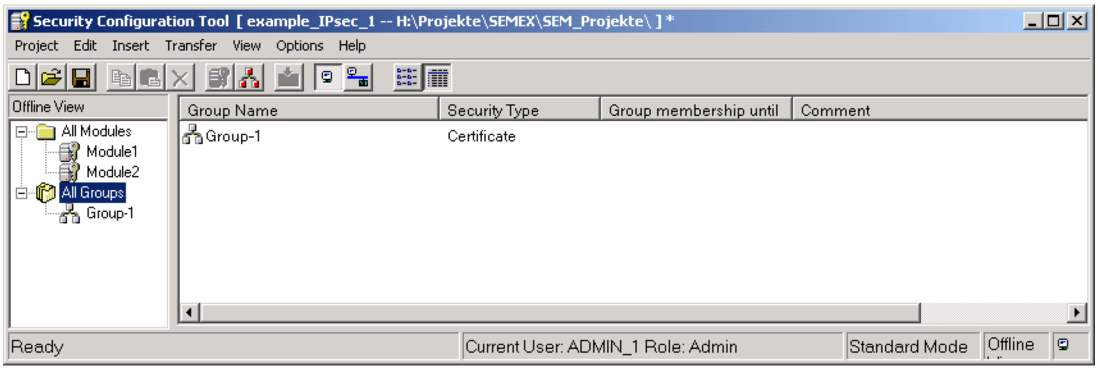
Ready | Current User: ADMIN_1 Role: Admin | Standard Mode | Offline

| | |
|---|---|
| 10. | Repeat steps 6. through 9. for ”Module 2”. |

### 3.1.5 Configure the tunnel connection

Two SCALANCE S modules establish an IPSec tunnel for secure communication when they are assigned to the same group in the project.

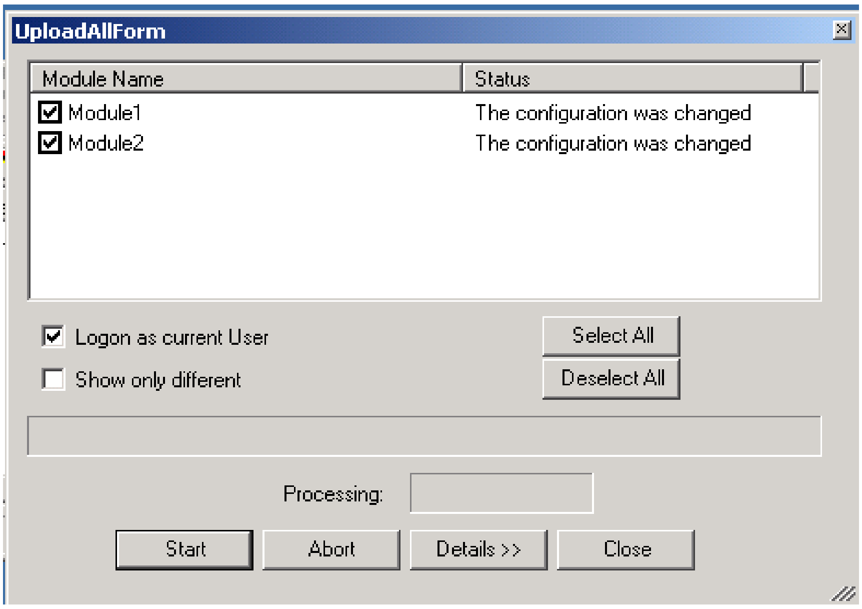
#### Follow the steps below:

| Step | Configure the tunnel connection - procedure |
|---|---|
| 1. | Select ”All Groups” in the navigation area and create a new group with the following menu command:<br>**Insert ▸ Group**<br>This group is automatically given the name ”Group 1” |
| | <br>Security Configuration Tool [ example_IPsec_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *<br> Project Edit Insert Transfer View Options Help<br>Offline View<br>All Modules<br>Module1<br>Module2<br>All Groups<br>Group-1<br>Group Name: Group-1 · Security Type: Certificate · Group membership until · Comment<br>Ready · Current User: ADMIN_1 Role: Admin · Standard Mode · Offline |
| 2. | Select the SCALANCE S module 1 in the content area and drag it to the ”Group 1” in the navigation area.<br>The module is now assigned to this group (is a member of the group).<br>The color of the key symbol of the module icon changes from gray to yellow. |
| 3. | Select the SCALANCE S module 1 in the content area and drag it to the ”Group 2” in the navigation area.<br>The module is now also assigned to this group. |

The configuration of the tunnel connection is now complete.

### 3.1.6 Download the configuration to the SCALANCE S modules

#### Follow the steps below:

| Step | Download configuration - procedure |
|---|---|
| 1. | Using the menu command below, open the following dialog:<br>**Transfer ▸ To All Modules...**<br>UploadAllForm<br>Module Name — Status<br>☑ Module1 — The configuration was changed<br>☑ Module2 — The configuration was changed<br>☑ Logon as current User<br>☐ Show only different<br>Processing:<br> Select All<br>Deselect All<br>Start<br>Abort<br>Details >><br>Close |
| 2. | Select the two modules using the "Select All" button. |
| 3. | Start the download with the "Start" button. |

If the download was completed free of errors, the SCALANCE S is restarted automatically and the new configuration activated.

#### Result: SCALANCE S in productive operation

The SCALANCE S is now in productive operation. This mode is indicated by the Fault LED being lit green.

The configuration has now been commissioned and the two SCALANCE S modules can now establish a communication tunnel via which network nodes from the two internal networks can communicate.

## 3.1.7 Test the tunnel function (ping test)

### How can you test the configured function?

The function can be tested as described below using a ping command.

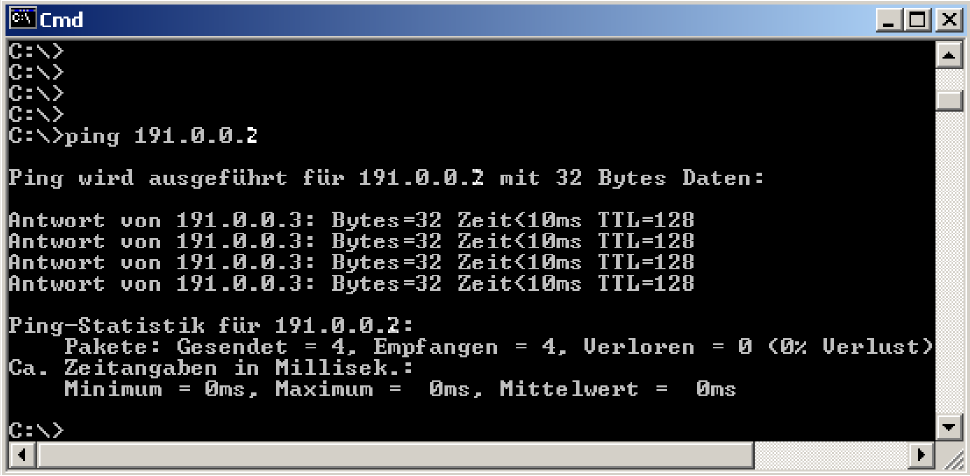
As an alternative, you can also use other communication programs to test the configuration.

**Notice**

With Windows XP SP2, the firewall can be set as default so that the PING commands do not pass through. If necessary, you will need to enable the ICMP services of the type Request and Response.

### Test section 1

Now test the function of the tunnel connection established between PC1 and PC2.

| Step | Test the tunnel function (ping test) - procedure |
|---|---|
| 1. | Open the following menu command from the taskbar Start menu on PC2.<br>**Programs ▸ Accessories ▸ Command Prompt** |
| 2. | Enter the Ping command from PC1 to PC2 (IP address 191.0.0.2)<br>In the command line of the Command Prompt window (here Windows 2000) enter the command **ping 191.0.0.2** at the cursor position.<br>You will then receive the following message: (positive reply from PC2).<br> |

```
C:\>
C:\>
C:\>
C:\>
C:\>ping 191.0.0.2

Ping wird ausgeführt für 191.0.0.2 mit 32 Bytes Daten:

Antwort von 191.0.0.3: Bytes=32 Zeit<10ms TTL=128
Antwort von 191.0.0.3: Bytes=32 Zeit<10ms TTL=128
Antwort von 191.0.0.3: Bytes=32 Zeit<10ms TTL=128
Antwort von 191.0.0.3: Bytes=32 Zeit<10ms TTL=128

Ping-Statistik für 191.0.0.2:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust)
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum =  0ms, Mittelwert =  0ms

C:\>
```

## Result

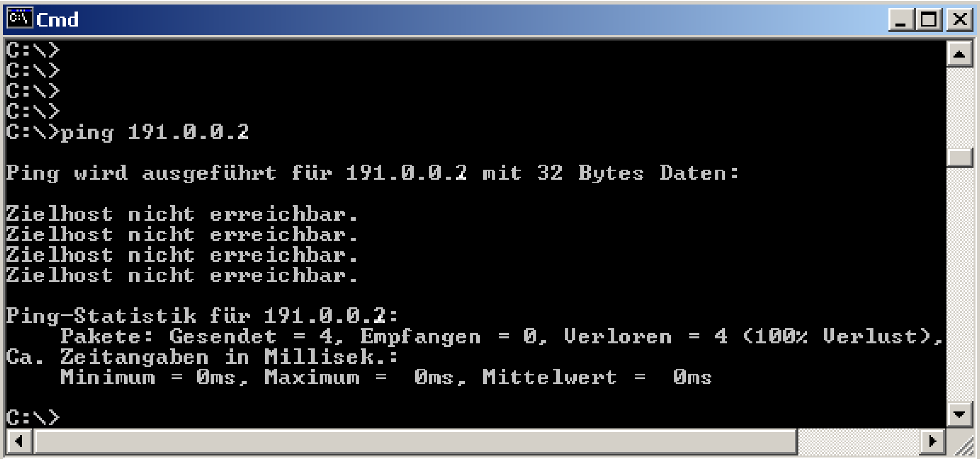
If the IP packets have reached PC3, the ”Ping statistics for 191.0.03” display the following:

- Sent = 4
- Received = 4
- Lost = 0 (0% loss)

Since no other communication is permitted, these packets must have been transported through the VPN tunnel.

## Test section 2

Now repeat the test by sending a ping command from PC3.

| Step | Test the tunnel function (ping test) - procedure |
|---|---|
| 1. | Open the following menu command from the taskbar Start menu on PC3.<br>**Programs ▸ Accessories ▸ Command Prompt** |
| 2. | Send the same ping command (**ping 191.0.0.3**) in the Command Prompt window of PC3.<br>You will then receive the following message: (no reply from PC3).<br> |

```
C:\>
C:\>
C:\>
C:\>
C:\>ping 191.0.0.2

Ping wird ausgeführt für 191.0.0.2 mit 32 Bytes Daten:

Zielhost nicht erreichbar.
Zielhost nicht erreichbar.
Zielhost nicht erreichbar.
Zielhost nicht erreichbar.

Ping-Statistik für 191.0.0.2:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4 (100% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum =  0ms, Mittelwert =  0ms

C:\>
```

## Result

The IP frames from PC3 must not reach PC2 since neither tunnel communication between these two devices is configured nor is normal IP data traffic permitted.

This is shown in the ”Ping statistics for 191.0.0.3” as follows:

- Sent = 4
- Received = 0
- Lost = 4 (100% loss)

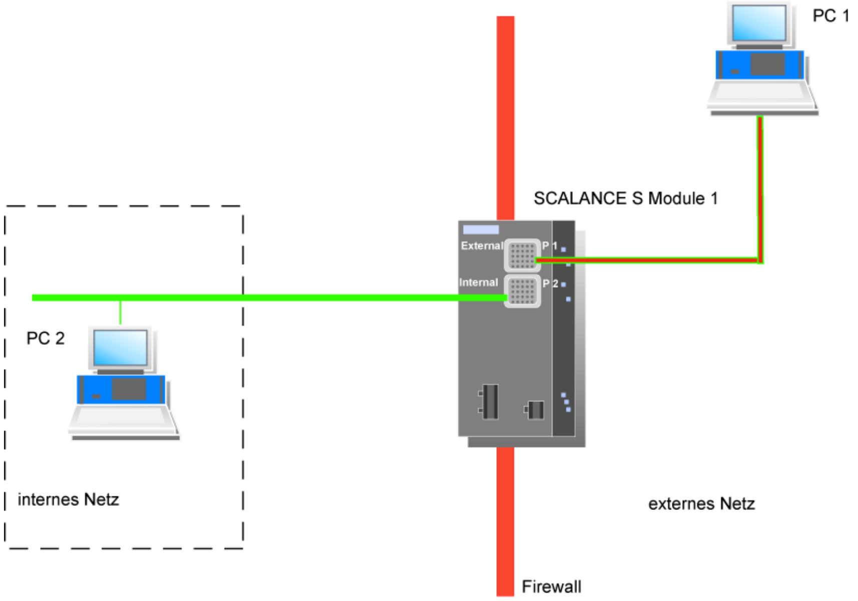
# 3.2 Example 2: Operating a SCALANCE S as firewall

## 3.2.1 Overview

In this example, the firewall is configured in the ”standard mode” project engineering view. The standard mode includes predefined sets of rules for data traffic.

With this configuration, IP traffic can only be initiated from the internal network; only the response is permitted from the external network.

### Setup of the test network



- Internal network - attachment to SCALANCE S port 2

  In the test setup, in the internal network, the network node is implemented by one PC connected to the ”internal port” (port 2, green) of a SCALANCE S module.

  - PC2: Represents the internal network
  - SCALANCE S Module 1: SCALANCE S module for the internal network

- External network - attachment to SCALANCE S port 1

  The unprotected network (”external network”) is attached to the ”external port” (port 1, red) of a SCALANCE S module.

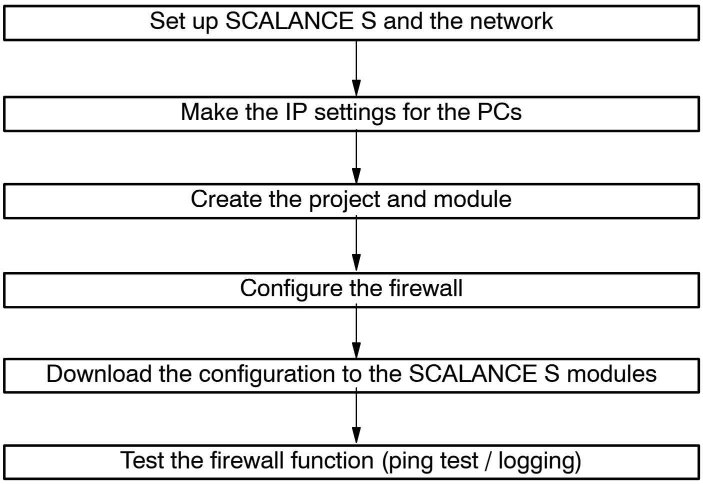
  - PC1: PC with the Security Configuration Tool

### Required devices/components:

Use the following components to set up to the network:

- 1 SCALANCE S module, (additional option: 1 suitably installed standard rail with fittings);
- 1 24 V power supply with cable connectors and terminal block plugs;
- 1 PC on which the Security Configuration Tool is installed;
- 1 PC in the internal network to test the configuration;
- The required network cable, TP cable (twisted pair) complying with the IE FC RJ-45 standard for Industrial Ethernet.

### Overview of the next steps:


Set up SCALANCE S and the network
Make the IP settings for the PCs
Create the project and module
Configure the firewall
Download the configuration to the SCALANCE S modules
Test the firewall function (ping test / logging)

## 3.2.2 Set up SCALANCE S and the network

### Follow the steps below:

| Step | Set up SCALANCE S and the network - procedure |
|---|---|
| 1. | First unpack the SCALANCE S and check that it is undamaged. |
| 2. | Connect the power supply to the SCALANCE S modules.<br>Result: After connecting the power, the Fault LED (F) is lit yellow. |

**Warning**

The SCALANCE S is designed for operation with safety extra-low voltage. This means that only safety extra-low voltages (SELV) complying with IEC950/EN60950/ VDE0805 can be connected to the power supply terminals.

The power supply unit to supply the SCALANCE S must comply with NEC Class 2 (voltage range 18 - 32 V, current requirement approx. 250 mA)

When installing and connecting the SCALANCE S modules, refer to the section 2 ”Hardware description of the SCALANCE S”

| Step | Set up SCALANCE S and the network - procedure |
|---|---|
| 3. | Now establish the physical network connections by plugging the network cable connectors into the ports being used (RJ-45 jacks):<br>- Connect PC2 with port 2 of module 1.<br>- Connect port 1 of module 1 with PC1. |
| 4. | Now turn on the PCs. |

**Notice**

The Ethernet attachments at port 1 and port 2 are handled differently by the SCALANCE S and must not be swapped over when connecting to the communication network.

- Port 1 - external network

  Upper RJ-45 jack, marked red = unprotected network area;
- Port 2 - internal network

  Lower RJ-45 jack, marked green = network protected by SCALANCE S;

If the ports are swapped over, the device loses its protective function.

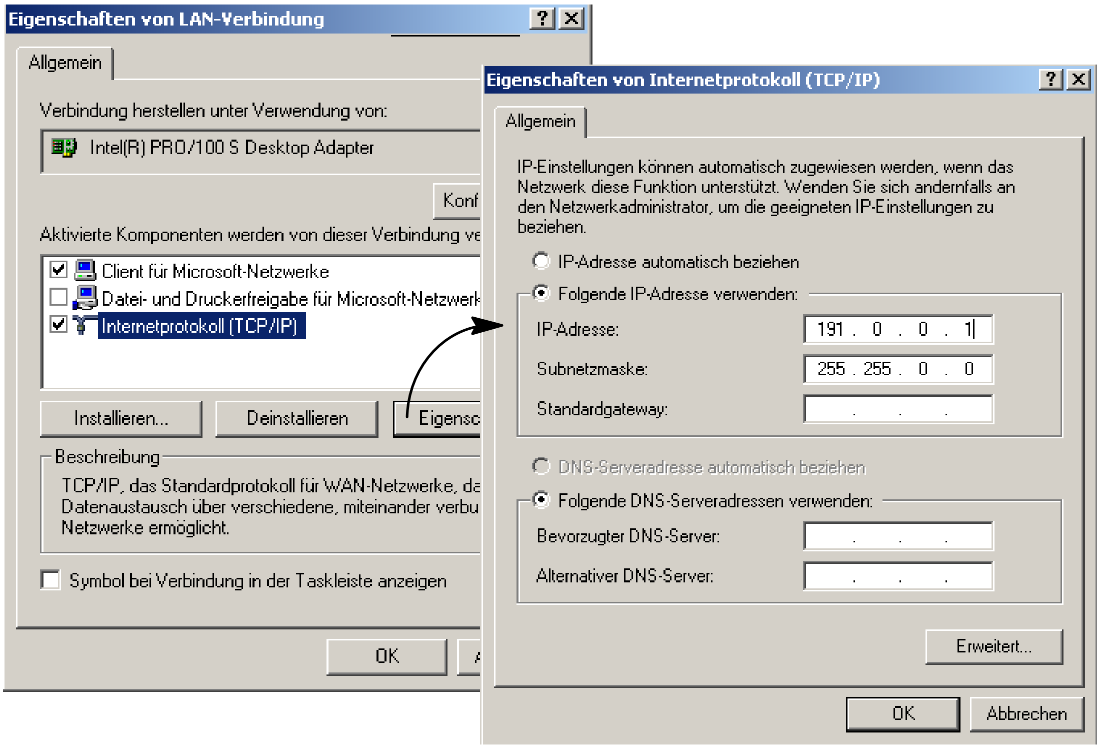
## 3.2.3 Make the IP settings for the PCs

For the test, the PCs should be given the following IP address settings:

Table 3-2

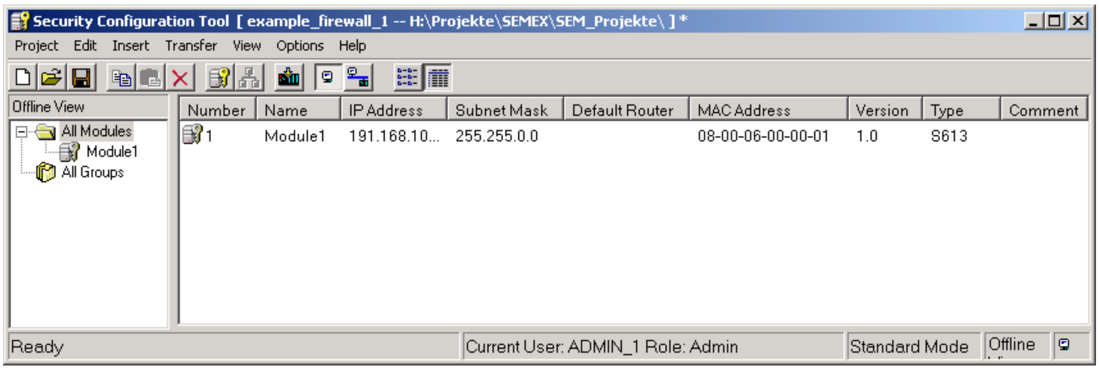
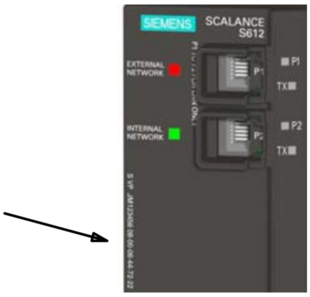
| PC | IP address | Subnet mask |
|---|---|---|
| PC1 | 191.0.0.1 | 255.255.0.0 |
| PC2 | 191.0.0.2 | 255.255.0.0 |

### Follow the steps below for PC1 and PC2:

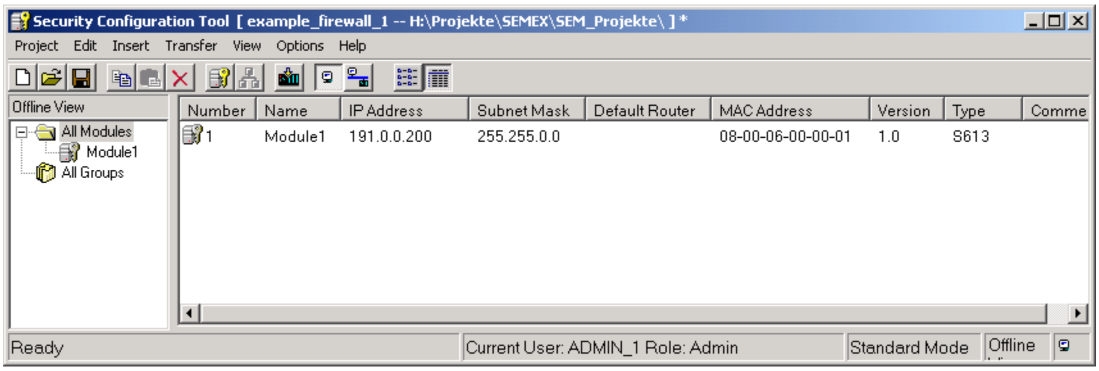
| Step | Make the IP settings for the PCs - procedure |
|---|---|
| 1. | On the relevant PC, open the Control Panel with the following menu command:<br>**Start ▸ Settings ▸ Control Panel** |
| 2. | Open the ”Network and Dial-up Connections” Icon |
| 3. | In the ”Local Area Connection Properties” dialog, enable the ”Internet Protocol (TCP/IP” check box and click the ”Properties” button.<br><br>Eigenschaften von LAN-Verbindung<br>Allgemein<br>Verbindung herstellen unter Verwendung von:<br>Intel(R) PRO/100 S Desktop Adapter<br>Konf<br>Aktivierte Komponenten werden von dieser Verbindung ve<br>☑ Client für Microsoft-Netzwerke<br>□ Datei- und Druckerfreigabe für Microsoft-Netzwerk<br>☑ Internetprotokoll (TCP/IP)<br>Installieren... Deinstallieren Eigensc<br>Beschreibung<br>TCP/IP, das Standardprotokoll für WAN-Netzwerke, da Datenaustausch über verschiedene, miteinander verbu Netzwerke ermöglicht.<br>□ Symbol bei Verbindung in der Taskleiste anzeigen<br>OK A<br>Eigenschaften von Internetprotokoll (TCP/IP)<br>Allgemein<br>IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.<br>○ IP-Adresse automatisch beziehen<br>● Folgende IP-Adresse verwenden:<br>IP-Adresse: 191 . 0 . 0 . 1<br>Subnetzmaske: 255 . 255 . 0 . 0<br>Standardgateway: . . .<br>○ DNS-Serveradresse automatisch beziehen<br>● Folgende DNS-Serveradressen verwenden:<br>Bevorzugter DNS-Server: . . .<br>Alternativer DNS-Server: . . .<br>Erweitert...<br>OK Abbrechen |
| 4. | In the ”Internet Protocol (TCP/IP) Properties” dialog, select the ”Use the following IP address:” option button and enter the values for the PC from the table 3-2 in the relevant boxes.<br>Close the dialogs with ”OK” and exit the Control Panel. |

## 3.2.4 Create the project and module

### Follow the steps below:

| Step | Create the project and module - procedure |
|---|---|
| 1. | Install and start the Security Configuration Tool on PC1. |
| 2. | Create a new project with the following menu command:<br>**Project ▸ New**<br>You will be prompted to enter a user name and a password. The user entry you specify here will be assigned the role of an administrator. |
| 3. | Enter a user name and a password and confirm your entries to create a new project. |
|  | <br>Security Configuration Tool [ example_firewall_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *<br>Offline View: All Modules / Module1 / All Groups<br>Number: 1 · Name: Module1 · IP Address: 191.168.10... · Subnet Mask: 255.255.0.0 · Default Router: · MAC Address: 08-00-06-00-00-01 · Version: 1.0 · Type: S613 · Comment:<br>Ready · Current User: ADMIN_1 Role: Admin · Standard Mode · Offline<br> |
| 4. | In the navigation area, click on ”All Modules” and then on the row with ”Module 1” in the content area. |
| 5. | Click on the ”Type” column and select the type of module you are using. |
| 6. | Now click on the ”MAC Address” column and enter the MAC address in the specified format.<br>You will find this address on the front panel of the SCALANCE S module (see picture)<br><br> SIEMENS SCALANCE S612 EXTERNAL NETWORK INTERNAL NETWORK P1 TX P2 TX |

| Step | Create the project and module - procedure |
|---|---|
| 7. | Now click on the ”IP Address” column and enter the IP address in the specified format:<br>191.0.0.200 |



Security Configuration Tool [ example_firewall_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *

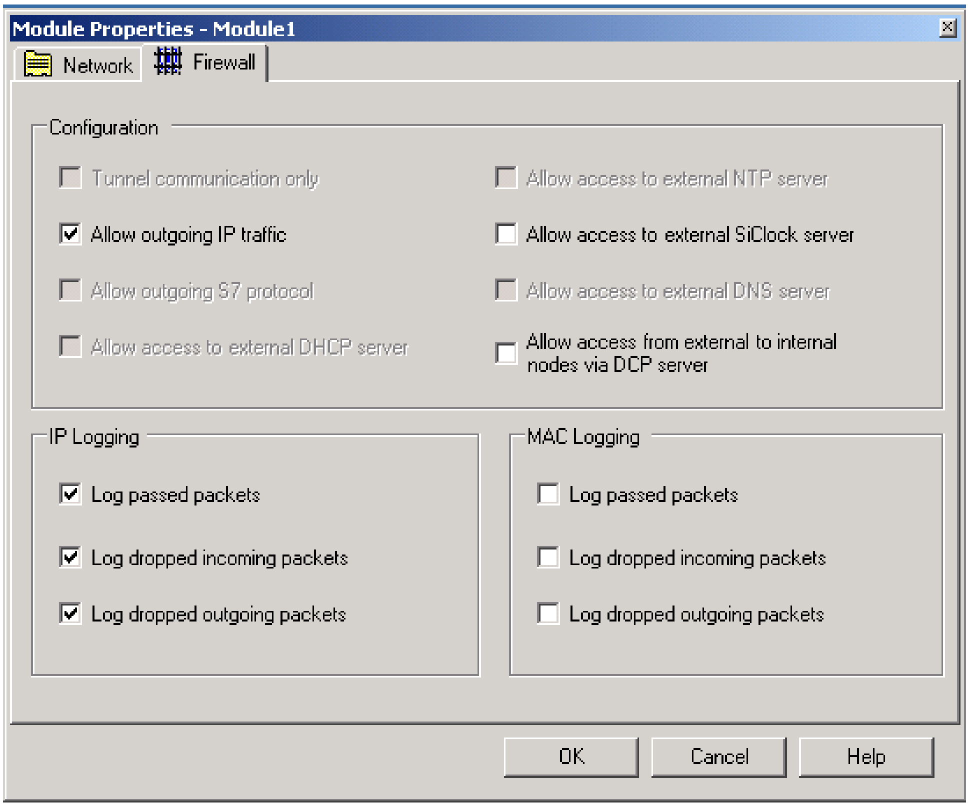
| Number | Name | IP Address | Subnet Mask | Default Router | MAC Address | Version | Type | Comme |
|---|---|---|---|---|---|---|---|---|
| 1 | Module1 | 191.0.0.200 | 255.255.0.0 |  | 08-00-06-00-00-01 | 1.0 | S613 |  |

Ready | Current User: ADMIN_1 Role: Admin | Standard Mode | Offline

### 3.2.5 Configure the firewall

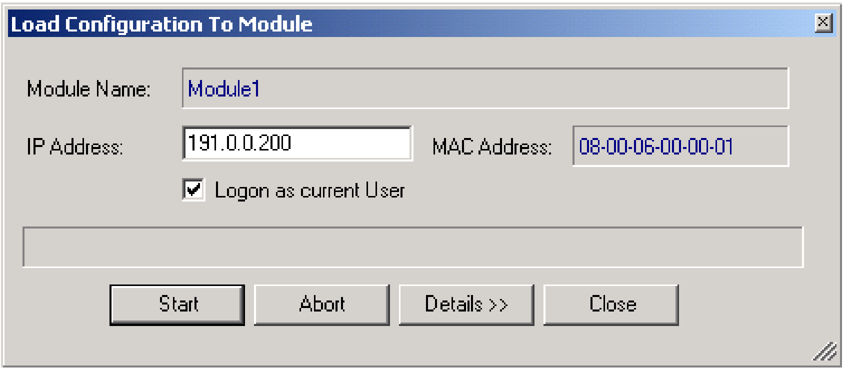
The simple operation of the firewall in standard mode includes predefined sets of rules. You can activate these sets of rules by clicking on them.

