SIEMENS

SIMATIC NET

Industrial Ethernet Security Basics and application

Configuration Manual

03/2012

C79000-G8976-C286-01

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree 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 **may** result if proper precautions are not taken.

⚠ CAUTION
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE
indicates that an unintended result or situation can occur if the relevant information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

Order number: C79000-G8976-C286-01
Ⓟ 04/2012 Technical data subject to change

Preface

Preface

This manual…

... supports you during the configuration of the security functions of the following products:

"Security Appliances":

- SCALANCE S: S602/ S612/ S623
- SOFTNET Security Client

"Security Integrated" products:

- S7-CPs: CP 343-1 Advanced, CP 443-1 Advanced
- PC-CP: CP 1628
- SCALANCE M: SCALANCE M87x and MD74x

General terminology "security module"

In this documentation, the term "security module" includes the following products: CP 343-1 Advanced, CP 443-1 Advanced, CP 1628, SCALANCE S 602 V3/SCALANCE S 612 V3/SCALANCE S 623 V3.

Functional differences are indicated by symbols (refer to the section "Explanation of the symbols"). You will find hardware descriptions and installation instructions in the documents relating to the individual modules.

New in this issue

This issue includes descriptions of the following new functions:

- New documentation concept

  The previous operating instructions "SCALANCE S and SOFTNET Security Client" are replaced by a cross-product SIMATIC NET Security manual that applies to all security modules.

- Security configuration for SCALANCE S V3.0

  The configuration of SCALANCE S V3.0 security modules with new functions is covered.

- Security configuration for CP 343 Advanced, CP 443-1 Advanced

  In addition to the SCALANCE S modules, security can now also be configured for the S7 CPs 343-1 Advanced and CP 443-1 Advanced. These two modules are grouped together in this manual under "CP x43-1 Adv.". SCT is integrated in STEP 7.

  Users, NTP servers or entries in the IP access control lists previously managed in STEP 7 can be migrated to SCT.

- **Security configuration for CP 1628**

  In addition to the SCALANCE S modules, security can now also be configured for the PC CP, CP 1628. SCT is integrated in STEP 7.

- **Security Configuration Tool 3.0 - new functions**
  - New concept for user management

    Apart from users, roles and rights can also be created. There are system-defined roles that cannot be modified or you can create new user-defined roles and assign rights to them.
  - Project-wide certificate manager

    Certificates are managed on a cross-project basis in the certificate manager.
  - Project-wide NTP server

    NTP servers can be created throughout the project and assigned to individual modules. For CPs, secure transfer of the time of day via secure NTP servers is supported.
  - The configuration of SNMPv3 is supported
- **SOFTNET Security Client V4.0**
  - You can configure a SOFTNET Security Client V4.0 along with the security modules and generate the relevant configuration files.

Validity of this manual

This manual is valid for the following devices and components:

- SIMATIC NET SCALANCE S602 6GK5 602-0BA10-2AA3 - with firmware version as of V3.0
- SIMATIC NET SCALANCE S612 6GK5 612-0BA10-2AA3 - with firmware version as of V3.0
- SIMATIC NET SCALANCE S623 6GK5 623-0BA10-2AA3 - with firmware version as of V3.0
- CP 343-1 Advanced 6GK7 343-1GX31-0XE0 - with firmware version as of V3.0
- CP 443-1 Advanced 6GK7 443-1GX30-0XE0 - with firmware version as of V3.0
- CP 1628 6GK1162-8AA00 - with firmware version as of V1.0
- SIMATIC NET SOFTNET Security Client 6GK1 704-1VW04-0AA0 - version as of 4.0
- Security Configuration Tool - version V3.0

Audience

This manual is intended for persons setting up the Industrial Ethernet security functions in a network.

CP documentation in the Manual Collection (order no. A5E00069051)

The SIMATIC NET Manual Collection ships with each S7 CP. This DVD is regularly updated and contains the device manuals and descriptions valid at the time it is created.

See also

/7/ (Page 209)

Symbols used in this manual

S≥V3.0

The chapter described / the section described / the line described is only relevant for SCALANCE S as of V3.0.

SCA.

The chapter described / the section described / the line described is only relevant for SCALANCE S.

~~S602~~

The chapter described / the section described / the line described is relevant for all security modules except SCALANCE S 602.

S623

The chapter described / the section described / the line described is only relevant for SCALANCE S 623.

S7-CP

The chapter described / the section described / the line described is only relevant for S7 CPs.

~~S7-CP~~

The chapter described / the section described / the line described is relevant for all security modules except the S7 CPs.

PC-CP

The chapter described / the section described / the line described is only relevant for PC CPs.

~~PC-CP~~

The chapter described / the section described / the line described is relevant for all security modules except the PC CPs.

CP

The chapter described / the section described / the line described is relevant for all S7 CPs and PC CPs.

The chapter described / the section described / the line described is relevant for all security modules except the CPs.

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.

References /.../

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.

See also

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

SIMATIC NET glossary

Explanations of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection

  The DVD ships with certain SIMATIC NET products.

- On the Internet under the following entry ID:

  50305045 (http://support.automation.siemens.com/WW/view/en/50305045)

Table of contents

Introduction and basics 1

Security messages

NOTICE
For its automation and drives product portfolio, Siemens provides IT security mechanisms to support secure operation of the plant/machine. Our products are continuously being further developed also taking into account the aspect of IT security. We therefore recommend that you regularly check for updates of our products and that you only use the latest versions. You will find information in: (http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en) Here, you can register for a product-specific newsletter. For the secure operation of a plant/machine, it is also necessary to integrate the automation components in a full IT security concept for the entire plant/machine that represents the state of the art in IT technology. You will find information on this in: (http://www.siemens.com/industrialsecurity) Products from other manufacturers that are being used must also be taken into account.

1.1 Important information

General

NOTICE
Protection from unauthorized access Make sure that the configuration computer and PC/PG as well as the project are protected from unauthorized access.

NOTICE
Disabling the guest account Make sure that the guest account is disabled on the configuration computer.

NOTICE
Current date and current time of day on the security modules When using secure communication (for example HTTPS, VPN...), make sure that the security modules involved have the current time of day and the current date. Otherwise the certificates used will not be evaluated as valid and the secure communication will not work.

Note

Up-to-date anti-virus software

We recommend that up-to-date anti-virus software is always installed on all configuration computers.

Note

FTPS

Where the term "FTPS" is used in this documentation, FTPS in the explicit mode is meant (PTPES).

Note

No return to standard mode possible

If you switch to the advanced mode and change the configuration for the current project, you can no longer switch back. Switching over to advanced mode is a setting that applies to the entire project and therefore also to all modules of the project.

Remedy for SCT Standalone: You close the project without saving and open it again.

CP x43-1 Advanced

NOTICE
Additional security settings To avoid unauthorized configuration data being downloaded to the CP, you will need to make additional security settings in the firewall of the CP (blocking S7 communication or only tunneled communication) or take external security measures.

STEP 7

Note

"Save and compile" after changes

To have the security settings adopted in the corresponding (offline) system data blocks, after making changes, select the "Station" > "Save and Compile" menu in HW Config or "Network" > "Save and Compile" in NetPro.

Note

Opening a station with the Security Configuration Tool open

Close the Security Configuration Tool before you open another station with the SIMATIC Manager or NetPro.

1.2 Introduction and basics

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

Note

Up-to-date anti-virus software

We recommend that up-to-date anti-virus software is always installed on all configuration computers.

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

- SCALANCE S
- CP x43-1 Advanced
- CP 1628
- SOFTNET Security Client

Tip:

The document "SIMATIC NET Security - Getting Started" will help you to start working with the security modules in a short time.

1.3 Product characteristics

1.3.1 Overview of the functions

Overview of the functions of the device types

The following table shows the functions supported by the individual security modules.

Note

This manual describes all functions. Based on the following table, note which functions are relevant for the security module you are using.

You should also note the additional information in the titles of the sections.

Table 1- 1 Overview of the functions

Function	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V3.0
Configuration using			
Security Configuration Tool	-	-	x
Security Configuration Tool integrated in STEP 7	x	x	x
Compatibility with			
Other security modules	x	x	x
IP Access control lists (ACL)	x	-	-
SOFTNET Security Client	x	x	x ~~S602~~
General			
NAT/NAPT router	x	-	x
DHCP server	-	-	x
Firewall			
Local firewall rules	x	x	x
Global firewall rules	x	x	x
User-specific firewall rules	-	-	x
IPsec			
Establishment of IPsec tunnels	x	x	x ~~S602~~
User management			
Configuring user administration	x	x	x
Migration of the current user management	x	-	-
Secure protocols			
SNMPv3	x	x	x

Function	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V3.0
HTTPS	x	-	x
FTPS server	x	-	-
FTPS client	x	-	-
NTP	x	x	x
Secure NTP	x	x	-
Other protocols			
PPPoE client	-	-	x
DynDNS	-	-	x
Logging			
Logging system events	x	x	x
Logging audit events	x	x	x
Logging packet filter events	x	x	x
Audit messages in the diagnostics buffers of the security module	x	x	-
Access to the log buffer of the security module using the Security Configuration Tool	x	x	x
Web diagnostics	x	-	-
VPN diagnostics with the Security Configuration Tool (VPN=Virtual Private Network)	x	x	x
Sending messages to Syslog server	x	x	x

x Function supported

- Function not supported

1.3.2 Configuration limits

Note

You will find a complete overview of the permitted configuration limits on the Internet at the following address: http://support.automation.siemens.com/WW/view/en/58217657 (http://support.automation.siemens.com/WW/view/en/58217657).

Configuration limits

Function	CP x43-1 Adv.	CP 1628	SCALANCE S ≥ V3.0
VPN tunnels per security module	Max. 16 *		Max. 128
Firewall rules per security module	Max. 256		
NTP servers that can be created throughout the project (assignable NTP server per security module)	32 (4)		

* Planned as of SCT V3.1:
- Max. 32 for CP x43-1 Adv.
- Max. 64 for CP 1628

Which rules apply to user names, role names and passwords?

When creating or modifying a user, a role or a password, remember the following rules:

Permitted characters	0123456789 A...Z a...z !"#$%&'()*+,-./:;<=>?@ [\]_{|}~¦^`
Length of the user name	1 ... 32 characters
Length of the password	8 ... 32 characters
Length of the role name	1 ... 32 characters
Maximum number of users per project	128
Maximum number of users on one security module	32 + 1 administrator when creating the project
Maximum number of roles per project	121 user-defined + 4 system-defined
Maximum number of roles on one security module	37

1.3.3 Replacing a module

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Replace module" menu command.
3. Depending on the product type of the selected module, you can adapt the module type and/or the firmware release in the dialog.

Based on a following table, you can see which modules you can replace without data loss and which could involve a possible data loss.

Note

Replacing modules of different types

- To replace a module with a different module type, you need to create a new module and configure this appropriately.
- You will find information about replacing CPs in the relevant device manual.

Table 1- 2 Compatible modules

Initial module	Possible module replacement	
	without losses	possibly with losses
S602 V2 and V3	S612 V2 S613 V2	S612 V1 S613 V1
S612 V1	S612 V2 S613 V1 S613 V2	S602 V2 and V3
S612 V2	S613 V2 S612 V3 S623 V3	S602 V2 and V3 S612 V1 S613 V1
S613 V1	S613 V2 S612 V3 S623 V3	S602 V2 and V3 S612 V1 S612 V2
S613 V2	S612 V3 S623 V3	S602 V2 and V3 S612 V1 S612 V2 S613 V1
SOFTNET Security Client 2005	SOFTNET Security Client 2008 SOFTNET Security Client V3.0 SOFTNET Security Client V4.0	-
SOFTNET Security Client 2008	SOFTNET Security Client 2005 * SOFTNET Security Client V3.0 SOFTNET Security Client V4.0	-
SOFTNET Security Client V3.0	SOFTNET Security Client 2005 * and ** SOFTNET Security Client 2008 **	-
SOFTNET Security Client V4.0	SOFTNET Security Client 2005 * and ** SOFTNET Security Client 2008 ** SOFTNET Security Client V3.0	-
SCALANCE M	-	-

* If the module is not in a routing group.

** If the module is not in a VPN group with an MD module.

See also

User interface and menu commands (Page 34)

/2/ (Page 208)

1.4 Use of the SOFTNET Security Client

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

With the SOFTNET Security Client PC software, secure remote access is possible from PGs/PCs to automation systems protected by security modules via public networks.

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

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

The SOFTNET Security Client PC software is also configured with the Security Configuration Tool ensuring fully integrated configuration.

1.5 Using the SCALANCE S602

Firewall and router - the job of the SCALANCE S602

With a combination of different security measures such as firewall and NAT/NAPT routers, the SCALANCE S602 protects individual devices or even entire automation cells from:

- Data espionage
- Unauthorized access

SCALANCE S602 allows this protection flexibly and without complicated handling.

SCALANCE S602 is configured with the Security Configuration Tool.

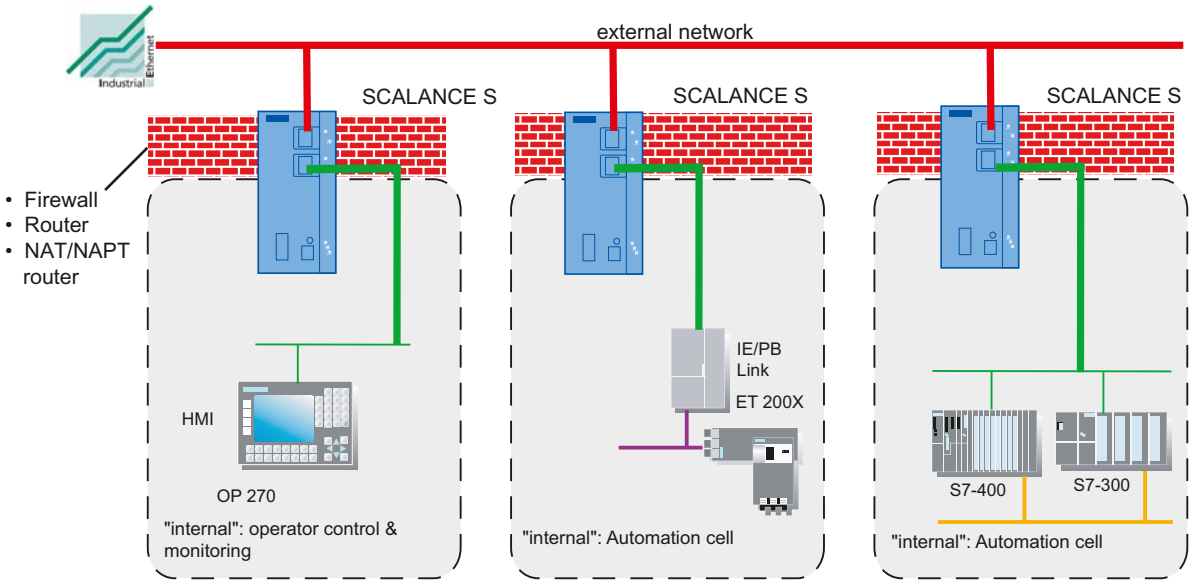


Figure 1-1 Network configuration with SCALANCE S602

Security functions

- Firewall
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Firewall also for Ethernet "non-IP" packets according to IEEE 802.3

    (Layer 2 packets: does not apply to S602 if router mode is used);
  - Bandwidth limitation

  All network nodes located in the internal network segment of a SCALANCE S are protected by its firewall.
- Router mode

  By operating the SCALANCE S as a router, you separate the internal network from the external network. The internal network connected over SCALANCE S therefore becomes a separate subnet; SCALANCE S must be addressed explicitly as a router using its IP address.
- Protection for devices and network segments

  The firewall protective function can be applied to the operation of single devices, several devices, or entire network segments.
- No repercussions when included in flat networks (bridge mode)

  This means that when a SCALANCE S602 is installed in an existing network infrastructure, the settings of end devices do not need to be made again.

Internal and external network nodes:

SCALANCE S602 divides 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!

1.6 Use of SCALANCE S612 and S623

All-round protection - the job of SCALANCE S612 and SCALANCE S623

With a combination of different security measures such as firewall, NAT/NAPT routers and VPN (Virtual Private Network) over IPsec tunnels, the security modules SCALANCE S612 and SCALANCE S623 protect individual devices or even entire automation cells from:

- Data espionage
- Data manipulation
- Unauthorized access

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 and SOFTNET Security Client are configured with the Security Configuration Tool.

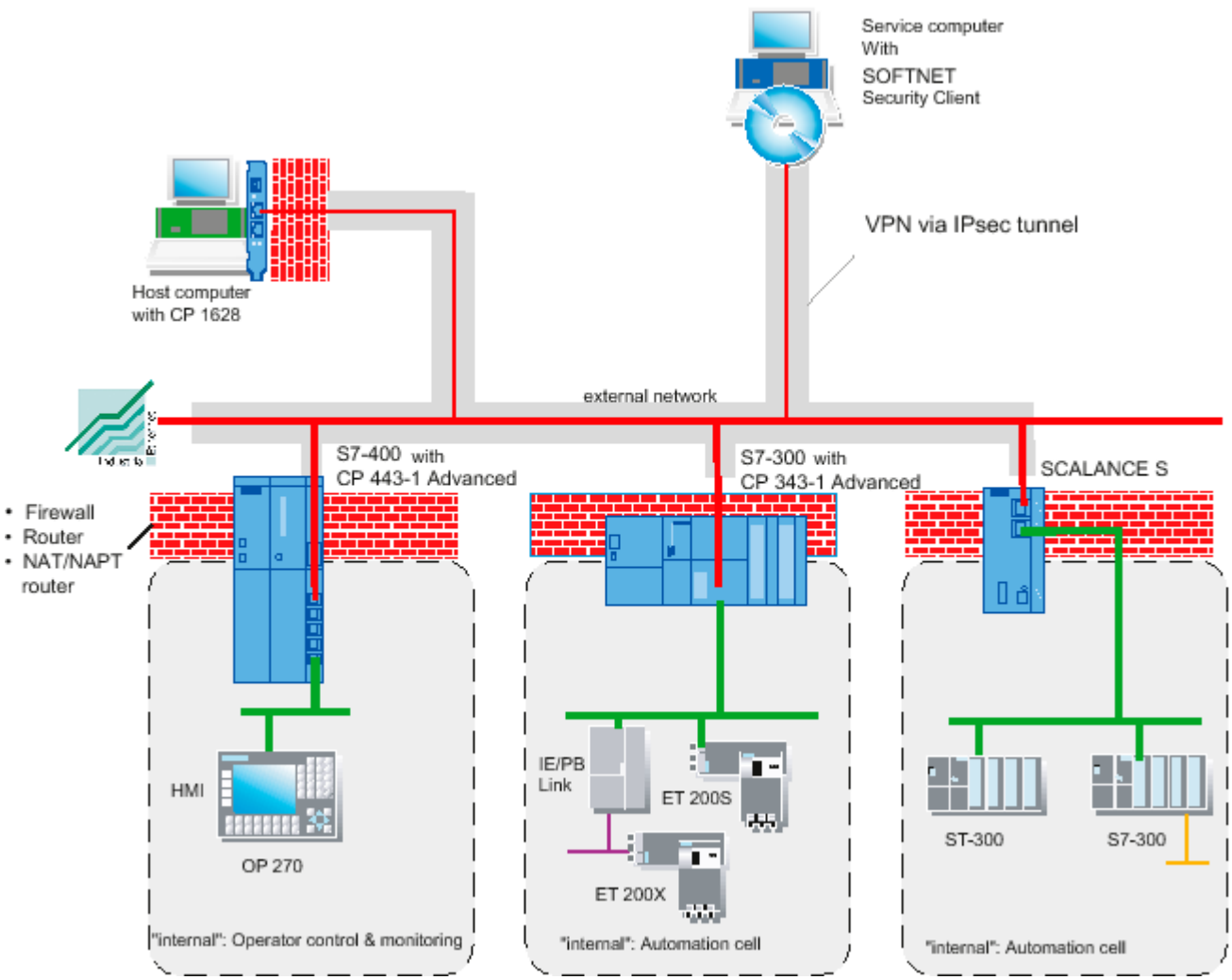


Figure 1-2 Network configuration with SCALANCE S612

Security functions

- Firewall
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Firewall also for Ethernet "non-IP" frames according to IEEE 802.3

    (Layer 2 frames: does not apply if router mode is used)
  - Bandwidth limitation
  - Global and user-specific firewall rules

  All network nodes located in the internal network segment of a SCALANCE S are protected by its firewall.
- Communication made secure by IPsec tunnels

  SCALANCE S can be grouped together with other security modules during configuration. IPsec tunnels are created between all security modules of a group (VPN, Virtual Private Network). All internal nodes of this SCALANCE S can communicate securely with each other through these tunnels.
- Protocol-independent

  Tunneling also includes Ethernet frames according to IEEE 802.3 (layer 2 frames; does not apply if router mode is used).