**Follow the steps below:**

| Step | Configure firewall - procedure |
|---|---|
| 1. | Select the ”Module 1” row in the content area. |
| 2. | Select the following menu command:<br>**Edit ▸Properties...** |
| 3. | Select the ”Firewall” tab in the displayed dialog. |
| 4. | Enable the option shown below:<br><br>Module Properties - Module1<br>Network / Firewall<br>Configuration<br>☐ Tunnel communication only<br>☑ Allow outgoing IP traffic<br>☐ Allow outgoing S7 protocol<br>☐ Allow access to external DHCP server<br>☐ Allow access to external NTP server<br>☐ Allow access to external SiClock server<br>☐ Allow access to external DNS server<br>☐ Allow access from external to internal nodes via DCP server<br>IP Logging<br>☑ Log passed packets<br>☑ Log dropped incoming packets<br>☑ Log dropped outgoing packets<br>MAC Logging<br>☐ Log passed packets<br>☐ Log dropped incoming packets<br>☐ Log dropped outgoing packets<br>OK / Cancel / Help<br>This means that IP traffic can only be initiated from the internal network; only the response is permitted from the external network. |
| 5. | You should also select the Logging options to record data traffic. |
| 6. | Close the dialog with ”OK”. |
| 7. | Save this project under a suitable name with the following menu command:<br>**Project ▸Save As...** |

## 3.2.6 Download the configuration to the SCALANCE S modules

### Follow the steps below:

| Step | Download configuration - procedure |
|---|---|
| 1. | Select the module in the content area. |
| 2. | Select the following menu command:<br>**Transfer ▸ To Module..**<br><br>Load Configuration To Module<br>Module Name: Module1<br>IP Address: 191.0.0.200<br>MAC Address: 08-00-06-00-00-01<br>☑ Logon as current User<br> |
| 3. | Start the download with the ”Start” button. |

If the download was completed free of errors, the SCALANCE S module is restarted automatically and the new configuration activated.

### Result: SCALANCE S in productive operation

The SCALANCE S is now in productive operation. This mode is indicated by the Fault LED being lit green.

Commissioning the configuration is now complete and the SCALANCE S is now protecting the internal network (PC2) with the firewall according to the configured rule: ”Allow outgoing IP traffic” from the internal to the external network.

## 3.2.7 Test the firewall function (ping test)

### How can you test the configured function?

The function can be tested as described below using a ping command.

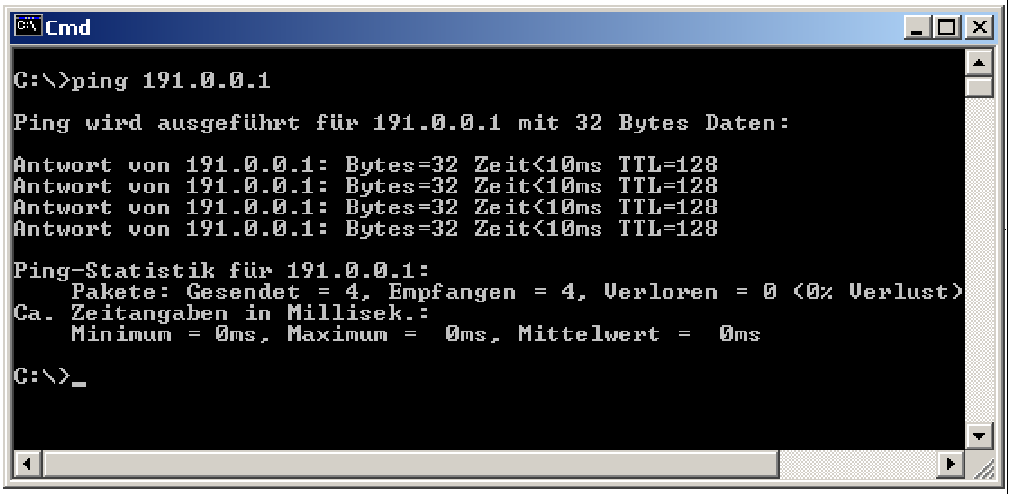
As an alternative, you can also use other communication programs to test the configuration.

**Notice**

With Windows XP SP2, the firewall can be set as default so that the PING commands do not pass through. If necessary, you will need to enable the ICMP services of the type Request and Response.

### Test section 1

Now test the function of the firewall configuration, first with allowed outgoing IP data traffic as follows:

| Step | Test the firewall function (ping test) - procedure |
|---|---|
| 1. | Open the following menu command from the taskbar Start menu on PC2.<br>**Start ▸Run** |
| 2. | In the ”Run” dialog, enter the command ”cmd”. |
| 3. | Enter the Ping command from PC2 to PC1 (IP address 191.0.0.1)<br>In the command line of the Command Prompt window (here Windows 2000), enter the following command:<br>**ping 191.0.0.1**<br>You will then receive the following message: (positive reply from PC1).<br> |
| | |

```
C:\>ping 191.0.0.1

Ping wird ausgeführt für 191.0.0.1 mit 32 Bytes Daten:

Antwort von 191.0.0.1: Bytes=32 Zeit<10ms TTL=128
Antwort von 191.0.0.1: Bytes=32 Zeit<10ms TTL=128
Antwort von 191.0.0.1: Bytes=32 Zeit<10ms TTL=128
Antwort von 191.0.0.1: Bytes=32 Zeit<10ms TTL=128

Ping-Statistik für 191.0.0.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust)
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum =  0ms, Mittelwert =  0ms

C:\>_
```

## Result

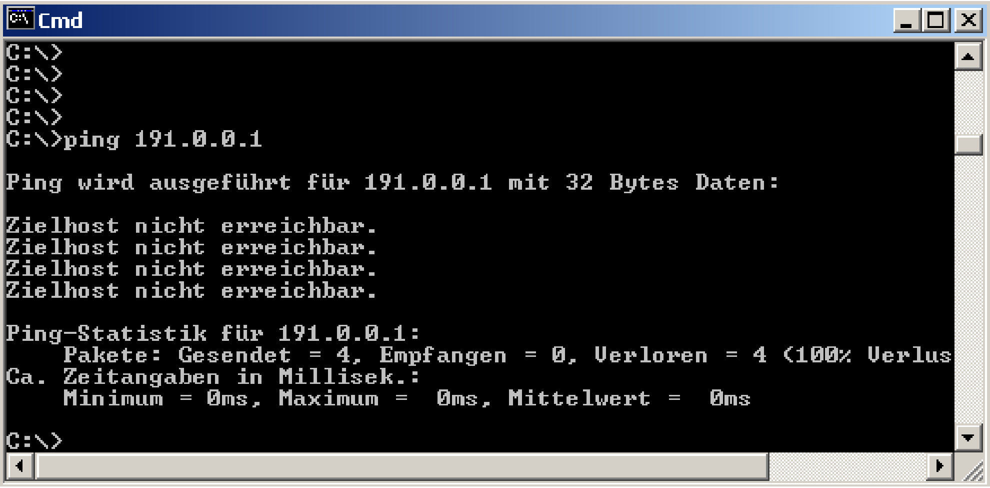
If the IP packets have reached PC1, the ”Ping statistics for 191.0.01” display the following:

- Sent = 4
- Received = 4
- Lost = 0 (0% loss)

Due to the configuration, the ping packets can pass from the internal network to the external network. The PC in the external network has replied to the ping packets. Due to the ”stateful inspection” function of the firewall, the reply packets arriving from the external network are automatically passed into the internal network.

## Test section 2

Now test the function of the firewall configuration with blocked outgoing IP data traffic as follows:

| Step | Test the firewall function (ping test) - procedure |
|---|---|
| 4. | Now change back to offline mode on PC1 in the Security Configuration Tool with the following menu command:<br>**View ▸Offline** |
| 5. | Now reopen the firewall dialog as described above. |
| 6. | Uncheck the ”Allow outgoing IP traffic” box in the ”Firewall” tab.<br>Close the dialog with ”OK”. |
| 7. | Now download the modified configuration to the SCALANCE S module again (see Section 3.2.6) |
| 8. | If the downloading is completed free of errors, enter the same ping command again (**ping 191.0.0.1**) in the Command Prompt window of PC2 as described above.<br>You will then receive the following message: (no reply from PC1).<br> |

```
C:\>
C:\>
C:\>
C:\>
C:\>ping 191.0.0.1

Ping wird ausgeführt für 191.0.0.1 mit 32 Bytes Daten:

Zielhost nicht erreichbar.
Zielhost nicht erreichbar.
Zielhost nicht erreichbar.
Zielhost nicht erreichbar.

Ping-Statistik für 191.0.0.1:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4 (100% Verlus
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum =  0ms, Mittelwert =  0ms

C:\>
```

## Result

The IP packets from PC2 must not reach PC1 since the data traffic from the ”internal network” (PC2) to the ”external network” (PC1) is not permitted.

This is shown in the ”Ping statistics for 191.0.0.1” as follows:

- Sent = 4
- Received = 0
- Lost = 4 (100% loss)

### 3.2.8 Log firewall data traffic

On the SCALANCE S, the logging of system and packet filter events is active as default.

While working through this example, you also activated the logging options when configuring the firewall (see page 60).

You can therefore display the recorded events in online mode

#### Follow the steps below:

| Step | Log firewall data traffic - procedure |
|---|---|
| 1. | Now change back to online mode on PC1 in the Security Configuration Tool with the following menu command:<br>**View ▸Online** |
| 2. | Select the following menu command**:**<br>**Edit ▸ Online Diagnostics..** |
| 3. | Wählen Sie das Register ”Packetfilter Log”. |
| 4. | Betätigen Sie die Schaltfläche ”Starte Lesen” |
| 5. | Acknowledge the displayed dialog with OK.<br>Result: The log entries are read from the SCALANCE S and displayed here. |
| | |

# 4 Configuring with the Security Configuration Tool

The Security Configuration Tool is the configuration tool is supplied with SCALANCE S.

This chapter will familiarize you with the user interface and the functionality of the configuration tool.

You will learn how to set up, work with, and manage SCALANCE S projects.

## Further information

How to configure modules and IPSec tunnels is described in detail in the next chapters of this manual.

HLP
F1

You will find detailed information on the dialogs and parameter settings in the online help. You can call this with the F1 key or using the ”Help” button in the relevant dialog.

## 4.1 Range functions and how they work

### Scope of performance

You use the Security Configuration Tool for the following tasks:

- Configuration of the SCALANCE S and SOFTNET Security Client;
- Management of projects and users;
- Test and diagnostics functions, status displays.

### Modes

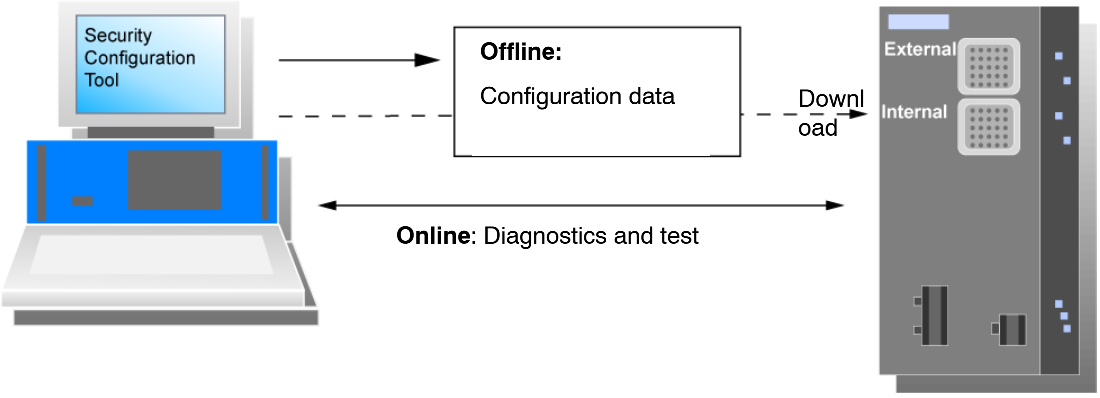
The Security Configuration Tool has two modes:

- Offline - configuration view

  In offline mode, you create the configuration data for the SCALANCE S modules and SOFTNET Security Clients. Prior to downloading, there must already be a connection to a SCALANCE S.

- Online

  The online mode is used for testing and diagnostics of a SCALANCE S.



### Two operating views

The Security Configuration Tool provides to operating views in offline mode:

- Standard mode

  Standard mode is the default mode in the Security Configuration Tool. It allows fast, uncomplicated configuration of SCALANCE S operation.

- Advanced mode.

  Advanced mode provides extended options allowing individual settings for the firewall rules and security functionality.

## 4.2 Installation

You install the Security Configuration Tool from the supplied SCALANCE S CD.

### Prerequisites

The prerequisites for installation and operation of the Security Configuration Tool on a PC/PG are as follows:

- Windows 2000 and Windows XP / SP1 or SP2 as operating system;
- PC/PG with at least 128 Mbytes of RAM and a 1 GHz CPU or faster.

### Follow the steps below:

**Notice**

Before you install the Security Configuration Tool, make sure that you read the ”README” file on the CD. This file contains important notes and any late modifications.

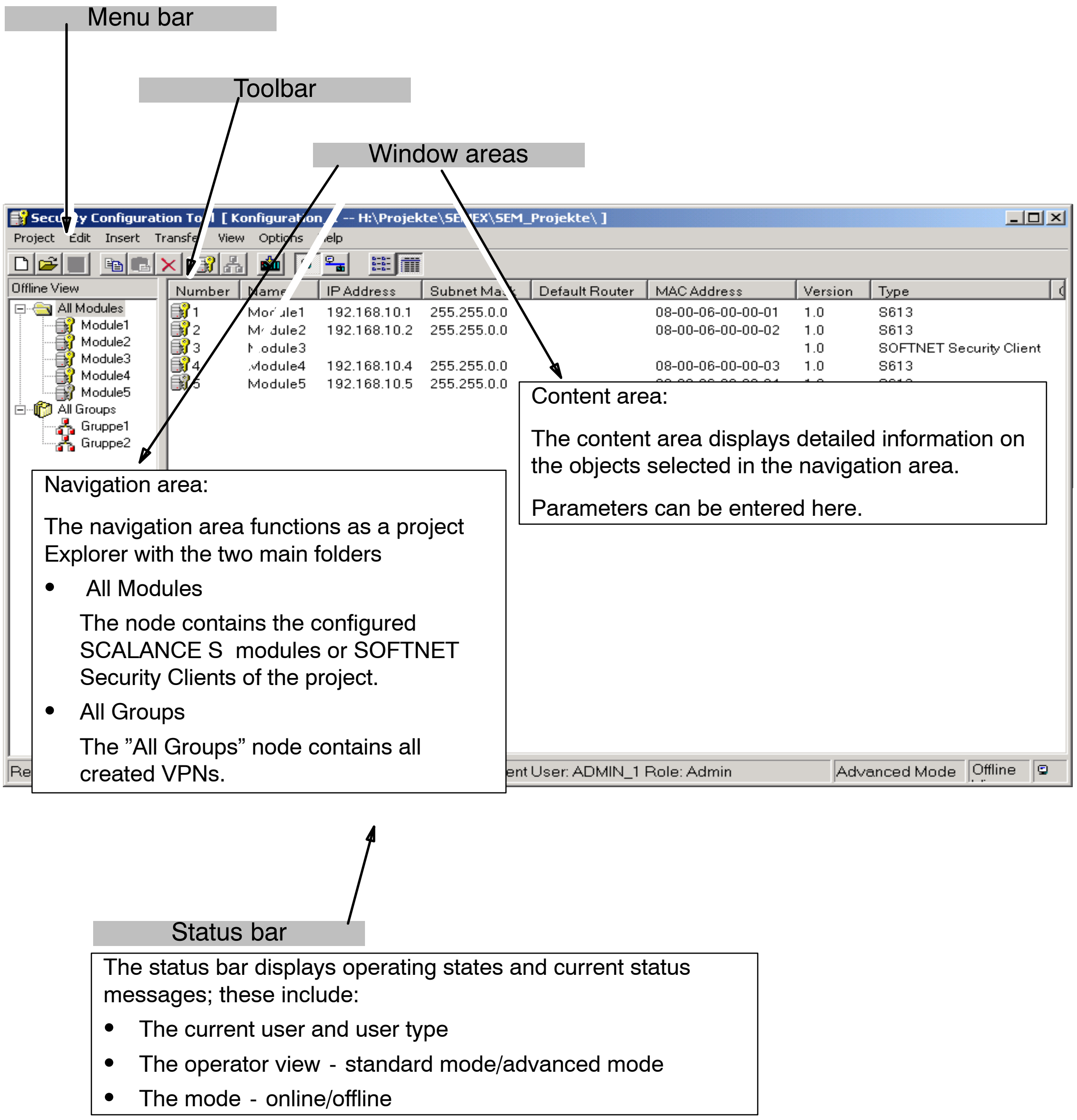
- Insert the SCALANCE S CD in your CD-ROM drive; if the Autorun function is active, the user interface with which you make the installation starts automatically.

or

- Start ”Start.exe” on the SCALANCE S CD supplied.

## 4.3 User interface and menu commands

### Layout of the user interface



| Number | Name | IP Address | Subnet Ma k | Default Router | MAC Address | Version | Type |
|---|---|---|---|---|---|---|---|
| 1 | Mor ule1 | 192.168.10.1 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 |
| 2 | M dule2 | 192.168.10.2 | 255.255.0.0 | | 08-00-06-00-00-02 | 1.0 | S613 |
| 3 | odule3 | | | | | 1.0 | SOFTNET Security Client |
| 4 | Module4 | 192.168.10.4 | 255.255.0.0 | | 08-00-06-00-00-03 | 1.0 | S613 |
| 5 | Module5 | 192.168.10.5 | 255.255.0.0 | | [illegible] | [illegible] | [illegible] |

Content area:

The content area displays detailed information on the objects selected in the navigation area.

Parameters can be entered here.

Navigation area:

The navigation area functions as a project Explorer with the two main folders

- All Modules

  The node contains the configured SCALANCE S modules or SOFTNET Security Clients of the project.

- All Groups

  The ”All Groups” node contains all created VPNs.

The status bar displays operating states and current status messages; these include:

- The current user and user type
- The operator view - standard mode/advanced mode
- The mode - online/offline

When you select an object in the navigation area, you will see detailed information on this object in the content area.

## Menu bar

Below, you will see an overview of the available menu commands and their meaning.

| Menu command | Meaning / remarks | Shortcut |
|---|---|---|
| **Project** ►.. | Functions for project-specific settings and for downloading and saving the project file. | |
| New | Create a new project | |
| Open... | Open the existing project. | |
| Save | Save the open project in the current path and under the current project name. | |
| Save As... | Save the open project in a selectable path and under a selectable project name. | |
| Properties... | Open dialog for project properties. | |
| | | |
| **Edit** ►.. | Note:<br>If you have selected an object, some of the functions listed here are also available in the popup menu available with the right mouse button. | |
| Copy | Copy the selected object. | Ctrl+C |
| Paste | Fetch object from the clipboard and paste. | Ctrl+V |
| Delete | Delete the selected object. | Ctrl+Del |
| Rename | Rename the selected object. | Ctrl+R |
| Properties | Open the properties dialog for the selected object. | |
| Online Diagnostics... | Access test and diagnostic functions. | |
| **Insert** ►.. | (Menu commands only in offline mode) | |
| Module | Create new module. | Ctrl+M |
| Group | Create new group. | Ctrl+G |

| Menu command | Meaning / remarks | Shortcut |
|---|---|---|
| | | |
| **Transfer ▶..** | | |
| To Module... | Download data to the selected modules. | |
| To all Modules... | Download data to all configured modules. | |
| Configuration Status... | Display configuration status of the configured modules in a list. | |
| Firmware Update | Download new firmware to the selected SCALANCE S. | |
| | | |
| **View ▶..** | | |
| Advanced mode | Switch from the standard to the advanced mode.<br>Notice: If you switch to the advanced mode for the current project, you can only switch back as long as you have made no modifications.<br>The standard mode is the default. | Ctrl+E |
| Offline | Is the default. | Ctrl+Shift+D |
| Online | | Ctrl+D |
| Icons / Details | Display of objects on the user interface - as icons or ”detailed”. | |
| | | |
| **Options ▶..** | | |
| IP Service Definition ... | Open a dialog for service definitions for IP firewall rules.<br>(Menu commands only in advanced mode) | |
| MAC Service Definition... | Open a dialog for service definitions for MAC firewall rules.<br>(Menu commands only in advanced mode) | |
| Change Password... | Function for changing the user password. | |
| Network Adapter... | Function for selecting the local network adapter over which a connection will be established to a SCALANCE S. | |
| Log Files... | | |
| | | |
| **Help ▶..** | Help on the functions and parameters required in the Security Configuration Tool. | Ctrl+Shift+F1 |

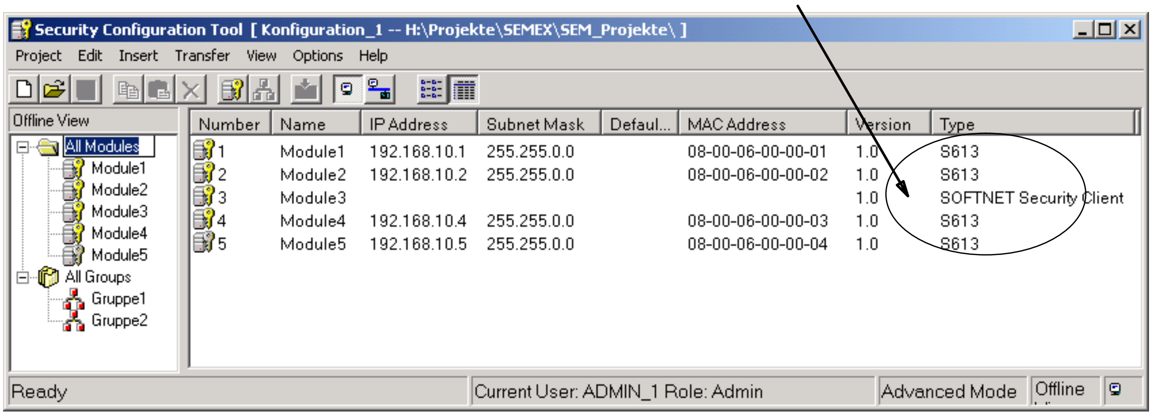
# 4.4 Managing projects

## 4.4.1 Overview

### SCALANCE S project

A project in the Security Configuration Tool includes all the configuration and management information for one or more SCALANCE S devices and SOFTNET Security Clients.

You create a module for each SCALANCE S device and each SOFTNET Security Client in the project.



| Number | Name | IP Address | Subnet Mask | Defaul... | MAC Address | Version | Type |
|---|---|---|---|---|---|---|---|
| 1 | Module1 | 192.168.10.1 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 |
| 2 | Module2 | 192.168.10.2 | 255.255.0.0 | | 08-00-06-00-00-02 | 1.0 | S613 |
| 3 | Module3 | | | | | 1.0 | SOFTNET Security Client |
| 4 | Module4 | 192.168.10.4 | 255.255.0.0 | | 08-00-06-00-00-03 | 1.0 | S613 |
| 5 | Module5 | 192.168.10.5 | 255.255.0.0 | | 08-00-06-00-00-04 | 1.0 | S613 |

Generally, the configurations of a project contain the following:

- Firewall rules for modules

  These are module-specific rules for data traffic in the following directions:

  - from the internal to the external network and vice versa;
  - from the internal network into an IPSec tunnel and vice versa.

- Group assignments for IPSec tunnel

  These specify which modules can communicate with each other over an IPSec tunnel.

  By assigning modules to a group, these modules can establish a communication tunnel over a VPN (virtual private network).

  Only modules in the same group can communicate securely with each other over tunnels and modules can belong to several groups at the same time.

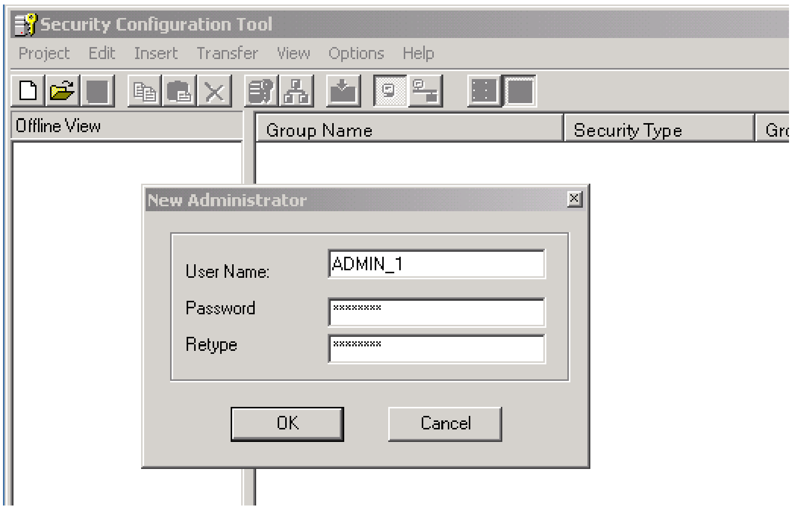
User management also handles access permissions to the project data and therefore to the SCALANCE S devices.

## 4.4.2 Creating and editing projects

### How to create a project

Select the menu command **Project ▸ New..**

You will be prompted to assign a user name and a password. The user you create here is on the type Administrator.


Security Configuration Tool
Project Edit Insert Transfer View Options Help
Offline View
Group Name
Security Type
Gr
New Administrator
OK
Cancel

User Name: ADMIN_1

Password: ********

Retype: ********

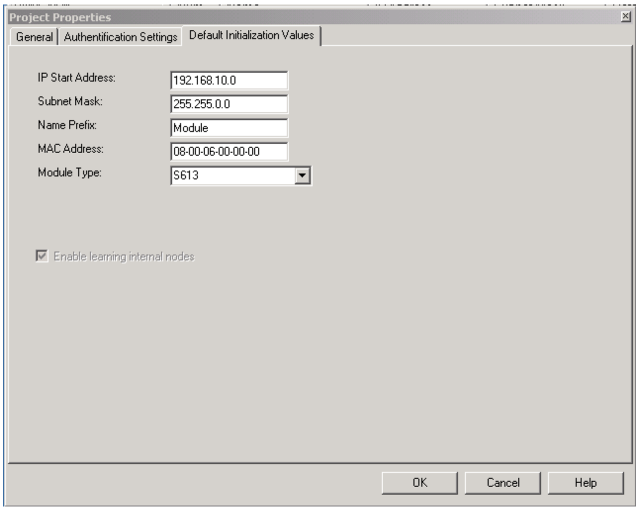
The Security Configuration Tool then creates a default project with 1 SCALANCE S module.

### Specifying initialization values for a project

With the initialization values, you specify the properties to be adopted when you create new modules.

To enter the initialization values, select the following menu command:

**Project ▸ Properties..**



IP Start Address: 192.168.10.0

Subnet Mask: 255.255.0.0

Name Prefix: Module

MAC Address: 08-00-06-00-00-00

Module Type: S613

☑ Enable learning internal nodes

### Protecting project data by encryption

The saved project and configuration data are protected by encryption both in the project file and on the SCALANCE S.

## 4.4.3 Setting up users

### User types and permissions

Access to projects is managed by configurable user settings. SCALANCE S recognizes to user types with different permissions:

- Administrators

  With the ”Administrator” user role, you have unrestricted access to all configuration data.
- User

  With the ”User” user role, you have the following access permissions:

  - Read access to configurations; exception: You are not permitted to change your own password.
  - Read access to a SCALANCE S in the ”Online” mode for testing and diagnostics.

### User authentication

The users of the project must authenticate themselves during access. For each user, you can select either password or certificate authentication.

**Notice**

You must keep your passwords in a secure location.

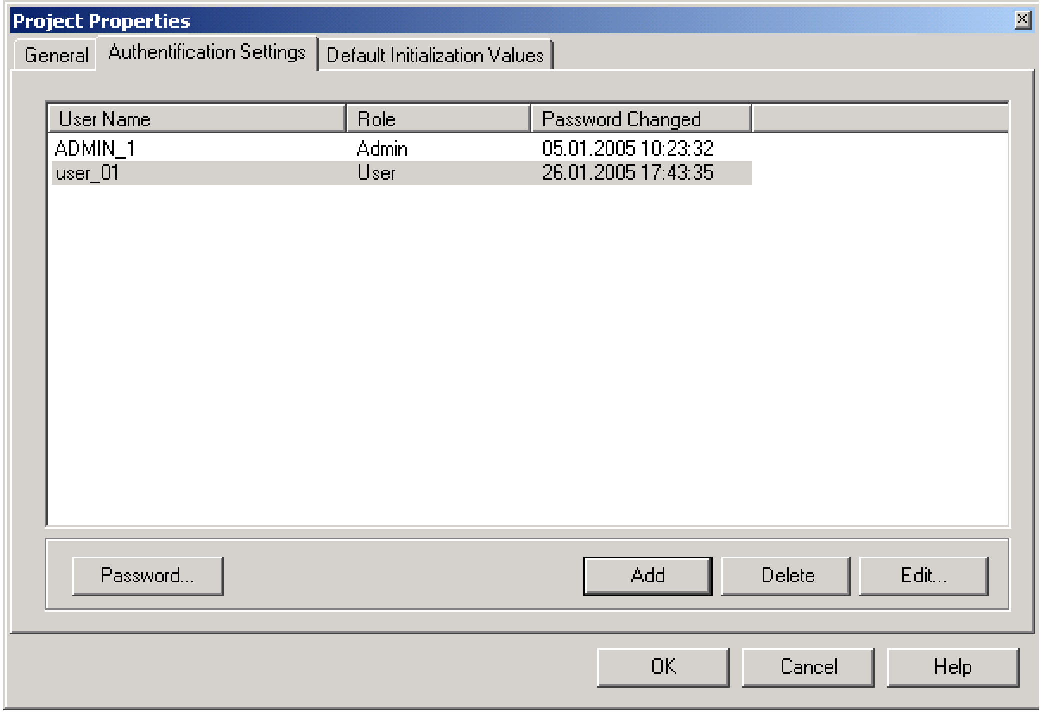
If you have forgotten your passwords, you can no longer access the relevant project and its configurations or the SCALANCE S modules.

You can then only access the SCALANCE S modules by resetting them, although you will lose the configurations.

## Dialog for setting up users

Select the following menu command to set up users:

**Project ▸ Properties..** , ”Authentication Settings” tab.



| User Name | Role | Password Changed |
|---|---|---|
| ADMIN_1 | Admin | 05.01.2005 10:23:32 |
| user_01 | User | 26.01.2005 17:43:35 |

## Protection against accidental prevention of access

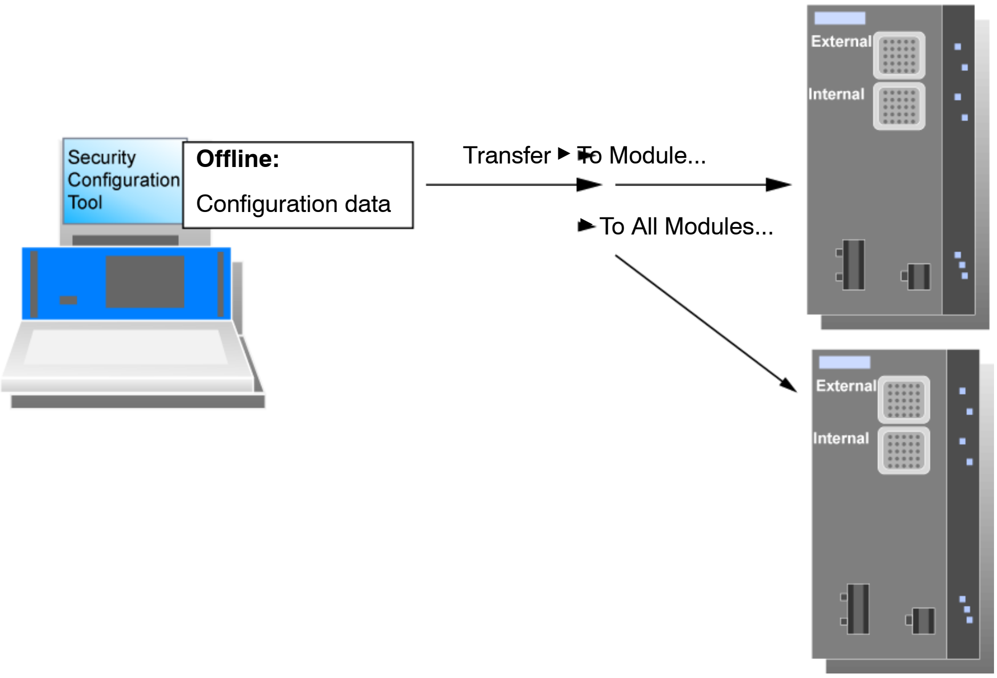
The system makes sure that always one user of the type ”Administrator” is retained in a project.  This prevents access to a project being lost entirely by accidentally deleting yourself.

**Notice**

If the authentication settings are changed, the SCALANCE S modules first have to be reloaded so that the settings (e.g. new user, password changes) become active on the modules.

### 4.4.4 Downloading a configuration to a SCALANCE S

The configuration data created offline is downloaded to the SCALANCE S modules available on the network using suitable menu commands.



**Follow the steps below:**

To download, use the following alternative menu commands:

- **Transfer ▸ To Module...**

  This transfers the configuration to all selected modules.

- **Transfer ▸ To All Modules...**

  This transfers the configuration to all modules configured in the project.

**Prerequisites**

- Ports

  In principle, you can download the configuration data both over device port 1 or device port 2.

  Ideally, you should configure the modules of a group over the common external network of these modules (device port 1). If the configuration computer is located in an internal network, you must enable the IP addresses of the other modules of the group explicitly in the firewall of this SCALANCE S and configure this module first.

**Notice**

If you are using more than one network adapter on your PC/PG, first choose the network adapter via which you can access the SCALANCE S module.

To do so, choose ”Options -> Network adapter...”

- Operating state

  Configurations can be downloaded while the SCALANCE S devices are operating. The devices are only restarted when the IP address has been changed.

**Notice**

- As long as a module has not yet set IP parameters (in other words, prior to the first configuration), there must be no router between the module and the configuration computer.
- If you swap a PC from the internal to the external interface of the SCALANCE S, access from this PC to the SCALANCE S is blocked for approximately 10 minutes.

## Secure transfer

The data is transferred with a secure protocol (SSL - see Section 5.3.9). in addition to this, both communication partners must authenticate themselves.

## Synchronizing configuration discrepancies

It is not possible to read back configuration data from the SCALANCE S module to the project.

# 5 Module properties and firewall

This chapter familiarizes you with the procedures for creating modules and the possible settings for the individual modules in a project. The main emphasis is on the settings for the firewall function of SCALANCE S.

The firewall settings you can make for the individual modules can also influence communication handled over the IPSec tunnel connections in the internal network (VPN).

## Further information

How to configure IPSec tunnels is described in detail in the next chapter of this manual.

You will find additional information on configuring modules of the type SOFTNET Security Client in Chapter 7.

HLP

You will find detailed information on the dialogs and parameter settings in the online help.

F1

You can call this with the F1 key or using the ”Help” button in the relevant dialog.

## 5.1 Creating modules and setting network parameters

### Creating modules

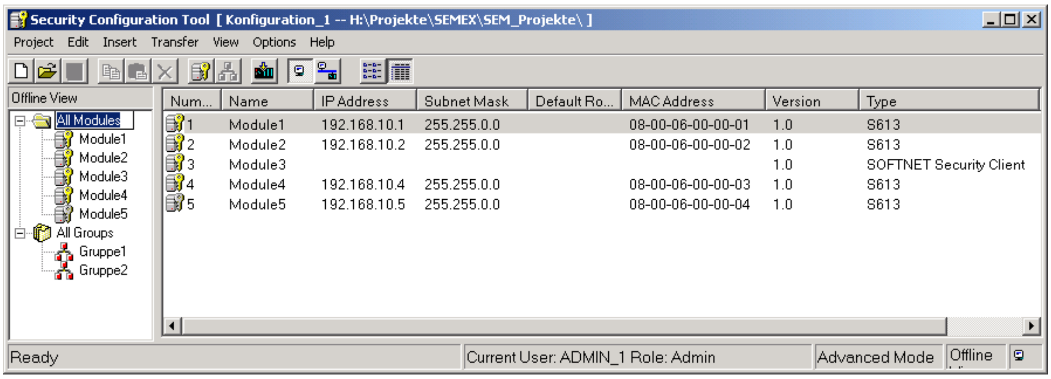
When you create a new project, the Security Configuration Tool creates a default module of the type SCALANCE S.

You can create further modules with the following menu commands:

**Insert ▸ Module**

As an alternative: Using the context menu with the ”All Modules” object selected.

In the next step, select the module type in the ”Type” column.


Security Configuration Tool [ Konfiguration_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ]
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
Module3
Module4
Module5
All Groups
Gruppe1
Gruppe2
Ready
Current User: ADMIN_1 Role: Admin
Advanced Mode
Offline

| Num... | Name | IP Address | Subnet Mask | Default Ro... | MAC Address | Version | Type |
|---|---|---|---|---|---|---|---|
| 1 | Module1 | 192.168.10.1 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 |
| 2 | Module2 | 192.168.10.2 | 255.255.0.0 | | 08-00-06-00-00-02 | 1.0 | S613 |
| 3 | Module3 | | | | | 1.0 | SOFTNET Security Client |
| 4 | Module4 | 192.168.10.4 | 255.255.0.0 | | 08-00-06-00-00-03 | 1.0 | S613 |
| 5 | Module5 | 192.168.10.5 | 255.255.0.0 | | 08-00-06-00-00-04 | 1.0 | S613 |

### Network settings of a module

The network settings of a module include the following:

- Address parameters of the module
- Addresses of external routers

### Address parameters

You can also enter the address parameters in the content area by selecting the ”All Modules” object in the navigation area:

The following properties of the modules are displayed in columns:

Table 5-1 IP parameters - ”All Modules” selected

| Property/column | Meaning | Comment/selection |
|---|---|---|
| Number | Consecutive module number | Assigned automatically |
| Name | Module name reflecting the technology | Freely selectable |
| IP Address | IP address | Assigned as suitable in the network |

Table 5-1 IP parameters - ”All Modules” selected

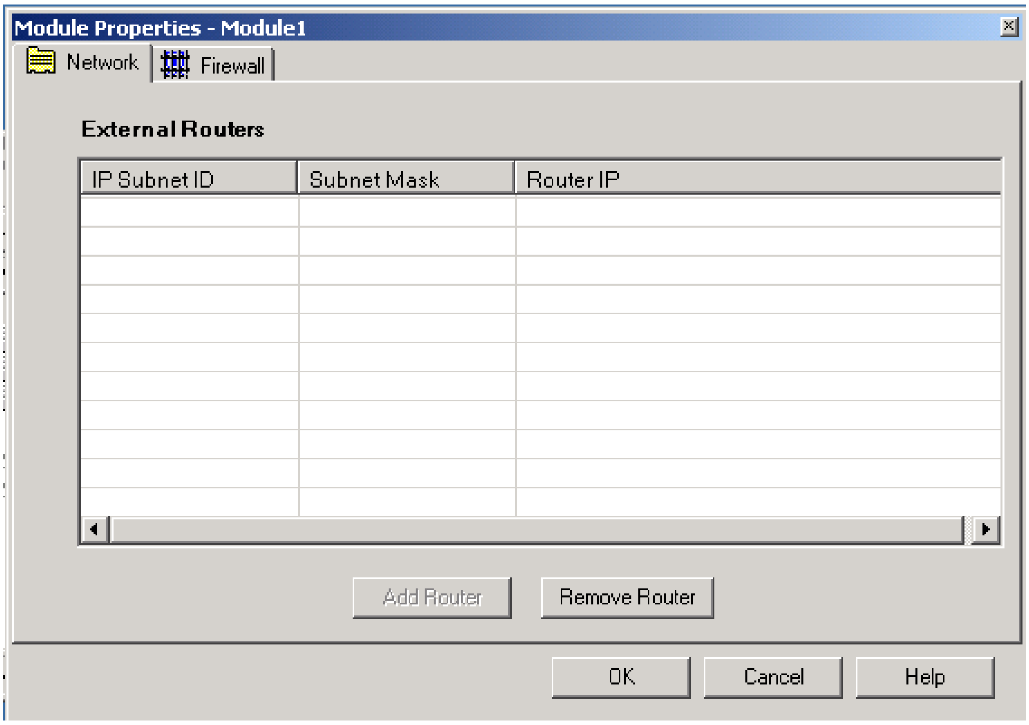
| Property/column | Meaning | Comment/selection |
|---|---|---|
| Subnet Mask | Subnet mask | Assigned as suitable in the network |
| Default Router | IP address of the router in the external network | Assigned as suitable in the network |
| MAC Address | Hardware address of the module | Can be read from the housing of the module |
| Version | Version ID of the selected module type | |
| Type | Device type | • SCALANCE S612<br>• SCALANCE S613<br>• SOFTNET Security Client<br>For this module type, it is not possible to set any further properties and there is therefore no ”Properties Dialog” (for more detailed information on handling, refer to Chapter 7). |
| Comment | Comment | Freely selectable |

## ”Network / External Routers” dialog

Depending on the existing network structure, it is possible that you must specify further routers in addition to the standard router.

Select the module you want to edit and then select the following menu command to set up external routers:

**Edit ▸ Properties..** , ”Network” tab.



# 5.2 Module properties in standard mode

## 5.2.1 Firewall

### Protection from disturbance from the external network

The firewall functionality of SCALANCE S has the task of protecting the internal network from influences or disturbances from the external network. This means that only certain previously specified communication relations between network nodes from the internal network and network nodes from the external network are allowed.

With packet filter rules, you define whether the data traffic passing through is permitted or restricted based on properties of the data packets.

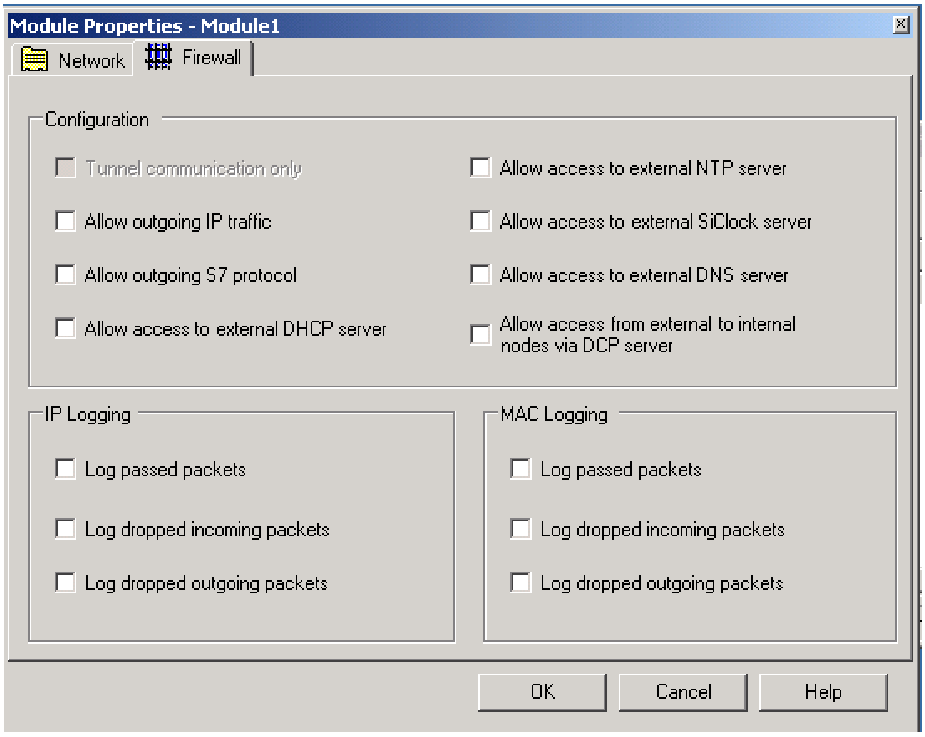
The firewall can be used for encrypted (IPSec tunnel) and unencrypted data traffic.

In standard mode, it is only possible to make settings for unencrypted data traffic.

### Dialog

Select the module you want to edit and then select the following menu command to set up the firewall**:**

**Edit ▸ Properties..**



Module Properties - Module1

Network | Firewall

Configuration

□ Tunnel communication only

□ Allow outgoing IP traffic

□ Allow outgoing S7 protocol

□ Allow access to external DHCP server

□ Allow access to external NTP server

□ Allow access to external SiClock server

□ Allow access to external DNS server

□ Allow access from external to internal nodes via DCP server

IP Logging

□ Log passed packets

□ Log dropped incoming packets

□ Log dropped outgoing packets

MAC Logging

□ Log passed packets

□ Log dropped incoming packets

□ Log dropped outgoing packets

## ”Configuration” option group - predefined rules

**Notice**

Please remember that the risks increase the more options you enable.

The standard mode includes the following predefined rules for the firewall that you can select in the ”Configuration” input area:

Table 5-2 Predefined rules of the simple firewall

| Rule/option | Function | Default Setting |
|---|---|---|
| Tunnel communication only | This is the default setting (for details, see also Section 5.2.2 Firewall defaults).<br>With this setting, only encrypted IPSec data transfer is permitted; only nodes in the internal networks of SCALANCE S can communicate with each other.<br>This option can only be selected when the module is in a group.<br>If this option is deselected, tunnel communication and the type of communication selected in the other check boxes are permitted. | On |
| Allow outgoing IP traffic | Internal nodes can initiate a communication connection to nodes in the external network. Only response packets from the external network are passed on to the internal network.<br>No communication connection can be initiated from the external network to nodes in the internal network. | Off |
| Allow outgoing S7 protocol | Internal nodes can initiate an S7 communication connection (S7 protocol - TCP/port 102) to nodes in the external network. Only response packets from the external network are passed on to the internal network.<br>No communication connection can be initiated from the external network to nodes in the internal network. | Off |
| Allow access to external DHCP server | Internal nodes can initiate a communication connection to a DHCP server in the external network. Only the response packets of the DHCP server are passed into the internal network.<br>No communication connection can be initiated from the external network to nodes in the internal network. | Off |

Table 5-2 Predefined rules of the simple firewall

| Rule/option | Function | Default Setting |
|---|---|---|
| Allow access to external NTP server | Internal nodes can initiate a communication connection to an NTP (Network Time Protocol) server in the external network. Only the response packets of the NTP server are passed into the internal network.<br>No communication connection can be initiated from the external network to nodes in the internal network. | Off |
| Allow access to external SiClock server | This option allows SiClock time-of-day frames from the external network to the internal network. | Off |
| Allow access to external DNS server | Internal nodes can initiate a communication connection to a DNS server in the external network. Only the response packets of the DNS server are passed into the internal network.<br>No communication connection can be initiated from the external network to nodes in the internal network. | Off |
| Allow access from external or internal nodes via DCP server | The DCP protocol is used by the PST tool to set the IP parameters (node initialization) of SIMATIC NET network components.<br>This rule allows nodes in the external network to access nodes in the internal network using the DCP protocol. | Off |

## ”Log” group - setting recording options

You can log the incoming and outgoing data traffic (See Chapter 8).

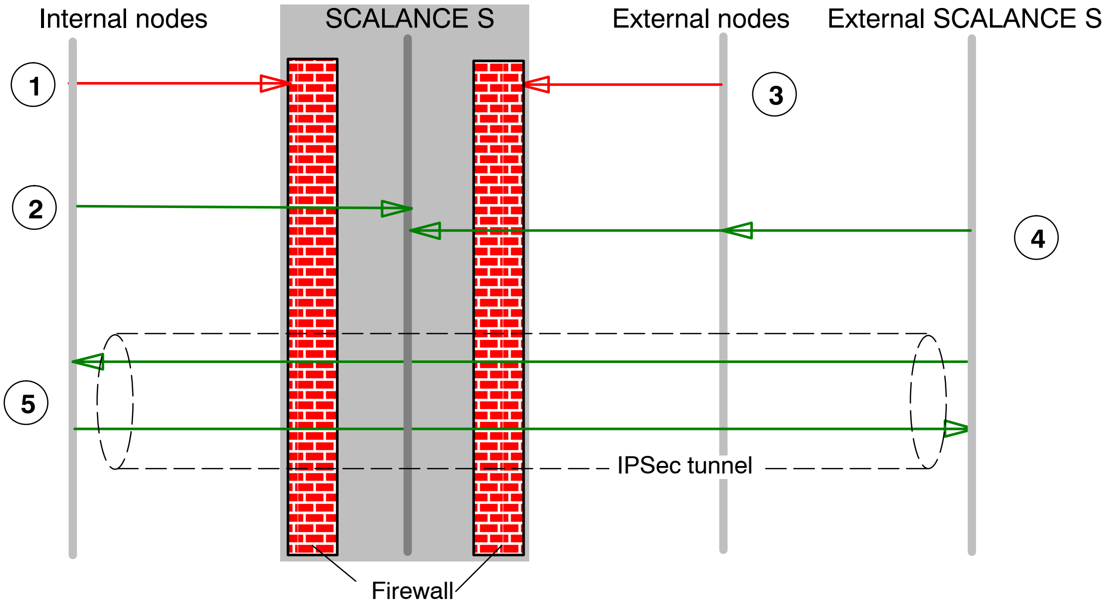
## 5.2.2 Firewall defaults

### Response with defaults

The firewall defaults have been selected so that no IP data traffic is possible. Communication between the nodes in the internal networks of SCALANCE S modules is allowed only if you have configured an IPSec tunnel (see also Table 5-2).

The following diagrams show the default settings in detail for the IP packet filter and the MAC packet filter.

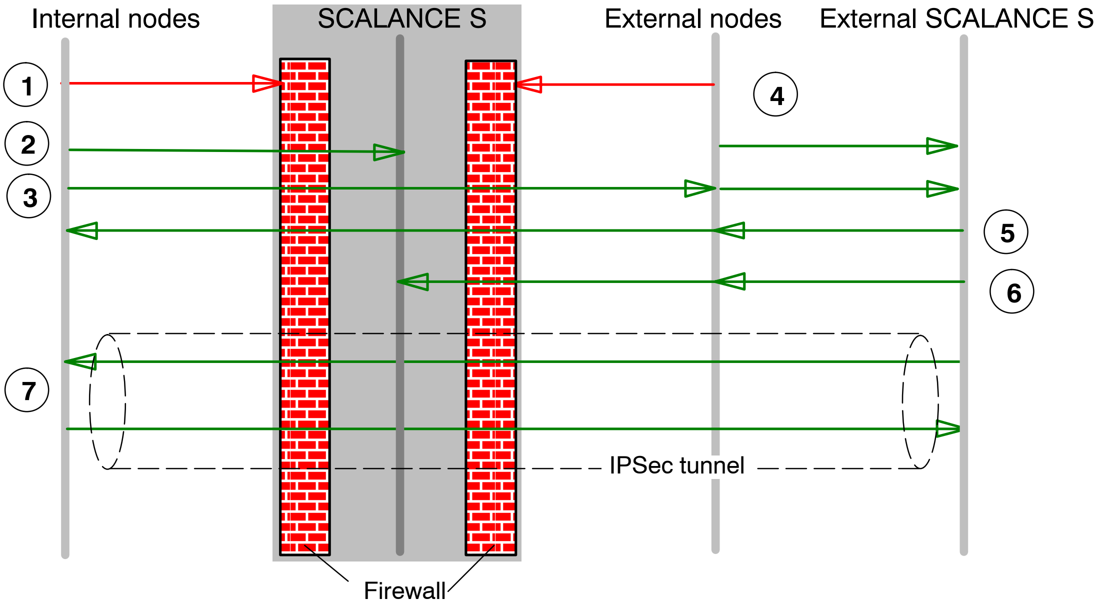
### Default setting for the IP packet filter



Legend:

1. All packet types from internal to external are blocked (except ARP).
2. All packets from internal to SCALANCE S are allowed (only useful for HTTPS).
3. All packets from external to internal and to SCALANCE S are blocked (including ICMP echo request).
4. Packets from external to SCALANCE S of the following types are allowed:
    - HTTPS (SSL)
    - ESP protocol (encryption)
    - IKE (protocol for establishing the IPSec tunnel)
5. IP communication over an IPSec tunnel is allowed.

### Default setting for the MAC packet filter



Legend:

1. All packet types from internal to external are blocked.
2. All packets from internal to SCALANCE S are allowed.
3. ARP packets from internal to external are allowed.
4. All packets from external to internal and to SCALANCE S are blocked.
5. Packets from external to internal of the following types are allowed:
   - ARP with bandwidth limitation
6. Packets from external to SCALANCE S of the following types are allowed:
   - ARP with bandwidth limitation
   - DCP
7. MAC protocols sent through an IPSec tunnel are permitted.

## 5.3 Module properties in advanced mode

Advanced mode provides extended options allowing individual settings for the firewall rules and security functionality.

### Switch over to advanced mode

To use all the functions and menu commands described in section, switch over the mode:

**View ▸ Advanced Mode...**

---

**Note**

If you switch to the advanced mode for the current project, you can no longer switch back if you make any modifications.

---

### 5.3.1 Firewall

In contrast to the configuration of fixed packet filter rules in standard mode, you can configure individual packet filter rules in the Security Configuration Tool in advanced mode.

You can set the packet filter rules in selectable tabs for the following protocols:

- IP protocol
- MAC protocol (layer 3 and 2)

If you do not enter any rules in the dialogs described below, the default settings apply as described in Section5.2.2, Firewall defaults.

## 5.3.2 Firewall: Setting IP rules

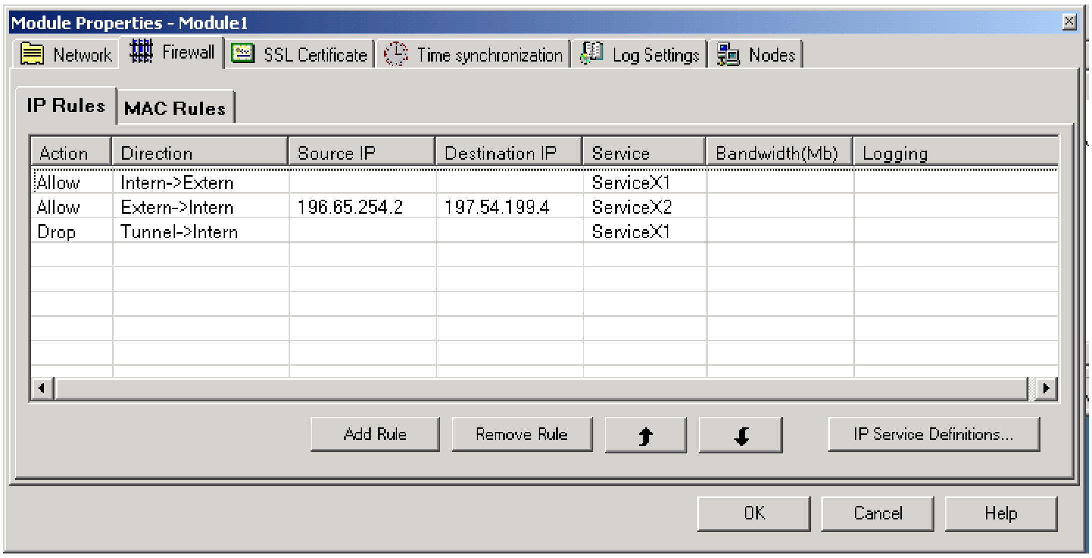
Using the IP packet filter rules, you can filter IP packets such as UDP, TCP, ICMP packets.

Within a packet filter rule, you can also use the service definitions as a basis. This can greatly simplify rule definition (see Section5.3.3).

### Opening the dialog for packet filter rules

Select the module you want to edit and then select the following menu command to set up the firewall:

**Edit ▸ Properties..**



| Action | Direction | Source IP | Destination IP | Service | Bandwidth(Mb) | Logging |
|---|---|---|---|---|---|---|
| Allow | Intern->Extern | | | ServiceX1 | | |
| Allow | Extern->Intern | 196.65.254.2 | 197.54.199.4 | ServiceX2 | | |
| Drop | Tunnel->Intern | | | ServiceX1 | | |

### Entering packet filter rules

Enter the firewall rules in the list one after the other; note the following parameter description and the examples.

HLP

F1

The online help explains the meaning of the individual buttons.

## IP packet rules

The configuration of an IP rule includes the following parameters:

Table 5-3 IP rules: parameter

| Name | Meaning/comment | Selection options / possible values |
|---|---|---|
| Action | Allow/disallow (enable/block) | • Allow<br>Allow packets according to definition.<br>• Drop<br>Block packets according to definition. |
| Direction | Specifies the direction of data traffic | • Internal->external<br>• Internal<-external<br>• Tunnel->internal<br>• Tunnel<-internal<br>• Internal->any<br>• Internal<-any |
| Source IP | Source IP address | Refer to the section "IP addresses in IP packet filter rules" in this chapter. |
| Destination IP | Destination IP address | |
| Service | Name of the IP/ICMP service used.<br>Using the service definitions, you can define succinct and clear packet filter rules.<br>Here, you select one of the services you defined in the IP services dialog:<br>• IP services - see Section 5.3.3<br>or<br>• ICMP services - see Section 5.3.4<br>If you have not yet defined any services or want to define a further service, click the "IP/MAC Service Definition.." button. | The drop-down list box displays the configured services you can select.<br>No entry means: No service is checked, the rule applies to all services. |
| Bandwidth (Mb), | Option for setting a bandwidth limitation.<br>A packet passes through the firewall if the pass rule matches and the permitted bandwidth for this rule has not yet been exceeded. | Value range:<br>0...100 Mbit/s |
| Logging | Enable or disable logging for this rule<br>See also Chapter 8 | |

## IP addresses in IP packet filter rules

The IP address consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 141.80.0.16

In the packet filter rule, you have the following options for specifying IP addresses:

- Nothing specified

  There is no check, the rule applies to all IP addresses.