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

  Point-to-Point Protocol over the Ethernet (RFC 2516) for obtaining IP addresses automatically from the provider so that the use of a separate DSL router is not necessary.
- DynDNS

  Dynamic Domain Name Service for the use of dynamic IP addresses when a SCALANCE S is used as a VPN server in remote maintenance scenarios.
- SNMPv3

  For secure transmission of network analysis information safe from eavesdropping.
- Router mode

  By operating the SCALANCE S as a router, you connect the internal network with the external network. The internal network connected by SCALANCE S therefore becomes a separate subnet.
- 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.

- Additional DMZ port S623
- No repercussions when included in flat networks (bridge mode)

  Internal network nodes can be found without configuration. This means that when a SCALANCE S is installed in an existing network infrastructure, the end devices do not need to be reconfigured.

  The module attempts to find internal nodes; internal nodes that cannot be found in this way must nevertheless be configured.

Internal and external network nodes:

SCALANCE S divides 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.

1.7 Use of the SCALANCE S623 DMZ port

Additional task of SCALANCE S623

In addition to the functions of the SCALANCE S612, the SCALANCE S623 with an additional port (DMZ) provides the option of connecting an additional network.

With the SCALANCE S623, a DMZ (demilitarized zone) can be set up in which servers can be placed that need to be reached both from the non-secure network (e.g. Internet or external network) as well as from the secure network (internal network).

Depending on the particular use case, the port can perform various functions (not at the same time):

- DMZ port
- Remote maintenance port

In typical DMZ applications, the user should configure the firewall rules so that (external) access from the Internet to the server in the DMZ is possible (optionally further secured by a VPN tunnel) but not to devices in the secure area (internal).

1.8 Use of the CP 343-1 Advanced and CP 443-1 Advanced

Cell protection concept - job of the CP x43-1 Adv.

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected. In addition to this, data transmission can be protected by a combination of different security measures such as a firewall, NAT/NAPT routers and VPN (Virtual Private Network) via an IPsec Tunnel:

- Data espionage
- Data manipulation
- Unauthorized access

The security functions of the CP x43-1 Adv. are configured with the Security Configuration Tool configuration tool integrated in STEP 7.

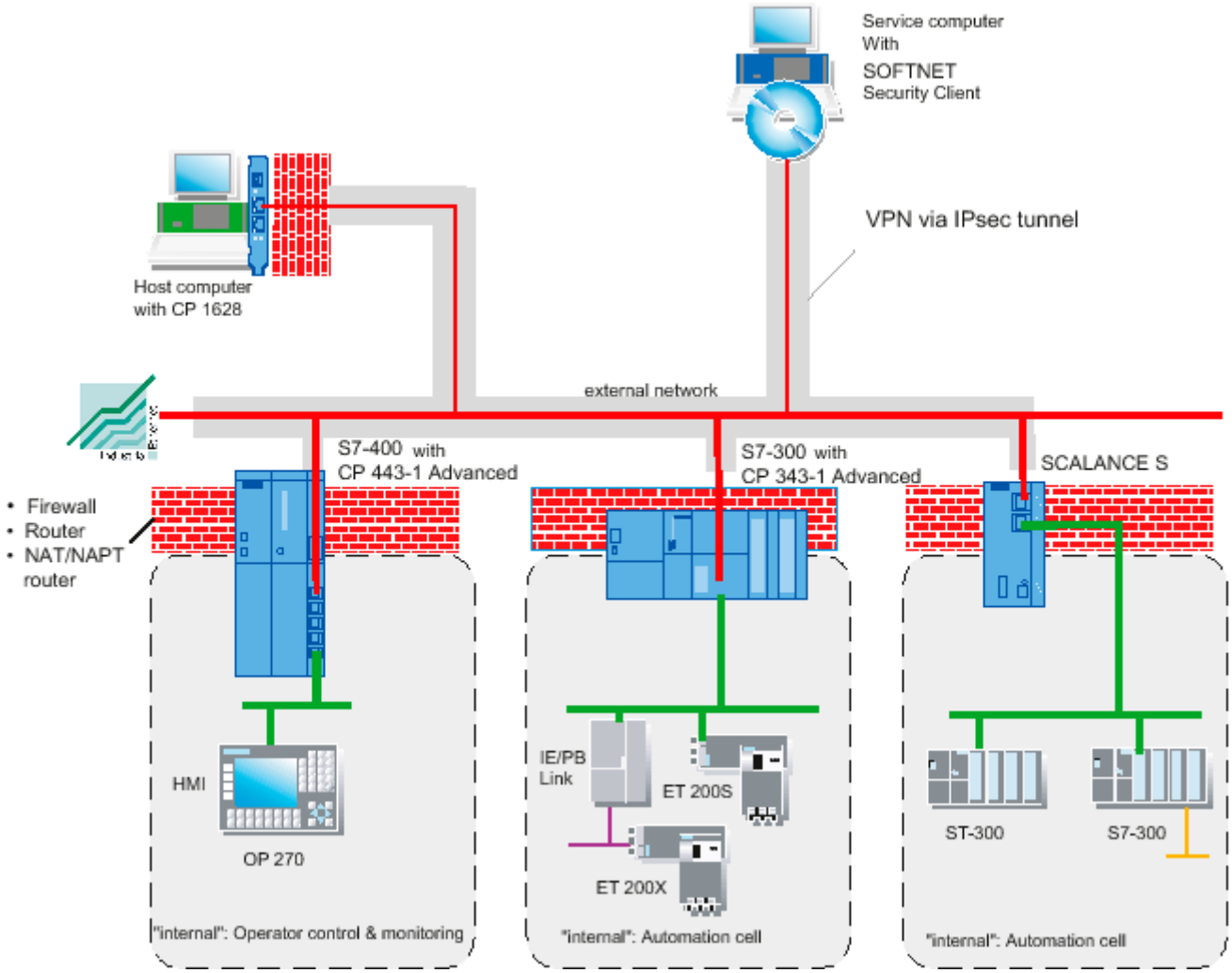


Figure 1-3 Network configuration with CP x43-1 Adv.

Security functions

- Firewall
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)
  - Bandwidth limitation
  - Global firewall rules

  All network nodes located in the internal network segment of a CP x43-1 Adv. are protected by its firewall.
- Communication made secure by IPsec tunnels

  The CP x43-1 Adv. can be grouped together with other security modules during configuration. IPsec tunnels are created between all security modules of a group (VPN). All internal nodes of these security modules can communicate securely with each other through these tunnels.
- Logging

  To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a Syslog server.
- HTTPS

  For the encrypted transfer of Web pages, for example in process control.

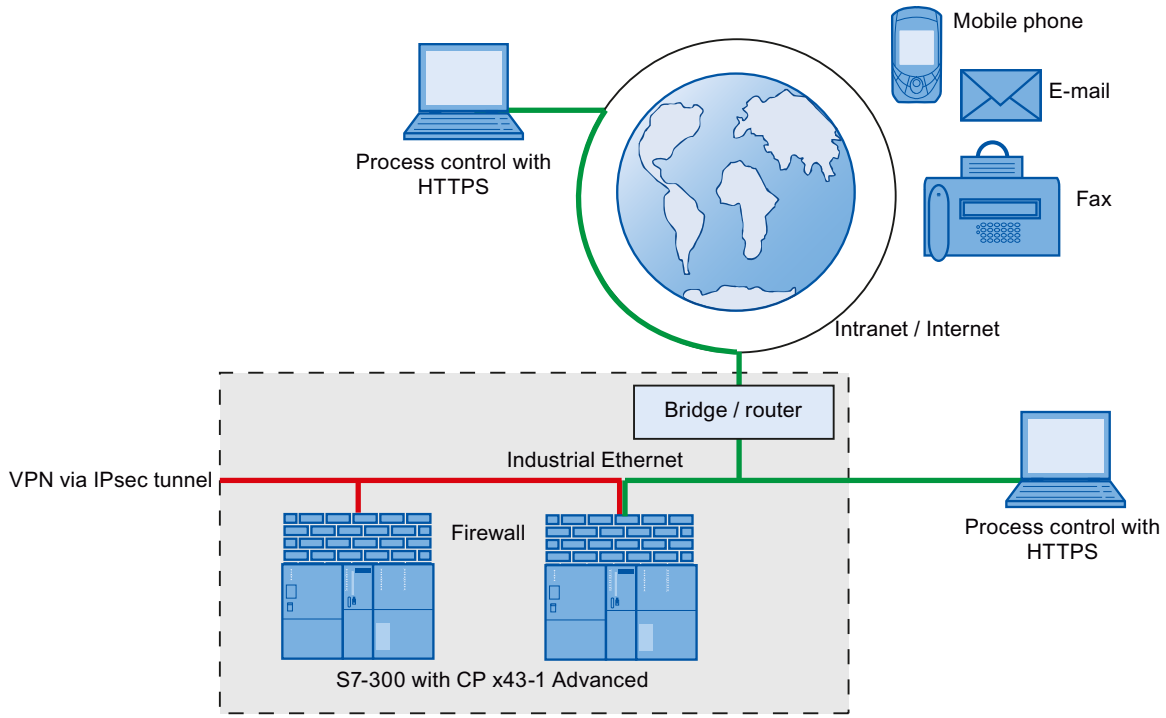


Figure 1-4 Process control with HTTPS

- FTPS (explicit mode)

  For encrypted transfer of files.

- Secure NTP

  For secure time-of-day synchronization and transmission.
- SNMPv3

  For secure transmission of network analysis information safe from eavesdropping.
- 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.

Internal and external network nodes:

CP x43-1 Adv. divides networks into two areas:

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

  Internal nodes are all the nodes secured by a CP x43-1 Adv..
- 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 CP x43-1 Adv.. There must be no other paths connecting the internal and external network.

Information on the general functions of the CP x43-1 Adv.

This manual explains the security functions of the CP x43-1 Adv. For descriptions of the general functions, refer to /1/ (Page 207) or /2/ (Page 208).

1.9 Use of CP 1628

Cell protection concept - job of the CP 1628

The integrated security mechanisms of the CP 1628 allow computer systems to be secured including the data communication within an automation network or secure remote access via the Internet. The CP 1628 allows access to individual devices or even to entire automation cells protected by security modules and it allows secure connections via non-secure network structures.

With the combination of different security measures such as firewall and VPN (Virtual Private Network) via an IPsec tunnel, the CP 1628 protects from the following:

- Data espionage
- Data manipulation
- Unauthorized access

The security functions of the CP 1628 are configured with the Security Configuration Tool configuration tool integrated in STEP 7.

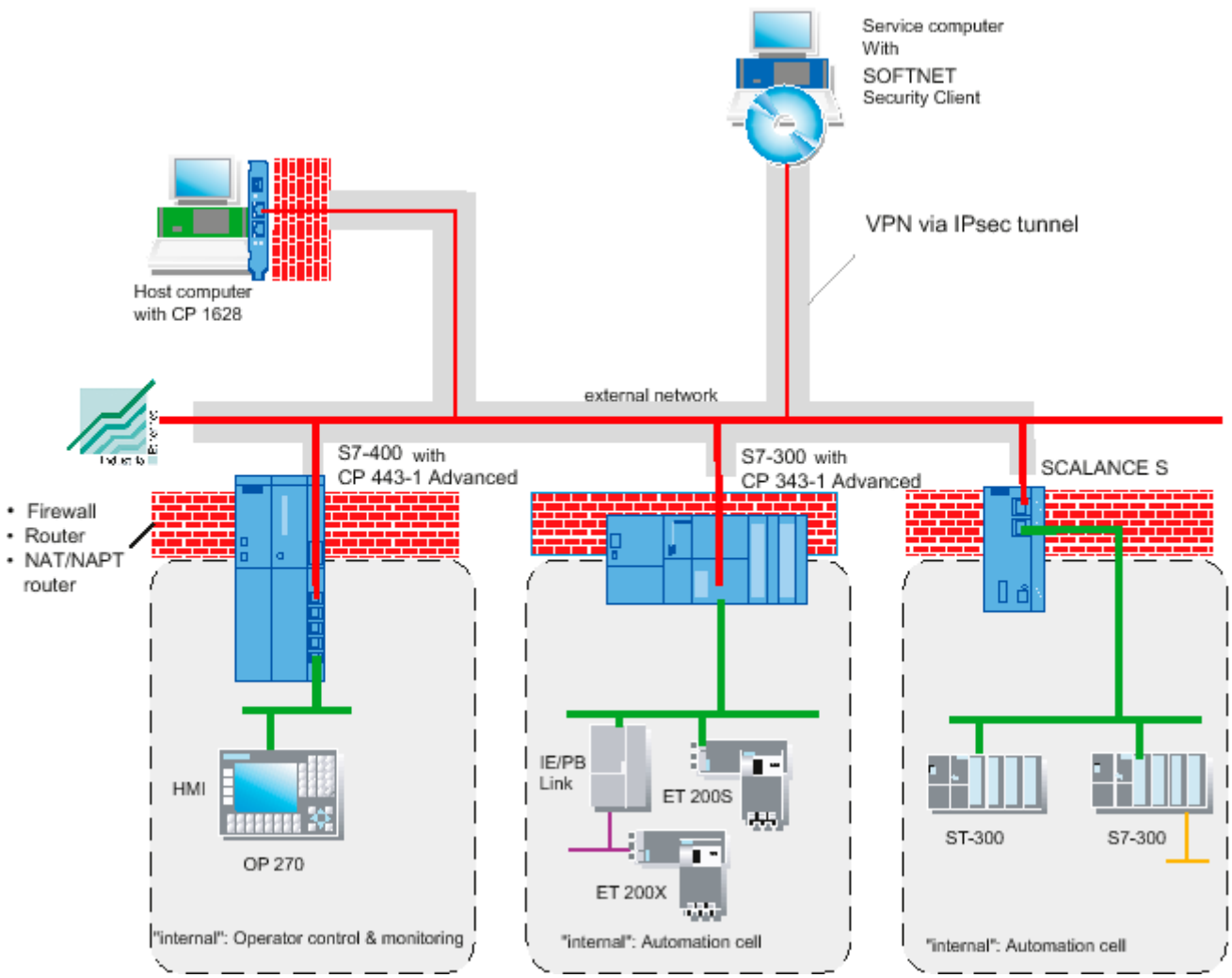


Figure 1-5 Network configuration with CP 1628

Security functions

- Firewall
  - IP firewall with stateful packet inspection (layer 3 and 4)
  - Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)
  - Bandwidth limitation
  - Global firewall rules
- Communication made secure by IPsec tunnels

  The CP 1628 can be grouped together with other security modules during configuration. IPsec tunnels are created between all security modules of a group (VPN, Virtual Private Network).

  Note

  Remember the order when downloading to the modules if you configure the firewall or make VPN settings.

  First download all VPN partners and finally the CP 1628.

- Logging

  To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a Syslog server.
- Secure NTP

  For secure time-of-day synchronization and transmission.
- SNMPv3

  For secure transmission of network analysis information safe from eavesdropping.

Information on the general functions of the CP 1628

This manual explains the security functions of the CP 1628. For descriptions of the general functions, refer to /11/ (Page 211).

1.10 Configuration and administration

The most important features at a glance

In conjunction with the Security Configuration Tool, you are guided to a simple and secure application of the security modules:

- Configuration without expert IT knowledge with the Security Configuration Tool

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

- Secure administrative communication

  The transfer of the settings is signed and encrypted and must only be performed by authorized persons.

- Access protection in the Security Configuration Tool

  The user administration of the Security Configuration Tool ensures access protection for the security modules 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. When replacing a security module, this allows configuration without a PG/PC as long as the security module supports data management on the C-PLUG.

Configuring with the Security Configuration Tool 2

The Security Configuration Tool is the configuration tool is supplied with the security modules.

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 security projects.

Further information

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

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.

2.1 Range functions and how they work

Scope of performance

You use the Security Configuration Tool for the following tasks:

- Configuration of the security modules
- Configuration of SOFTNET Security Client
- Creating the configuration data of the SCALANCE M
- Test and diagnostic functions, status displays

Two modes of the Security Configuration Tool

The Security Configuration Tool exists in two modes:

- Security Configuration Tool Standalone: Can be called up independent of STEP 7. No security configuration of CPs possible.
- Security Configuration Tool integrated in STEP 7: Security configuration of CPs and the range of functions of the Standard Security Configuration Tool. Can only be called up from the STEP 7 user interface.

Modes

The Security Configuration Tool has two modes:

- Offline configuration view

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

- Online

  The online mode is used for testing and diagnostics of a security module.

Two operating views

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

- Standard mode

  The standard mode is the default mode in the Security Configuration Tool. This mode allows fast, uncomplicated configuration for operating security modules.

- Advanced mode

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

How it works - security and consistency

- Access only for authorized users

  Every project is protected from unauthorized access by assigning user names and passwords.

- Consistent project data

  Consistency checks are running even while you make the entries in the dialogs. You can also run a project-wide consistency check for all dialogs at any time.

  Only consistent project data can be downloaded to the security modules.

- Protecting project data by encryption

  The project and configuration data is protected by encryption both in the project file and on the C-PLUG (not for the CP 1628).

2.2 Installation

2.2.1 Supported operating systems

Operating systems supported

The following operating systems are supported:

- Microsoft Windows XP 32-bit + Service Pack 3 ~~PG CP~~
- Microsoft Windows 7 Professional 32/64-bit or
- Microsoft Windows 7 Professional 32/64-bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64-bit
- Microsoft Windows 7 Ultimate 32/64-bit + Service Pack 1
- Windows Server 2008 R2 64-bit
- Windows Server 2008 R2 64-bit + Service Pack 1
- PG/PC with at least 128 Mbytes of RAM and a 1 GHz CPU or faster.

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.

SCALANCE S and CP x34-1 Adv. - Follow the steps below

You install the Security Configuration Tool from the supplied product CD.

- Insert the product 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 the "start.exe" application on the supplied product S CD.

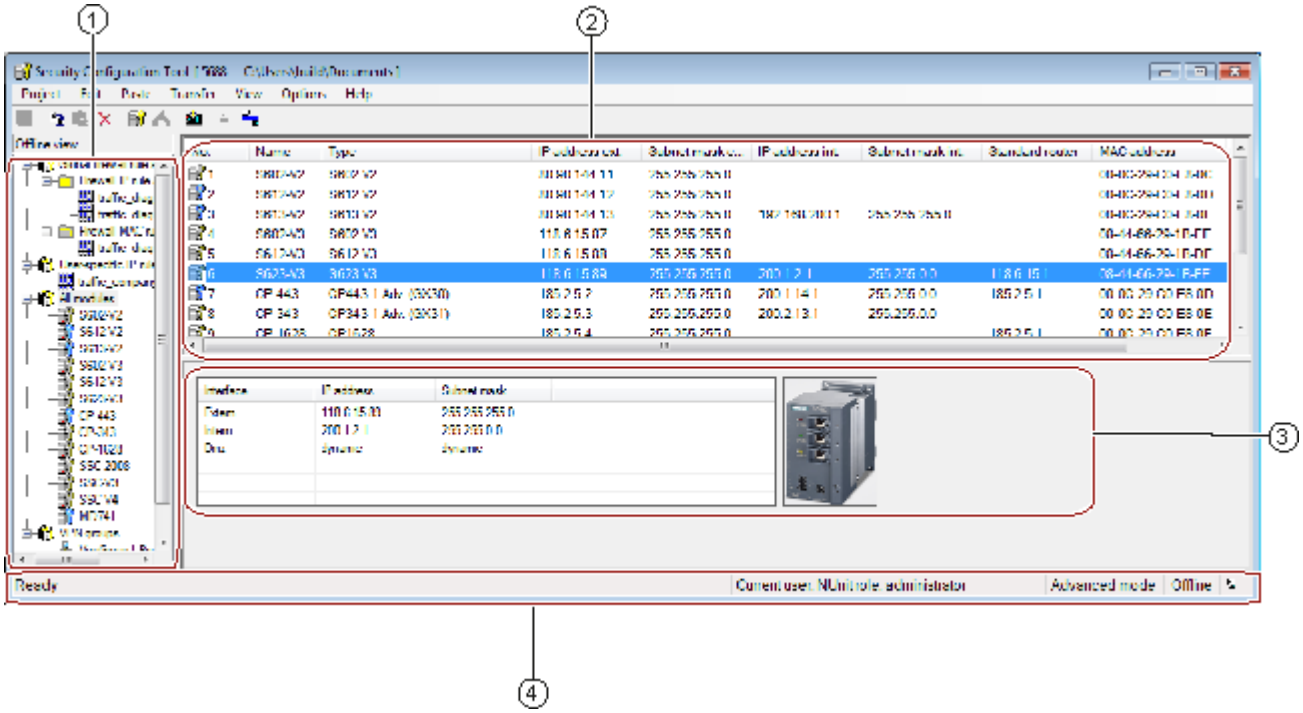
CP 1628 - Follow the steps below

You install the Security Configuration Tool from the supplied DVD "SIMATIC NET PC Software".

1. Start the "setup.exe" application in the "sw > Driverdisk > CP1628 > SCT" folder.
2. Click through the setup and go to the "Programs" > "Selection of programs to install" and select "Security Configuration Tool V3.0".

2.3 User interface and menu commands

Structure of the user interface in advanced mode



① The navigation area functions as a project Explorer with the following main folders:

- Global FW rule sets

  The object contains the configured global firewall rule sets. Other folders:

  – IP rule sets
  – MAC rule sets

- User-specific IP rule sets S≥V3.0
- All Modules

  The object contains all the configured security modules or SOFTNET security clients of the project.

- VPN groups

  The object contains all generated VPNs.

② Content area:

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

The address details can be configured for SCALANCE S. For SCALANCE M, you can only configure the IP addresses and the subnet masks.

By double-clicking on the objects, properties dialogs open in which you can enter further parameters (not for SOFTNET security client and SCALANCE M).

③ Details window:

Additional details about the selected object are displayed in the Details window. The details window can be hidden and shown.

④ Status bar:

The status bar displays operating states and current status messages. This includes:

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

Toolbar

Below, you will find an overview of the icons you can select in the toolbar and their meaning.

Symbol	Meaning / remarks
	Create a new project.
	Open the existing project.
	Save the open project in the current path and under the current project name.
	Copy the selected object.
	Paste object from the clipboard.
	Delete the selected object.
	Create new module. The symbol is only active if you are located in the navigation area in the "All modules" folder or on a VPN group.
	Create new group. The symbol is only active if you are located in the navigation panel in the "VPN groups" folder.
	Create a new globally valid or user-specific IP rule set or MAC rule set. The symbol is only active if you are located in the navigation panel in a subfolder of "Global firewall rule sets" or on the "User-specific IP rule sets" folder.
	GR Download the configuration to the selected security module or create configuration data for SOFTNET security client / SCALANCE M.
	Switch over to offline mode.
	Switch over to online mode.

Menu bar

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

Menu command		Meaning / remarks	Keyboard shortcut
Project ▸…		Functions for project-specific settings and for downloading and saving the project file.	
CP	New...	Create a new project. For CPs: Projects are created as a result of STEP 7 configuration.	
CP	Open...	Open the existing project. For CPs: Existing projects can only be opened using STEP 7 projects.	
	Save...	Save the open project in the current path and under the current project name.	
CP	Save As...	Save the open project in a selectable path and under a selectable project name. For CPs: The project is part of the STEP 7 project. The path name cannot be changed.	
	Properties...	Open dialog for project properties.	
CP	Recent Projects	Allows you to select previously opened projects directly. For CPs: Existing projects can only be opened using STEP 7 projects.	
	Exit	Close project.	
Edit ▸…		Menu commands only in offline mode **Note** When an object is selected, you can also activate some of the functions in the shortcut menu.	
CP	Copy	Copy the selected object.	Ctrl + C
	Paste	Fetch object from the clipboard and paste.	Ctrl + V
	Delete	Delete the selected object.	Del
	Rename	Rename the selected object.	F2
	Replace module...	Replace the selected security module with another.	
	Properties...	Open the properties dialog for the selected object.	F4
	Online Diagnostics...	Access test and diagnostic functions. This menu command is only available in the online view.	
Insert ▸…		Menu commands only in offline mode	
	Module	Create new module. The menu command is enabled only when a module or a group is selected in the navigation area.	Ctrl + M

Menu command		Meaning / remarks	Keyboard shortcut
	Group	Create new group. The menu command is enabled only when a group object is selected in the navigation area.	Ctrl + G
	Firewall rule set	Create a new globally valid set of firewall IP rules or MAC rules. The menu command is enabled only when a firewall object is selected in the navigation area.	Ctrl + F
Transfer ▸…			
CP	To module(s)...	Download the configuration to the selected security modules or create configuration data for SOFTNET security client / SCALANCE M. Note: Only consistent project data can be downloaded. For CPs: Project data can only be downloaded using STEP 7.	
	To all modules...	Download configuration to all security modules. Note: Only consistent project data can be downloaded.	
	Configuration Status...	Display configuration status of the configured security modules in a list.	
CP	Firmware Update...	Download new firmware to the selected security module. For S7-CPs: The firmware is loaded on the CP via the update center of Web diagnostics.	
View ▸…			
	Advanced mode	Switch over from the standard (default) to the advanced mode. **Notice** If you switch to the advanced mode for the current project, you can only switch back if you have made no modifications.	Ctrl + E
	Hide Details window	Hide and show additional details about the selected object.	Ctrl + Alt + D
	Offline	Is the default. Switch over to the configuration mode.	Ctrl + Shift + D
	Online	Switch over to the test and diagnostics mode.	Ctrl + D
Options ▸…			
	IP services...	Open a dialog for service definitions for IP firewall rules. The menu command is only visible in advanced mode.	
	MAC services...	Open a dialog for service definitions for MAC firewall rules. The menu command is only visible in advanced mode.	

Menu command		Meaning / remarks	Keyboard shortcut
SP	Network adapter...	The SCALANCE S is assigned an IP address via the selected network adapter.	
	Languages...	Select the language in which the SCT user interface is displayed. For SCT in STEP 7, the language of the SCT user interface is specified by the language selection in STEP 7.	
	Log files...	Displays stored log files.	
	Symbolic Names...	Assign symbolic names for IP or MAC addresses.	
	NTP server...	Create and edit NTP servers.	
	Consistency checks...	Check the consistency of the entire project. The result is output in the results list.	
	User management...	Create and edit users and roles and assign rights.	
	Certificate manager...	Display or import / export certificates.	
Help ▸…			
	Contents...	Help on the functions and parameters in the SCT.	Ctrl + Shift + F1
	Index...	Help on the functions and parameters in the SCT.	Ctrl + Shift + F2
	About...	Information on the version and revision of the SCT.	

2.4 Creating and managing projects

2.4.1 Security Configuration Tool Standalone

SP

Configuration with the Security Configuration Tool Standalone

The Security Configuration Tool Standalone is used to create security projects in which no security modules are configured that need to be created and configured in STEP 7.

With the "Project" > "New" menu command, you create a new project. This includes all the configuration and management information for one or more SCALANCE S devices, SOFTNET Security Clients and SCALANCE M devices. For each device, you create a module in the project.

2.4.2 Security Configuration Tool in STEP 7

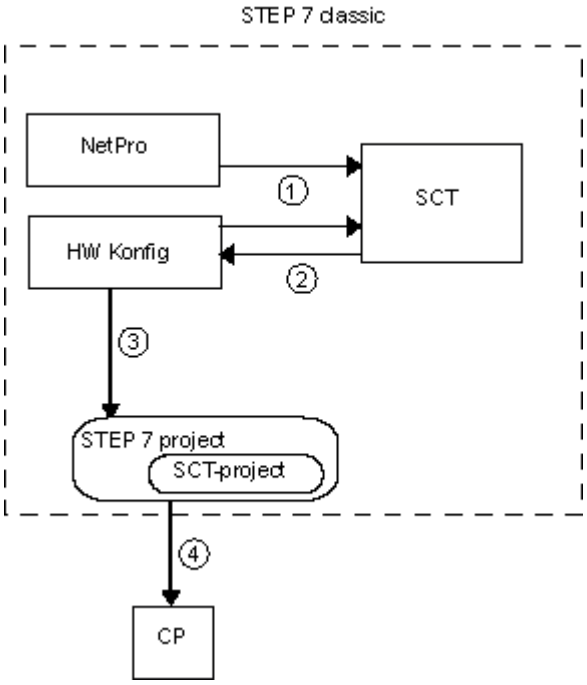
Project engineering

The Security Configuration Tool in STEP 7 is used to create security projects in which security modules are configured that need to be created and configured in STEP 7. All security modules of the stand-alone variant are also supported.

As soon as you enable the security functions for a security module in STEP 7, an SCT project is created automatically in which the data of the security configuration is stored and managed. All the data for the security configuration is processed internally by the SCT and the result is returned to STEP 7.

Interaction of STEP 7 and SCT

The interaction of STEP 7 and SCT is explained based on the following diagram:



① If you make security settings using STEP 7, SCT is called because the data for security is maintained and managed there.

If specified connections are configured in NetPro, firewall rules are created in SCT automatically for these after saving and compiling.

② You then make further security settings in SCT. SCT processes the data internally and returns the result to STEP 7.

③ Actions such as "Save as" and "Compile" are performed in STEP 7. The security data is stored as an SCT project under an automatically assigned name in a subfolder of the STEP 7 project. The name and storage location must not be changed. Precisely one SCT project can be created for a STEP 7 project. An SCT project created in STEP 7 with the Security Configuration Tool cannot be opened with the Security Configuration Tool in standalone mode.

④ The configured security data of the CP is downloaded to the module using STEP 7.

Which data is migrated to SCT from STEP 7 and displayed in the content area?

The following configuration data created in STEP 7 is automatically adopted by SCT but it cannot be modified there:

- Device name
- Internal IP address
- External IP address
- Internal subnet mask
- External subnet mask
- MAC address
- Default router

Which data can be migrated to SCT and modified there?

The following data created in STEP 7 can be migrated to SCT and changed there:

- Access control lists PC-CP
- User
- NTP server

You will find more detailed information in the online help of SCT.

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

Automatic firewall rules for specified connections

With specified connections configured in STEP 7, firewall rules are automatically created in SCT that allow connection establishment. For more detailed information, refer to section Connection-related automatic firewall rules (Page 105).

With unspecified connections, you need to configure firewall rules that allow connection establishment in SCT. For more detailed information, refer to section In advanced mode (Page 99).

Making security settings in STEP 7

As an alternative, you can make the security settings as follows:

- Using individual tabs of the object properties

  In the individual tabs, you can enable and execute CP-specific security functions. When the function executes, the relevant SCT dialog opens in which you can make security settings. You can make security settings in the following tabs:

	Tab	Function	Description
	Security	Enable security	• The security functions in the individual tabs become active. • The "Edit" > "Security Configuration Tool" menu becomes active and you can then open the Security Configuration Tool. There, you can make further general security module settings, such as creating VPN groups or adding security modules that cannot be configured in STEP 7. • If you have configured users for the security module in STEP 7, the window "Data migration of security-relevant project data" opens in which you can migrate the users to the Security Configuration Tool.
		Start of security configuration	SCT opens in an overview mode in which you can configure specific properties for this security module.
		Reloading firewall rules	Adapted firewall settings are generated and downloaded to the CP without causing the CP to stop.
		Reloading firewall rules online (CP 1628)	Adapted firewall settings are generated and downloaded to the CP online.
	User	Start of user management	Starts the SCT user management in which users and roles can be created and rights assigned.
PC CP	IP access protection	Start of the firewall configuration	When you activate security, an existing IP access list is migrated and converted to firewall rules in the Security Configuration Tool.
	FTP	Permit access only with FTPS	Starts the SCT user management in which you can assign FTP rights to a role.
		Start of user management	
	Web	Permit access only with HTTPS	Starts the SCT user management in which you can assign Web rights to a role.
		Start of user management	

	Tab	Function	Description
	Time-of-day synchronization	Expanded NTP configuration	Starts SCT in the NTP configuration mode.
	SNMP	Start of SNMP configuration	Starts SCT in the SNMP configuration mode. You can choose between SNMPv1 and SNMPv3.
		Start of user management	Starts the SCT user management in which you can assign SNMP rights to a role.

- Directly in SCT

  You call SCT in STEP 7 using the "Edit" > "Security Configuration Tool" menu. In addition to the settings in the tabs of the object properties, here you can create for example VPN groups or add SCALANCE S modules. Although you can configure and download the SCALANCE S modules in SCT, the data is not returned to STEP 7. When SCT is exited, the modules are also not displayed in STEP 7.

Note

You will find more detailed information in the STEP 7 and SCT online help.

You will find general information on STEP 7 in /9/ (Page 210).

2.4.3 Migrating STEP 7 data

Migrating safety-related project data

S7-CP

When you activate security, the following settings made in STEP 7 are migrated to a secure application area:

- NTP server - see section Time synchronization (Page 145)
- IP access control lists - see section Configuring the access list (Page 87)

Users and their passwords are not automatically migrated.

Firewall rules for specified connections

With specified connections configured in STEP 7, firewall rules are automatically created in SCT that allow connection establishment.

With unspecified connections, you need to configure firewall rules that allow connection establishment in SCT.

Migrating STEP 7 device users to the SCT user management

In the migration dialog, select how the users created in STEP 7 will be migrated to the SCT user management. Here, you can choose from the following actions:

Action	Description
Adopt as...	The user is migrated to the SCT user management under a different name. Enter the name in the "Migrated user name" column. The migrated user is assigned an automatically generated role in SCT.
Merge	If a user with the same name has already been created in the SCT project, the two users are merged. The role of this user is expanded by the rights selected for the migrated user.
Do not adopt	The user of the security module is not migrated to the SCT user management. Migration at a later point in time is not possible.

Note

The following data is not migrated

- Passwords of users already created in STEP 7. For all users, you should therefore select how they will be migrated and assign a new password using the "Assign password" button.
- The system-defined user "everybody" available in STEP 7. This user's rights are not adopted for migrated users.

Migrating STEP 7 device rights to the SCT user management

The following rights are migrated:

Right in STEP 7	Right after migration to SCT	Service
To access the configured symbols	Applet: Read tags using configured symbols	PLC
	Applet: Write tags using configured symbols	
To read tags using absolute addresses	Applet: Read tags using absolute addresses	
To write tags using absolute address	Applet: Write tags using absolute addresses	
Access files on the S7 station with FTP	FTP: Read files (DBs) from the S7 CPU	
	FTP: Write files (DBs) to the S7 CPU	
	FTP: Read files from the CP file system	File system
	FTP: Write files to the CP file system	
	Web: Format CP file system	
Send a test mail using the system page	Web: Access Web diagnostics and CP file system	Web
	Web: Send test mail	

Right in STEP 7	Right after migration to SCT	Service
Query the status of modules	Applet: Read status of the modules in the rack	PLC
Query order number of modules	Applet: Read order number of the modules in the rack	

2.4.4 Overview

General contents

In both SCT versions come when you create a new project you will be prompted to assign a user name and a password. The user you create here is of the type "administrator". After making this entry, you can make the settings in the project.

Generally, the configurations of a project contain the following:

- Valid settings throughout the project
- Settings for specific modules
- Group assignments for IPsec tunnel ~~S662~~

User management also handles access permissions to the project data and therefore to the security modules.

Valid settings throughout the project

- Project properties

  These include not only address and name information but also initialization values.
- Global firewall rule sets

  Global firewall rules can be assigned to several modules at the same time. In many situations, this simplifies the configuration compared with configuring local sets of firewall rules in the settings for specific modules.
- Service definitions

  Using the IP service or MAC service definitions, you can define succinct and clear firewall rules.
- NTP server

  NTP servers are created throughout the project and can then be assigned to several security modules in SCT.
- Certificate management

  All the certificates of the project are managed in the certificate management.

- User management

  In the user management, you can manage all users of the project and their rights.

- Symbolic names

  In a project, you can assign symbolic names in a table that stand for IP and MAC addresses.

Settings for specific modules

Most functions are configured in the properties dialog of a module. Here, you will find an overview of the tabs available and their functions:

	Function / tab in the properties dialog	Specified in mode ...	
		Standard	Advanced
	Interfaces Overview of the individual port settings. For CPs: The settings are taken from STEP 7 and cannot be modified. For SCALANCE S ≥ V3.0: You can also make settings for the DMZ port, activation of DynDNS and PPPoE etc.	X	X
CP	**Routing** Here, enter the data for the default router and/or specify a route. For CPs: The specification of a default router is adopted from STEP 7 and can only be changed there. This is displayed in the content area of SCT. The tab does not therefore exist in the module properties.	X	X
	Firewall In standard mode, you enable the firewall with simple standard rules. You can also enable log settings. In advanced mode, you can define detailed packet filter rules. You can also define explicit log settings for each packet filter rule. For CPs: If an access control list was migrated, this is displayed here and can be edited.	X	X
	Time synchronization Here, you specify the type of synchronization for the date and time.	X	X
	Log settings Here you can specify the recording and storage mode of log events in greater detail and configure the transfer to a Syslog server.	-	X
S602	**Nodes** Depending on the security module settings for subnets, specify IP/MAC nodes and NDIS nodes that also need to be reached via the VPN tunnel. For SCALANCE S: The learning of internal nodes can be enabled or disabled.	-	X
S602	**VPN** If the module is in a group, you can configure dead peer detection, the type of connection establishment and, if applicable, the WAN IP address here.	X	X

	Function / tab in the properties dialog	Specified in mode ...	
		Standard	Advanced
~~PC CP~~	**NAT** Enable NAT/NAPT routers and specify the address translation in a list.	-	X
~~CP~~	**DHCP server** You can enable the module as a DHCP server for the internal network. For SCALANCE S 623: If the DMZ port is in DMZ mode, a DHCP server can be set up for this port.	-	X
	SNMP In this tab, set the SNMP protocol version and the authentication/encryption method.	-	X
S≥V3.0	**Proxy ARP** Make static entries for proxy ARP on external interface.	-	X

You will find a detailed description of these functions in the section Configuring additional module properties (Page 125).

Group assignments for IPsec tunnel

~~S602~~

VPN groups specify which security modules, SOFTNET Security Clients and SCALANCE M modules communicate with each other via an IPsec tunnel.

By assigning security modules, SOFTNET Security Clients and SCALANCE M modules to a group, these modules can establish communications tunnels via a VPN (Virtual Private Network).

Only modules in the same group can communicate securely with each other over tunnels; security modules, SOFTNET Security Clients and SCALANCE M modules can belong to several groups at the same time.