- An IP address

  The rule applies specifically to the specified address.

- Address range

  The rule applies to all the IP addresses covered by the address range.

  An address range is defined by specifying the number of valid bit places in the IP address in the format:

  **[IP address]/[number of bits to be included]**

  - [IP address]/24 therefore means that only the most significant 24 bits of the IP address are included in the filter rule: These are the first 3 octets or numbers numbers in the IP address.
  - [IP address ]/25 means that only the first three octets and the highest bit of the fourth octet of the IP address are included in the filter rule.

Table 5-4 Examples of address ranges in IP addresses

| **Source IP or destination IP** | **Address range** | | **Number Addresses *)** |
|---|---|---|---|
| | **from** | **to** | |
| 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** | 192.168.10.128 | 192.168.10.255 | 128 |
| 192.168.10.0/**26** | 192.168.10.192 | 192.168.10.255 | 64 |
| 192.168.10.0/**27** | 192.168.10.224 | 192.168.10.255 | 32 |
| 192.168.10.0/**28** | 192.168.10.240 | 192.168.10.255 | 16 |
| 192.168.10.0/**29** | 192.168.10.248 | 192.168.10.255 | 8 |
| 192.168.10.0/**30** | 192.168.10.252 | 192.168.10.255 | 4 |

*) Note: Note that the address values 0 and 255 in the IP address have a special function (0 stands for a network address, 255 for a broadcast address). The number of actually available addresses is therefore reduced.

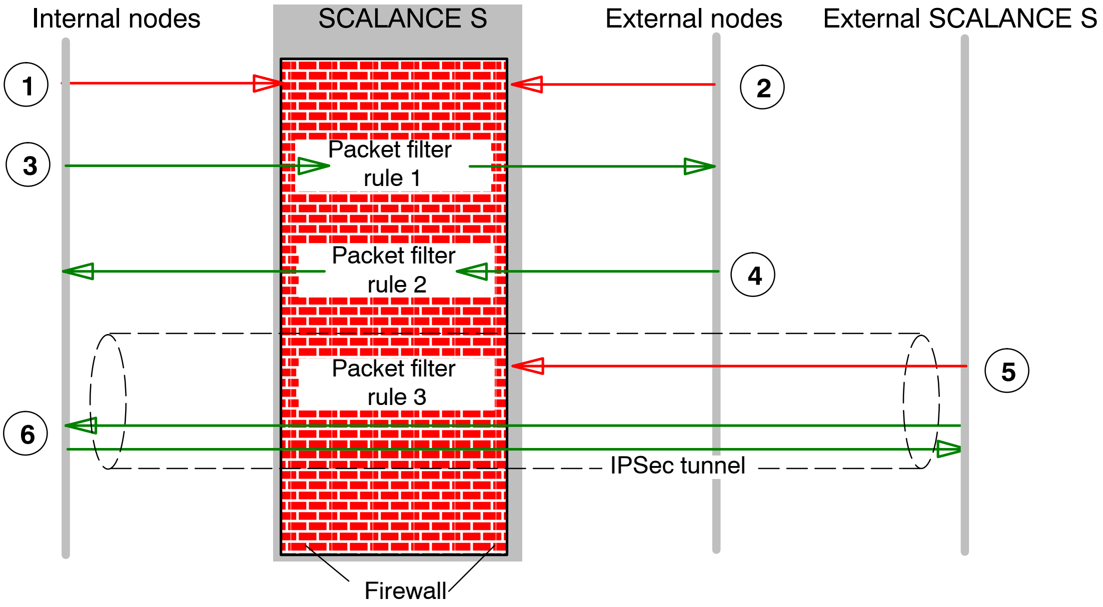
## How SCALANCE S evaluates the rules

The packet filter rules are evaluated by a SCALANCE S as follows:

- The list is evaluated from top to bottom; if rules are contradictory, the rule higher in the list is therefore applied.
- In rules for communication between the internal and external network, the final rule is: All packets except for the packets explicitly allowed in the list are blocked.
- In rules for communication between the internal network and IPsec tunnel, the final rule is: All packets except for the packets explicitly blocked in the list are allowed.

## Example

The packet filter rules shown as examples on page 88 have the following effects:



Legend:

1. All packet types from internal to external are blocked as default, except for those explicitly allowed.
2. All packet types from external to internal are blocked as default, except for those explicitly allowed.
3. IP packet filter rule 1 allows packets with the service definition ”Service X1” from internal to external.
4. IP packet filter rule 2 allows packets from external to internal when the following conditions are met:
   - IP address of the sender: 196.65.254.2
   - IP address of the recipient: 197.54.199.4

- Service definition: ”Service X2”

5. IP packet filter rule 3 blocks packets with the service definition ”Service X2” in the VPN (IPsec tunnel).
6. IPsec tunnel communication is allowed as default except for the explicitly blocked packet types.

### 5.3.3 Firewall: defining IP services

Using the IP service definitions, you can define succinct and clear firewall rules. You select a name and assign the service parameters to it.

These services defined in this way can also be grouped together under a group name (see also Section 5.3.7).

When you configure the packet filter rule, you simply use this name.

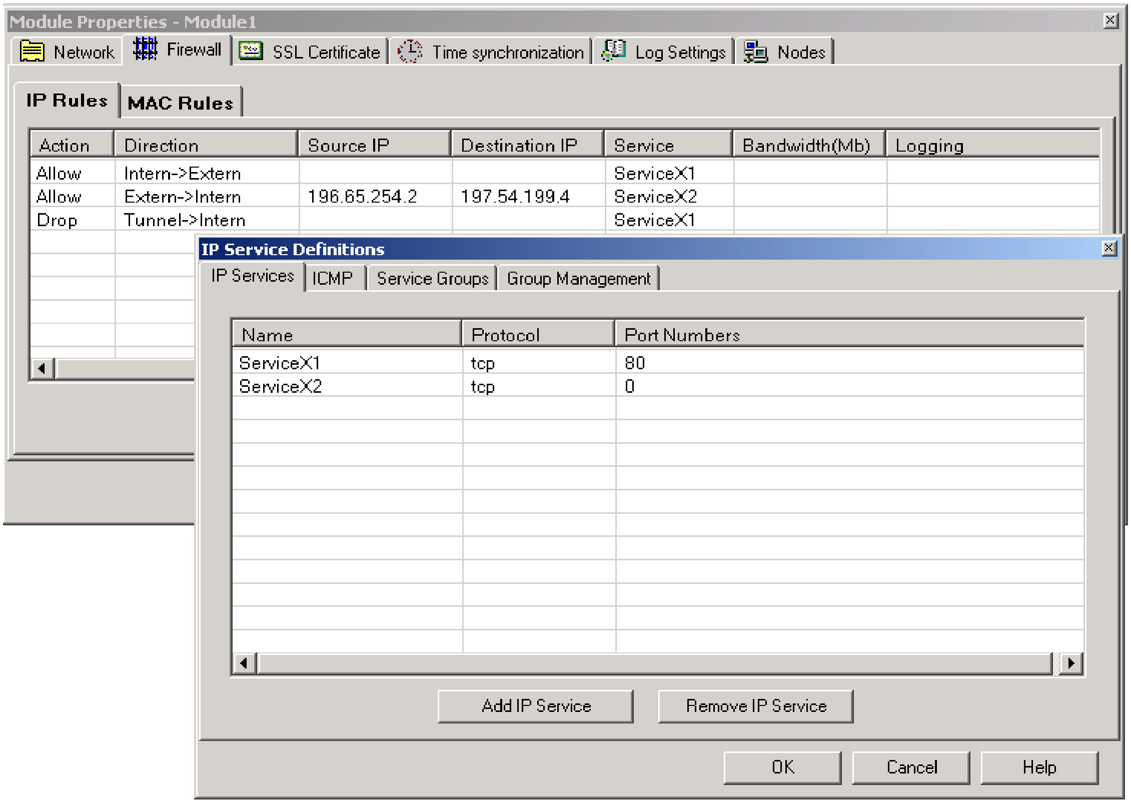
## Dialog / tab

Open the dialog as follows:

- With the menu command **Options ▸ IP/MAC Service Definition...**

  or

- From the ”Firewall/IP Rules” tab with the ”IP/MAC Service Definition..” button. .



| Action | Direction | Source IP | Destination IP | Service | Bandwidth(Mb) | Logging |
|---|---|---|---|---|---|---|
| Allow | Intern->Extern | | | ServiceX1 | | |
| Allow | Extern->Intern | 196.65.254.2 | 197.54.199.4 | ServiceX2 | | |
| Drop | Tunnel->Intern | | | ServiceX1 | | |

| Name | Protocol | Port Numbers |
|---|---|---|
| ServiceX1 | tcp | 80 |
| ServiceX2 | tcp | 0 |

## Parameters for IP services

You define the IP services using the following parameters:

Table 5-5 IP services: parameter

| Name | Meaning/comment | Selection options / possible values |
|---|---|---|
| Name | User-definable name for the service that is used as identification in the rule definition or in the group. | Can be selected by user |
| Protocol | Name of the protocol type | TCP<br>UDP<br>Any (TCP and UDP) |
| Port Number | Port number that defines a specific service | Examples:<br>80: Web HTTP service<br>102: S7 protocol - TCP/port |

## 5.3.4 Firewall: defining ICMP services

Using the ICMP service definitions, you can define succinct and clear firewall rules. You select a name and assign the service parameters to it.

These services defined in this way can also be grouped together under a group name (see also Section 5.3.7).

When you configure the packet filter rule, you simply use this name.

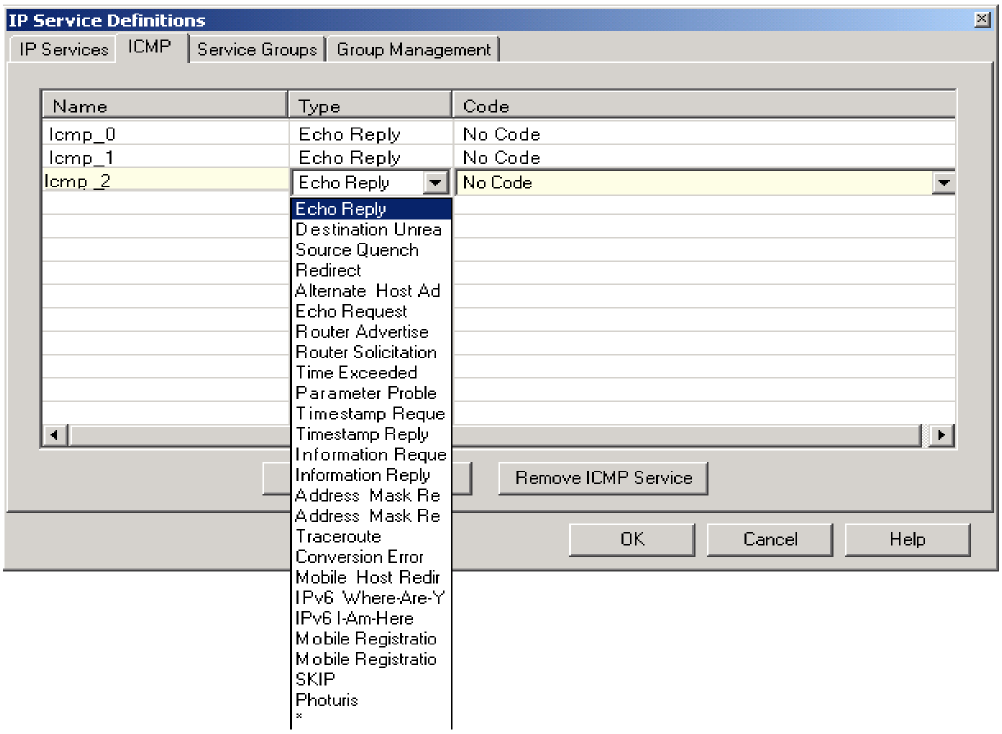
### Dialog / tab

Open the dialog as follows:

- With the menu command **Options ▸ IP/MAC Service Definition...**

  or

- From the ”Firewall” tab with the ”IP/MAC Service Definition..” button. .



IP Service Definitions

| Name | Type | Code |
|---|---|---|
| Icmp_0 | Echo Reply | No Code |
| Icmp_1 | Echo Reply | No Code |
| Icmp_2 | Echo Reply | No Code |

## Parameters for ICMP services

You define the ICMP services using the following parameters:

Table 5-6 ICMP services: parameter

| Name | Meaning/comment | Selection options / possible values |
|---|---|---|
| Name | User-definable name for the service that is used as identification in the rule definition or in the group. | Can be selected by user |
| Type | Type of ICMP message | • See dialog box |
| Code | Codes of the ICMP type | Values depend on the selected type. |

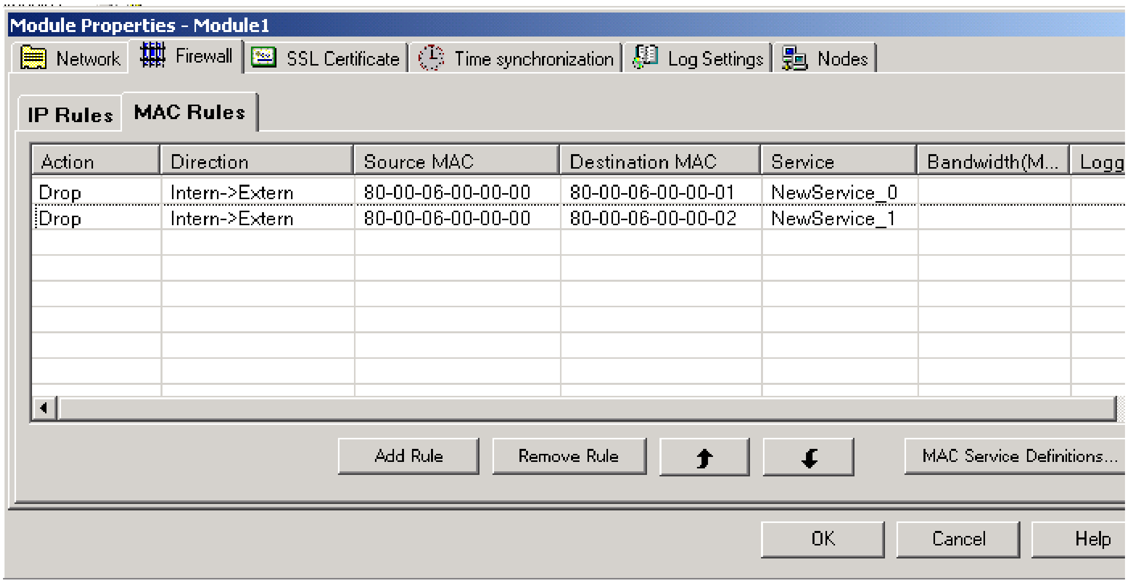
## 5.3.5 Firewall: Setting MAC packet filter rules

With MAC packet filter rules, you can filter MAC packets.

### Dialog / tab

Select the module you want to edit and then select the following menu command to set up the firewall:

**Edit ▸ Properties..**



| Action | Direction | Source MAC | Destination MAC | Service | Bandwidth(M... | Logg |
|---|---|---|---|---|---|---|
| Drop | Intern->Extern | 80-00-06-00-00-00 | 80-00-06-00-00-01 | NewService_0 | | |
| Drop | Intern->Extern | 80-00-06-00-00-00 | 80-00-06-00-00-02 | NewService_1 | | |

### Entering packet filter rules

Enter the firewall rules in the list one after the other.

HLP
F1

The online help explains the meaning of the individual buttons.

## MAC packet filter rules

The configuration of a MAC rule includes the following parameters:

Table 5-7 MAC rules: parameter

| Name | Meaning/comment | Selection options / possible values |
|---|---|---|
| Action | Allow/disallow (enable/block) | • Allow<br>Allow packets according to definition.<br>• Drop<br>Block packets according to definition. |
| Direction | Specifies the direction and type of data traffic | • Internal->external<br>• Internal<-external<br>• Tunnel->internal<br>• Tunnel<-internal<br>• Internal->any<br>• Internal<-any |
| Source MAC | Source MAC address | |
| Destination MAC | Destination MAC address | |
| Service | Name of the MAC service being used | |
| Bandwidth (Mb), | Option for setting a bandwidth limitation.<br>A packet passes through the firewall if the pass rule matches and the permitted bandwidth for this rule has not yet been exceeded. | Value range:<br>0...100 Mbit/s |
| Logging | Enable or disable logging for this rule | |

## How SCALANCE S evaluates the rules

The packet filter rules are evaluated by a SCALANCE S as follows:

- The list is evaluated from top to bottom; if rules are contradictory, the rule higher in the list is therefore applied.
- In rules for communication between the internal and external network, the final rule is: All packets except for the packets explicitly allowed in the list are blocked.
- In rules for communication between the internal network and IPsec tunnel, the final rule is: All packets except for the packets explicitly blocked in the list are allowed.

## Examples

You can apply the example of an IP packet filter in Section 5.3.2 analogously to the MAC packet filter rules.

## 5.3.6 Firewall: defining MAC services

Using the MAC service definitions, you can define succinct and clear firewall rules. You select a name and assign the service parameters to it.

These services defined in this way can also be grouped together under a group name (see also Section 5.3.7).

When you configure the packet filter rule, you simply use this name.

### Dialog

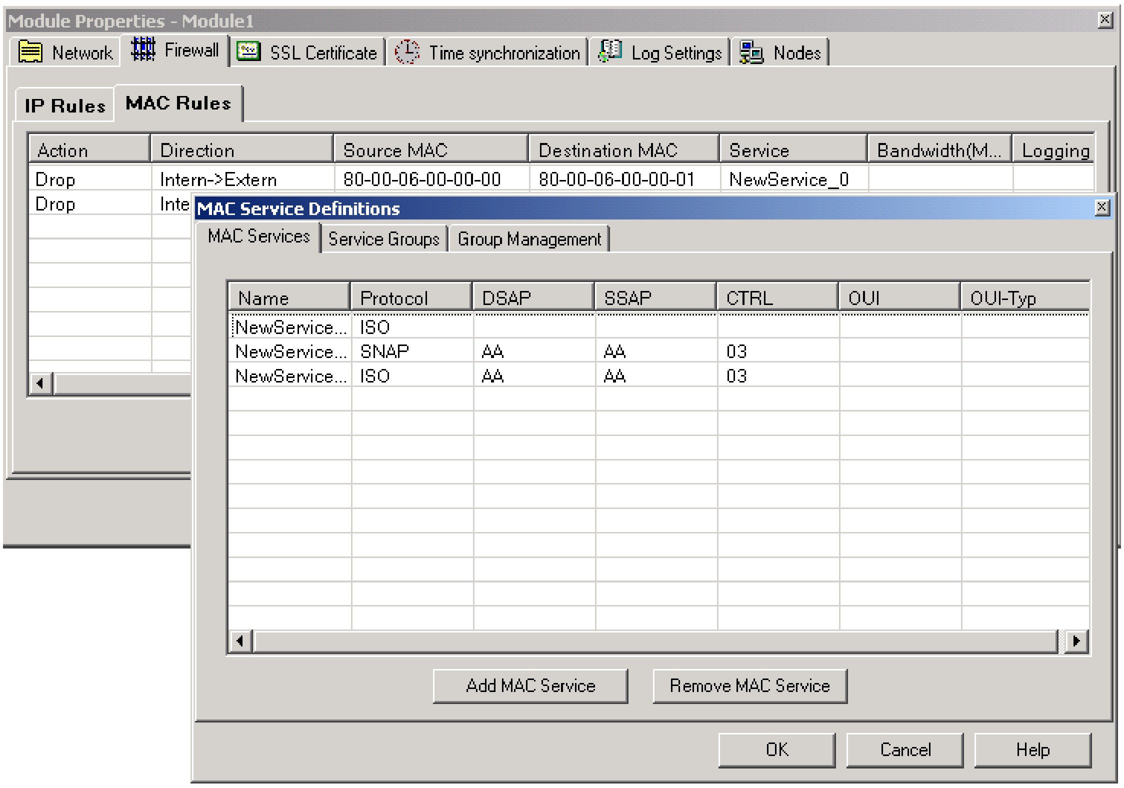
Open the dialog as follows:

- Using the following menu command:

  **Options ▸ IP/MAC Service Definition...**

  or

- From the ”Firewall/MAC Rules” tab with the ”IP/MAC Service Definition..” button. .



| Action | Direction | Source MAC | Destination MAC | Service | Bandwidth(M... | Logging |
|---|---|---|---|---|---|---|
| Drop | Intern->Extern | 80-00-06-00-00-00 | 80-00-06-00-00-01 | NewService_0 | | |
| Drop | Inte | | | | | |

| Name | Protocol | DSAP | SSAP | CTRL | OUI | OUI-Typ |
|---|---|---|---|---|---|---|
| NewService... | ISO | | | | | |
| NewService... | SNAP | AA | AA | 03 | | |
| NewService... | ISO | AA | AA | 03 | | |

## Parameters for MAC services

A MAC service definition includes a category of protocol-specific MAC parameters:

Table 5-8 MAC services - parameters

| Name | Meaning/comment | Selection options / possible values |
|---|---|---|
| Name | User-definable name for the service that is used as identification in the rule definition or in the group. | Can be selected by user |
| Protocol | Name of the protocol type:<br>• ISO<br>ISO identifies packets with the following properties:<br>Lengthfield <= 05DC (hex),<br>DSAP= user-defined<br>SSAP= user-defined<br>CTRL= user-defined<br>• SNAP<br>SNAP identifies packets with the following properties:<br>Lengthfield <= 05DC (hex),<br>DSAP=AA (hex),<br>SSAP=AA (hex),<br>CTRL=03 (hex),<br>OUI=user-defined,<br>OUI-Type=user-defined | • ISO<br>• SNAP<br>• 0x (code entry) |
| DSAP | Destination Service Access Point: LLC recipient address | |
| SSAP | Source Service Access Point: LLC sender address | |
| CTRL | LLC control field | |
| OUI | Organizationally Unique Identifier (the first three bytes of the MAC address = vendor identification) | |
| OUI-Type | Protocol type/identification | |

*) The protocol entries 0800 (hex) and 0806 (hex) are not accepted since these value is apply to IP or ICMP packets. These packets are filtered using IP rules.

## Special settings for SIMATIC NET services

To filter special SIMATIC NET services, please use the following SNAP settings:

- DCP (Primary Setup Tool):

  OUI= 08 00 06 (hex) , OUI-Type= 01 FD (hex)
- SiClock :

  OUI= 08 00 06 (hex) , OUI-Type= 01 FD (hex)

## 5.3.7 Firewall: setting up service groups

### Creating service groups

You can put several services together by creating service groups. In this way, you can set up more complex services that can be used in the packet filter rules simply by selecting the name.

### Dialogs / tabs

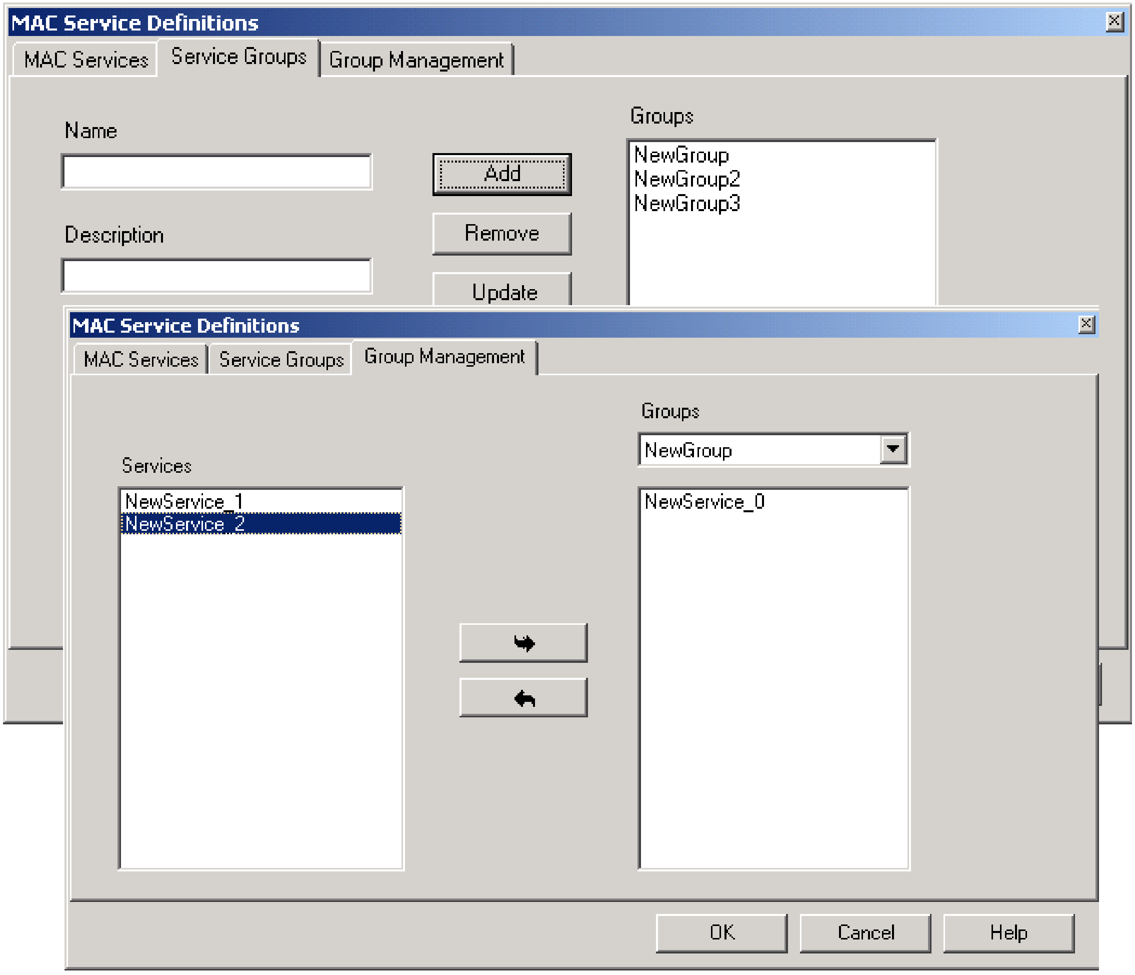
Open the dialog as follows:

- Using the following menu command:

  **Options ▸ IP/MAC Service Definition...**

  or

- From the ”Firewall/IP Rules” tab or ”Firewall/MAC Rules” with the ”IP/MAC Service Definition..” button. .



Groups: NewGroup, NewGroup2, NewGroup3

Groups: NewGroup

Services: NewService_1, NewService_2

NewService_0

### 5.3.8 Time synchronization

#### Meaning

The date and time are kept on the SCALANCE S module to check the validity (time) of a certificate and for the time stamps of log entries.

#### Alternative methods of timekeeping

The following alternatives can be configured:

- Local PC clock

  The module time is set automatically to the PC time when a configuration is downloaded.

- NTP server

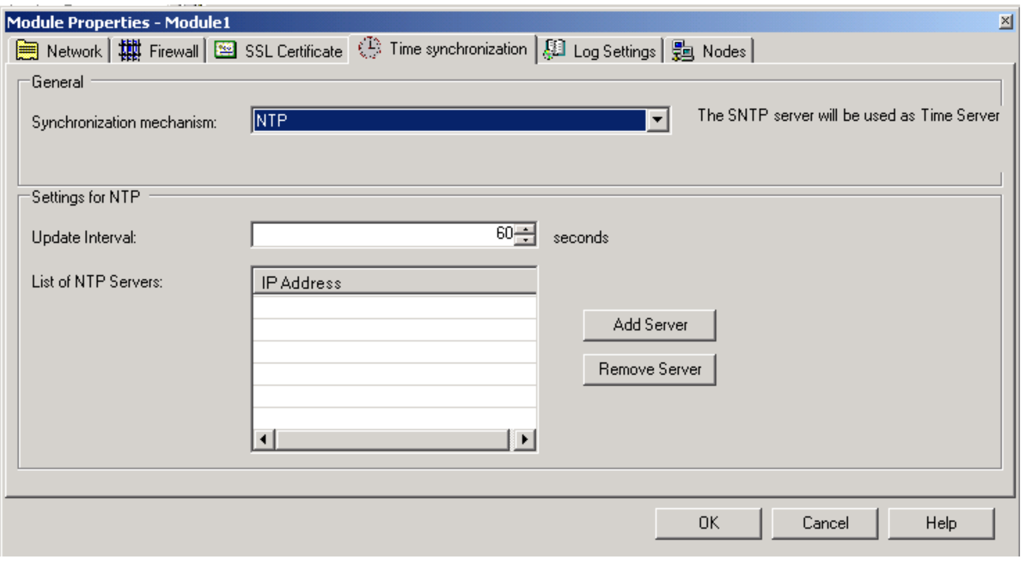
  Automatic setting and periodic synchronization of the time using an NTP server (Network Time Protocol).

It is also possible to set the module time manually in the online view in the ”Test/Control” tab (see also Section 8.1).

#### Opening the dialog for configuring time synchronization

Select the module you will want to edit and then the following menu command:

**Edit ▸ Properties..** , ”Time Synchronization” tab



Module Properties - Module1

General

Synchronization mechanism: NTP

The SNTP server will be used as Time Server

Settings for NTP

Update Interval: 60 seconds

List of NTP Servers:

| IP Address |
|---|

#### Synchronization by an NTP time server

If you want the time to be synchronized by an NTP time server, specify the two following parameters in the configuration:

- IP address of the NTP server
- The update interval in seconds

**Notice**

If the NTP server cannot be reached by the SCALANCE S over an IPsec tunnel connection, you must allow the packets from the NTP server explicitly in the firewall (UDP, Port 123).

### External time frames

External time frames are not secure and can be corrupted/counterfeited in the external network. This can, for example, lead to falsification of the local time in the internal network and on SCALANCE S modules.

For this reason, NTP servers should be located in internal networks:

### 5.3.9 Creating SSL certificates

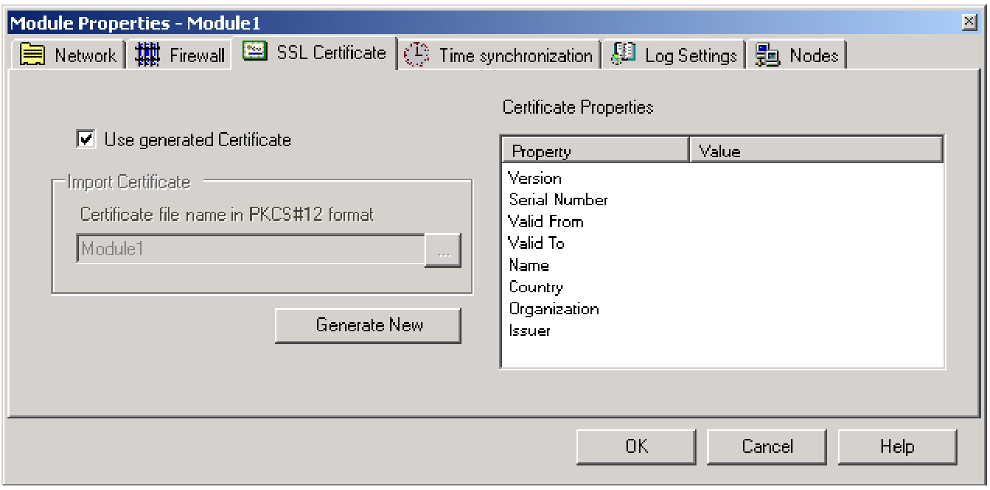
#### Meaning

SSL certificates are used for authentication of the communication between PG/PC and SCALANCE S when downloading the configuration and when logging.

#### Opening the dialog for managing SSL certificates

Select the module you will want to edit and then the following menu command:

**Edit ▸ Properties..** , ”Certificates” tab



☑ Use generated Certificate

Certificate file name in PKCS#12 format: Module1

Certificate Properties

| Property | Value |
|---|---|
| Version | |
| Serial Number | |
| Valid From | |
| Valid To | |
| Name | |
| Country | |
| Organization | |
| Issuer | |

# 6 Secure communication in the VPN over an IPsec tunnel

This chapter describes how to connect the IP subnets protected by a SCALANCE S to a virtual private network using drag-and-drop.

As already described in Chapter 5 in the module properties, you can once again use the default settings to achieve secure communication within your internal networks.

## Further information

You will find additional information on configuring modules of the type SOFTNET Security Client in Chapter 7.

HLP

You will find detailed information on the dialogs and parameter settings in the online help.

F1

You can call this with the F1 key or using the ”Help” button in the relevant dialog.

## 6.1 VPN with SCALANCE S

### Secure connection through an unprotected network

In the internal networks protected by a SCALANCE S, IPsec tunnels allow a secure data connection through the non-secure external network.

Data exchange between devices through the IPsec tunnel in the VPN has the following properties:

- Confidentiality

  The data exchanged is safe from eavesdropping;

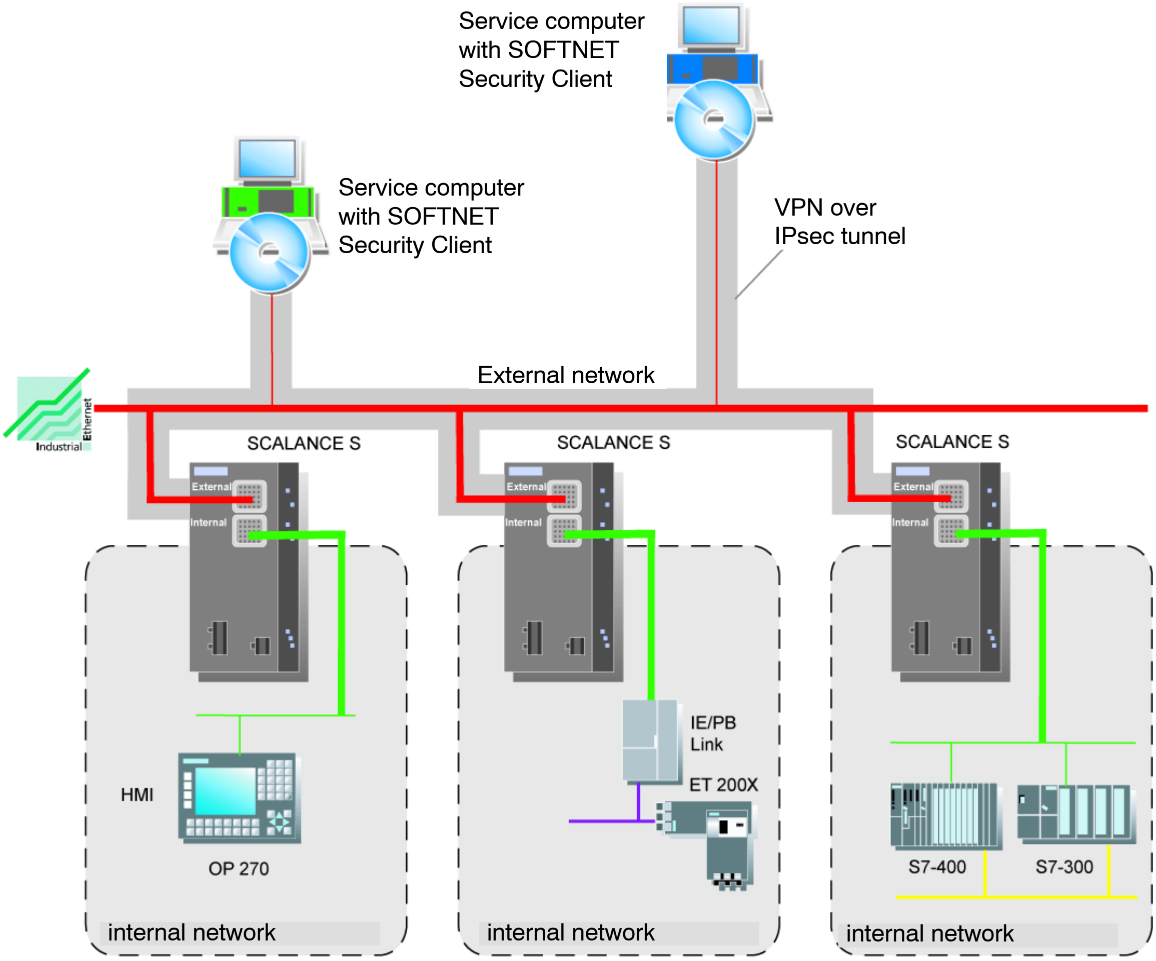
- Integrity

  The data exchanged is safe from corruption/counterfeiting;

- Authenticity

  Only users with the appropriate authorization can create a tunnel.

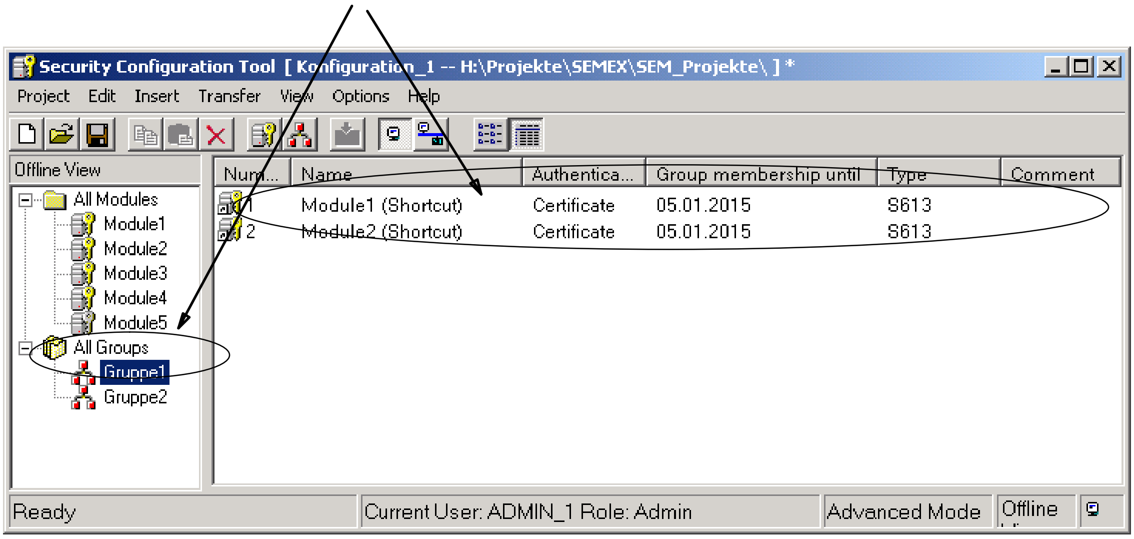
SCALANCE S uses the IPsec protocol for tunneling (tunnel mode of IPsec).



## Tunnel connection between modules are the same group (VPN)

The properties of a VPN are put together in a module group on the SCALANCE S for all IPsec tunnels.

IPsec tunnels are established automatically between all SCALANCE S modules and SOFTNET Security Client modules that belong to the same group.



| Num... | Name | Authentica... | Group membership until | Type | Comment |
|---|---|---|---|---|---|
| 1 | Module1 (Shortcut) | Certificate | 05.01.2015 | S613 | |
| 2 | Module2 (Shortcut) | Certificate | 05.01.2015 | S613 | |

SCALANCE S modules can belong to several different groups at the same time in one project.

**Notice**

If the name of a SCALANCE S module is changed, all the SCALANCE S modules in the groups to which the modified module belongs must be reconfigured.

**Notice**

Layer 2 frames are tunneled only when there is no router between two SCALANCE S modules.

The following applies in general: Non-IP packets are transferred through a tunnel only when the devices that send or receive the packets were able to communicate previously; in other words, without using the SCALANCE S.

Whether or not the network nodes were able to communicate prior to the use of the SCALANCE S is decided based on the IP networks in which the security modules are located. If the SCALANCE S modules are located in the same IP subnet, it is assumed that the end devices in the networks secured by the SCALANCE S were able to communicate with non-IP packets prior to the use of the SCALANCE S. The non-IP packets are then tunneled.

## Authentication method

The authentication method is specified within a group (within a VPN) and decides the type of authentication used.

Key-based or certificate-based authentication methods are supported:

- Preshared keys

  The ”preshared keys” method is asymmetrical key method.

  The key must be known at both ends prior to communication.

  This key is generated automatically when a group is created and is distributed to all modules automatically during downloads. To achieve this, you enter a password in the ”Key” box in the ”Group Properties” dialog from which the key is generated.

- Certificate

  Certificate-based authentication is the default that is also active in standard mode. The procedure is as follows:

  - When a group is generated, a group certificate is generated (group certificate = CA certificate).
  - Each SCALANCE S in the group receives a certificate signed with the certificate of the group.

  All certificates are based on the ITU standard X.509v3 (ITU, International Telecommunications Union).

  The certificates can be generated by a certification center in the Security Configuration Tool (see Section 5.3.9).

**Notice**

Restriction in VLAN operation

Within a VLAN, it is not possible to operate a VPN setup with SCALANCE S.

Reason: The VLAN tags are lost in unicast packets when they pass through the SCALANCE S because IPsec is used to transfer the IP packets. Only IP packets (not Ethernet packets) are transferred through an IPsec tunnel and the VLAN tags are therefore lost.

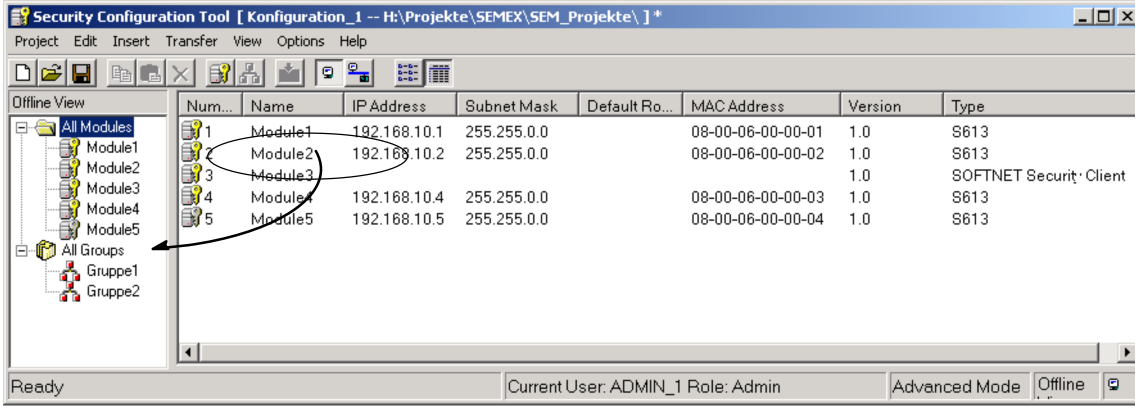
As default, broadcast or multicast packets cannot be transferred with IPsec. With SCALANCE S, IP broadcast packets are ”packaged” and transferred just like MAC packets in UDP including the Ethernet header. With these packets, the VLAN tagging is therefore retained.

## 6.2 Creating groups and assigning modules

### Follow the steps below to configure a VPN

Create a group with the menu command **Insert ▸ Group**.

Assign the SCALANCE S modules and SOFTNET Security Client modules intended for an internal network to the group by dragging the module to the required group with the mouse.


Security Configuration Tool [ Konfiguration_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
Module3
Module4
Module5
All Groups
Gruppe1
Gruppe2

| Num... | Name | IP Address | Subnet Mask | Default Ro... | MAC Address | Version | Type |
|---|---|---|---|---|---|---|---|
| 1 | Module1 | 192.168.10.1 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 |
| 2 | Module2 | 192.168.10.2 | 255.255.0.0 | | 08-00-06-00-00-02 | 1.0 | S613 |
| 3 | Module3 | | | | | 1.0 | SOFTNET Securit Client |
| 4 | Module4 | 192.168.10.4 | 255.255.0.0 | | 08-00-06-00-00-03 | 1.0 | S613 |
| 5 | Module5 | 192.168.10.5 | 255.255.0.0 | | 08-00-06-00-00-04 | 1.0 | S613 |

Ready | Current User: ADMIN_1 Role: Admin | Advanced Mode | Offline

### Configuring properties

Just as when configuring modules, the two selectable operator views in the Security Configuration Tool have an effect on configuring groups:

(Menu command **View ▸ Advanced Mode...**)

- Standard mode

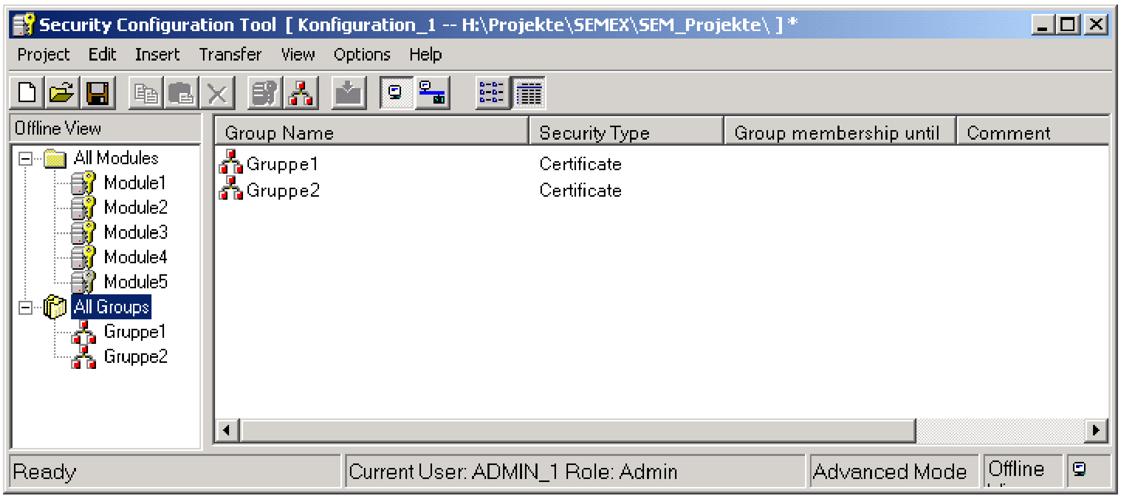
  In standard mode, you retain the defaults set by the system. Even if you are not an IT expert, you can nevertheless configure IPsec tunnels and operate secure data communication in your internal networks.

- Advanced mode

  The advanced mode provides you with options for setting specific configurations for tunnel communication.

## Displaying all configured groups and their properties

Select ”All Groups” in the Navigation Area


Security Configuration Tool [ Konfiguration_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *
Project Edit Insert Transfer View Options Help
Offline View
All Modules
Module1
Module2
Module3
Module4
Module5
All Groups
Gruppe1
Gruppe2
Ready
Current User: ADMIN_1 Role: Admin
Advanced Mode
Offline

| Group Name | Security Type | Group membership until | Comment |
|---|---|---|---|
| Gruppe1 | Certificate | | |
| Gruppe2 | Certificate | | |

The following properties of the groups are displayed in columns:

Table 6-1 Group properties

| Property/column | Meaning | Comment/selection |
|---|---|---|
| Group Name | Group Name | Freely selectable |
| Security Type | Type of authentication | • Preshared keys<br>• Certificate |
| Comment | Lifetime of certificates | See below |
| Comment | Comment | Freely selectable |

## Setting the lifetime of certificates

To open the dialog box in which you can set the expiry date of the certificate, carry out the following:

- Double-click a module in the properties window or click the right mouse button and choose ”Properties”.

**Notice**

Communication via the tunnel is not possible once the certificate has expired.

## 6.3 Tunnel configuration in standard mode

### Group properties

The following properties apply in standard mode:

- All parameters of the IPsec tunnel and the authentication are preset.

  You can display the set default values in the properties dialog for the group.
- The learn mode is active for all modules (See also Section 6.5)

### Opening the dialog for displaying default values

With a group selected, select the following menu command:

**Edit ▸ Properties...**

The display is identical to the dialog in advanced mode (see next section); the values cannot, however, be modified.

## 6.4 Tunnel configuration in advanced mode

The advanced mode provides you with options for setting specific configurations for tunnel communication.

### Switch over to advanced mode

To use all the functions and menu commands described in section, switch over the mode:

**View ▸ Advanced Mode...**

**Note**

If you switch to the advanced mode for the current project, you can no longer switch back if you make any modifications.

## 6.4.1 Configuring group properties

### Group properties

The following group properties can be set in the ”Advanced Mode” operator view:

- Authentication method
- IKE settings (dialog area: Advanced Settings Phase 1)
- IPsec settings (dialog area: Advanced Settings Phase 2)

**Notice**

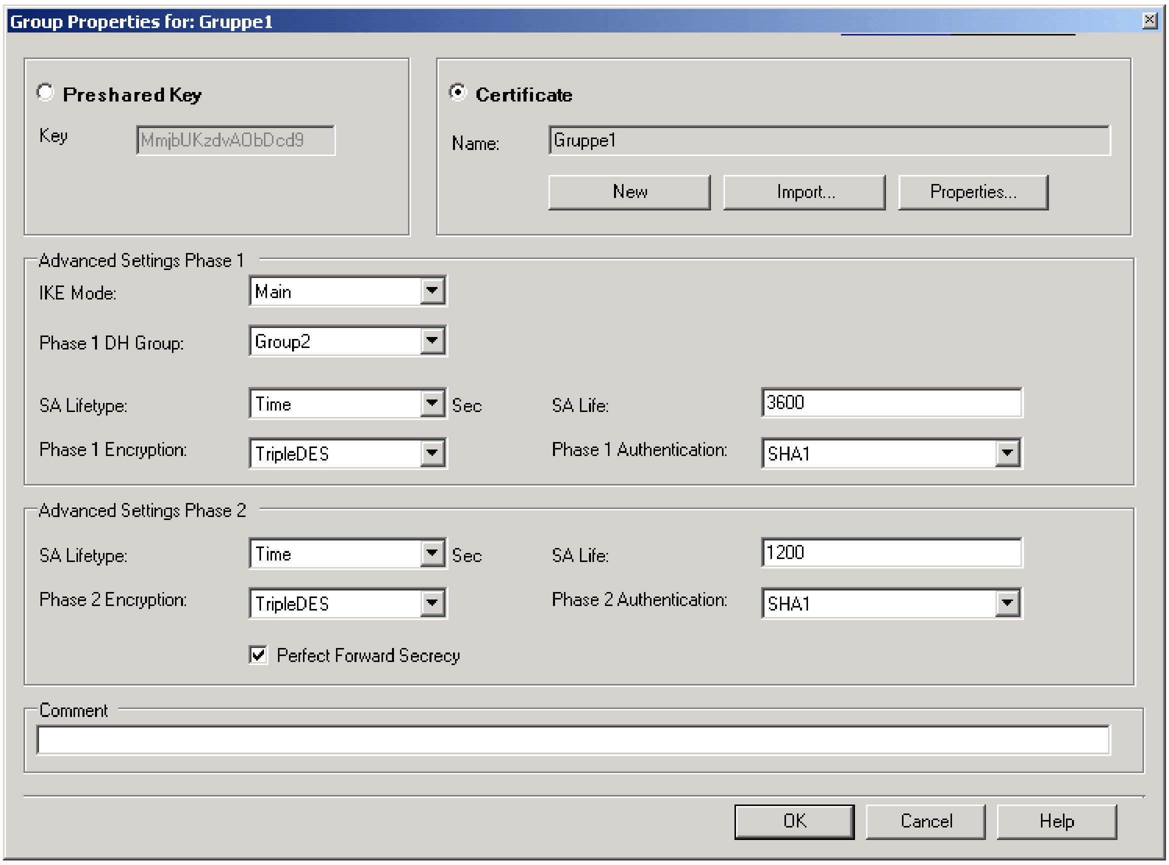
To be able to set these parameters, you require IPsec experience.

If you do not make or modify any settings, the defaults of standard mode apply.

### Opening the dialog for entering group properties

- With a group selected, select the following menu command:

  **Edit ▸ Properties...**



Group Properties for: Gruppe1

○ Preshared Key
Key: MmjbUKzdvA0bDcd9

● Certificate
Name: Gruppe1

Advanced Settings Phase 1
IKE Mode: Main
Phase 1 DH Group: Group2
SA Lifetype: Time Sec
SA Life: 3600
Phase 1 Encryption: TripleDES
Phase 1 Authentication: SHA1

Advanced Settings Phase 2
SA Lifetype: Time Sec
SA Life: 1200
Phase 2 Encryption: TripleDES
Phase 2 Authentication: SHA1
☑ Perfect Forward Secrecy

Comment

## Parameters for advanced settings phase 1 - IKE settings

Phase 1: IKE (Internet Key Exchange):

Here, you can set parameters for the protocol of IPsec key management. The key exchange uses the standardized IKE method.

You can set the following IKE protocol parameters:

Table 6-2 IKE protocol parameters (parameter group ”Advanced Settings Phase 1’” in the dialog)

| Parameter | Values/selection | Comment |
|---|---|---|
| | • Main Mode<br>• Aggressive Mode | Key exchange method<br>The difference between the main and aggressive mode is the ”identity protection” used in the main mode. The identity is transferred encrypted in main mode but not in aggressive mode. |
| Phase 1 DH Group | • Group 1<br>• Group 2<br>• Group 5 | Diffie-Hellman key agreement:<br>Diffie-Hellman groups (selectable cryptographic algorithms in the Oakley key exchange protocol) |
| SA Lifetype | • Time<br>• Limit | Phase 1 Security Association (SA)<br>• Time limitation (sec., default: 1 h)<br>The lifetime of the current key material is limited in time. When the time expires, the key material is renegotiated.<br>• Data amounts limited (Kbytes, default 100 Kbytes) |
| SA Life | Numeric value | (”Time”->sec., ”Limit”-> Kbytes) |
| Phase 1 Encryption | • DES<br>• TripleDES | Encryption algorithm<br>• Data Encryption Standard (56 Bit)<br>• Triple DES |
| Phase 1 Authentication | • MD5<br>• SHA-1 | Authentication algorithm<br>• Message Digest Version 5<br>• Secure Hash Algorithm 1 |

## Parameters for advanced settings phase 2 - IPsec settings

Phase 2: Data exchange (ESP, Encapsulating Security Payload)

Here, you can set parameters for the protocol of the IPsec data exchange. Data is exchanged over the standardized security protocol ESP.

You can set the following ESP protocol parameters:

Table 6-3 IPsec protocol parameters (parameter group ”Advanced Settings Phase 2’” in the dialog)

| Parameter | Values/selection | Comment |
|---|---|---|
| SA Lifetype | <br>• Time<br><br>• Limit | Phase 2 Security Association (SA)<br>• Time limitation (sec., default: 1 h)<br>The lifetime of the current key material is limited in time. When the time expires, the key material is renegotiated.<br>• Data amounts limited (Kbytes, default 100 Kbytes) |
| SA Life | Numeric value | (”Time”->sec., ”Limit”-> Kbytes) |
| Phase 2 Encryption | <br>• TripleDES<br>• DES<br>• AES<br>• No Encryption | Encryption algorithm<br>• Special triple DES<br>• Data Encryption Standard (56-bit key length)<br>• Advanced Encrypting Standard (128,192,256 bits)<br>• No encryption |
| Phase 2 Authentication | <br>• MD5<br>• SHA-1 | Authentication algorithm<br>• Message Digest Version 5<br>• Secure Hash Algorithm 1 |
| Perfect Forward Secrecy | • On<br>• Off | Each time an IPsec-SA is renegotiated, the key is negotiated again using the Diffie-Hellman method. |

## 6.4.2 Including a SCALANCE S in a configured group

The configured group properties are adopted for a SCALANCE S to be included in an existing group.

### Follow the steps below:

Depending on whether you have changed any group properties or not, you must make a distinction between the following:

- Case a: When you have not changed group properties
  1. At the new SCALANCE S to the group.
  2. Download the configuration to the new modules.
- Case b: When you have changed group properties
  1. At the new SCALANCE S to the group.
  2. Download the configuration to all modules that belong to the group.

### Advantage

Existing SCALANCE S modules that have already been commissioned do not need to be reconfigured and downloaded. There is no effect on or interruption of active communication.

## 6.4.3 SOFTNET Security Client

### Compatible settings for SOFTNET Security Client

Please note the following special features if you include modules of the type SOFTNET Security Client in the configured group:

Table 6-4

| Parameter | Setting / special feature |
|---|---|
| Authentication Method | Preshared keys can only be used for communication between the SCALANCE S modules. |
| Phase 1 DH Group | **No** Group14 can be selected. |
| SA Lifetype | Must be selected identical for both phases. |
| Phase 2 Authentication | **No** AES possible. |

## 6.5 Configuring internal network nodes

Each SCALANCE S must know the network nodes in the entire internal network to be able to recognize the authenticity of a packet.

SCALANCE S must know both its own internal nodes as well as the internal nodes of the SCALANCE S modules in its group. This information is used on a SCALANCE S to decide which data packet will be transferred in which tunnel.

SCALANCE S allows network nodes to be learnt automatically or configured statically.

### 6.5.1 How the learning mode works

#### Finding nodes for tunnel communication automatically

One great advantage of configuration and operation of tunnel communication is that SCALANCE S can find nodes in the internal network automatically.

New nodes are detected by SCALANCE S during operation. The detected nodes are signaled to the SCALANCE S modules belonging to the same group. This allows data exchange within the tunnels of a group in both directions at any time.

#### Prerequisites

The following nodes are detected:

- Network nodes with IP capability

  Network nodes with IP capability are found when they send an ICMP response to the ICMP subnet broadcast.

  IP nodes downstream from routers can be found if the routers pass on ICMP broadcasts.

- ISO network nodes

  Network nodes without IP capability but that can be addressed over ISO protocols can also be learnt.

  This is only possible if they reply to XID or TEST packets. TEST and XID (Exchange Identification) are auxiliary protocols for exchanging information on layer 2. By sending these packets with a broadcast address, these network nodes can be located.

Network nodes that do not meet these conditions must be configured.

## Subnets

Subnets located downstream from internal routers must also be configured.