2.4.5 Specifying initialization values for a project

~~CP~~

Specifying initialization values for a project

With the initialization values, you specify the properties to be adopted when you create new modules. You also specify whether or not a window for setting the properties will be opened when you create a new security module or whether the security module should be inserted directly.

Select the "Project" > "Properties" menu command, "Default initialization values" tab.

Protecting project data by encryption

The saved project and configuration data is protected by encryption both in the project file and on the C-PLUG (not for the CP 1628).

2.4.6 Consistency checks

Overview

The Security Configuration Tool distinguishes between:

- Local consistency checks
- Project-wide consistency checks

The checked rules where care is required when you enter them can be found in the relevant dialog descriptions under the keyword "Consistency check".

Local consistency checks

A consistency check is local when it can be performed directly within a dialog. Checks can be made during the following actions:

- After exiting a box
- After exiting a row in a table
- When you close the dialog with "OK"

Project-wide consistency checks

Project-wide consistency checks provide you with information on correctly configured modules. Since inconsistent project data is often configured when creating a project and a permanent project-wide consistency check would take too much time, there is an automatic check only with the following actions:

- When you save the project
- When you open the project
- Before you download a configuration

NOTICE
You can only download configuration data when the entire project is consistent.

How to start a project-wide consistency check

Run a consistency check for an open project as follows:

Menu command: "Options" > "Consistency checks".

The test result is output in the form of a list. If the project contains inconsistent data, the status is displayed in the status bar of the SCT window. Click on the status bar to display the check list.

2.4.7 You can assign symbolic names for IP / MAC addresses.

How to access this function

Menu command: "Options" > "Symbolic names...".

Meaning and advantages

In a security project, you can assign symbolic names in a table that stand for IP and MAC addresses.

This makes it simpler and more reliable when configuring the individual services.

Symbolic names within the project are taken into account by the following functions and can be used during their configuration:

- Firewall
- NAT/NAPT router
- Syslog
- DHCP

Validity and uniqueness

The validity of the symbolic names specified in the table is restricted to configuration within a security project.

Each symbolic name must be assigned uniquely to a single IP address or MAC address within the project.

Automatic adoption of symbolic names in the symbol table of SCT

You can use symbolic names instead of IP addresses for the listed functions - for example, when creating firewall rules - without these already being assigned in the table described here.

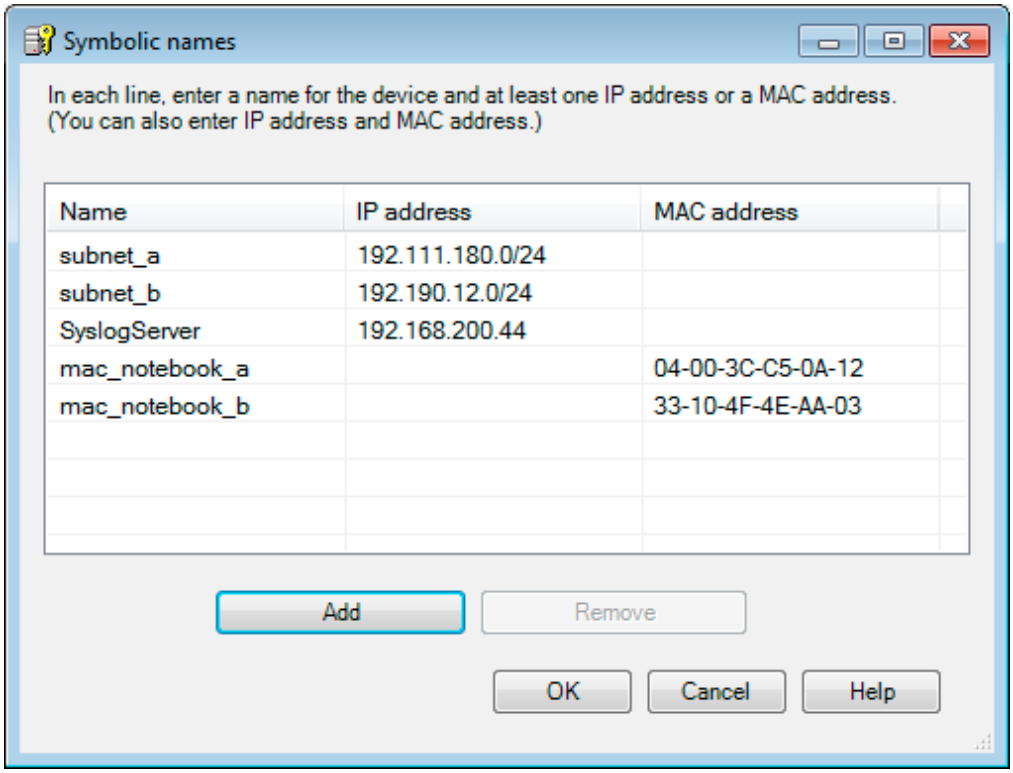
Symbolic names assigned in this way are automatically entered in the table and can be assigned at a later point in time. Within the framework of the consistency check, you will be informed of missing assignments.

Dialog for assigning symbolic names

To avoid inconsistencies between an "IP address - symbolic name" assignment, and "MAC address - symbolic name", the symbolic names are managed in a single table.

Follow the steps below to include new entries in the symbol table of SCT:

1. Click the "Add" button to add a new symbolic name in the next free table row.
2. Enter the symbolic name so that it is DNS-compliant. See section DNS compliance (Page 205).
3. Add either the IP address or the MAC address to the entry. You can also specify both addresses.



Follow the steps below to include entries in the table automatically:

If the symbolic name has already been assigned within the framework of the definition of a service, you will find a corresponding entry in the table.

1. Click on the relevant table row in the column for the IP address or for the MAC address.
2. Add either the IP address or the MAC address to the entry. You can also specify both addresses.

If you delete an entry in the table, the symbolic names used in the services remain. In this case, the consistency check recognizes undefined symbolic names. This applies both to manual as well as to automatically generated entries.

Tip:

The use of the project-wide consistency check is especially practical for the table described here. Based on the list, you can recognize inconsistencies and correct them.

Start the consistency check for an open project using the menu command "Options" > "Consistency checks".

Consistency check - these rules must be adhered to

Remember the following rules when making the entries.

Check / rule	Check made[1]	
	locally	project-wide
The assignment of a symbolic name to an IP or MAC address must be unique. The symbol name and the address may only be assigned once and must not be used in another list entry.	x	
The symbolic names must be DNS-compliant.	x	
A symbolic name must be assigned either an IP address or a MAC address or both.	x	
No symbolic names may be assigned to the IP addresses of the security modules.		x
Symbolic names used in the project for IP or MAC addresses must be included in the table. Inconsistencies can occur when entries in the table are deleted and not removed or corrected in the configuration dialogs.		x

[1] Note the explanations in the section Consistency checks (Page 47).

2.5 Configuration data for SCALANCE M

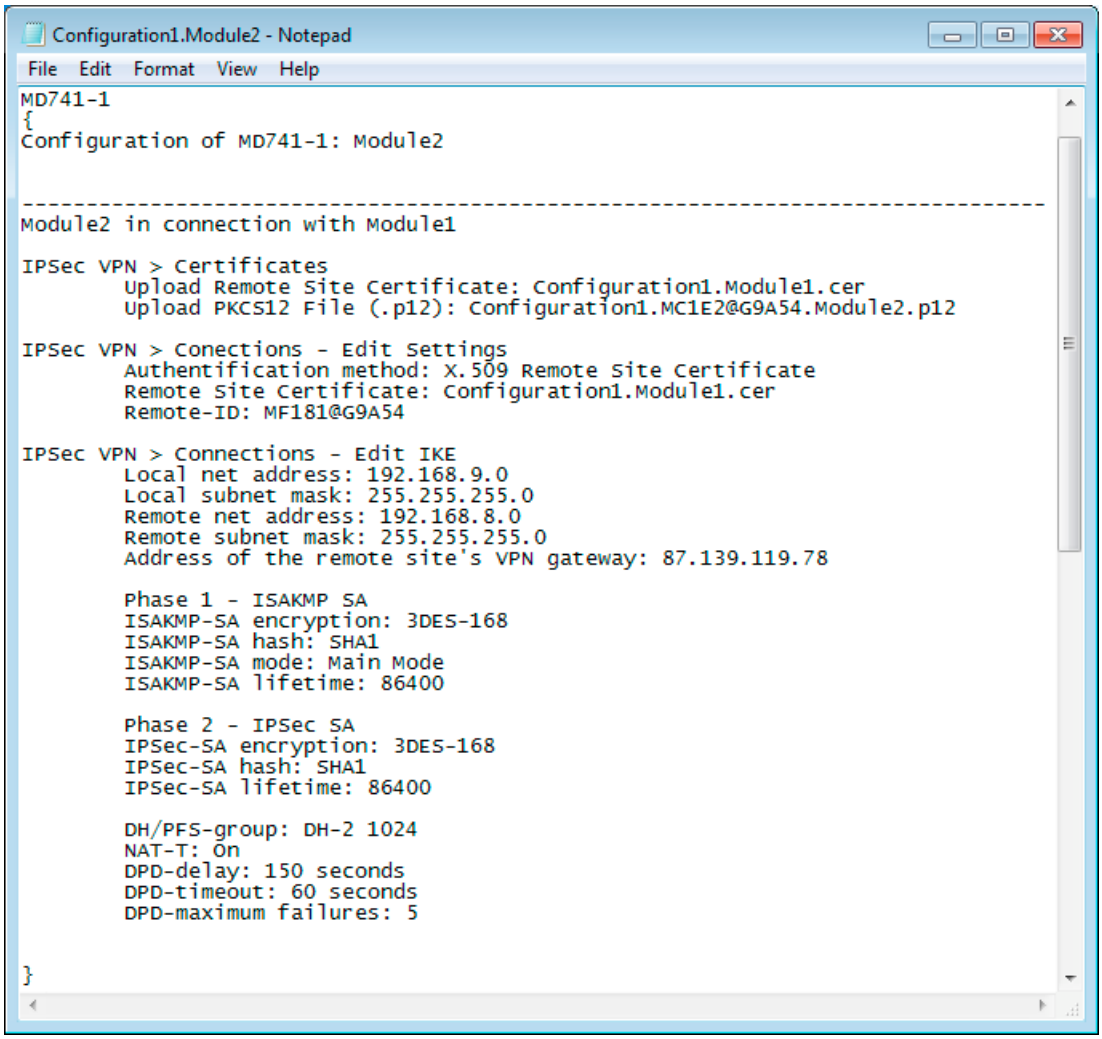
Transferring to a module

You can generate your VPN information for the assignment of parameters to a SCALANCE M using the Security Configuration Tool. With the generated files, you can then configure the SCALANCE M.

The following file types are generated:

- Export file with the configuration data
  - File type: ".txt" file in ASCII format
  - Contains the exported configuration information for the SCALANCE M including information on the additionally generated certificates.
- Module certificate
  - File type: *.p12 file
  - The file contains the module certificate and the key material.
  - Access is password protected.
- Group certificate
  - File type: *.cer file

The configuration files for the SCALANCE M can also be used to configure other VPN client types that are not included in the module selection. Requirement for the use of these VPN clients is support of IPsec VPNs in tunnel mode.




```
MD741-1
{
Configuration of MD741-1: Module2


--------------------------------------------------------------------------------
Module2 in connection with Module1

IPSec VPN > Certificates
        Upload Remote Site Certificate: Configuration1.Module1.cer
        Upload PKCS12 File (.p12): Configuration1.MC1E2@G9A54.Module2.p12

IPSec VPN > Conections - Edit Settings
        Authentification method: X.509 Remote Site Certificate
        Remote Site Certificate: Configuration1.Module1.cer
        Remote-ID: MF181@G9A54

IPSec VPN > Connections - Edit IKE
        Local net address: 192.168.9.0
        Local subnet mask: 255.255.255.0
        Remote net address: 192.168.8.0
        Remote subnet mask: 255.255.255.0
        Address of the remote site's VPN gateway: 87.139.119.78

        Phase 1 - ISAKMP SA
        ISAKMP-SA encryption: 3DES-168
        ISAKMP-SA hash: SHA1
        ISAKMP-SA mode: Main Mode
        ISAKMP-SA lifetime: 86400

        Phase 2 - IPSec SA
        IPSec-SA encryption: 3DES-168
        IPSec-SA hash: SHA1
        IPSec-SA lifetime: 86400

        DH/PFS-group: DH-2 1024
        NAT-T: On
        DPD-delay: 150 seconds
        DPD-timeout: 60 seconds
        DPD-maximum failures: 5


}
```

Figure 2-1 Export file for SCALANCE M

Note

Configuration files are not transferred to the module. An ASCII file is generated with which you can configure the SCALANCE M. Fur this to be possible, the module must be in at least one VPN group with a security module or a SOFTNET Security Client as of V3.0.

Follow the steps below

1. Select the "SCALANCE M" module in the content area.
2. Select the "Transfer" > "To module(s)..." menu command.
3. In the save dialog that then opens, enter the path and file name of the configuration file and click the "Save" button.
4. In the dialog that follows, choose whether you want to create your own password for the two created certificate files.

   If you select "No", the name of the configuration is assigned as the password (for example DHCP_without_Routing_02), not the project password.

   If you select "Yes" (recommended), you enter a password in the next dialog.

Result: The files (and certificates) are stored in the folder you specify.

Note

You will find further information on configuration in the operating instructions for the SCALANCE M87x and MD74x.

2.6 Managing users

2.6.1 Overview of user management

How is the user management structured?

Access to the security configuration is managed by configurable user settings. Set up users with a password for authentication. Assign a system-defined or a user-defined role to the user. The roles are assigned configuration- and module-specific rights. When creating users remember the specified configuration limits (Page 15).

Migrating existing users from STEP 7 to SCT

S7-CP

Users already created in STEP 7 can be migrated to SCT. When doing this, new passwords have to be assigned.

You will find more detailed information in the online help.

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

Order for making entries when creating users and roles

Select one of the two options for the order of the entries:

- First, create a new user, then specify a role and as the last step assign the role to the user.
- First, define a new role and then create a user and in the last step assign the role to the user.

User authentication

The users of the project must authenticate themselves during access. For each user, you therefore need to specify a password authentication.

NOTICE
Make sure that you keep your passwords safe. If you forget your user passwords, you can no longer access the relevant project and its configurations nor the security modules. You can then only access the security modules by resetting them to factory settings. You will, however, lose the configurations.

NOTICE
If the authentication settings are changed, the configuration must be downloaded to the security modules again before the settings (for example, new users, password changes) become active on the modules.

2.6.2 Create users

How to access this function

Menu command SCT: "Options" > "User management", "Users" tab.

STEP 7 menu command: "Users" > "Start of user administration", "Run" button. The user administration can also be called up from individual tabs.

Table 2- 1 Information in the "Users" tab

Parameter	Meaning
User name	Freely selectable user name.
Role	Depending on the assignment made.
Comment	Entry of additional comments.

Table 2- 2 Buttons in the "Users" tab

Name	Meaning / effect
Edit	Select an entry and then click the button. In the dialog that is displayed, change the user name, password and role.
Add	With this button, you can add a new user. In the dialog this is then displayed, enter the user name and specify the password and the system-or user-defined role.
Delete	Use the button to delete the selected entry. Note • Within a project, there must always be one user with the "Administrator" role. The administrator that is created automatically when you create the project can only be deleted if at least one other user exists that has complete configuration rights.

2.6.3 Creating roles

Which roles are available?

You can assign a system-defined or a user-defined role to a user. Specify the rights of the role for each security module.

System-defined roles

The following system-defined roles are predefined. Certain rights are assigned to the roles that are the same on all modules and that the administrator can neither change nor delete.

- administrator

  Default role when creating an SCT project.

  Unrestricted access rights to all configuration data.
- standard

  All rights except manage users/roles.
- diagnostics

  Default role when creating new user.

  – Read access to configurations.

  – Read access to the security module in the "Online" mode for testing and diagnostics.
- remote access

  No rights except for logging on to the Internet page for user-specific firewall rules. For more detailed information, refer to section User-specific firewall rules (Page 103).

Migrating existing SCT users

During the migration, existing SCT users are assigned the following system-defined roles.

- Existing users with the "Admin" role are assigned the system-defined role "administrator".
- Existing users with the "User" role are assigned the system-defined role "diagnostics".

User-defined role

In addition to the system-defined roles, you can create user-defined roles. For a user-defined role, select the configuration or module rights and specify the appropriate rights for every security module used in the project. You assign the user-defined roles to the relevant user manually.

How to access this function

Menu command SCT: "Options" > "User management", "Roles" tab.

STEP 7 menu command: "Users" > "Start of user administration", "Run" button. The user administration can also be called up from individual tabs.

Table 2- 3 Information in the "Roles" tab

Parameter	Meaning
Role name	Freely selectable role name.
Comment	Entry of additional comments.

Table 2- 4 Buttons in the "Roles" tab

Name	Meaning / effect
Edit	Select a user-defined role in the list and click the button. In the dialog that opens, change the role name and the rights assigned to the role. System-defined roles cannot be edited.
Add	With this button, you can add a new user-defined role. In the dialog that opens, enter the role name and assign the appropriate rights to the role from the rights list. The rights of the system-defined role selected in the rights template are displayed.
Delete	Use the button to delete the selected entry. Note • A user-defined role that has already been created can only be deleted when it is no longer assigned to any user. If necessary, assign the user a different role. • System-defined roles cannot be deleted.

2.6.4 Managing rights

How to access this function

Menu command SCT: "Options" > "User management", "Roles" tab, "Edit..." or "Add..." button.

STEP 7 menu command: "Users" > "Start of user administration", "Run" button. The user administration can also be called up from individual tabs.

Creating and assigning a user-defined role

1. Enter a role name.
2. Select a system-defined role from the rights template. User-defined roles are not displayed for selection.

   Result: Depending on the selected role, the rights for every security module used in the project are displayed in the rights list. The rights of the security modules not used in the project are grayed out.
3. For each security module, enable or disable the rights to be assigned to the user-defined role.

4. Click the "Apply" button to save the selection or "OK" to save and close window.
5. Assign the role to a user.

Copying the role rights of a module

In the shortcut menu of a security module, select the "Copy rights" command and assign these to another module using the "Paste rights" command.

Configuration rights

Depending on the user type, the following configuration rights are available for selection for each security project:

Table 2- 5 Configuration rights for all security modules

Configuration right	administrator	standard	diagnostics
Diagnose security	x	x	x
Configure security	x	x	-
Manage users and roles	x	-	-

Module rights

The "Service" column displays the system that is influenced by the particular right.

Depending on the user type, the following module rights are available for selection for each security project:

Table 2- 6 Module rights CP x43-1 Adv.

Right within the service	administrator	standard	diagnostics	Service
Web: Format CP file system *	x	-	-	File system
FTP: Read files from the CP file system **	x	x	x	
FTP: Write files to the CP file system	x	x	-	
FTP: Read files (DBs) from the S7 CPU **	x	x	x	PLC
FTP: Write files (DBs) to the S7 CPU ***	x	x	-	
Applet: Read tags using configured symbols *	x	x	x	
Applet: Write tags using configured symbols *				
Applet: Read tags using absolute addresses *	x	x	x	
Applet: Write tags using absolute addresses *	x	x	-	
Applet: Read status of the modules in the rack *	x	x	x	
Applet: Read order number of the modules in the rack *	x	x	x	
SNMP: Read MIB-II	x	x	x	SNMP
SNMP: Write MIB-II	x	x	-	
SNMP: Read automation MIB	x	x	x	
SNMP: Read LLDP-MIB	x	x	x	
SNMP: Read SNMPv2-MIB	x	x	x	
SNMP: Read MRP MIB	x	x	x	
SNMP: Write MRP MIB	x	x	-	
SCT: Run diagnostics of the security module ****	x	x	x	Safety
Web: Expand IP access control list *	x	-	-	
Web: Access Web diagnostics and CP file system	x	x	x	Web
Web: Send test mail *	x	x	x	
Web: Update firmware *	x	x	-	Maintenance
Web: Load diagnostics texts later *	x	x	-	

* To be able to use the function, the device right "Web: access Web diagnostics and CP file system" must also be enabled.