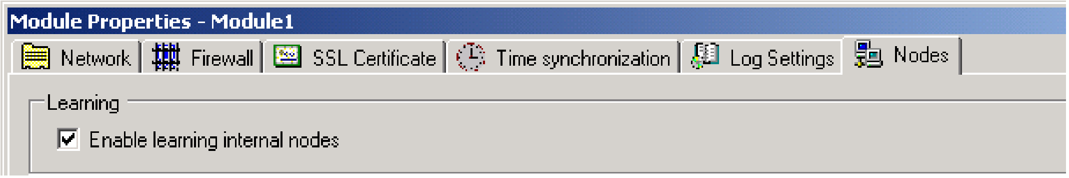
## Enabling/disabling the learning mode

The learning function is enabled in the configuration as default for every SCALANCE S module by the Security Configuration Tool configuration software.

Learning can also be disabled completely. In this case, you must configure all internal nodes participating in the tunnel communication manually.

You can open the dialog in which you select the option as follows:

- With the module selected, using the menu command **Edit ▸ Properties...**, ”Nodes” tab.



Module Properties - Module1

Learning

☑ Enable learning internal nodes

## When is it useful to disable the automatic learning mode?

The default settings for SCALANCE S assume that internal networks are always ”secure”; in other words, in a normal situation no network node is connected to the internal network if it is not trustworthy.

Disabling the learning mode can be useful if the internal network is static; in other words, when the number of internal notes and their addresses do not change.

If the learning mode is disabled, this reduces the load on the medium and the nodes in the internal network resulting from the learning packets. The performance of the SCALANCE S is also slightly improved since it does not need to process the learning packets.

Note: In the learning mode, all nodes in the internal network are detected regardless of whether they belong to a VPN group. The information relating to numbers of stations etc. in the VPN relates only to nodes that communicate over VPN in the internal network.

**Notice**

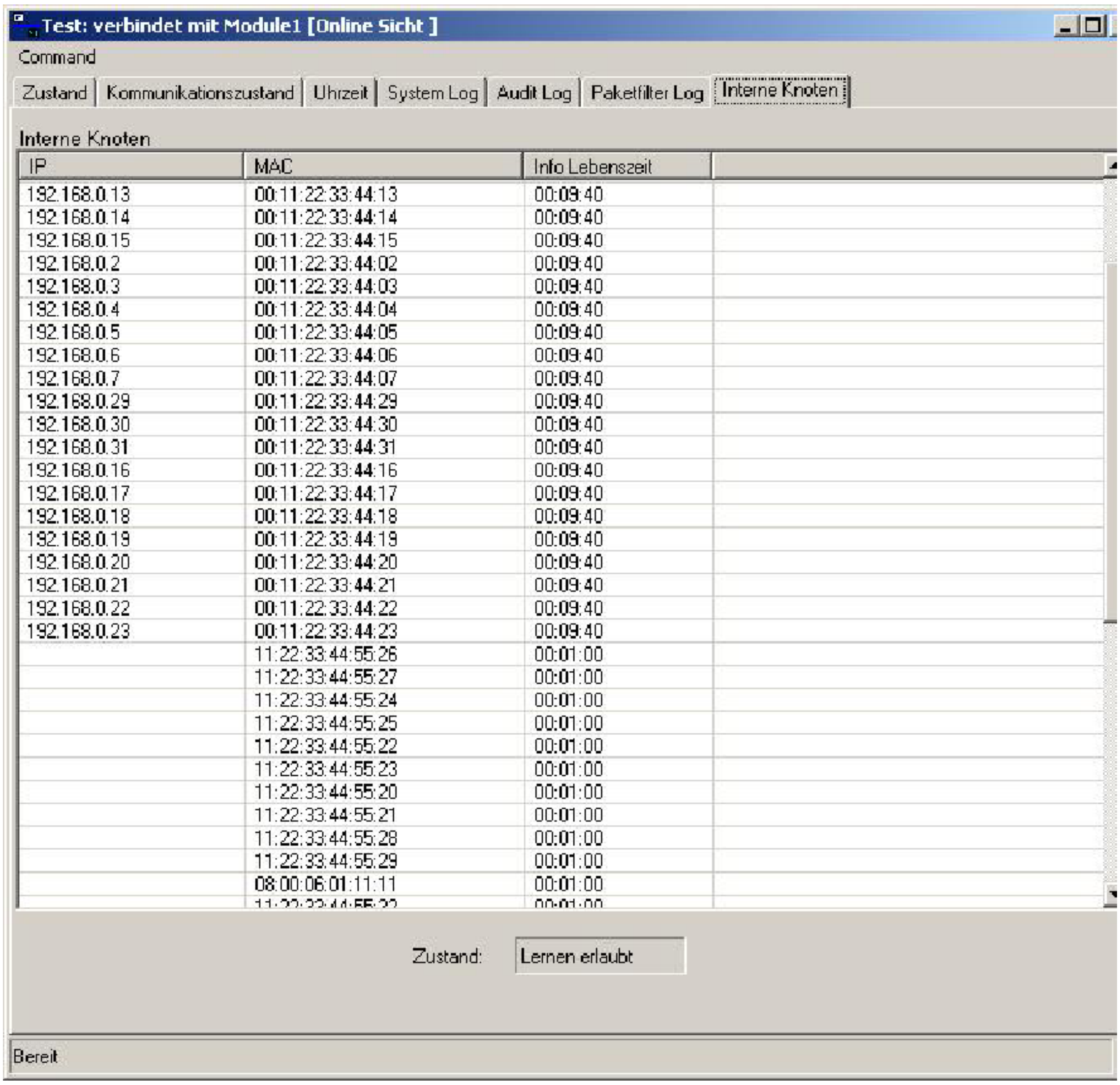
If more than 64 (for SCALANCE S613) or 32 (for SCALANCE S612) internal nodes are operated in the internal network, the permissible quantity structure is exceeded, which results in an impermissible operating status. Due to the dynamics of the network traffic, internal nodes that have already been taught are replaced by new, unknown internal nodes.

## 6.5.2 Displaying the detected internal nodes

All detected nodes can be displayed in the Security Configuration Tool in the ”Online” mode in the ”Internal Nodes” Tab. This is only possible if you have activated the advanced mode in the Security Configuration Tool.

Select the following menu command:

**Edit ▸ Online Diagnostics..**



Interne Knoten

| IP | MAC | Info Lebenszeit | |
|---|---|---|---|
| 192.168.0.13 | 00:11:22:33:44:13 | 00:09:40 | |
| 192.168.0.14 | 00:11:22:33:44:14 | 00:09:40 | |
| 192.168.0.15 | 00:11:22:33:44:15 | 00:09:40 | |
| 192.168.0.2 | 00:11:22:33:44:02 | 00:09:40 | |
| 192.168.0.3 | 00:11:22:33:44:03 | 00:09:40 | |
| 192.168.0.4 | 00:11:22:33:44:04 | 00:09:40 | |
| 192.168.0.5 | 00:11:22:33:44:05 | 00:09:40 | |
| 192.168.0.6 | 00:11:22:33:44:06 | 00:09:40 | |
| 192.168.0.7 | 00:11:22:33:44:07 | 00:09:40 | |
| 192.168.0.29 | 00:11:22:33:44:29 | 00:09:40 | |
| 192.168.0.30 | 00:11:22:33:44:30 | 00:09:40 | |
| 192.168.0.31 | 00:11:22:33:44:31 | 00:09:40 | |
| 192.168.0.16 | 00:11:22:33:44:16 | 00:09:40 | |
| 192.168.0.17 | 00:11:22:33:44:17 | 00:09:40 | |
| 192.168.0.18 | 00:11:22:33:44:18 | 00:09:40 | |
| 192.168.0.19 | 00:11:22:33:44:19 | 00:09:40 | |
| 192.168.0.20 | 00:11:22:33:44:20 | 00:09:40 | |
| 192.168.0.21 | 00:11:22:33:44:21 | 00:09:40 | |
| 192.168.0.22 | 00:11:22:33:44:22 | 00:09:40 | |
| 192.168.0.23 | 00:11:22:33:44:23 | 00:09:40 | |
| | 11:22:33:44:55:26 | 00:01:00 | |
| | 11:22:33:44:55:27 | 00:01:00 | |
| | 11:22:33:44:55:24 | 00:01:00 | |
| | 11:22:33:44:55:25 | 00:01:00 | |
| | 11:22:33:44:55:22 | 00:01:00 | |
| | 11:22:33:44:55:23 | 00:01:00 | |
| | 11:22:33:44:55:20 | 00:01:00 | |
| | 11:22:33:44:55:21 | 00:01:00 | |
| | 11:22:33:44:55:28 | 00:01:00 | |
| | 11:22:33:44:55:29 | 00:01:00 | |
| | 08:00:06:01:11:11 | 00:01:00 | |
| | 11:22:33:44:55:22 | 00:01:00 | |

Zustand: Lernen erlaubt

Bereit

## 6.5.3 Configuring nodes manually

### Nodes that cannot be learnt

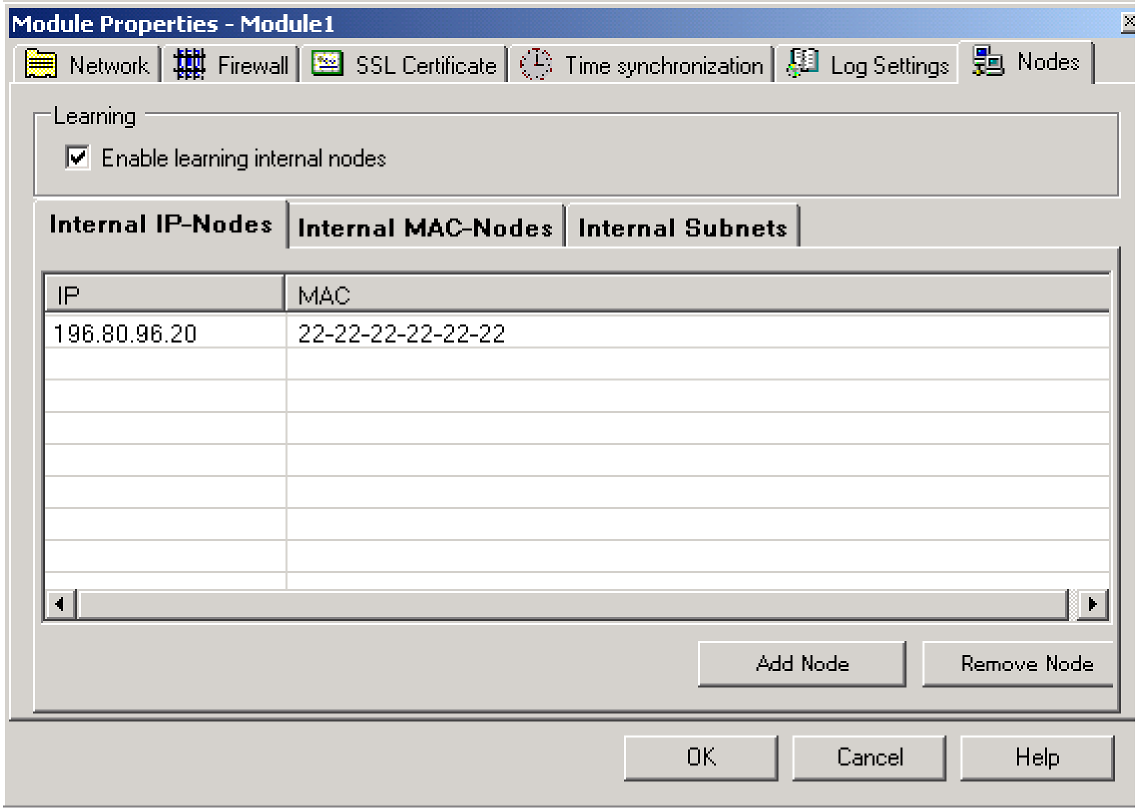
There are nodes in the internal network that cannot be learnt. You must then configure these nodes.

You must also configure subnets located in the internal network of the SCALANCE S.

### Dialog / tab

You can open the dialog in which you configure the nodes as follows:

- With the module selected, using the menu command **Edit ▸ Properties...**, ”Nodes” tab.



☑ Enable learning internal nodes

| IP | MAC |
|---|---|
| 196.80.96.20 | 22-22-22-22-22-22 |

Here, in the various tabs, enter the required address parameters for all network nodes to be protected by the selected SCALANCE S module.

### ”Internal IP Nodes” tab

Configurable parameters: IP address and optionally the MAC address

### ”Internal MAC Nodes” tab

Configurable parameter: MAC address

### ”Internal Subnets” tab

In the case of an internal subnet (a router in the internal network), you must specify the following address parameters:

| Parameter | Function | Example of a value |
|---|---|---|
| IP Subnet ID | Network ID of the subnet: Based on the network ID, the router recognizes whether a target address is inside or outside the subnet. | 196.80.96.0 |
| Subnet Mask | Subnet Mask: The subnet mask structures the network and is used to form the subnet ID. | 255.255.255.0 |
| Router IP | IP address of the router: | 196.80.100.1 |

# 7 SOFTNET Security Client

With the SOFTNET Security Client PC software, secure IP-based access is possible from PCs/PGs to automation systems protected by SCALANCE S.

This chapter describes how to configure the SOFTNET Security Client in the Security Configuration Tool and then commission it on the PC/PG.

## Further information

You should also be familiar with the description of IPsec told communication in Chapter 6.

You will also find detailed information on the dialogs and parameter settings in the online help of the SOFTNET Security Client.

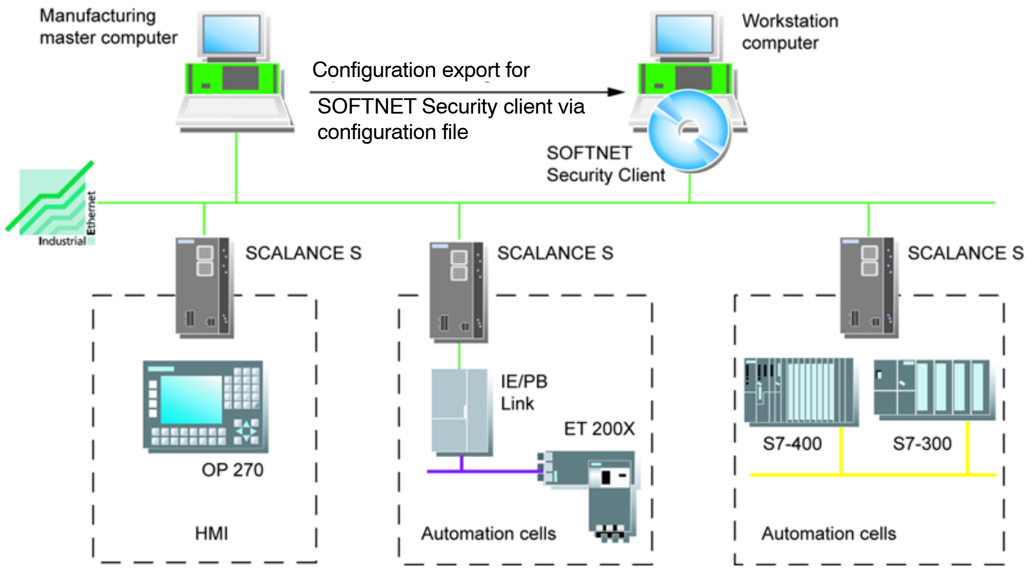
You can call this with the F1 key or using the ”Help” button in the relevant dialog.

## 7.1 Using the SOFTNET Security Client

### Area of application - access over VPN

With the SOFTNET Security Client, a PC/PG is configured automatically so that it can establish IPsec tunnels to one or more SCALANCE S modules.

Thanks to this IPsec tunnel communication, it is possible to access devices or networks located in an internal network protected by SCALANCE S securely using PG/PC applications such as NCM Diagnostics or STEP 7.



### Automatic communication over VPN

Your application, it is important that the SOFTNET Security Client automatically detects access to the IP address of a VPN node. You address the node simply using the IP address as if it was located in the local subnet to which the PC/PG with the application is attached.

**Notice**

Note that only IP-based communication between the SOFTNET Security Client and SCALANCE S can take place via the IPSec tunnel.

## Operation

The SOFTNET Security Client PC software has a straightforward user interface for configuration of the security properties required for communication with devices protected by SCALANCE S. Following configuration, the SOFTNET Security Client runs in the background - visible as an icon in the SYSTRAY on your PG/PC.

## Details in the online help

You will find detailed information on the dialogs and input boxes in the online help of the SOFTNET Security Client user interface.

You can open the online help with the ”Help” button or the F1 key.

## How does the SOFTNET Security Client work?

The SOFTNET Security Client reads in the configuration created with the Security Configuration Tool and gets the required information on the certificates to be imported from the file.

The root certificate and the private keys are imported and stored on the local PG/PC.

Following this, security settings are made based on the data from the configuration so that applications can access IP addresses downstream from the SCALANCE S modules.

If a learning mode for the internal nodes or programmable controllers is enabled, the configuration module first sets a security policy for the secure access to SCALANCE S modules. The SOFTNET Security Client then addresses the SCALANCE S modules to obtain the IP addresses of the relevant internal nodes.

SOFTNET Security Client enters these IP addresses in special filter lists belong to this security policy. Following this, applications such as STEP 7 can communicate with the programmable controllers over VPN.

**Notice**

On a Windows system, the IP security guidelines are user specific. Only one set of security guidelines can be valid for a single user.

If an existing set of IP security guidelines is not be overwritten when the SOFTNET Security Client is installed, you should create a separate user for installing and using the SOFTNET Security Client.

## Environment

The SOFTNET Security Client is designed for use with the Windows 2000 Professional SP4 or Windows XP SP1 and 2 (not Home Edition) operating systems.

**Notice**

The SOFTNET Security Client cannot be operated in conjunction with the SIMATIC NET CD 5/2000 on Windows 2000.

Reason:
The Sim9sync of the SIMATIC NET CD 5/2000 is incompatible with the version required by the SOFTNET Security Client. This problem cannot be rectified by reinstalling the system.

## Response to problems

If problems occur on your PG/PC, SOFTNET Security Client reacts as follows:

- An established security policy is retained when you turn your PG/PC off and on again;
- Messages are displayed if a configuration is not found.

# 7.2 Creating a configuration file with the Security Configuration Tool

## Configuring a SOFTNET Security Client module in the project

The SOFTNET security client is created as a module in the project. In contrast to the SCALANCE S modules, no further properties can be configured.

You simply assign the SOFTNET Security Client module to one or more module groups in which you want to set up IPsec tunnels to the PC/PG.

The group properties you configured for these groups are then decisive.

**Notice**

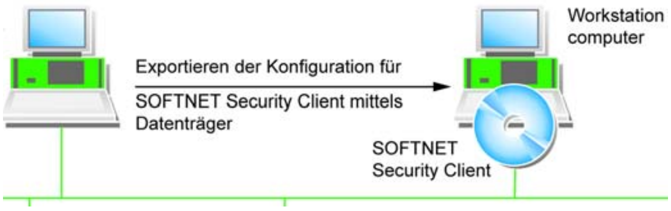
Please refer to the information on the parameters in Section 6.4, subsection ”Compatible settings for SOFTNET Security Client”.

**Note**

If you create more than one SOFNET Security Client within a group, tunnels are only established from the individual clients to the SCALANCE S modules rather than between the clients themselves.

## Configuration files for the SOFTNET Security Client

The interface between the Security Configuration Tool and the SOFTNET Security Client is controlled by configuration files.


Workstation computer
Exportieren der Konfiguration für
SOFTNET Security Client mittels Datenträger
SOFTNET Security Client

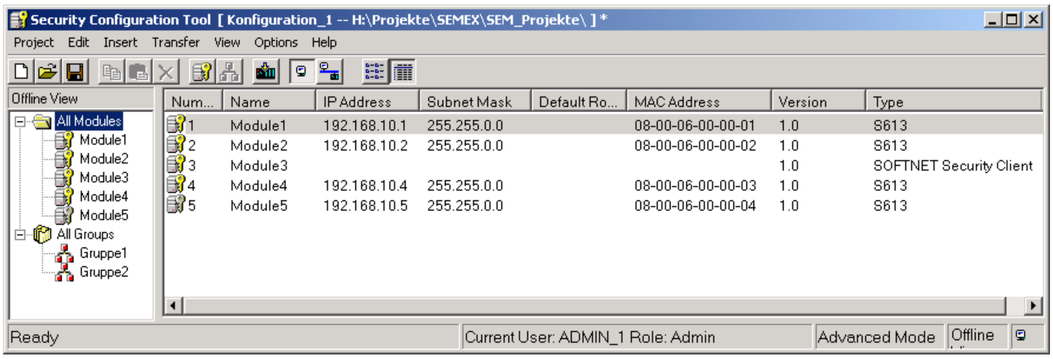
The configuration is stored in three file types:

- *.dat
- *.p12
- *.cer

## Procedure

Follow the steps below in the Security Configuration Tool to create the configuration files:

| Steps | Procedure |
|---|---|
| 1. | First, create a module of the type SOFTNET Security Client in your project. |

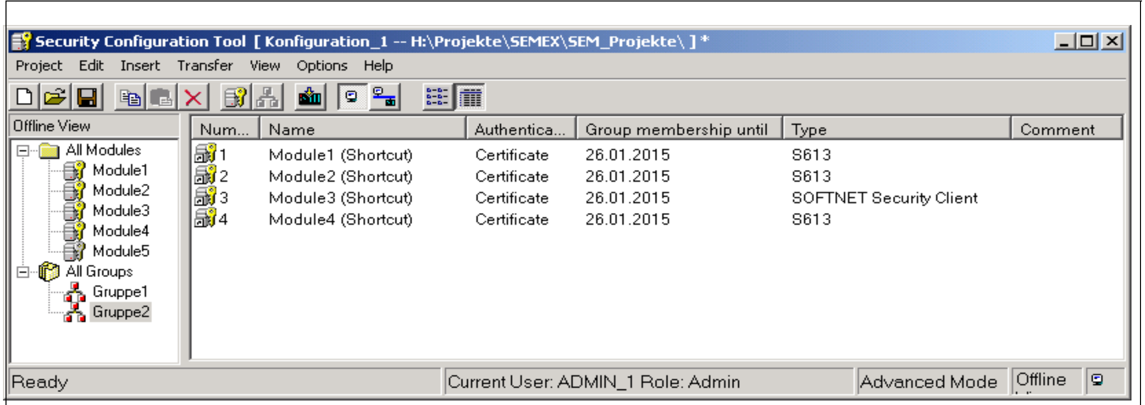


Security Configuration Tool [ Konfiguration_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *

| Num... | Name | IP Address | Subnet Mask | Default Ro... | MAC Address | Version | Type |
|---|---|---|---|---|---|---|---|
| 1 | Module1 | 192.168.10.1 | 255.255.0.0 | | 08-00-06-00-00-01 | 1.0 | S613 |
| 2 | Module2 | 192.168.10.2 | 255.255.0.0 | | 08-00-06-00-00-02 | 1.0 | S613 |
| 3 | Module3 | | | | | 1.0 | SOFTNET Security Client |
| 4 | Module4 | 192.168.10.4 | 255.255.0.0 | | 08-00-06-00-00-03 | 1.0 | S613 |
| 5 | Module5 | 192.168.10.5 | 255.255.0.0 | | 08-00-06-00-00-04 | 1.0 | S613 |

Ready | Current User: ADMIN_1 Role: Admin | Advanced Mode | Offline

| Steps | Procedure |
|---|---|
| 2. | Assign the module to the module groups in which the PC/PG will communicate over IPsec tunnels. |



Security Configuration Tool [ Konfiguration_1 -- H:\Projekte\SEMEX\SEM_Projekte\ ] *

| Num... | Name | Authentica... | Group membership until | Type | Comment |
|---|---|---|---|---|---|
| 1 | Module1 (Shortcut) | Certificate | 26.01.2015 | S613 | |
| 2 | Module2 (Shortcut) | Certificate | 26.01.2015 | S613 | |
| 3 | Module3 (Shortcut) | Certificate | 26.01.2015 | SOFTNET Security Client | |
| 4 | Module4 (Shortcut) | Certificate | 26.01.2015 | S613 | |

Ready | Current User: ADMIN_1 Role: Admin | Advanced Mode | Offline

| Steps | Procedure |
|---|---|
| 3. | Select the required SOFTNET Security Client with the right mouse button and then select the following menu command:<br>**Transfer ▸ to Module...** |
| 4. | In the dialog that appears, select the storage location for the configuration file. |
| 5. | In the next step, you will be prompted to specify a password for the private key of the configuration. You can either assign a new password for the configuration file or use the current user password.<br>As usual, the password you enter must be repeated.<br>This completes export of the configuration files. |
| 6. | Apply the files of the type *.dat, *.p12, *.cer on the PC/PG on which you want to operate the SOFTNET Security Client. |

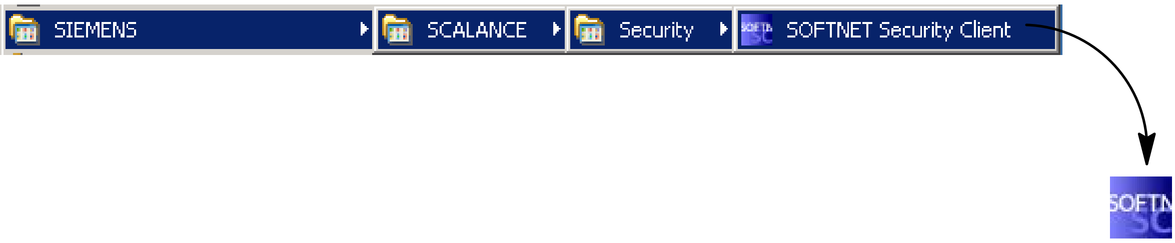
## 7.3 Installation and commissioning of the SOFTNET Security Client

### 7.3.1 Installing and starting SOFTNET Security Client

You install the SOFTNET Security Client PC software from the SCALANCE S CD.

| Steps | Procedure |
|---|---|
| 1. | First read the information in the README file of your SCALANCE S CD and follow any additional installation instructions it contains. |
| 2. | Run the SETUP program;<br>The simplest way is to open the overview of the contents of your SCALANCE S CD -> this is started automatically when you insert the CD or can be opened from the start_en.htm file. You can then select the entry ”Installation SOFTNET Security Client” directly |

Following installation and startup of the SOFTNET Security Client, the icon of the SOFTNET Security Client appears in the Windows taskbar:



### Setting up the SOFTNET Security Client

Once activated, the most important functions run in the background on your PG/PC.

The SOFTNET Security Client is configured in two steps:

- Export of a security configuration from the SCALANCE S Security Configuration Tool (see Section 7.2).
- Import of the security configuration in its own user interface as described in the next section.

### Startup behavior

With a maximum configuration and depending on the system, the SOFTNET Security Client can require up to 15 minutes to load the security rules. The CPU of the on PG/PC is at 100% usage during this time.

### Exiting SOFTNET Security Client - effects

If SOFTNET Security Client is exited, the security policy is also deactivated.

You can exit SOFTNET Security Client as follows:

- Using the menu command in the SYSTRAY of Windows; select the icon of the SOFTNET Security Client with the right mouse button.
- Using the ”Quit” button of the user interface.

## 7.3.2 Uninstalling SOFTNET Security Client

When you uninstall, the security properties set by the SOFTNET Security Client are reset.

## 7.4 Working with SOFTNET Security Client

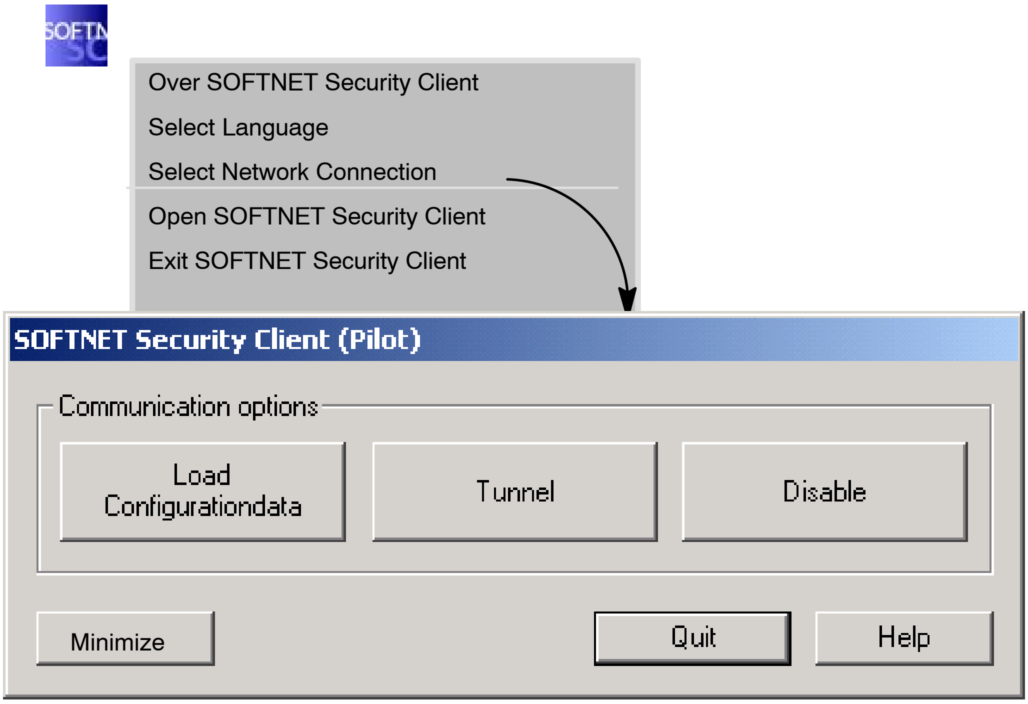
### Configurable properties

You can use the following individual services:

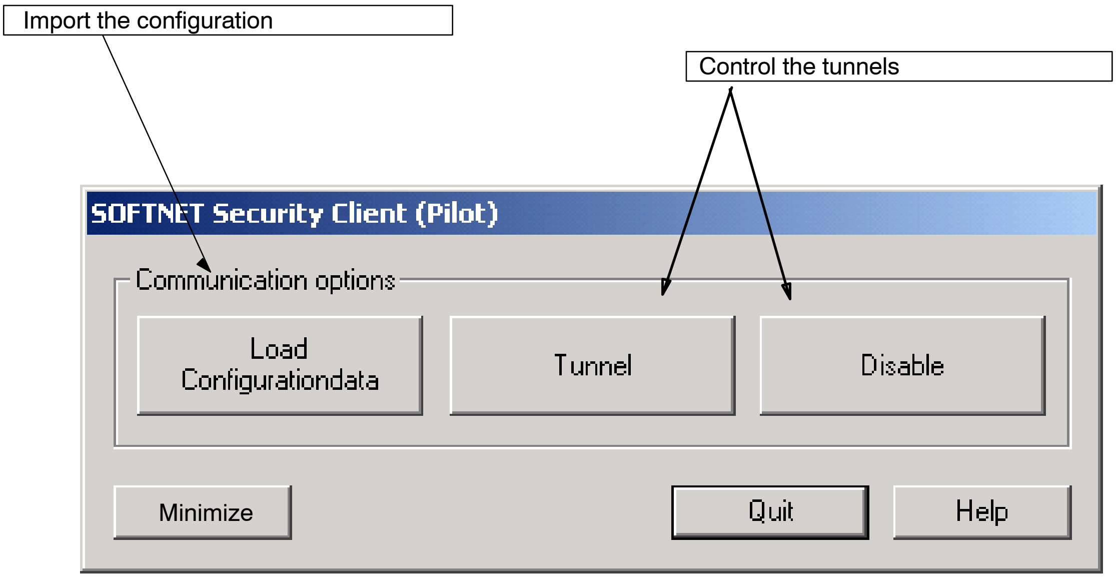
- Setting up secure IPsec tunnel communication (VPN) between the PC/PG and all SCALANCE S modules of a project or individual SCALANCE S modules. The PC/PG can access the internal nodes over this IPsec tunnel.
- Enable and disable existing secure connections;
- Set up connections when end devices are added later; (only possible when the learning mode is activated)
- Check a configuration; in other words, which connections are set up or possible.