** To be able to use the function, the device right "FTP: Read files from CP file system" must also be enabled.

*** To be able to use the function, the device right "FTP: Write files to the CP file system" must also be enabled.

**** To use the function, the configuration right "Diagnose security" must also be enabled.

Table 2- 7 Module rights CP 1628

Right within the service	administrator	standard	diagnostics	Service
SNMP: Read MIB-II	x	x	x	SNMP
SNMP: Write MIB-II	x	x	-	
SNMP: Read automation MIB	x	x	x	
SNMP: Read SNMPv2-MIB	x	x	x	
SCT: Run diagnostics of the security module	x	x	x	Safety

Table 2- 8 Module rights SCALANCE S ≥ V3.0

Right within the service	administrator	standard	diagnostics	Service
SNMP: Read MIB-II	x	x	x	SNMP
SNMP: Write MIB-II	x	x	-	
SNMP: Read automation MIB	x	x	x	
SNMP: Read SNMPv2-MIB	x	x	x	
SNMP: Read MRP MIB	x	x	x	
SNMP: Write MRP MIB	x	x	-	
SCT: Run diagnostics of the security module	x	x	x	Safety
Download the configuration files	x	x	-	
Web: Update firmware	x	x	-	Maintenance

Table 2- 9 Module rights SCALANCE S < V3.0

Right within the service	administrator	standard	diagnostics	Service
Download the configuration files	x	x	-	Safety
SCT: Run diagnostics of the security module	x	x	x	

2.7 Managing certificates

2.7.1 Overview

How do you manage certificates?

In the certificate manager, you have an overview of all the certificates / CA certificates used in the project with information about the applicant, issuer, validity, use in SCT and the existence of a private key.

The CA certificate is a certificate issued by a certificate authority from which the device certificates are derived. These include the SSL certificates required for authentication during online communication between a device and a security module. Certificate authorities can be:

- SCT itself. If the "applicant" and "issuer" are the same, this is a self-signed certificate; in other words, issued by SCT.
- A higher ranking (commercial) certificate authority. These third-party certificates are external to the project and are imported and stored in the certificate store of SCT.

Certificates created by one of the two certificate authorities always have a private key so that the device certificates can be derived from them.

The following functions are also available in the certificate manager:

- Modification of existing certificates (for example duration of validity).
- Import of new certificates and certificate authorities.
- Import of FTPS certificates. S7-CP
- Export of the certificates and certificate authorities used in the project.
- Renewal of expired certificates and certificate authorities.
- Replacement of existing certificate authorities with others.

Note

Downloading projects

After replacing or renewing certificates, the project must be downloaded to the relevant security module.

After replacing or renewing CA certificates, the project must be downloaded to all security modules.

NOTICE
Current date and current time of day on the security modules When using secure communication (for example HTTPS, VPN...), make sure that the security modules involved have the current time of day and the current date. Otherwise the certificates used will not be evaluated as valid and the secure communication will not work.

How to access this function

Menu command SCT: "Options" > "Certificate manager...".

In the individual tabs, you have the following buttons available:

Button	Description
Import / Export	Import / export of device certificates or CA certificates that were not created in SCT. The certificates are transferred to the security module. The following formats are permitted: *.pem (certificate only) *.crt (certificate only) *.p12 (certificate and corresponding private key) Note • Users with the "Diagnostics" role must not use the export function.
Displays	Opens the certificate dialog of Windows where you will see an overview of all certificate data.

"Certification authority" tab

The certificates displayed here are created by a certificate authority.

- CA certificates of a project: When you create a new SCT project, a CA certificate is generated for the project. The SSL certificates for the individual security modules are derived from this certificate.
- CA group certificates: When you create a new VPN group, a CA certificate is generated for the group.

"Device certificates" tab

Display of the device-specific certificates generated by SCT for a security module. These include:

- SSL certificates: An SSL certificate that is derived from a CA certificate of the project is generated for each security module created. SSL certificates are used for authentication during communication between PG/PC and security module, when downloading the configuration (not for CPs) and when logging.
- Group certificates: A group certificate is also generated for each security module for each VPN group in which it is located.

"Trusted root certification authorities" tab

Display of the third-party certificates imported into SCT. Server certificates can be imported for example from external FTP servers or project certificates from other SCT projects.

CP

The imported third-party certificate is transferred to all the CPs managed in the SCT project. The security module can then identify itself with this certificate, for example when accessing an FTPS server. The SCT configuration itself does not use the imported certificate.

SCA.

Display of the certificate authorities required for verifying the security modules using external services such as DynDNS.

2.7.2 Renewing certificates

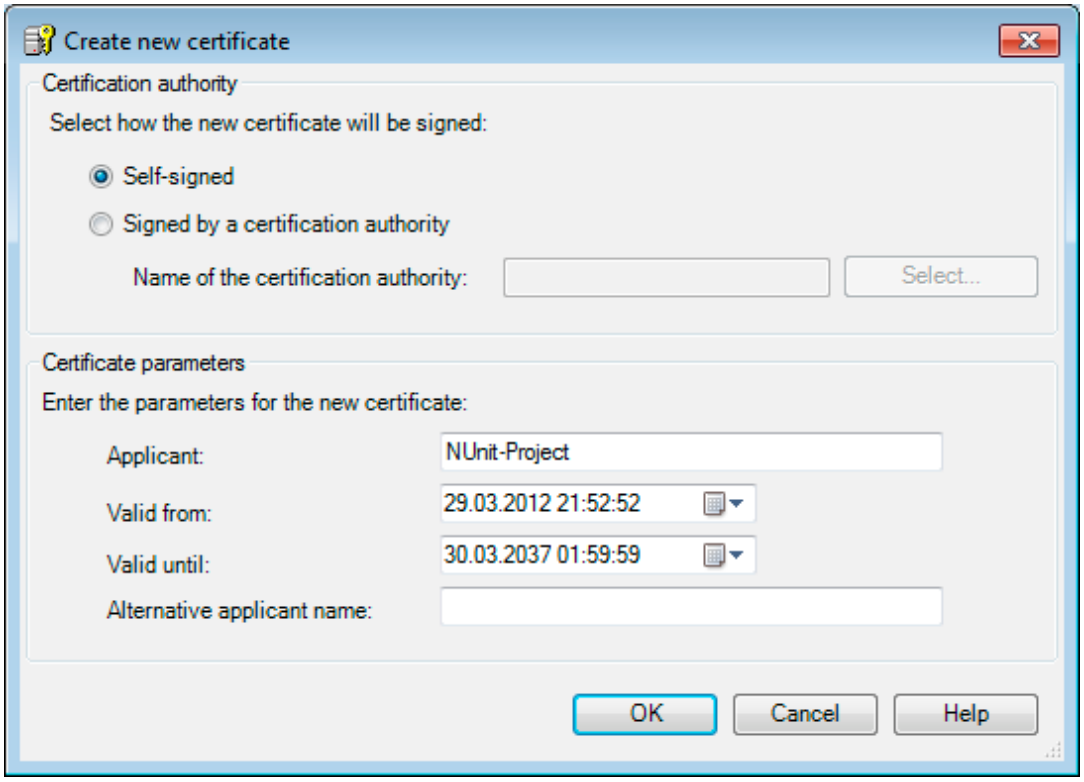
Meaning

In this dialog, you renew certificates and CA certificates. If necessary, for example with compromised certificates, you can import a certificate or have a new certificate generated by the Security Configuration Tool.

How to access this function

1. Right-click on a list entry in the certificate manager.

2. Select the "Renew certificate..." entry.



3. Decide whether or not the new certificate will be self-signed or signed by a certificate authority.
4. If the certificate is to be signed by a certificate authority, select the certificate authority to be used with the "Select..." button. Only certificate authorities stored in the certificate store of the current SCT project can be selected.
5. Select a period during which the certificate is valid. Normally, the current time is entered in the "Valid from:" box and the value from the current certificate in the "Valid until:" box.
6. Depending on the certificate, enter the following values:

Certificate to be renewed	Parameter	
	Applicant	Alternative applicant name
CA certificates of the project	Name of the CA certificate	-
CA group certificate	Name of the CA group certificate	-
SSL certificate for S7 CP	Name of the security module	IP addresses of the gigabit and PROFINET interface separated by a comma.
SSL certificate for PC CP	Name of the security module	IP address of the security module.

Certificate to be renewed	Parameter	
	Applicant	Alternative applicant name
SSL certificate for SCALANCE S, SCALANCE M and SOFTNET Security Client	Name of the security module	-
Group certificate of the security module	Name of the group certificate	Derived from the CA.

Configuring additional parameters

Click the "Configure additional parameters" button to store data such as the e-mail address.

2.7.3 Replacing certificates

Meaning

In the dialog, replace the existing CA certificate of the project or CA group certificate with a new one.

How to access this function

1. Right-click on a list entry in the "Certificate authorities" tab.
2. Select the "Replace certificate..." entry.
3. The "Change certification authority" dialog opens.

All the certificates listed in the "Certificates involved" box are derived again. This means that the CA group certificate of an already configured VPN group can be replaced in the SCT project by the CA group certificate of a different SCT project. The group certificates for the VPN group members are therefore derived from the same CA group certificate in both projects.

If an information dialog opens when you close the certificate manager, download the changed configuration to the security module again.

Which format can the certificate have?

Other certificates are derived from the imported CA in SCT. For this reason, you can only select certificates with a private key:

- *.p12

Creating modules and setting network parameters 3

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 and NAT/NAPT function of the security modules.

Note

S602

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 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 SCT dialog.

NOTICE
Performance features and device types Note which functions the device type you are using supports.

See also

Online functions - test, diagnostics, and logging (Page 193)

Creating modules in SCT - how to access this function

1. Select the "All Modules" object in the navigation area.

2. Select the "Insert" > "Module" menu command.

3. Make the following settings. You can also enter or change the address parameters in the "Configuration" box in the content area. (You will find information on this in the section Parameters in the content area (Page 69)).

Parameter	Meaning
Product Type	Product type used when a new module is created. SCALANCE S SOFTNET Configuration (SOFTNET Security Client, SCALANCE M87x/MD74x)
Module	Depending on the selected product type, you can select the module type here that will be used when you create a new module. Select "VPN client" to insert any product with VPN capability of a different manufacturer. Note Whether or not the checked out configuration file works depends on the particular partner product.
Firmware Release	You can specify the firmware/software versions here for the SCALANCE S modules and the SOFTNET Security Client.
Name of Module	Freely selectable name for the module.
MAC address	Note on the structure of the MAC address: The MAC address consists of a fixed and a variable part. The fixed part ("basic MAC address") identifies the manufacturer (Siemens, 3COM, ...). The variable part of the MAC address distinguishes the various Ethernet nodes.
IP Address (ext.)	IP start address for the external interface. Format / range of values for IP address 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
Subnet Mask (ext.)	Range of values for subnet mask. Is proposed according to the IP address entered. The subnet mask consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 255.255.0.0
Enable Routing	If you select this option, the security module is in routing mode.
IP address (int.) Only needs to be specified when routing mode is enabled	IP start address for the internal interface. The IP address consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 141.80.0.17

Parameter	Meaning
Subnet mask (int.) Only needs to be specified when routing mode is enabled	Range of values for subnet mask. The subnet mask is proposed according to the entered IP address. The subnet mask consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 255.255.0.0
Save selection	If you enable this function, the currently set configuration is adopted in the default initialization values. When you insert new modules the "Selection of a module or software configuration" dialog is no longer opened and a module is inserted in the project according to the settings made. To cancel this function again and to select a different module type, you will need to disable this function in the following menu path: "Project" > "Properties" > "Default Initialization values"

Note

Additional settings

S≥V3.0

Port settings, settings for the DMZ port, activation of PPPoE etc. are made in the "Interfaces" tab. For information on this, refer to section Configuring interfaces (SCALANCE S) (Page 71).

Creating CPs in STEP 7

CPs are created only in STEP 7. After they have been created and specified as security modules, they appear with their properties in the list of configured modules in SCT. The address data is taken from STEP 7 and cannot be modified in SCT.

See also

Range of values for IP address, subnet mask and address of the gateway (Page 205)

MAC address (Page 206)

3.1 Parameters in the content area

How to access this view

Select the "All Modules" object in the navigation area.

The following properties of the modules are displayed in columns:

Property/column	Meaning	Comment/selection
Number	Consecutive module number	Assigned automatically
Name	Unique module name.	Freely selectable
Type	Device type	Note For devices of the "SOFTNET Configuration" product type, there is no properties dialog. For SCALANCE M, you can only set the IP addresses and the subnet masks in the content area.
IP address ext.	IP address via which the device can be reached in the external network, for example for downloading the configuration.	Assigned as suitable in the network.
Subnet mask ext.	Subnet mask	Assigned as suitable in the network.
IP address int.	IP address over which the device can be reached in the internal network when it is configured as a router.	Assigned as suitable in the network. The input box can only be edited when routing mode is enabled.
Subnet mask int.	Subnet mask	Assigned as suitable in the network. The input box can only be edited when routing mode is enabled.
Default router	IP address of the default router.	Assigned as suitable in the network.
MAC address	Hardware address of the module.	The MAC address is printed on the module housing.
Comment	Useful technological information on the module and the subnet protected by the module.	Freely selectable

Changing address parameters for SCALANCE S

For SCALANCE S, the address parameters can be entered and modified in the content area.

Meaning of the address parameters for CPs

CP

For the CPs, the following addresses from STEP 7 are displayed:

Box in SCT	CP x43-1	CP 1628
IP address ext.	IP address gigabit	IP address IE (Industrial Ethernet)
IP address int.	IP address PROFINET	Is not displayed
Subnet mask ext	Subnet mask gigabit	Subnet mask IE
Subnet mask int.	Subnet mask PROFINET	Is not displayed
MAC address	MAC address gigabit	MAC address IE

The address data is also displayed in the "Interfaces" tab.

Dynamically assigned IP address

S7-CP

If the IP address has been configured in STEP 7 so that it is assigned dynamically, this is shown in SCT as follows depending on the settings:

Table 3- 1 Gigabit interface

Mode in STEP 7	IP address ext. / Subnet mask ext.
Obtain an IP address from a DHCP server	dynamic

Table 3- 2 PROFINET interface

Mode in STEP 7	IP address ext. / Subnet mask int.
Obtain an IP address from a DHCP server	dynamic
Set IP address in the user program	dynamic
Set IP address using a different method	dynamic

3.2 Configuring interfaces (SCALANCE S)

3.2.1 Overview of the ports

SCA.

Supported ports and possible connections

The SCALANCE S V3.0 supports the following ports:

- Red port (eth0): Non-secure network
- Green port (eth1): Secure network
- Yellow port (eth2): DMZ (demilitarized zone) or as remote maintenance access via PPPoE S623

Yellow port as DMZ port

The DMZ is used when services for an external network need to be available and the internal network that supplies data for these services needs to remain separated from the external network.

The DMZ can, for example, contain terminal servers on which maintenance and diagnostics programs are installed that allow defined access to certain systems in the secure network. Only permitted users or clients from the non-secure network or clients connected via VPN have access.

The firewall rules can be configured so that devices in the DMZ can be accessed from the Internet but devices in the internal network connected to the green port cannot be accessed. To improve protection, it is also possible to allow access only to VPN data traffic.

To be able to assign a dynamic IP address to devices in the DMZ as well, a DHCP server can be activated on the yellow port. However, with such a use case, it must be ensured that the devices in the DMZ always receive the same IP address by DHCP because these IP addresses need to be used when configuring the firewall. This means that the dynamic address assignment cannot be used in the DHCP configuration but rather static address assignment based on the MAC address or based on the client ID.

Yellow port as remote maintenance port

The yellow port can be used as a VPN endpoint to allow it to be used as the connection port for remote maintenance. In conjunction with the DSL modem, the yellow port is then operated in PPPoE mode or in conjunction with an upstream DSL router with a static IP address.

Point to Point Protocol over Ethernet

To dial in to the Internet / WAN, PPPoE is used. PPPoE can be configured either at the external port or at the DMZ port.

Settings for the external port with address via PPPoE

To allow an Internet/WAN access directly via a DSL modem, the IP address at the external port is assigned via PPPoE. PPPoE is a dial-in protocol for obtaining IP addresses from an Internet service provider (ISP). SCALANCE S is operated here in routing mode.

Note

A configured standard router is not taken into account when using PPPoE.

Functions of the individual ports

The following functions can be used on the individual ports:

Function	Green (internal)	Red (external)	Yellow	
			Remote maintenance mode	DMZ mode
Static IP address	x	x	-	x
Dynamic IP address (via PPPoE)	-	x	x	-
WAN access via DSL modem or DSL router	-	x (when not on yellow port)	x (when not on red port)	-
Bridge mode	x		-	
Routing mode	x	x	x	
DHCP server	x	-	-	x
Remote maintenance with VPN	-	With DSL router	With DSL modem	With DSL router

3.2.2 Interfaces

SCA.

Interface routing - options available

If the security module is not in a VPN group, the mode for interface routing is set automatically and can be changed in this field. The selection is valid for port 1 and port 2.

If the security module is in a VPN group, the mode for interface routing cannot be changed.

Bridge mode	For operation in flat networks. External and internal port are in the same IP subnet. For S623: The DMZ port must be in different subnet or must be in "Off" mode.
Routing mode	All ports are in different IP subnets. **Note** If you have enabled the routing mode for the SCALANCE S module, no MAC firewall rules can be defined.

Input options for static address assignment

- IP address with subnet mask
- DNS server if dynamic DNS is used

Address assignment using PPPoE

- IP address is set by the ISP

Resolving FQDNs (Fully Qualified Domain Name) in IP addresses

To resolve FQDNs, DNS servers are required that return the IP address corresponding to the FQDN.

- Enter the preferred and alternative DNS server.
- IP assignment using PPPoE: The DNS servers can be obtained automatically via PPPoE. Can only be set for the external port and the DMZ port in the "Remote maintenance" mode.

Additional MAC address

The additional MAC addresses are derived as follows:

- MAC address (internal) = printed MAC address + 1
- MAC address (DMZ port) = MAC address + 2 printed on the module

When operating in flat networks (bridge mode), the printed MAC address is valid both on the internal and on the external interface.

Additional settings for the DMZ port

S623

The DMZ port always routes to the external and internal port even when Bridge mode is selected in the interface routing.

Note

External and DMZ port as Internet access

The simultaneous operation of PPPoE at the external port and in the "Remote maintenance" mode at the DMZ port (dual ISP) is not possible.

Box	Description
Operating mode	Specify how the DMZ port will be used. Depending on the application you require, select between the following functions: • DMZ: No IP assignment possible using PPPoE. • Remote maintenance: Port is connected to the Internet (ISP) directly using PPPoE.
IP assignment	In the "DMZ" mode, the IP assignment is static. In the "Remote maintenance" mode, the IP address is assigned by the ISP.

See also

Dynamic DNS (Page 75)

3.2.3 Dynamic DNS

S≥V3.0

What is dynamic DNS?

With dynamic DNS, you can access a constantly changing IP address with a permanently defined name (FQDN). This is necessary, for example if you want to access a server that can be reached via a public, changing IP address.

How does dynamic DNS work?

The security module signals the current WAN IP via which the module can be reached to a provider for dynamic DNS (for example DynDNS.org, no-ip.com). The provider makes sure that DNS queries sent to the FQDN of the module are replied to with the WAN IP of the module.

Dynamic DNS is permitted at the following ports:

- External port
- DMZ port in "Remote maintenance" mode

Setting up dynamic DNS - requirements

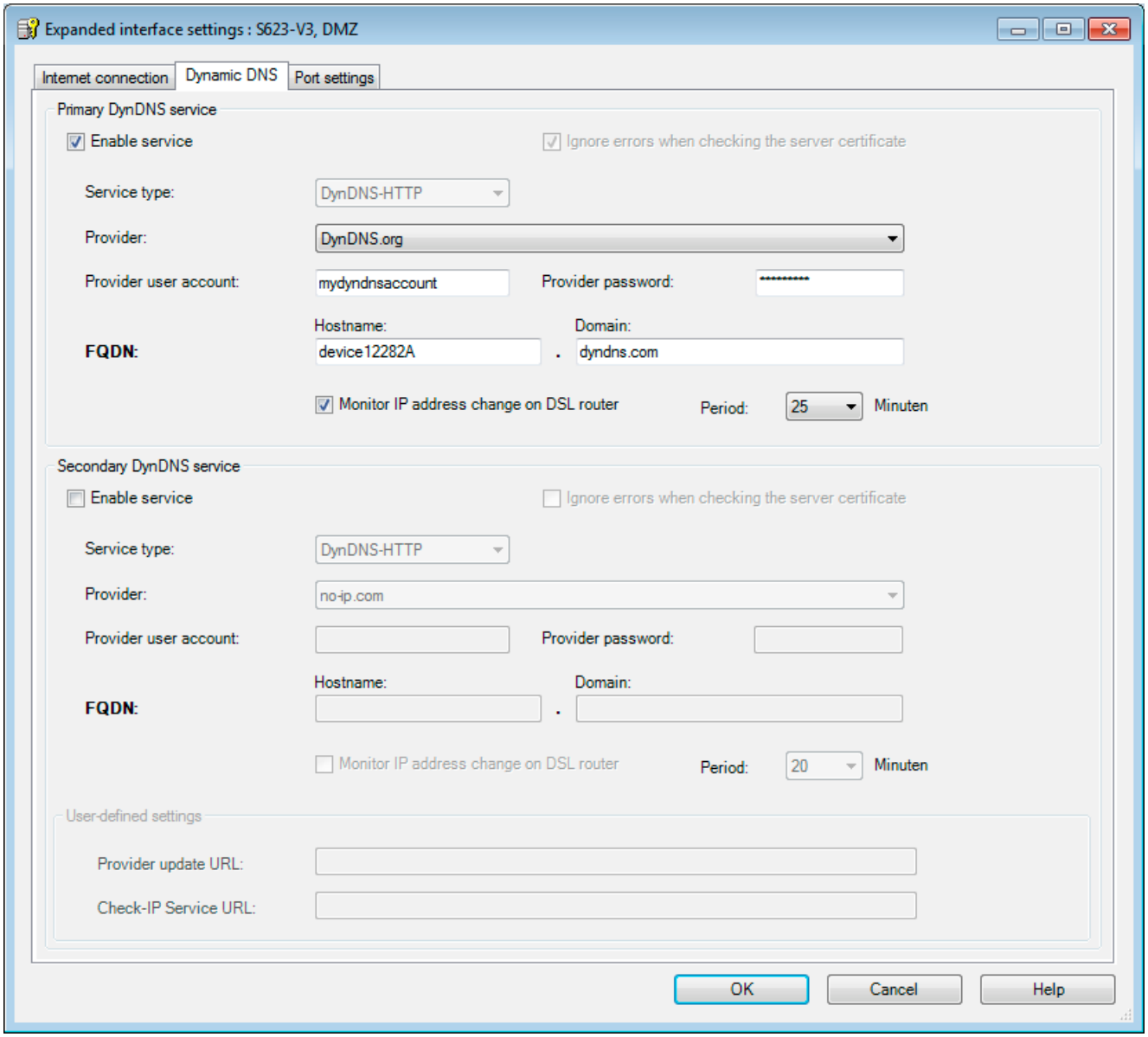
Requirement:

- An account has been created with one of the supported providers of dynamic DNS and an FQDN has been registered.
- If the security module is downstream from a DSL router, a valid DNS server must be entered in the "Interfaces" tab.

How to access this function

1. Select the "Interfaces" tab in the module properties of the security module.
2. Click the "Advanced settings…" button.

3. Select the "Dynamic DNS" tab.



4. Select the "Enable service" check box.
5. Make the following settings.

Enabling the primary DynDNS service

IP settings	
Provider	Choose the DynDNS provider with which you have set up a DynDNS account.
Provider user account	Enter the user name that you specified when you created the DynDNS account.
Provider password	Enter the user password that you specified when you created the DynDNS account.
FQDN	Enter the host name (e.g. www) and the domain name (e.g. abc.de) that is registered with the DynDNS provider.
Monitor IP address change on DSL router	If the security module is connected via a DSL router, enabling this activates the function of the Check IP service. The security module periodically sends queries to determine the current IP address of the DSL router and to detect an IP address change on the DSL router. Specify the interval at which the Check IP service is called. Period: 10 … 1440 minutes

Result: After making the entry, in the online view the current, public IP address is shown instead of the host name that was entered.

Enabling the secondary DynDNS service

Create a further DynDNS update provider in case the primary provider fails. In addition to the entries in the "Primary DynDNS service" box, make the following entries:

IP settings	
Provider update URL	With the predefined providers (DynDNS.org and No-IP.com), the URL is already completed.
Check IP service URL	With the predefined providers (DynDNS.org and No-IP.com), the URL is already completed.
Ignore errors when checking the server certificate	To ensure that the authentication data is protected, the certificate of the DynDNS update server is normally checked. If the certificate check fails, the https connection is terminated and the account data is not transferred. If you select the check box, the function is disabled, for example if the server certificate of the DynDNS service is invalid (for example expired).

3.2.4 Port settings

S≥V3.0

Configuring ports

Make the connection settings for the ports.

- Half duplex: At any one time, the security module can either receive or send data.
- Full duplex: The security module can receive and send data at the same time.

Select the transmission speed and duplex setting

Follow these steps:

1. Select the "Interfaces" tab in the module properties of the security module.
2. Click the "Advanced settings…" button.
3. Select the "Port settings" tab.

The following transmission rates are supported:

Selection	Description
Autonegotiation	The transmission speed and the duplex setting are selected automatically. **Note** The autocrossing function is supported only if autonegotiation is selected.
10 Mbps, half and full duplex	Transmission speed of 10 Mbps.
100 Mbps, half and full duplex	Transmission speed of 100 Mbps.

3.2.5 Internet connection

S≥V3.0

Additional parameters

If you have set a connection using PPPoE, make the settings for the ISP.

Follow these steps

1. Select the "Interfaces" tab in the module properties of the security module.
2. For the DMZ port, select the "Remote maintenance" mode.
3. Click the "Advanced settings…" button.

4. Select the "Internet connection" tab.
5. Make the following settings:

Function	Description
User name	Enter the name for logging on with the ISP account.
Password	Enter the password for logging on with the ISP account.
Password confirmation	Enter the password for logging on with the ISP account again.
Authentication	Select none or one of the following authentication protocols: • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) **Note** Both communications partners must use the same authentication protocol otherwise no connection will be established.

Settings for the ISP account

Function	Description
Permanent connection	Permanent Internet connection. After the connection has been terminated by the provider, the connection is automatically restored even if there are no packets to be sent.
On-demand connection	The Internet connection is established automatically if packets need to be sent to the Internet. If no packets are sent during a certain time, the Internet connection is automatically terminated. In the "Maximum idle time" box, enter the number of minutes after which the connection will be terminated. Permitted values: 10 … 3600 Delays are then possible when sending packets because the Internet connection first needs to be established.
Forced disconnection	The provider terminates the Internet connection automatically after a certain period. If you enter a time of day in the "Forced disconnection", the security module terminates the Internet connection itself at this time. This prevents a forced disconnection in an unsuitable period. Permitted entries: 00:00 ... 23:59 Following this, the connection is established according to the selected type of connection: • Permanent: The Internet connection is re-established immediately. • On demand: The Internet connection is re-established when necessary, for example when packets need to be sent to the Internet.

Settings for the connection

Configuring a firewall

4

Meaning

The firewall functionality of the security modules is intended to protect networks and stations from third-party influence and interference. This means that only certain, previously specified communications relations are permitted. Disallowed frames are discarded by the firewall without you sending a response.

To filter the data traffic, IP addresses, IP subnets, port numbers or MAC addresses can be used.

The firewall functionality can be configured for the following protocol levels:

- IP firewall with stateful packet inspection (layer 3 and 4)
- Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)

~~S602~~

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

Firewall rules

Firewall rules describe which packets in which direction are permitted or forbidden.

Automatic firewall rules for STEP 7 connections

CP

With connections configured in STEP 7, firewall rules are automatically created in SCT that enable the communications partner. The connection establishment directions are taken into account.

The rules are only visible in advanced mode and can only be modified there.

Project engineering

A distinction must be made between the two operating views:

- In standard mode, simple, predefined rules are used. You can only enable service-specific rules. The enabled services are permitted for all nodes and full access is allowed in the specified direction.
- In advanced mode, you can make detailed firewall settings. You can allow individual services for a single node or all services for the node for access to the station or network.

  The following firewall rule sets must be distinguished in advanced mode:

  – Local firewall rules are always assigned to a module. They are configured in the properties dialog of the modules.

  – Global firewall rules can be assigned to several modules at the same time.

  – User-specific firewall rules can be assigned to several users and to individual security modules.

With the aid of service definitions, you can also define firewall rules clearly in a compact form. Service definitions can be used both in the local and in the global firewall rules. You can also set a bandwidth limitation.

Enabling the firewall

The firewall is controlled by selecting the "Enable firewall" check box both in standard and advanced mode. If you deselect the check box, the firewall rules you have entered remain displayed in the list but cannot be modified. If the security module is in a VPN group, the check box is enabled as default and cannot be deselected.

Enabling log settings

Configuration also differs here depending on the operating 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.

4.1 CPs in standard mode

Enabling packet filter rules

If you enable the security function for the CPs in STEP 7, initially all access to and via the CP is permitted. To enable individual packet filter rules, click the "Enable firewall" check box. Then enable the required services. Firewall rules created automatically due to a connection configuration have priority over the services set here. All other nodes have full access.

Detailed firewall settings in advanced mode

In advanced mode, you can restrict firewall rules to individual nodes. To change to advanced mode, select the "Advanced mode" check box.

Firewall configuration with VPN

If the security module is in a VPN group, the "Tunnel communication only" check box is enabled as default. This means that no communication can miss out the tunnel via the external interface and that only encrypted IPsec data transfer is permitted. The firewall rule "Drop" > "Any" > "External" is created automatically.

If you deselect the check box, tunneled communication and also the types of communication selected in the other boxes are permitted.

4.1.1 CP x43-1 Advanced

4.1.1.1 Default firewall setting

Response with defaults

The following diagrams show the standard settings in detail in each case for the IP packet filter and the MAC packet filter when the "Enable firewall" check box is selected and there are also no rules in advanced mode. The behavior can be modified by creating suitable firewall rules in advanced mode.

Default setting for CP x43 Adv.

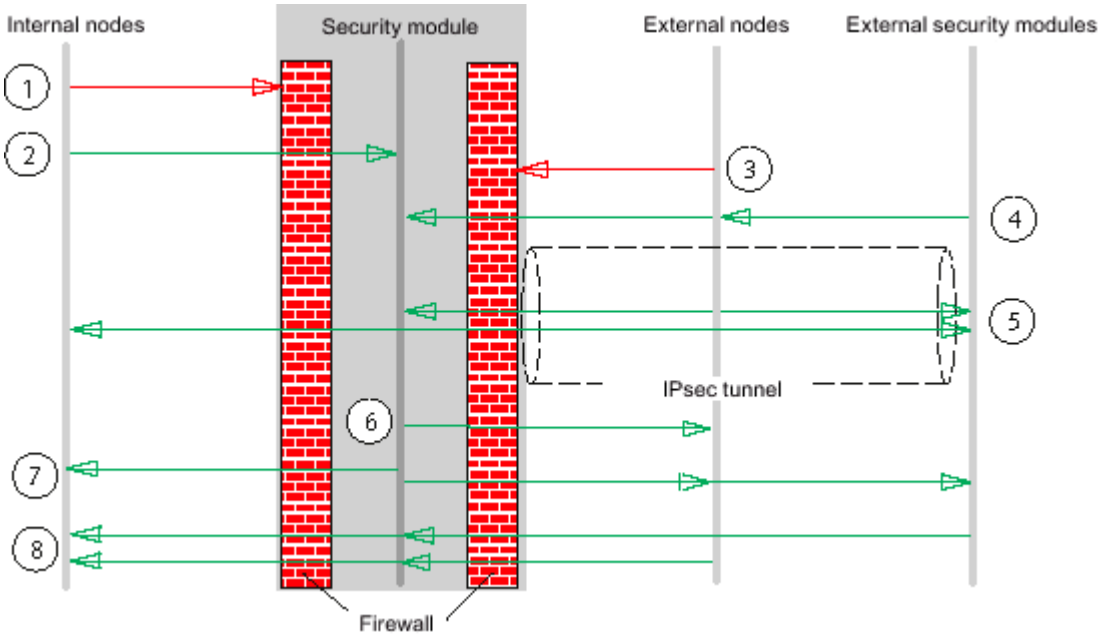


Figure 4-1 Default setting for the IP packet filter CP x43-1 Adv.

① All frame types from internal to external are blocked.

② All frames from internal to the security module are allowed.

③ All frames from external to internal and to the security module are blocked (including ICMP echo request).

④ Frames of the following types from external sources (external nodes and external security modules) to security module are permitted:

- ESP protocol (encryption)
- IKE (protocol for establishing the IPSec tunnel)
- NAT Traversal (protocol for establishing the IPSec tunnel)

⑤ IP communication over an IPSec tunnel is allowed.

⑥ Frames of the type Syslog in the direction of external are allowed by the security module and not influenced by the firewall.

Note

Since Syslog is an unreliable protocol there is no guarantee that the log data will be transferred reliably.

⑦ Frames from the security module to internal and external are allowed.

⑧ Responses to queries from the internal network from the security module are allowed.

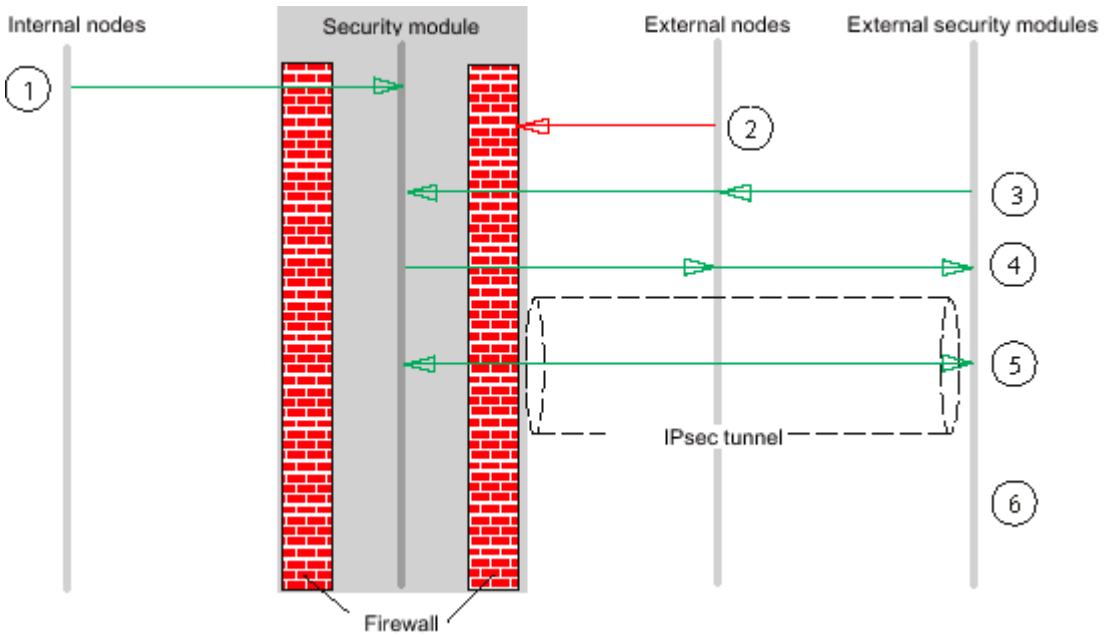


Figure 4-2 Default setting for the MAC packet filter CP x43-1 Adv.

① All frames from internal to the security module are allowed.

② All frames to the security module from external are blocked.

③ All frames of the following type from external to the security module are allowed:

- ARP with bandwidth limitation
- PROFINET DCP with bandwidth limitation
- LLDP

④ Frames of the following type from the security module to external are allowed:

- ARP with bandwidth limitation
- PROFINET DCP with bandwidth limitation

⑤ The following protocols sent through an IPsec tunnel are permitted:

- ISO
- LLDP

Note

No communication bypasses the VPN tunnel

Communication between the VPN endpoints is also prevented from bypassing the tunnel for all VPN partners known in the project. The behavior cannot be modified by creating suitable firewall rules in advanced mode.

4.1.1.2 Configuring a firewall

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Firewall" tab.

Table 4- 1 Available services and directions

Service	Station ⇒ External Internal ⇒ External	External ⇒ Internal	External ⇒ Station	External ⇔ Station	Enabled ports	Meaning
Allow IP communication	x	x	x	-	-	IP traffic for the selected communication directions is allowed.
Allow S7 protocol	x	x	x	-	TCP port 102	Communication of the nodes using the S7 protocol is allowed.
Allow FTP/FTPS (explicit mode)	x	x	x	-	TCP port 20 TCP port 21	For file management and file access between server and client.
Allow HTTP	x	x	x	-	TCP port 80	For communication with a Web server.
Allow HTTPS	x	x	x	-	TCP port 443	For secure communication with a Web server, for example for Web diagnostics.
Allow DNS	x	x	-	-	TCP port 53 UDP port 53	Communications connection to a DNS server is allowed.
Allow SNMP	x	x	x	-	TCP port 161/162 UDP port 161/162	For monitoring nodes capable of SNMP.
Allow SMTP	x	x	-	-	TCP port 25	For the exchange of e-mails between authenticated users via an SMTP server.
Allow NTP	x	x	-	-	UDP port 123	For synchronization of the time of day.
Allow MAC level communication	-	-	-	x	-	The MAC traffic from external to the station and vice versa is allowed.
Allow ISO communication	-	-	-	x	-	ISO traffic from external to the station and vice versa is allowed.

Table 4- 2 Logging for IP and MAC rule sets

Rule set	Action when activated	Created rule		
IP log settings		Action	From	To
Log tunneled packets	Only active if the security module is a member of a VPN group. All IP packets forwarded via the tunnel are logged.	Allow	Station	Tunnel
		Allow	Tunnel	Station
Log blocked incoming packets	All incoming IP packets that were discarded are logged.	Drop	External	Station
MAC log settings		Action	From	To
Log blocked incoming packets to station	All incoming MAC packets that were discarded are logged.	Drop	External	Station
Log blocked outgoing packets from station	All outgoing MAC packets that were discarded are logged.	Drop	Station	External

Note

Data traffic via configured connections is not logged.

4.1.1.3 Configuring the access list

Changing the IP access list / ACL entries

The list appears if the "Activate access protection for IP communication" check box is selected in the IP Access Protection tab in STEP 7.

You set access protection for certain IP addresses using the IP access lists. List entries already made in STEP 7 with the appropriate rights are displayed in SCT.

The right "Modify the access list (M)" that can be selected in STEP 7 is not transferred to the SCT. To be able to assign the additional IP access rights, you need to assign the "Web: Expand IP access control list" user right to the relevant user in SCT.

NOTICE

Modified behavior following migration

- Following migration, the access protection is effective only on the external interface. To make the access protection effective on the internal interface as well, configure suitable firewall rules in the advanced mode of SCT.
- The security module also responds to ARP queries from IP addresses that have not been enabled (layer 2).
- If you migrate an IP access control list without entries, the firewall is enabled and there is no longer any access to the CP from external. To make CP available, configure suitable firewall rules in the advanced mode of SCT.