### How to open SOFTNET Security Client for configuration

You open the SOFTNET Security Client user interface by double-clicking on the icon in the SYSTRAY or with the ”Open SW-SEM” context menu command (right mouse button):


SOFTN SC
Over SOFTNET Security Client
Select Language
Select Network Connection
Open SOFTNET Security Client
Exit SOFTNET Security Client
SOFTNET Security Client (Pilot)
Communication options
Load Configurationdata
Tunnel
Disable
Minimize
Quit
Help

## With the buttons, you can activate the following functions:



| Button | Meaning |
|---|---|
| Load Configuration Data | Import the configuration<br>You open a file dialog in which you select the configuration file.<br>After closing the dialog, the configuration is loaded and you are asked to assign a password for each configuration file.<br>In the dialog, you are asked whether you want to set up the tunnels for all SCALANCE S modules immediately. If IP addresses of SCALANCE S modules are entered in the configuration or if the learning mode is active, the tunnels for all configured or detected addresses are set up.<br>This procedure is fast and efficient particularly with small configurations.<br>As an option, you can set up all tunnels in the dialog for tunnel setup (see Section 7.5).<br>Note: You can import the configuration files from several projects created in the SOFTNET Security Client one after the other (see also the explanation of the procedure below). |

| Button | Meaning |
|---|---|
| Tunnel | Dialog for setting up editing tunnels.<br>This is the dialog in which you actually configure the SOFTNET Security Client.<br>In this dialog, you will find a list of the existing secure tunnels (see Section 7.5).<br>You can display/check the IP addresses for the SCALANCE S modules.<br>For PCs that have more than one IP address, you can open the ”Network Adapters” dialog and select which IP address of the PC will be used to communicate with the internal node |
| Disable | Disable all secure tunnels. |
| Minimize | The operator interface of the SOFTNET Security Client is closed.<br>The icon for the SOFTNET Security Client is then displayed in the Windows toolbar: |
| Quit | Quit configuration; SOFTNET Security Client is closed; all tunnels are deactivated. |
| Help | Open online help. |

## 7.5 Setting up and editing tunnels

### Setting up secure connections to all SCALANCE S modules

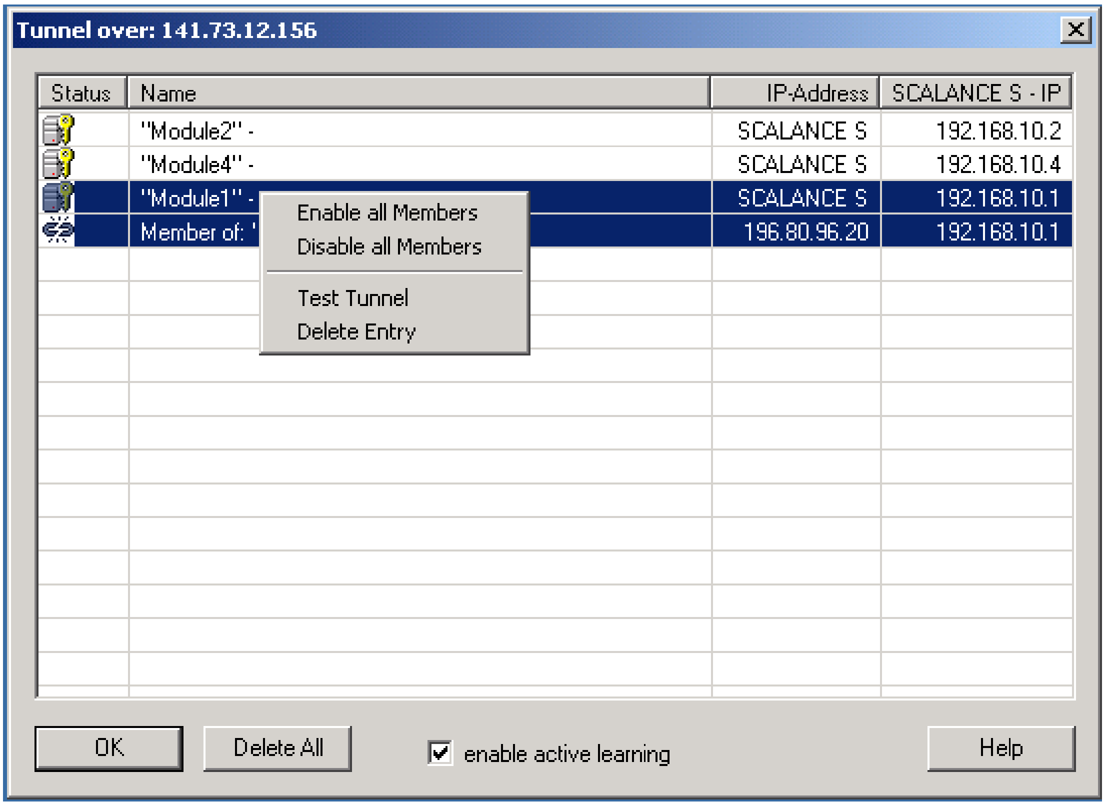
In the dialog for the configuration import, you can select whether or not the tunnels are set up for all SCALANCE S modules immediately. This results in the following possibilities:

- Enable tunnels automatically

  If IP addresses of SCALANCE S modules are entered in the configuration or if the learning mode is active, the tunnels for all configured or detected addresses are set up.

- Read in tunnel configuration only

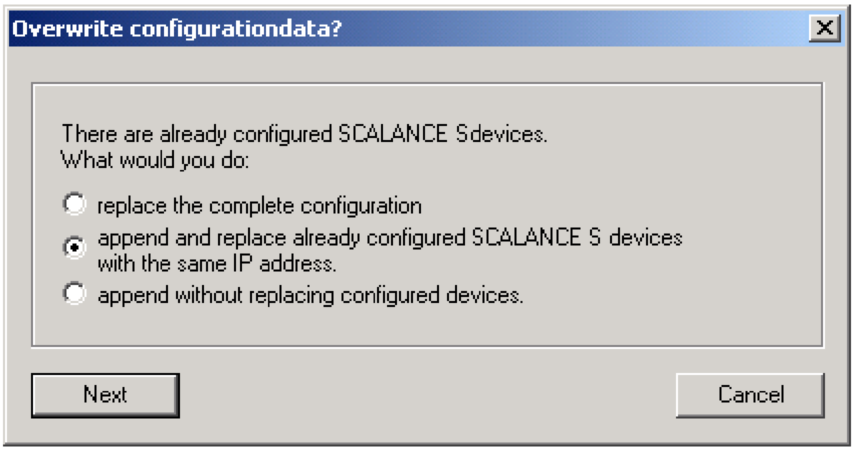
  As an option, you can simply read in the configured tunnels and then enable them individually in the dialog.

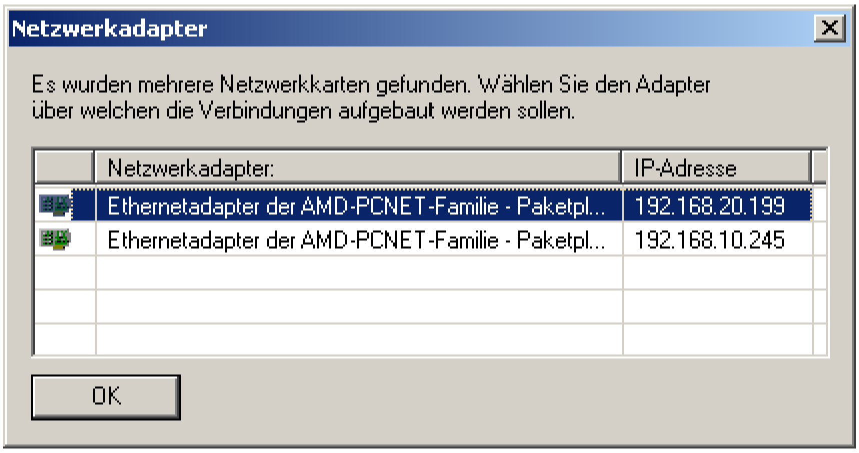
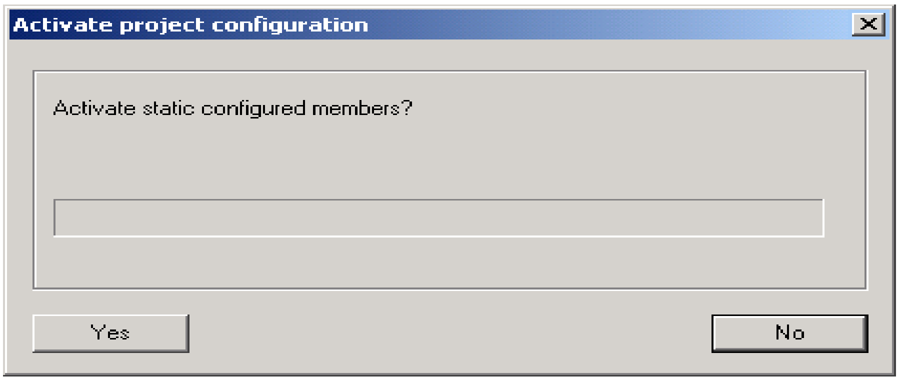


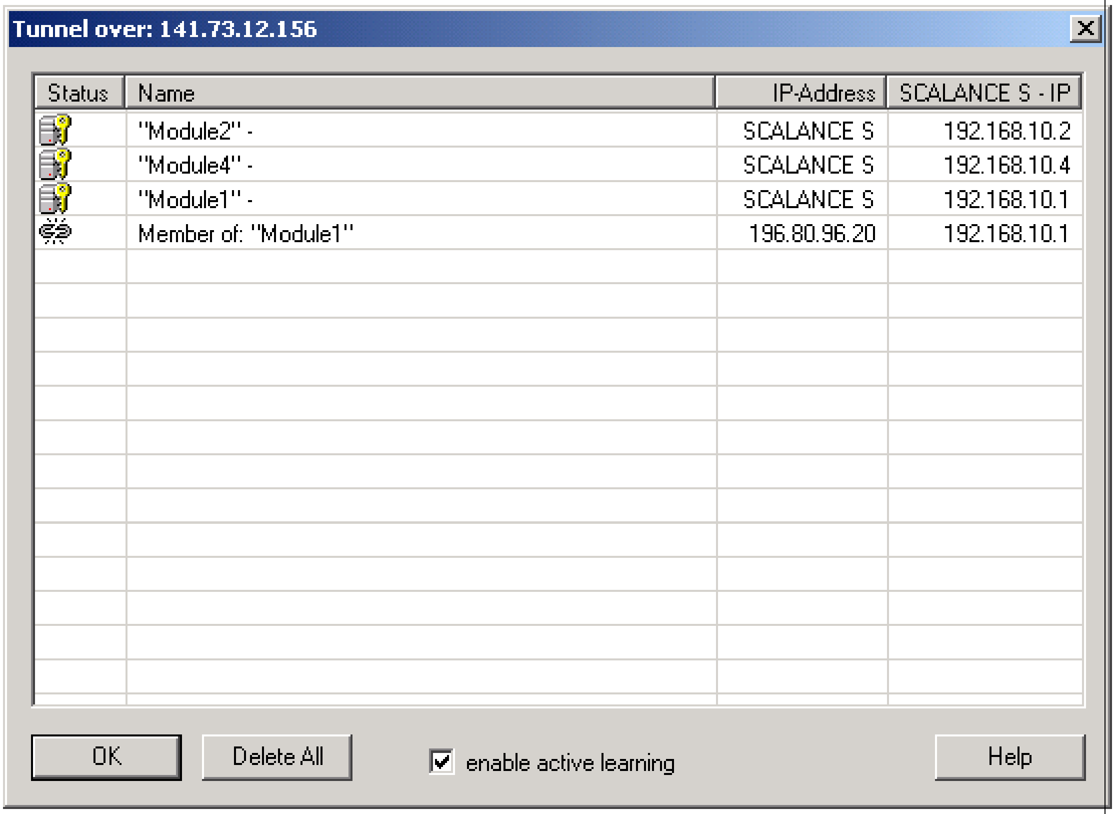
| Status | Name | IP-Address | SCALANCE S - IP |
|---|---|---|---|
| | "Module2" - | SCALANCE S | 192.168.10.2 |
| | "Module4" - | SCALANCE S | 192.168.10.4 |
| | "Module1" - | SCALANCE S | 192.168.10.1 |
| | Member of: ' | 196.80.96.20 | 192.168.10.1 |

☑ enable active learning

## How to set up tunnel connections

| Steps | Procedure |
|---|---|
| 1. | With the ”Load Configuration Data”, open the dialog for importing the configuration file. |
| 2. | Select the configuration file created with the Security Configuration Tool. |
| 3. | If configuration data already exists in SOFTNET Security Client, you will be prompted to decide how to handle the new configuration data. Select from the available options:<br><br>Overwrite configurationdata?<br>There are already configured SCALANCE Sdevices.<br>What would you do:<br>○ replace the complete configuration<br>● append and replace already configured SCALANCE S devices with the same IP address.<br>○ append without replacing configured devices.<br> |
|  | Notes on this dialog<br>The configuration data can be read in from several projects. This dialog takes this into account in the options it presents. The options therefore have the following effects:<br>• If you select ”Overwrite configuration data”, only the last configuration data to be read in exists.<br>• The second option is useful if you have modified configuration data, for example, you have only changed the configuration in project a, project b and c remain unchanged.<br>• The third option is useful if a SCALANCE S has been added to a project and you do not want to lose internal nodes that have already been learnt. |
| 4. | If you have more than one network adapter in your PG/PC, you will now be prompted to make a selection: |

| Steps | Procedure |
|---|---|
| | <br>Netzwerkadapter<br>Es wurden mehrere Netzwerkkarten gefunden. Wählen Sie den Adapter über welchen die Verbindungen aufgebaut werden sollen.<br>Netzwerkadapter: \| IP-Adresse<br>Ethernetadapter der AMD-PCNET-Familie - Paketpl... \| 192.168.20.199<br>Ethernetadapter der AMD-PCNET-Familie - Paketpl... \| 192.168.10.245<br>OK<br>Note:<br>If you have selected an address when reading in the configuration data or in the pulldown menu of the icon in the Windows SYSTRAY, this address applies for all entries in the tunnel table. |
| 5. | Now enter your password for authentication that you assigned during configuration in the SOFTNET Security Client. |
| 6. | Now decide whether or not to enable the tunnel connections for the nodes included in the configuration (statically configured nodes).<br>If you do not enable the tunnel connections here, you can do this at any time in the tunnel dialog described below.<br><br>Activate project configuration<br>Activate static configured members?<br>Yes No |
| | If you have decided to enable the tunnel connections, the tunnel connections between the SOFTNET Security Client and the SCALANCE S modules are now established.<br>This can take several seconds. |
| 7. | Now open the ”Tunnel over...” dialog with the ”Tunnel” button.<br>In the table that opens, you will see the modules and nodes with status information on the tunnel connections. |

| Steps | Procedure |
|---|---|
| |  |
| 8. | If you now recognize that require nodes or members are not displayed in the table, follow the steps outlined below:<br>Open the command prompt and send a PING command to the required node.<br>As a result of the ping, the SCALANCE S detects the node and passes this information on to SOFTNET Security Client.<br>Note:<br>If the dialog is not open while a node is detected, the dialog is displayed automatically. |
| 9. | Activate the nodes for which the status display indicates that no tunnel connection has yet established.<br>Once the connection has been established, you can start your application - for example STEP 7 - and establish a communication connection to one of the nodes. |

Tunnel over: 141.73.12.156

| Status | Name | IP-Address | SCALANCE S - IP |
|---|---|---|---|
| | "Module2" - | SCALANCE S | 192.168.10.2 |
| | "Module4" - | SCALANCE S | 192.168.10.4 |
| | "Module1" - | SCALANCE S | 192.168.10.1 |
| | Member of: "Module1" | 196.80.96.20 | 192.168.10.1 |

☑ enable active learning

## Meaning of the parameters

Table 7-1 Meaning of the parameters in the ”Tunnel over...” dialog box

| Parameter | Meaning / range of values |
|---|---|
| Status | Possible status displays are:<br>see Table 7-2 |
| Name | Name of the module or the node taken from the configuration created with the Security Configuration Tool. |
| IP address | For nodes: IP address of the internal node |
| SCALANCE S IP Address | IP address of the assigned SCALANCE S module |
| Tunnel over.. | Falls Sie in Ihrem PC mehrere Netzwerkkarten betreiben, wird hier die zugeordnete IP-Adresse angezeigt. |

Table 7-2 Status displays

| Symbol | Meaning |
|---|---|
| ✗ | There is no connection to the module or node. |
| ➥ | There are more nodes to be displayed. Click on the symbol to display further nodes |
| 🔗 | The node has been assigned parameters but not yet tested. |
| 🔗 | The node has been assigned parameters and has been tested. |
| 🔑 | Disabled SCALANCE S module. |
| 🔑 | Enabled SCALANCE S module. |

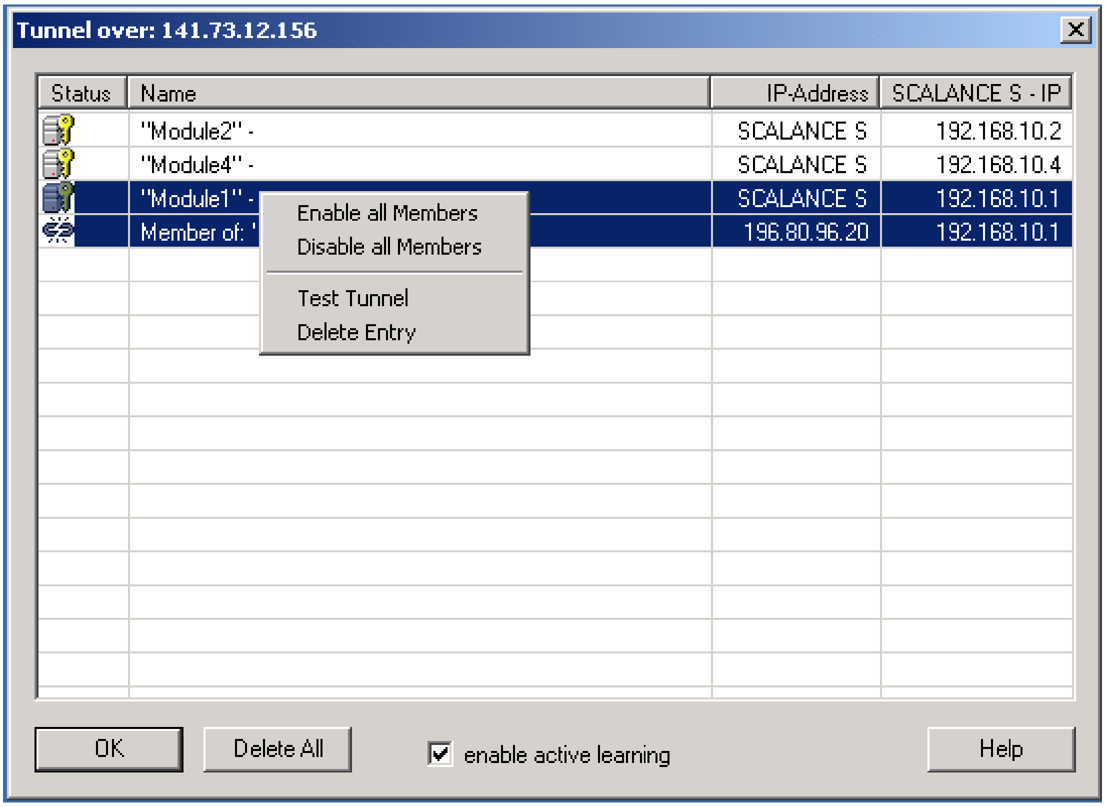
## ”Enable active learning” check box

If the learning mode has been enabled in the configuration of the SCALANCE S modules, you can also use the learning mode for the SOFTNET Security Client; You then obtain the information from the SCALANCE S modules automatically.

Otherwise the ”Activate learning mode” is inactive and grayed out.

## Selecting and working with a tunnel entry

In the ”Tunnel” dialog, you can select an entry and open several menu commands with the right mouse button.



| Status | Name | IP-Address | SCALANCE S - IP |
|---|---|---|---|
| | "Module2" - | SCALANCE S | 192.168.10.2 |
| | "Module4" - | SCALANCE S | 192.168.10.4 |
| | "Module1" - | SCALANCE S | 192.168.10.1 |
| | Member of: ' | 196.80.96.20 | 192.168.10.1 |

☑ enable active learning

**Notice**
If more than one IP address is used for a network adapter, you may have to assign the particular IP address to be used in the “Tunnel” dialog for each individual entry.

## ”Delete All” button

This allows you to delete all the security guidelines, including additional entries that were not created by the SOFTNET Security Client.

## Enabling and disabling existing secure connections

You can disable existing secure connections with the ”Disable” button. If you click the button, the text in the button changes to ”Connect” and the icon in the status bar is replaced.

Internally, the security policies now deactivated.

If you click on the button again, you can undo the change you made above and the tunnels are enabled again.

# 8 Online functions - test, diagnostics, and logging

For test and monitoring purposes, SCALANCE S has diagnostic and logging functions.

These functions can only be used when there is a network connection to the selected SCALANCE S module.

## Further information

For detailed information on the dialogs and the parameters recalled in diagnostics and logging, please refer to the online help of the Security Configuration Tool.

You can call this with the F1 key or using the ”Help” button in the relevant dialog.

## 8.1 Overview of the functions in the online dialog

Depending on the operator view in the Security Configuration Tool, SCALANCE S provides the following functions in the online dialog:

Table 8-1 Functions and logging in online diagnostics

| Function / tab in the online dialog | Meaning | Available in operator view | |
|---|---|---|---|
| | | Standard mode | Advanced mode |
| System and status functions | | | |
| **Status** | Display of the device status of the SCALANCE S module selected in the project. | X | X |
| **Communication Status** | Display of the communication status and the internal nodes for other SCALANCE S modules belonging to the VPN group. | | X |
| **Control** | Date and time setting. | | X |
| **Internal Nodes** | Display of the internal nodes of the SCALANCE S module. | | X |
| Logging functions | | | |
| **System Log** | Display of logged system events. | X | X |
| **Audit Log** | Display of logged security events. | | X |
| **Packet Filter Log** | Display of logged data packets and start and stop of packet logging. | X | X |

### Prerequisites for access

Before you can run the online functions on a SCALANCE S module, the following requirements must be met:

- The online mode is activated in the Security Configuration Tool;
- There is a network connection to the selected module;
- The corresponding project with which the module was configured is open.

**Note**

You can also use the diagnostic functions that are available only in advance mode even if you created the project in standard mode.

In this case, switch to advanced mode before starting online diagnostics.

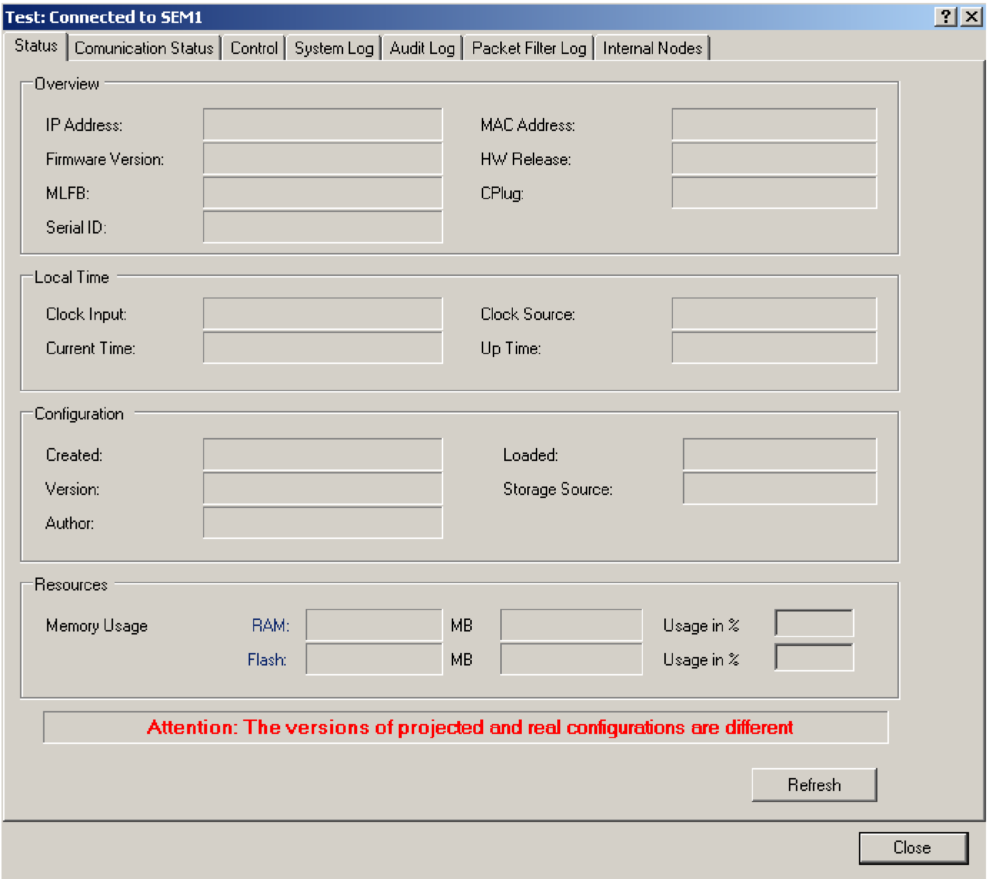
## Opening the online dialog

Switch over the mode of the Security Configuration Tool with the following menu command:

**View ▸Online**

Select the module you want to edit and then select the following menu command to open the online dialog:

**Edit ▸ Online Diagnostics...**



Attention: The versions of projected and real configurations are different

## Warning if the configuration is not up-to-date or the wrong project has been selected

When you open the online dialog, the program checks whether the current configuration on the SCALANCE S module matches the configuration of the loaded project. If there are differences between the two configurations, a warning is displayed. This signals that you have either not yet updated the configuration or have selected the wrong project.

### Online settings are not saved in the configuration

Settings you make in online mode are not saved in the configuration on the SCALANCE S module. Following a module restart, the settings in the configuration are therefore always effective.

## 8.2 Logging events

You can record events on the SCALANCE S. They are recorded in logs (log files).

Even during configuration, you can specify which data will be recorded and whether the recording is activated when the configuration is loaded.

The SCALANCE S recognizes three different types of events and therefore maintains three different logs:

Table 8-2 Logging in online diagnostics

| Function / tab in the online dialog | How it works | Remarks |
|---|---|---|
| **System Log**<br>(configurable) | The system log automatically records consecutive system events, for example the start of a process. | • System log data is retentive<br>The system.log files are stored in volatile memory on the SCALANCE S. This data is therefore no longer available after the power supply has been turned off. |
| **Audit Log**<br>(always enabled) | The audit log automatically recalls consecutive security-relevant events, such as the attempted use of an invalid certificate. | • Audit log data retentive<br>The audit log data is saved in retentive memory on the SCALANCE S. The data of the audit log is therefore available after turning off the power supply. |
| **Packet Filter Log**<br>(configurable) | The packet filter log records certain packets from the data traffic. Data packets are only logged if they match a configured packet filter rule (firewall). | • Packet filter log data is not retentive<br>The data is stored in volatile memory on the SCALANCE S and is therefore no longer available after the power supply has been turned off. |

### Enabling or disabling logging

You can enable or disable logging in the configurable functions.