How to access this function

Menu command SCT: Select the module to be edited and then select the menu command "Edit" > "Properties...", "Firewall" tab.

STEP 7 menu command: "IP access protection" > "Start of firewall configuration", "Run…" button.

Table 4- 3 Information

Parameter	Meaning
IP address	Permitted IP address or IP address range.
Rights	Depending on the assignment made. Rights that are enabled for the IP address.
Comment	Entry of additional comments.
Logging	If you select the check box, the rules are logged in the packet filter log.
Enable advanced mode	If you select the check box, the entries in the following firewall rules are converted.

Table 4- 4 Buttons

Name	Meaning / effect
New	Create a new IP address or a new IP address range with the corresponding rights.
Change	Select an entry and click this button to edit an existing entry.
Delete	Use this button to delete the selected entry.

4.1.1.4 Adding an entry in the access list

Make the following settings

Box	Description
IP address (or start of the IP range)	Enter the IP address or the start value of an IP range.
End of the IP range (optional)	Enter the end value of an IP range.
Comment	Entry of an additional comment, for example to describe the communication partner or the address range.
The IP address is authorized for	Access to station (A = access): Communications partners with addresses in the specified range have access to the station (CP / CPU) assigned to the CP. This access permission is set implicitly for IP addresses you have specified in the connection configuration (does not apply to specified connections). IP routing to another subnet (R = routing): Communications partners with addresses in the specified range have access to other subnets connected to CP. This access permission is not set automatically for IP addresses you have specified in the connection configuration. Where necessary, this access permission must be set here explicitly.

Other rules when making entries:

- There is a check to determine whether individual addresses are included more than once; here, the following is detected: Multiple single entries; overlapping ranges.
- IP addresses specified individually can also occur within a range; the access permissions assigned in total to an IP address then apply.
- The system does not check whether invalid addresses are included in a range (for example, subnet broadcast addresses could be specified here although they cannot occur as the IP address of a sender).

4.1.2 CP 1628

4.1.2.1 Default firewall setting

Response with defaults

The following diagrams show the standard settings in detail in each case for the IP packet filter and the MAC packet filter when the "Enable firewall" check box is selected and there are also no rules in advanced mode. The behavior can be modified by creating suitable firewall rules in advanced mode.

Default setting for CP 1628

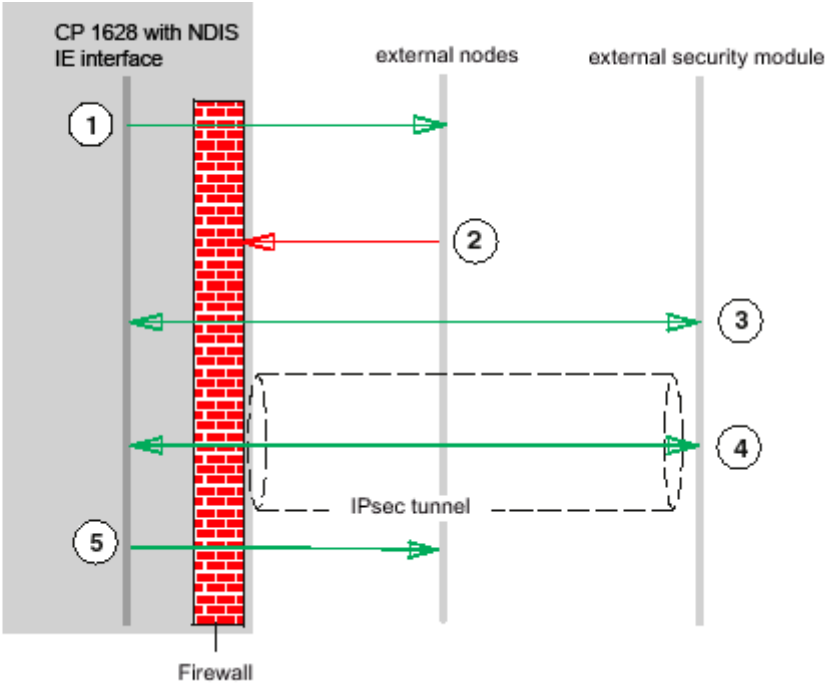


Figure 4-3 Default setting for the IP packet filter CP 1628

① All frames from the NDIS and IE (Industrial Ethernet) interface to external are allowed.

② All frames from external are blocked.

③ All frames of the following type from external to the security module and vice versa are allowed:

- ESP protocol (encryption)
- IKE (protocol for establishing the IPSec tunnel)

④ IP communication over an IPSec tunnel is allowed.

⑤ Frames of the type Syslog in the direction of external are allowed by the security module.

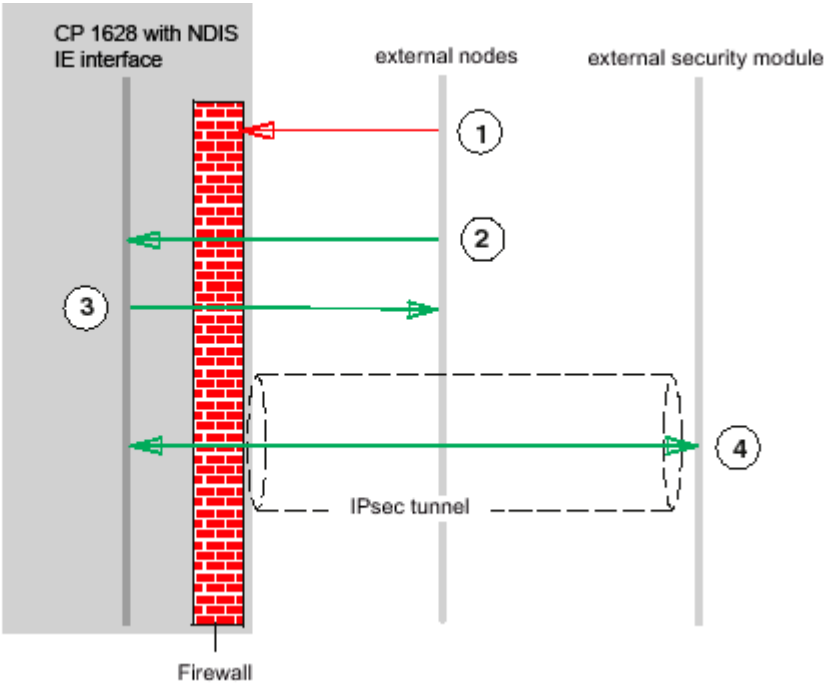


Figure 4-4 Default setting for the MAC packet filter CP 1628

① All frames from external are blocked.

② All frames of the following type from external are allowed:

- ARP with bandwidth limitation
- PROFINET DCP with bandwidth limitation

③ Frames of the following type from the security module to external are allowed:

- PROFINET DCP with bandwidth limitation

④ MAC protocols sent through an IPSec tunnel are permitted.

Note

No communication bypasses the VPN tunnel

Communication between the VPN endpoints is also prevented from bypassing the tunnel for all VPN partners known in the project. The behavior cannot be modified by creating suitable firewall rules in advanced mode.

4.1.2.2 Configuring a firewall

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Firewall" tab.

Table 4- 5 Available services and directions

Service	External ⇒ Station	External ⇔ Station	Enabled ports	Meaning
Allow IP communication	x	-	-	IP traffic for the selected communication directions is allowed.
Allow S7 protocol	x	-	TCP port 102	Communication of the nodes using the S7 protocol is allowed.
Allow FTP/FTPS (explicit mode)	x	-	TCP port 20 TCP port 21	For file management and file access between server and client.
Allow HTTP	x	-	TCP port 80	For communication with a Web server.
Allow HTTPS	x	-	TCP port 443	For secure communication with a Web server, for example for Web diagnostics.
Allow DNS	x	-	TCP port 53 UDP port 53	Communications connection to a DNS server is allowed.
Allow SNMP	x	-	TCP port 161/162 UDP port 161/162	For monitoring nodes capable of SNMP.
Allow SMTP	x	-	TCP port 25	For the exchange of e-mails between authenticated users via an SMTP server.
Allow NTP	x	-	UDP port 123	For synchronization of the time of day.
Allow MAC level communication	-	x	-	The MAC traffic from external to the station and vice versa is allowed.
Allow ISO communication	-	x	-	ISO traffic from external to the station and vice versa is allowed.
Allow SiClock	-	x	-	SiClock time-of-day frames from external to the station and vice versa are allowed.

Table 4- 6 Logging for IP and MAC rule sets

Rule set	Action when activated	Created rule		
IP log settings		Action	From	To
Log tunneled packets	Only active if the security module is a member of a VPN group. All IP packets forwarded via the tunnel are logged.	Allow	Station	Tunnel
		Allow	Tunnel	Station
Log blocked incoming packets	All incoming IP packets that were discarded are logged.	Drop	External	Station
MAC log settings		Action	From	To
Log blocked incoming packets	All incoming MAC packets that were discarded are logged.	Drop	External	Station
Log blocked outgoing packets	All outgoing MAC packets that were discarded are logged.	Drop	Station	External

Note

Data traffic via configured connections is not logged.

4.2 SCALANCE S in standard mode

4.2.1 Firewall defaults

Response with defaults

The following diagrams show the default settings in detail for the IP packet filter and the MAC packet filter. The behavior can be modified by creating suitable firewall rules in advanced mode.

Default setting for SCALANCE S

The firewall defaults have been selected so that no IP data traffic is possible. Communication between the nodes in the internal networks of security modules is allowed only if you have configured an IPSec tunnel.

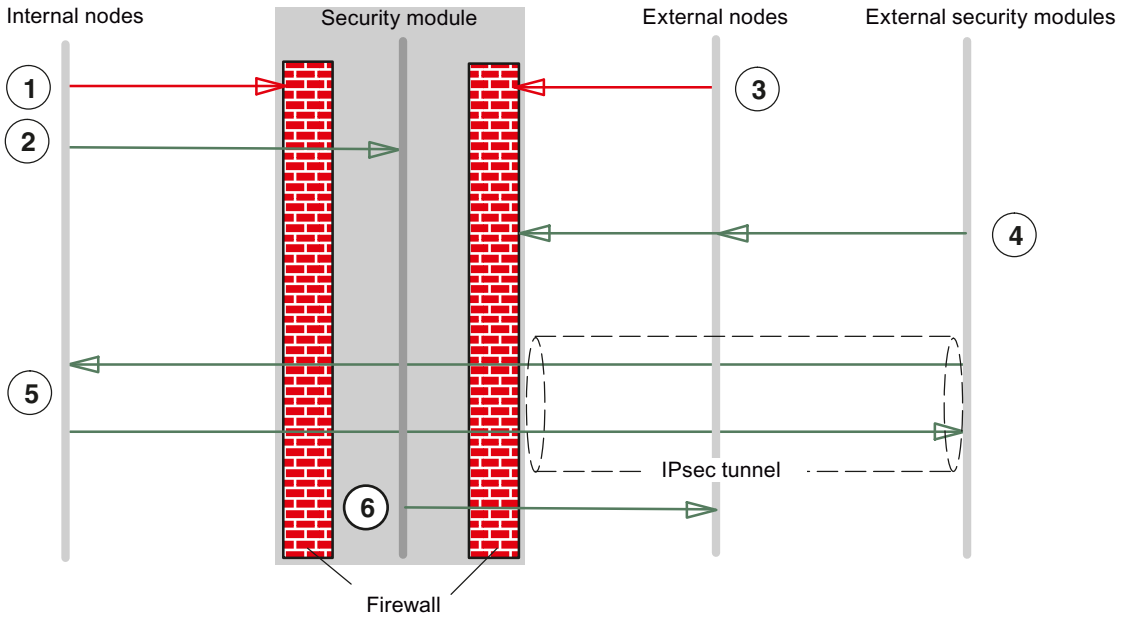


Figure 4-5 Default setting for the IP packet filter SCALANCE S

① All frame types from internal to external are blocked.

② All frames from internal to the security module are allowed.

③ All frames from external to internal and to the security module are blocked (including ICMP echo request).

④ Frames of the following types from external sources (external nodes and external security modules) to security modules are permitted:

- HTTPS (SSL)
- ESP protocol (encryption)
- IKE (protocol for establishing the IPSec tunnel)
- NAT Traversal (protocol for establishing the IPSec tunnel)

⑤ IP communication over an IPSec tunnel is allowed.

⑥ Frames of the type Syslog and NTP in the direction of external are allowed by the security module.

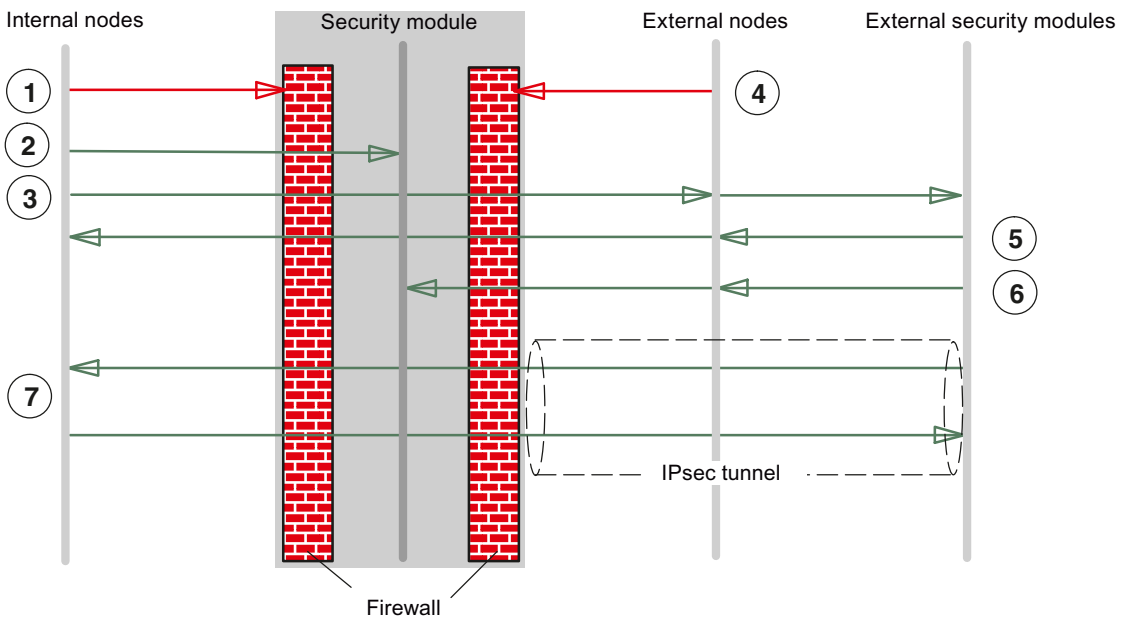


Figure 4-6 Default setting for the MAC packet filter SCALANCE S

① All frame types from internal to external are blocked.

② All frames from internal to the security module are allowed.

③ ARP frames from internal to external are allowed.

④ All frames from external to internal and to the security module are blocked.

⑤ Packets from external to internal of the following types are allowed:

- ARP with bandwidth limitation

⑥ Frames of the following type from external to security modules are allowed:

- ARP with bandwidth limitation
- PROFINET DCP with bandwidth limitation

⑦ MAC protocols sent through an IPSec tunnel are permitted.

4.2.2 Configuring a firewall ≥ V3.0

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Firewall" tab.

Firewall enabled as default

The "Enable firewall" check box is enabled by default. The firewall is therefore activated automatically and all access from external to the security module is blocked. By clicking the relevant check box, enable the firewall rules for the specific direction.

Detailed firewall settings in advanced mode

In advanced mode, you can restrict firewall rules to individual nodes.

Firewall configuration with VPN

If the security module is in a VPN group, the "Tunnel communication only" check box is enabled as default. This means that no communication can miss out the tunnel via the external interface and that only encrypted IPsec data transfer is permitted.

If you deselect the check box, tunneled communication and also the types of communication selected in the other boxes are permitted.

Table 4- 7 Available firewall rules and directions

Service	Internal ⇒ External	External ⇒ Internal	From internal	From external	Enabled ports	Meaning
Allow IP traffic	x	x	-	-	-	IP traffic for the selected communication directions is allowed.
Allow S7 protocol	x	x	-	-	TCP port 102	Communication of the nodes using the S7 protocol is allowed.
Allow FTP/FTPS (explicit mode)	x	x	-	-	TCP port 20 TCP port 21	For file management and file access between server and client.
Allow HTTP	x	x	-	-	TCP port 80	For communication with a Web server.
Allow HTTPS	x	x	-	-	TCP port 443	For secure communication with a Web server, for example for Web diagnostics.
Allow with DNS	x	x	-	-	TCP port 53 UDP port 53	Communications connection to a DNS server is allowed.
Allow with SNMP	x	x	-	-	TCP port 161/162 UDP port 161/162	For monitoring nodes capable of SNMP.
Allow with SMTP	x	x	-	-	TCP port 25	For the exchange of e-mails between authenticated users via an SMTP server.
Allow NTP	x	x	-	-	UDP port 123	For synchronization of the time of day.
Allow DHCP	x	x	-	-		
Allow MAC level communication	-	-	x	x	-	The MAC traffic from external to the station and vice versa is allowed.

Service	Internal ⇒ External	External ⇒ Internal	From internal	From external	Enabled ports	Meaning
Allow ISO protocol	-	-	x	x	-	ISO traffic from external to the station and vice versa is allowed.
Allow SiClock	-	-	x	x	-	SiClock time-of-day frames from external to the station and vice versa are allowed.
Allow DCP	-	-	x	x	-	

Table 4- 8 Logging for IP and MAC rule sets

Rule set	Action when activated
IP log settings	
Log tunneled packets	Only active if the security module is a member of a VPN group. All IP packets forwarded via the tunnel are logged.
Log blocked incoming packets	All incoming IP packets that were discarded are logged.
Log blocked outgoing packets	All outgoing IP packets that were discarded are logged.
MAC log settings	
Log tunneled packets	Only active if the security module is a member of a VPN group. All MAC packets forwarded via the tunnel are logged.
Log blocked incoming packets	All incoming MAC packets that were discarded are logged.
Log blocked outgoing packets	All outgoing MAC packets that were discarded are logged.

4.2.3 Configuring a firewall < V3.0

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Firewall" tab.

Note

Detailed firewall settings in advanced mode

In advanced mode, you can restrict firewall rules to individual nodes. To change to advanced mode, select the "Enable advanced mode" check box.

Table 4- 9 Available services and directions

Rule/option	Enabled ports	Function
Tunnel communication only	-	This is the default setting. This option can only be selected when the module is in a group. With this setting, only encrypted IPsec data transfer is permitted; only nodes in the internal networks of SCALANCE S can communicate with each other. If this option is deselected, tunnel communication and the type of communication selected in the other boxes are permitted.
Allow IP traffic from internal to external network	-	Internal nodes can initiate a communication connection to nodes in the external network. Only response frames from the external network are forwarded into the internal network. No communication connection can be initiated from the external network to nodes in the internal network.
Allow IP traffic with S7 protocol from internal to external network.	TCP port 102	Internal nodes can initiate an S7 communication connection to nodes in the external network. Only response frames from the external network are forwarded into the internal network. No communication connection can be initiated from the external network to nodes in the internal network.
Allow access to DHCP server from internal to external network.	UDP port 67 UDP port 68	Internal nodes can initiate a communication connection to a DHCP server in the external network. Only the response frames of the DHCP server are forwarded into the internal network. No communication connection can be initiated from the external network to nodes in the internal network.
Allow access to NTP server from internal to external network.	UDP port 123	Internal nodes can initiate a communication connection to an NTP (Network Time Protocol) server in the external network. Only the response frames of the NTP server are passed into the internal network. No communication connection can be initiated from the external network to nodes in the internal network.
Allow SiClock time-of-day frames from external to internal network.	-	This option allows SiClock time-of-day frames from the external network to the internal network.
Allow access to DNS server from internal to external network.	TCP port 53 UDP port 53	Internal nodes can initiate a communication connection to a DNS server in the external network. Only the response frames of the DNS server are forwarded into the internal network. No communication connection can be initiated from the external network to nodes in the internal network.
Allow the configuration of internal network nodes using DCP from the external to the internal network.	-	The DCP protocol is used by the PST tool to set the IP parameters (node initialization) of SIMATIC NET network components. This rule allows nodes in the external network to access nodes in the internal network using the DCP protocol.