## Storage of recorded data

There are two options for storage of recorded data:

- Ring buffer

  At the end of the buffer, the recording continues at the start of the buffer and overwrites the oldest entries.

- One-shot buffer

  Recording stops when the buffer is full.

### 8.2.1 Log settings in the configuration

In offline mode, you can specify the recording method in the log settings. These log settings are loaded on the module with the configuration and take effect when the SCALANCE S starts up.

If necessary, you can modify these configured log settings in the online functions. This does not change the settings in the project configuration.

#### Log settings in standard mode

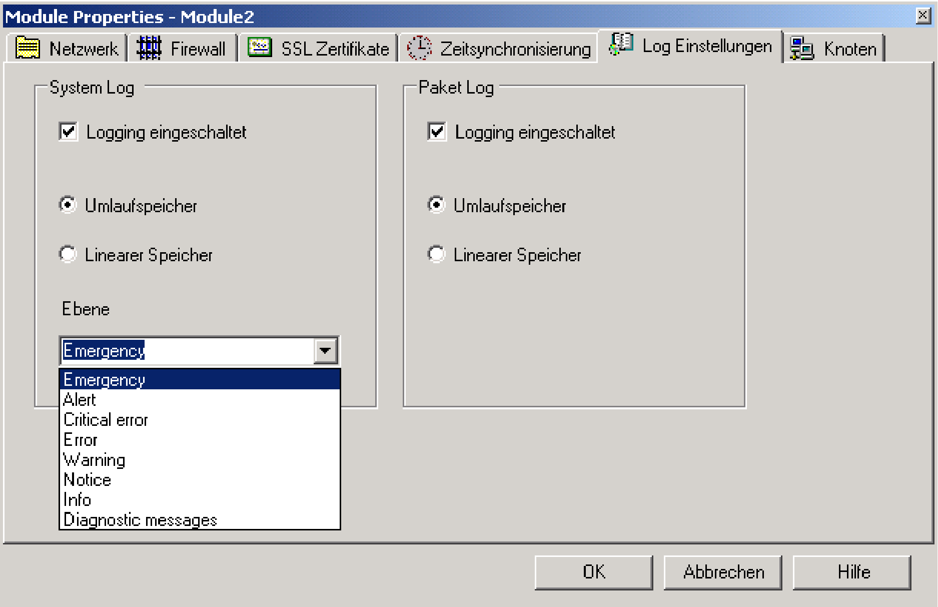
The log settings in standard mode correspond to the defaults in advanced mode. In standard mode, however, you cannot change the settings.

#### Log settings in advanced mode

Select the module you will want to edit and then the following menu command:

**Edit ▸ Properties..** , ”Log Settings” tab.

The following dialog shows the standard settings for SCALANCE S:



Module Properties - Module2

Netzwerk | Firewall | SSL Zertifikate | Zeitsynchronisierung | Log Einstellungen | Knoten

System Log

☑ Logging eingeschaltet

● Umlaufspeicher

○ Linearer Speicher

Ebene: Emergency

- Emergency
- Alert
- Critical error
- Error
- Warning
- Notice
- Info
- Diagnostic messages

Paket Log

☑ Logging eingeschaltet

● Umlaufspeicher

○ Linearer Speicher

#### ”Level” parameter

HLP F1

Here, you can specify a filter for recording system messages based on message priorities. You will find the possible values  for the settings and their meaning in the online help.

## 8.2.2 Configuring packet logging

The packet filter log records the data packets for which you activated logging in a packet filter rule (firewall) in the configuration. Activation must therefore be configured.

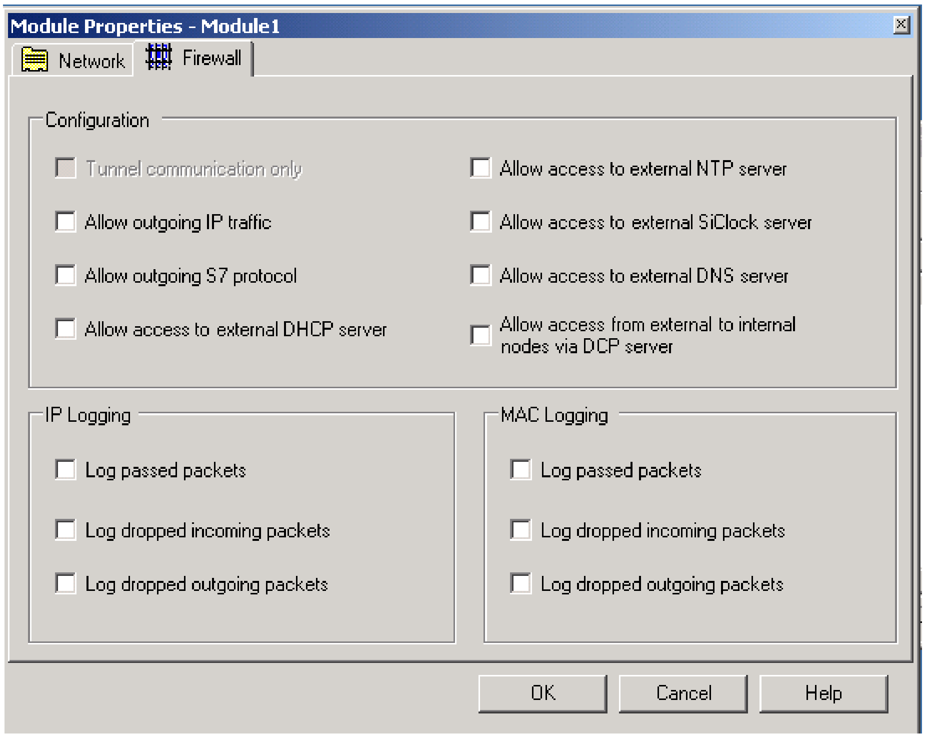
Configuration differs depending on the operator view. While in standard mode, logging can only be enabled for a few predefined, fixed sets of rules, in advanced mode, it can be enabled for individual packet filter rules.

### Configuring in standard mode

In standard mode, there are the following sets of rules for IP and MAC log settings that can be enabled for logging:

Table 8-3 IP and MAC log settings

| Rule | Action on activation |
|---|---|
| Log passed packets | All IP / MAC packets that were forwarded are logged. |
| Log dropped incoming packets | All incoming IP / MAC packets that were dropped are logged. |
| Log dropped outgoing packets | All outgoing IP / MAC packets that were dropped are logged. |



Configuration

□ Tunnel communication only
□ Allow outgoing IP traffic
□ Allow outgoing S7 protocol
□ Allow access to external DHCP server
□ Allow access to external NTP server
□ Allow access to external SiClock server
□ Allow access to external DNS server
□ Allow access from external to internal nodes via DCP server

IP Logging

□ Log passed packets
□ Log dropped incoming packets
□ Log dropped outgoing packets

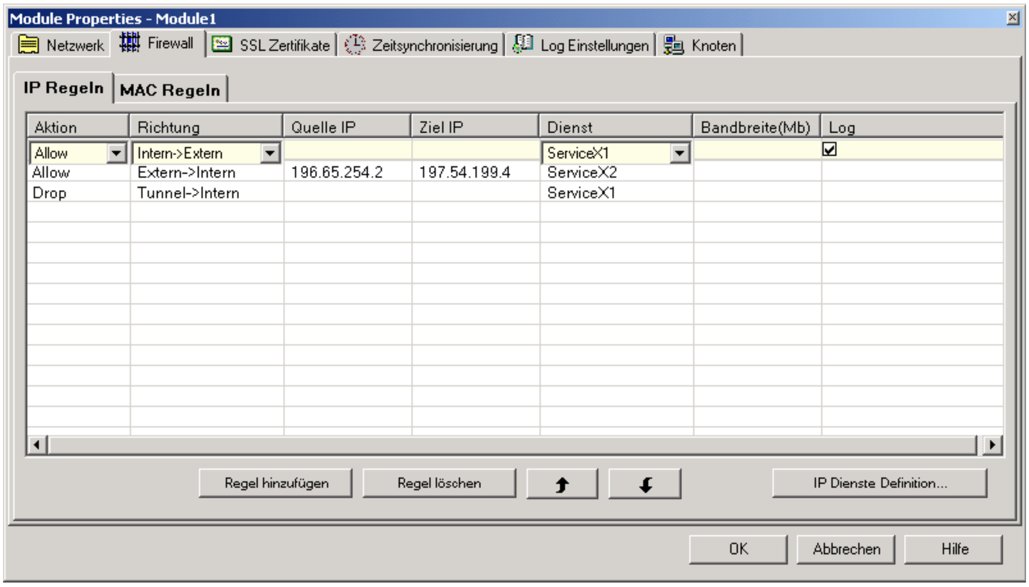
MAC Logging

□ Log passed packets
□ Log dropped incoming packets
□ Log dropped outgoing packets

## Configuring in advanced mode

Enabling logging is identical for both rule types (IP or MAC) and all rules.

To log data packets of specific packet filter rules, put a check mark in the ”Logging” column in the ”Firewall” tab.



| Aktion | Richtung | Quelle IP | Ziel IP | Dienst | Bandbreite(Mb) | Log |
|---|---|---|---|---|---|---|
| Allow | Intern->Extern | | | ServiceX1 | | ☑ |
| Allow | Extern->Intern | 196.65.254.2 | 197.54.199.4 | ServiceX2 | | |
| Drop | Tunnel->Intern | | | ServiceX1 | | |

## 8.2.3 Logging in online mode

### Opening online logging

With the SCALANCE S online, select the following menu command:

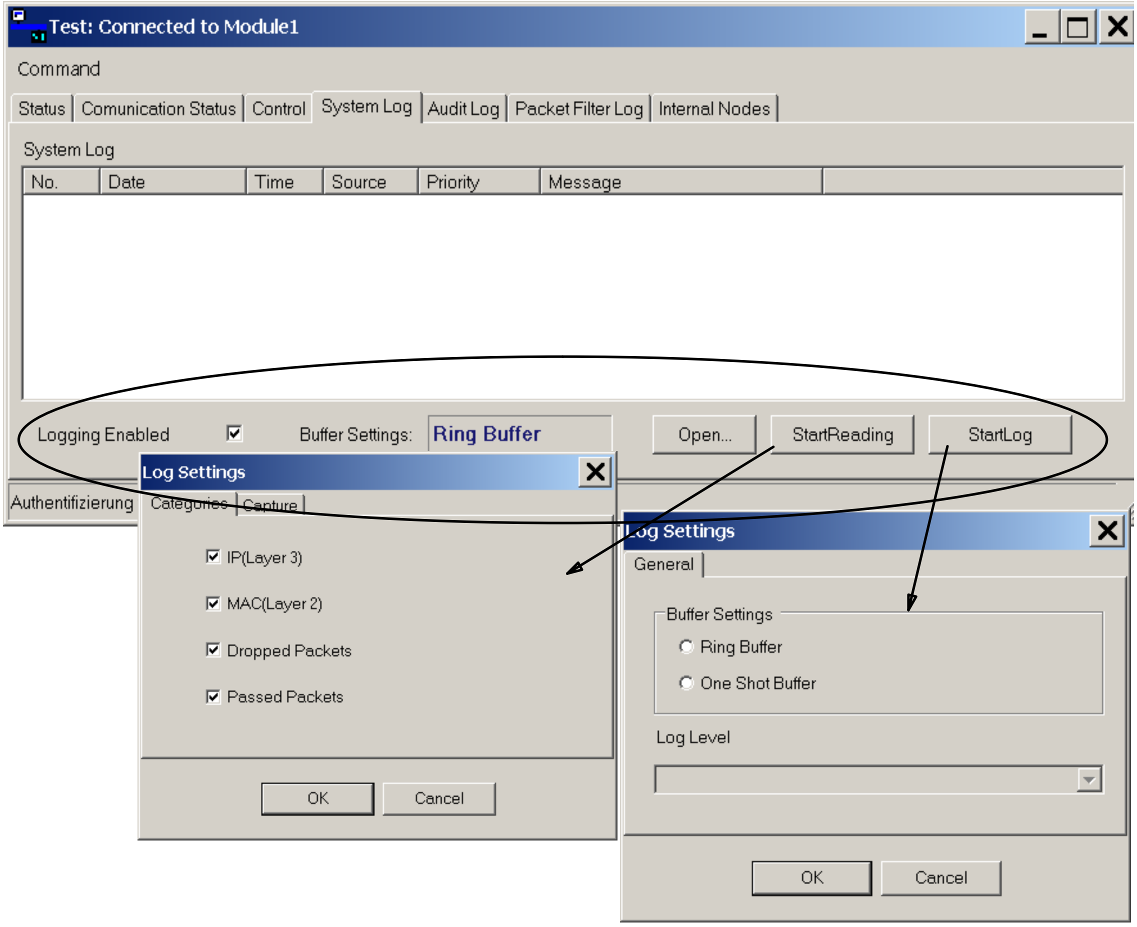
**Edit ▸ Online Diagnostics..**

As soon as you open one of the tabs for logging functions, you will see the current status of the logging function on the selected SCALANCE S module in the lower area of the tab.

- Logging Enabled: Yes/no
- Buffer Settings: Ring Buffer / One Shot Buffer

This current logging status is based either on the loaded configuration or on the previous use of the online function.

Using the buttons in the lower part of the tab, you can control logging and data output as described below.



Logging Enabled ☑ Buffer Settings: Ring Buffer

☑ IP(Layer 3)
☑ MAC(Layer 2)
☑ Dropped Packets
☑ Passed Packets

○ Ring Buffer
○ One Shot Buffer

## ”Start Reading” button - reading out log data from the SCALANCE S

Depending on the log function, you display a dialog with the following tabs:

- Categories

  The ”Categories” tab contains a display filter for the logged data in which you can select the following four categories:

  - IP (Layer 3), IP packets are displayed,
  - MAC (Layer 3), MAC packets are displayed,
  - Dropped Packets, dropped packets are displayed,
  - Passed Packets, forwarded packets are displayed,

- Capture

  With all three log functions, it is possible to write the recorded data to a file with the SCALANCE S.

  You can archive the log data in the ”Capture” tab.

  The logged data is then stored in the specified file when it is read from the buffer and transferred to the display. This procedure is started when you close the dialog with ”OK”.

## ”StartLog” button - selecting the storage procedure

You can select the storage method in the ”General” tab.

Logging is started when you close the dialog with ”OK”.

The ”StartLog” button of the Log dialog is then renamed to ”StopLog”.

If you click the renamed dialog button, logging is stopped.

## Archiving log data and reading in from the file

You can open and display stored log files as follows:

- ”Open” button in the relevant tab the log function.
- Menu command **View ▸ LogFile..**

# A Tips and help on problems

## A.1 SCALANCE S module does not boot correctly

If the fault LED of the SCALANCE S module is lit red after booting, you should first completely reset the module. Press the reset button until the fault LED starts to flash yellow. The module is then reset to the factory settings. For productive operation, you must then download the configuration to the module again.

If the fault display of the SCALANCE S module continues to be lit red, however, the module can only be repaired in the factory.

## A.2 Replacing a SCALANCE S module

A SCALANCE S module can be replaced without a PC (without needing to download the configuration to the new module). The C-PLUG of the module you are replacing is simply inserted in the new module you want to commission.

**Notice**

The C-PLUG may only be inserted or removed when the power is off!

## A.3 SCALANCE S module is compromised

A SCALANCE S module is compromised when

- the private key belonging to the server certificate,
- the private key of the CA or
- the password of a user has become known.

### Private key of the server certificate known

If the private key belonging to the server certificate has become known, the server certificate on the SCALANCE S module must be replaced. The user names stored on the SCALANCE S module do not need to be changed.

Follow the steps below:

| Step | Procedure |
|---|---|
| 1. | Select the module you want to edit and then select the menu command **Edit ▸ Properties..** , ”Certificates” tab. |
| 2. | Generate a new certificate. |
| 3. | Download the configuration to the SCALANCE S module. |

### The private key of the CA is known

If the private key of the CA has become known, the certificate of the CA must be replaced on the SCALANCE S module. The user names can remain unchanged. The users do, however, required new certificates provided by the new CA.

Follow the steps below:

| Step | Procedure |
|---|---|
| 1. | Select the group you want to edit and then select the menu command **Edit ▸ Properties..** |
| 2. | Generate a new certificate. |
| 3. | Download the configuration to all SCALANCE S modules that belong to the group. |

### Password of a user from the user group is known

If the password of a user from the user group has become known, the password of this user must be changed.

### Password of a user from the administrator group is known

If the user belongs to the administrators group, the server certificate of the SCALANCE S module should also be changed (see A.3).

## A.4 Key from the configuration data compromised or lost

### Key compromised

If a private key from the configuration data of the SCALANCE S module is compromised, the key must be changed using the configuration tool of the SCALANCE S module.

### Loss of the key

If the private key that authorizes access to the configuration data is lost, it is no longer possible to access the SCALANCE S module with the configuration tool. The only possibility to regain access is to delete the configuration data and therefore also the key. You can delete this information by pressing the reset button. Following this, the SCALANCE S module must be taken into operation again.

## A.5 General operational behavior

### Adjusting the MTU (maximum transmission unit)

The MTU defines the permissible size of a data packet that is transferred in the network. If these data packets are transferred by SCALANCE S via the IPSec tunnel, header information is added to the original data packet, which means that the packet may have to be segmented (depending on the MTU settings in the connected network). This can, however, compromise performance quite significantly.

You can avoid this by adjusting the MTU format, that is, reducing it to such an extent that the data packets received by SCALANCE S can be extended to include the required additional information without then having to segment them. Between 1000 and 1400 bytes is recommended.

# B Notes on the CE Mark

## B.1 Notes on the CE Mark

### Product Name:

| | | |
|---|---|---|
| SIMATIC NET | SCALANCE S612 | 6GK5612-0BA00-2AA3 |
| SIMATIC NET | SCALANCE S613 | 6GK5613-0BA00-2AA3 |

### EMC Directive

89/336/EEC ”Electromagnetic Compatibility”

### Area of Application

The product is designed for use in an industrial environment:

| **Area of Application** | **Requirements** | |
|---|---|---|
| | Noise emission | Noise immunity |
| Industrial operation | EN 61000-6-4: 2001 | EN 61000-6-2: 2001 |

### Installation Guidelines

The product meets the requirements if you keep to the installation instructions and safety-related notices as described here and in the manual ”SIMATIC NET Industrial Ethernet Twisted Pair and Fiber Optic Networks” /2/ when installing and operating the device.

## Conformity Certificates

The EU declaration of conformity is available for the responsible authorities according to the above-mentioned EU directive at the following address:

Siemens Aktiengesellschaft
Bereich Automatisierungs- und Antriebstechnik
Industrielle Kommunikation (A&D PT2)
Postfach 4848
D-90327 Nürnberg

## Notes for the Manufacturers of Machines

This product is not a machine in the sense of the EU directive on machines. There is therefore no declaration of conformity for the EU directive on machines 89/392/EEC.

If the product is part of the equipment of a machine, it must be included in the procedure for the declaration of conformity by the manufacturer of the machine.

# C Glossary / abbreviations and acronyms

### ARP

Address Resolution Protocol
The ARP protocol is used for address resolution. Its task is to find the corresponding network hardware address (MAC address) for a given protocol address.
An ARP protocol implementation is often found on hosts on which the Internet protocol family is used. IP forms a virtual network on the basis of IP addresses. These must be mapped to the given hardware addresses when the data is transported. To achieve this mapping, the ARP protocol is often used.

### Bandwidth

Maximum throughput of a connecting cable (normally specified in bps).
(Source: http://www.bktechnik.com/html/lexikon.htm)

### Broadcast

A broadcast is like ”calling all all stations”. Broadcast packets are received by all nodes configured to receive broadcasts.

### Bus segment

Part of a subnet. Subnets can be made up of the bus segments connected by connectivity devices such as repeaters and bridges. Segments are transparent for addressing.

### C-PLUG

The C-PLUG is an exchangeable medium for storage of the configuration and project engineering data of a basic device. This means that the configuration data remains available if the basic device is replaced.

### Client

A client is a device, or more generally an object, that requests a -> server to provide a service.

### CP

Communications processor. Module for communication tasks.

### Firewall

One or more devices that allow or prevent data access to interconnected networks according to given security restrictions.

### Gateway

Intelligent interface device that interconnects various -> LANs on ISO layer 7.

### HTTPS

Secure Hypertext Transfer Protocol or HyperText Transfer Protocol Secured Socket Layer (SSL)
Protocol for transmission of encrypted data.
Expansion of HTTP for secure transmission of confidential data with the aid of SSL.
HTTPS is based on HTTP and provides additional encryption between two partners.

### ICMP

The ICMP protocol (ICMP, Internet Control Message Protocol) is an auxiliary protocol of the IP protocol family and requires support of the IP protocol. It is used to exchange information and error messages.

### Ind. Ethernet node

A node is identified by a -> MAC address on -> Industrial Ethernet.

### Industrial Ethernet

A bus system complying with IEEE 802.3 (ISO 8802-2).

### IPsec

IP Security Protocol
This is a layer 3 tunneling protocol and is an expansion/addition to IP. IPsec (currently), however, only allows encryption of IP packets, does not transfer multicasts and only supports static routing.

### MAC address

Address to distinguish difference stations connected to a common transmission medium (Industrial Ethernet).

### Media Access Control (MAC)

Controls access by a station to a transmission medium shared with other stations.

### Network

A network consists of one or more interconnected subnets with any number of nodes. Several networks can coexist.

### Ping

A test protocol belonging to the IP protocol family. This protocol exists on every MS Windows computer under the same name as a console application (command prompt level). With ”Ping”, you can prompt a reply (sign of life) from an IP network node within a network as long as you know its IP address. You can find out whether this network node can be reached at the IP level and therefore check the effectiveness of the configured SCALANCE S functionality.

### PKCS

PKCS stands for Public Key Cryptographic Standards and is a specification developed by the RSA Laboratories among others from 1991 onwards.
A certificate links data of a cryptographic key (or key pair consisting of a public and private key) with data of the owner and a certification issuer as well as other specifications.

### PKCS#12 format

The standard specifies a PKCS format suitable for exchange of the public key and an additional password-protected private key.

### Preshared keys

Designates a symmetric key method. The key must be known at both ends prior to communication. This key is also generated automatically when a group is created. However, you must first enter a password in the ”Key” box in the Security Configuration Tool ”Group Properties” dialog from which the key is generated.

### Protocol

A set of rules for transferring data in a network. These rules specify both formats of the messages and the data flow for data transmission.

### Public key method

The purpose of encryption methods with public keys is to avoid all security risks when mutually exchanging keys. Each has a pair of keys with a public and a secret key. To encrypt a message, you use the public key of the recipient and only the recipient can decrypt the message using its secret key.

### Server

A server is a device, or more generally an object, that can provide certain services; the service is provided when requested by a -> client.

### Services

Services provided by a communication protocol.

### SIMATIC NET

Siemens SIMATIC Network and Communication. Product name for networks and network components from Siemens. (previously SINEC)

### SIMATIC NET Ind. Ethernet

SIMATIC NET bus system for industrial application based on Ethernet. (previously SINEC H1)

### System

All the electrical equipment within a system. A system includes, among other things, programmable logic controllers, devices for operator control and monitoring, bus systems, field devices, drives, power supply cabling.

### SSL connection

The SSL protocol is located between the TCP (OSI layer 4) and the transmission services (such as HTTP, FTP, IMAP etc.) and is used for a secure transaction. With SSL, the user is sure that it is connected to the required server (authentication) and that the sensitive data is transferred over a secure (encrypted) connection.

### Stateful packet inspection

Stateful Inspection (also known as Stateful Packet Filter or Dynamic Packet Filter) is a new firewall technology that operates both on the network and the application layer. The IP packets are accepted on the network layer, inspected according to their state by an analysis module and compared with a status table. For the communication partner, a firewall with stateful inspection appears as a direct cable that only allows communication according to the rules.

### Subnet mask

The subnet mask specifies which parts of an IP address are assigned to the network number. The bits in the IP address whose corresponding bits in the subnet mask have the value 1 are assigned to the network number.

### TCP/IP

TCP = Transport Connection Protocol; IP = Internet Protocol

### UDP

User Datagram Protocol. Datagram service for simple and data transfer beyond the boundaries of a network without acknowledgment.

**VLAN**

Virtual Local Area Network
A network structure with all the properties of a normal LAN although not spatially connected. While the distance between the stations of a LAN is restricted, a VLAN allows widely distant nodes to be connected to form a virtual local area network. The systems communicate with each other as though they were in the same physical LAN.
The advantages of VLANs include the absence of routers. This, for example, it improves the performance of the network since routers cause a certain latency. Security is also increased since the VLANs are isolated from each other. Search networks are also easier to administer. A system can be physically moved to a different location without needing to reconfigure it.

**VPN**

Virtual Private Network

# D References

## Sources of information and other documentation

1. SIMATIC NET Industrial Twisted Pair and Fiber Optic Networks, Release 05/2001
   Order numbers:

   6GK1970-1BA10-0AA0 German
   6GK1970-1BA10-0AA1 English
   6GK1970-1BA10-0AA2 French
   6GK1970-1BA10-0AA4 Italian

2. You will find further information on the SCALANCE system on the Internet at:

http://www2.automation.siemens.com/net/microsite/scalance/index.html

# E Dimension drawing

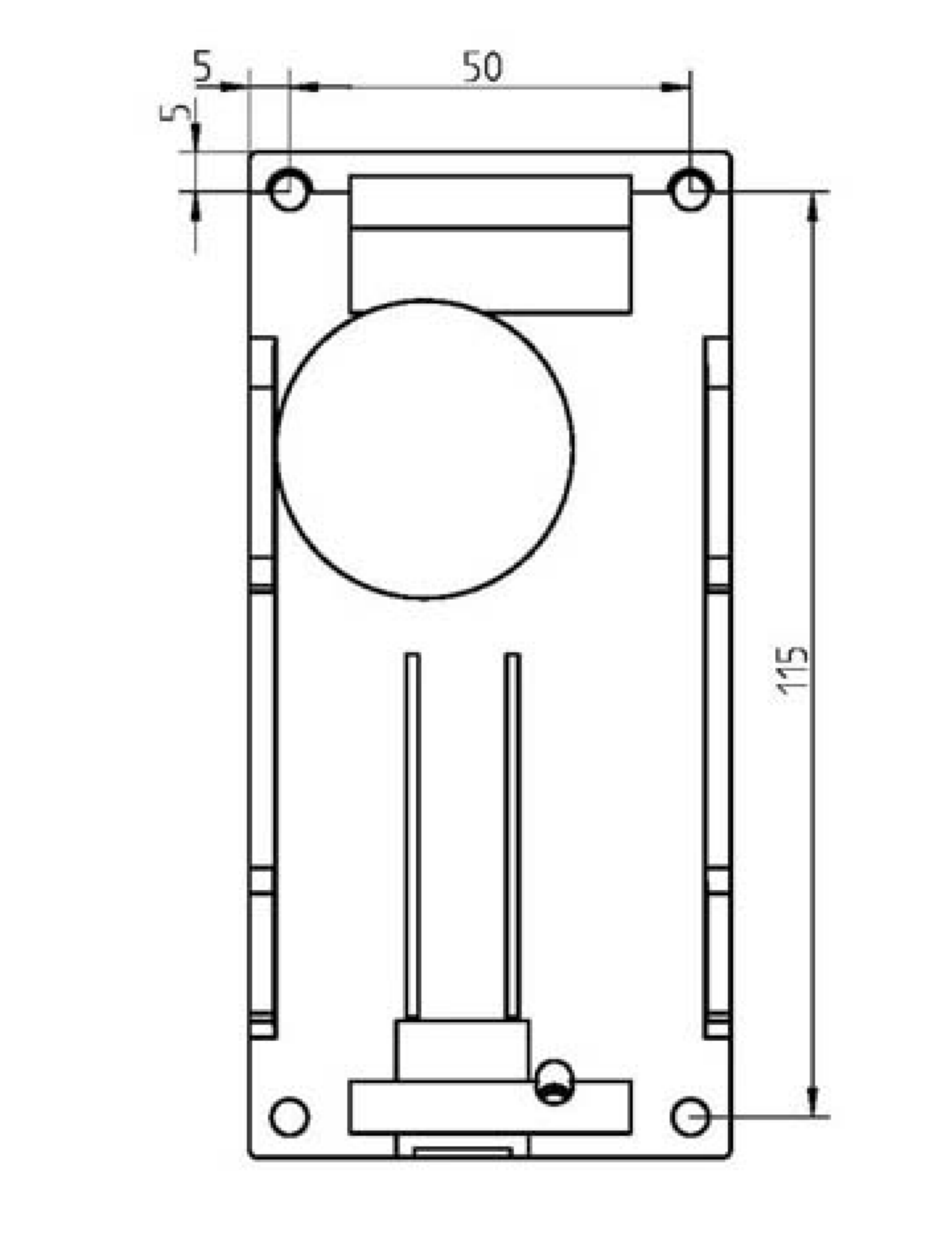


Figure A-1 Drilling template