Table 4- 10 Logging for IP and MAC rule sets

Rule set	Action when activated
IP log settings	
Log tunneled packets	Only if the security module is a member of a VPN group: All IP packets forwarded via the tunnel are logged.
Log blocked incoming packets	All incoming IP packets that were discarded are logged.
Log blocked outgoing packets	All outgoing IP packets that were discarded are logged.
MAC log settings	
Log blocked incoming packets	All incoming MAC packets that were discarded are logged.
Log blocked outgoing packets	All outgoing MAC packets that were discarded are logged.

4.3 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 described in this section, switch over to advanced mode.

Note

No return to standard mode possible

If you switch to the advanced mode and change the configuration for the current project, you can no longer switch back.

Remedy SCT standalone: You close the project without saving and open it again.

Symbolic names are supported

You can also enter the IP addresses or MAC addresses as symbolic names in the functions described below.

4.3.1 Configure the 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 (layer 3)
- MAC protocol (layer 2)

Note

No MAC rules if routing mode is enabled

SCA.

If you have enabled the routing mode for the security module, MAC rules are irrelevant (dialogs are disabled).

If you do not enter any rules in the dialogs described below, the default settings apply as described in the relevant subsections of the section CPs in standard mode (Page 83).

Global, user-specific and local definition possible

- Global firewall rules

  A global firewall rule can be assigned to several modules at the same time. This option simplifies configuration in many situations.

- User-specific firewall rules S≥V3.0

  A user-specific firewall rule can be assigned to one or more users and then to individual security modules.

- Local firewall rules

  A local firewall rule is assigned to a module. This is configured in the properties dialog of a module.

Several local firewall rules and several global firewall rules as well as several user-defined firewall rules can be assigned to a module.

4.3.2 Global firewall rules

Application

Global firewall rules are configured outside the module at the project level. They are visible in the navigation area of the Security Configuration Tool.

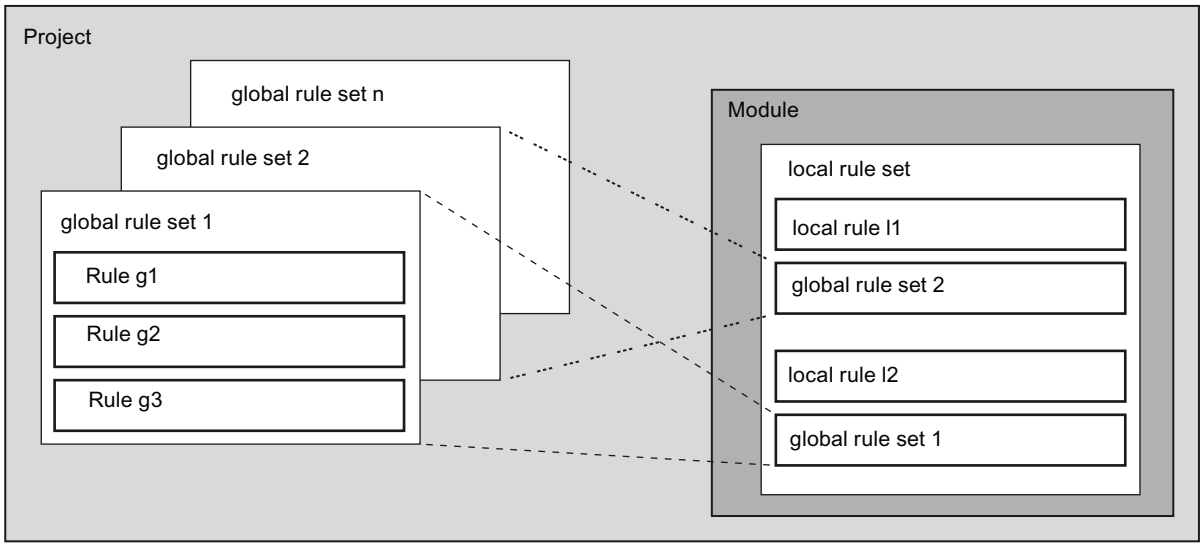
In the global firewall rules, a distinction is made between the following:

- IP firewall rules
- MAC firewall rules

You can define firewall rules for the following:

- IP rule sets
- MAC rule sets

The following schematic illustrates the relationship between globally defined rule sets and locally used rule sets.



When are global IP and MAC firewall rules useful?

Global firewall rules are useful if you want to define identical filter criteria for communication with several security modules.

Note

Only assign rule sets that are supported by the security module

A bad module assignment can lead to undesirable results. You should therefore always check the module-specific local firewall rules in the result. A bad rule assignment is not detected in the automatic consistency check. Only rules that are actually supported by the security module are adopted.

See also

User-specific firewall rules (Page 103)

4.3.2.1 Global firewall rule sets - conventions

Global firewall rules are used locally

The following conventions apply when creating a global set of firewall rules and when assigning it to a module:

- View in the Security Configuration Tool

  Global firewall rules can only be created in advanced mode.

- Priority

  Global IP and MAC firewall rules: As default, locally defined rules have higher priority than global IP and MAC firewall rules; newly assigned global IP and MAC firewall rules are therefore initially added to the bottom of the local rule list.

  The priority can be changed by changing the position in the rule list.

- Granularity

  Global firewall rules can only be assigned to a security module as an entire set.

- Entering, changing or deleting rule sets

  Global firewall rules cannot be edited in the local rule list of the firewall rules in the module properties. They can only be displayed there and positioned according to the required priority.

  It is not possible to delete a single rule from an assigned rule set. You can only take the entire set of rules out of the local rule list but this does not change the definition in the global rule list.

4.3.2.2 Creating and assigning global firewall rule sets

How to access this function

1. Select one of the following folders from the navigation area:
   - "Global firewall rule sets" > "Firewall IP rule sets"
   - "Global firewall rule sets" > "Firewall MAC rule sets"
2. Select the "Insert" > "Firewall rule set" menu command.
3. Enter the following data:
   - Name: Project-wide, unique name of the rule set; the name appears in the local rule list of the security module after the rule set is assigned.
   - Description: Enter a description of the global rule set.
4. Click the "Add rule" button.

5. Enter the firewall rules one by one in the list. Note the parameter description in the sections below:

   For IP rule sets: IP packet filter rules (Page 109).

   For MAC rule sets: MAC packet filter rules (Page 118).

6. Assign the global firewall rule to the modules in which you want it to be used. You do this by selecting a module in the navigation area and dragging it to the relevant global rule set in the navigation area.

Result

The global rule set is used by the assigned security module as a local rule set and appears automatically in the module-specific list of firewall rules.

See also

Global firewall rule sets - conventions (Page 102)

4.3.3 User-specific firewall rules

S≥V3.0

When is it useful to assign IP firewall rules to a user?

IP firewall rules are initially assigned to one or more users and then to individual security modules. This makes it possible, to allow user-specific access. If, for example all access to the networks downstream from a security module is blocked, certain IP addresses can be allowed for a user. This means that access is allowed for this user but access remains blocked for other users.

User logon via the Internet

The user can log on with the security module using a Web page. If authentication is successful, the predefined firewall rule set for this user is enabled. The connection of the security module is via HTTPS using the IP address of the connected port and taking into account the valid routing rules:

Example:

External port: 192.168.10.1

Logon via: https://192.168.10.1/

Users can log on with the administrator, diagnostics or remote access role as long as this is assigned to a user-specific firewall rule.

User-specific firewall rules are used locally - conventions

The same conventions apply as described in section Global firewall rule sets - conventions (Page 102).

4.3.3.1 Creating and assigning user-specific firewall rules

How to access this function

1. In the navigation area, select the "User-specific IP rule sets" folder.
2. Select the "Insert" > "Firewall rule set" menu command.
3. Enter the following data:
   – Name: Project-wide, unique name of the rule set; the name appears in the local rule list of the security module after the rule set is assigned.
   – Description: Enter a description of the user-defined rule set.
4. Click the "Add rule" button.
5. Enter the firewall rules one by one in the list. Note the parameter description in section IP packet filter rules (Page 109).
6. Assign the rule to one or more users.

Note

Assignment of user-specific rule sets

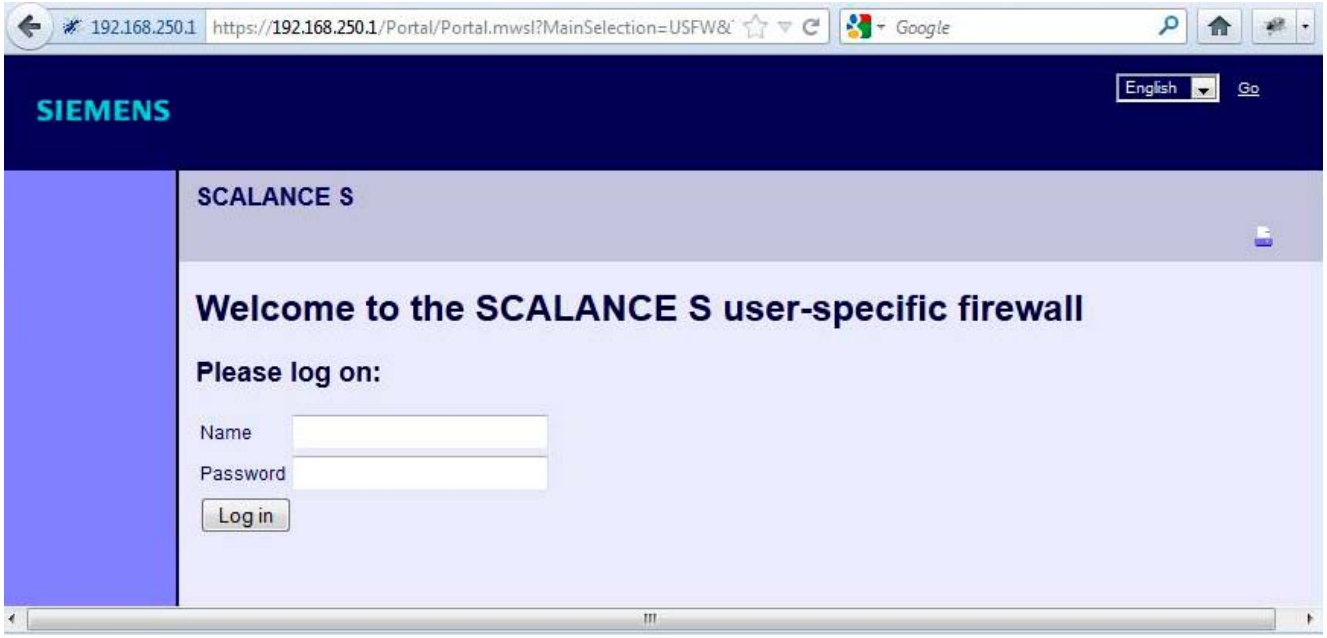
- A module can only be assigned one user-specific rule set per user.
- Due to the assignment, the right "User can log on with module" is enabled for all roles of the users specified in the rule set.

---

7. Assign the user-specific firewall rule to the security modules in which you want it to be used. You do this by selecting a module in the navigation area and dragging it to the relevant user-specific rule set in the navigation area.

Result

- The user-specific rule set is used by the assigned security module as a local rule set and automatically appears in the module-specific list of firewall rules.
- The user can log on with the security module.



Value ranges for timeout

The timeout time after which the user is automatically logged off is 30 minutes.

4.3.4 Connection-related automatic firewall rules

CP

Automatically created firewall rules in SCT

For the following application, the firewall rules are created automatically:

- Connections configured in STEP 7

Firewall rules for configured connections

If connections have been created in STEP 7, firewall rules are automatically created for these in SCT. To achieve this there is system synchronization between STEP 7 and SCT during which all connections configured in the project are checked. For each communications partner, the IP address, the action and the interface are synchronized automatically. Regardless of the number of connections, 2 rules result per communications partner.

Note

Enabling UDP multicast and UDP broadcast connections manually

S7-CP

No automatic firewall rules are created for UDP multicast and UDP broadcast connections. To enable the connections, add the relevant firewall rules manually in advanced mode.

Depending on how the connection establishment is configured in STEP 7, the following level 3 firewall rules are created in SCT:

CP->external	Action	From	To
active	Allow	Station	External
	Drop	External	Station
passive	Drop	Station	External
	Allow	External	Station
active and passive	Allow	External	Station
	Allow	Station	External

If the security module is in a VPN group, the direction "External" changes to "Tunnel".

CP->internal	Action	From	To
active	Allow	Station	Internal
	Drop	Internal	Station
passive	Drop	Station	Internal
	Allow	Internal	Station
active and passive	Allow	Internal	Station
	Allow	Station	Internal

For level 2 connections, only "Allow" rules are created.

Conventions for automatically created firewall rules

- Priority

  The rules have highest priority and are therefore inserted at the top in the local rule list.

- Changing or deleting rules

  The rule sets cannot be deleted. Logging can be enabled and services can be assigned. In addition to this, the bandwidth and a comment can be entered.

- Changing the action

  In SCT, if you set the action from "Allow" to "Drop" or vice versa, this will be overwritten again if the system synchronization is repeated. If you want the changes to be retained, select "Allow*" or "Drop*". In this case, only the IP address is synchronized with STEP 7 and the action and direction remain as set. If the IP address does not exist in STEP 7, the rule is removed from the list. Settings for logging, service, bandwidth and comment in SCT remain even after renewed system synchronization with STEP 7.

Security module in VPN group

As default, the "Tunnel communication only" check box is enabled. If you deselect the check box, communication can be through the tunnel or can bypass it.

- Communication is outside the tunnel if the partner address belongs to a station known in SCT for which no VPN tunnel is configured.
- Communication is through the tunnel if the partner address is a VPN endpoint.
- If it is not clear whether connection should bypass or run through the VPN tunnel, the connection is assigned to the VPN tunnel and a message to this effect is displayed. The assignment can be adapted in advanced mode, for example by changing the "From" direction "Tunnel" to "External".

Note

If you want to ensure that only communication through the tunnel is possible, you will need to create suitable firewall rules in advanced mode, for example for internal nodes or NDIS addresses.

To allow only tunneled communication for a CP, add a "Drop" > "Any" > "Station" rule at the end of the firewall rules.

4.3.5 Setting local IP packet filter rules

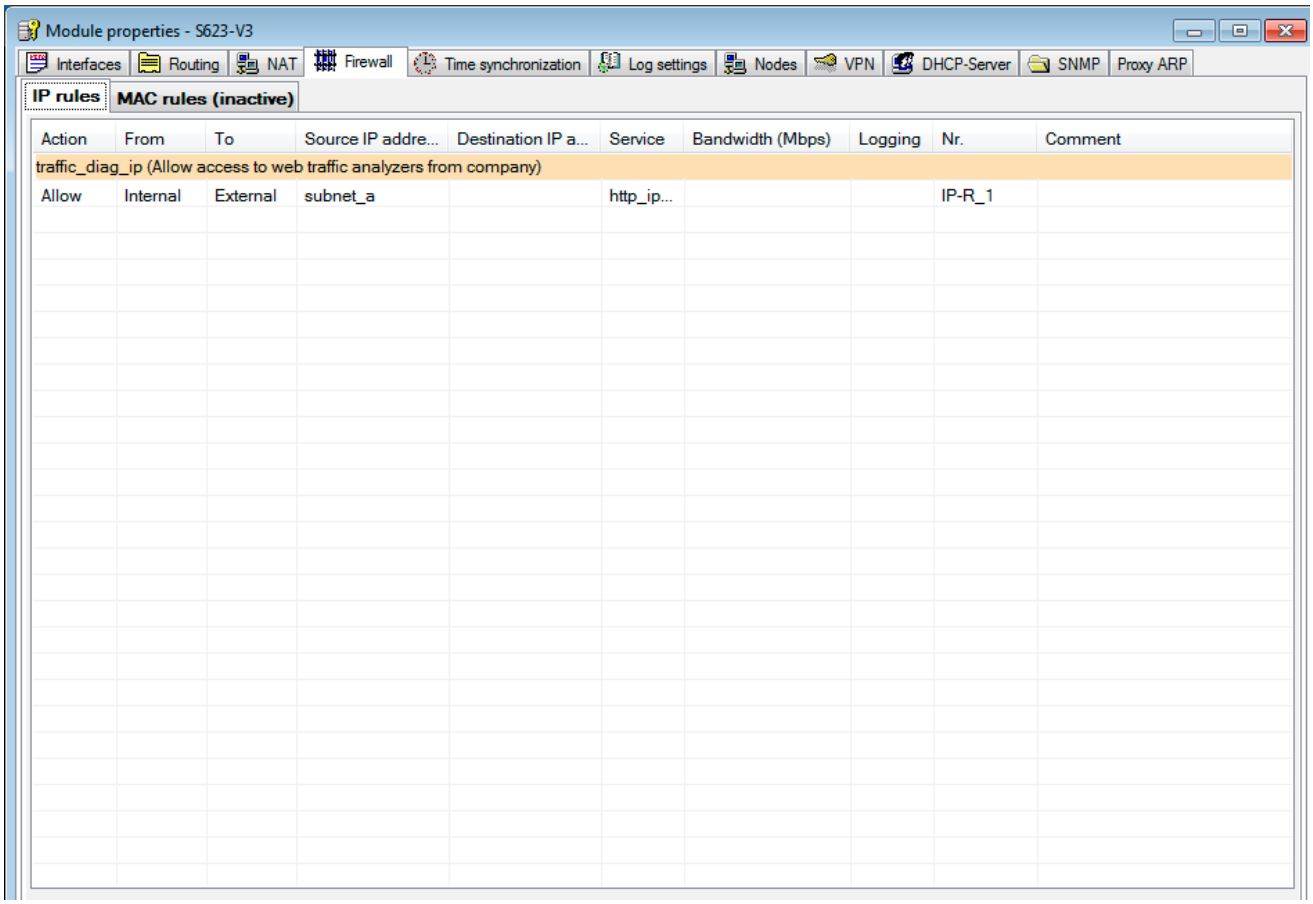
Using the IP packet filter rules, you can filter IP packets such as UDP, TCP, ICMP packets.

Within an IP packet filter rule, you can also include service definitions and further restrict the filter criteria. If you do not specify services, the IP packet filter rule applies to all services.

Opening the dialog for local IP packet filter rules

SCT: Select the module to be edited and then select the menu command "Edit" > "Properties...", "Firewall" tab.

STEP 7: In the "Security" tab, click the "Run" button beside "Start of security configuration", "Firewall tab.



Entering IP packet filter rules

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

Using global and user-specific firewall rule sets

Global and user-specific rule sets you have assigned to the module are automatically entered in the local rule set. If the rule set appears at the end of the rule list, it is processed with the lowest priority. You can change the priority by changing the position in the rule list.

The online help explains the meaning of the individual buttons.

4.3.6 IP packet filter rules

IP packet rules are processed based on the following evaluations:

- Parameters entered in the rule;
- Order and associated priority of the rule within the rule set.

Parameter

The configuration of an IP rule includes the following parameters:

Name	Meaning/comment	Available options / ranges of values
Action	Allow/disallow (enable/block)	• Allow Allow frames according to definition. • Drop Block frames according to definition. For automatically created connection rules: • Allow* • Drop* If you select these rules, there is no synchronization with STEP 7. Modified rules are therefore not overwritten in SCT.
From / To	The permitted communications directions.	Is described in the following tables.
Source IP address	Source address of the IP packets	Refer to the section "IP addresses in IP packet filter rules" in this chapter. As an alternative, you can enter symbolic names.
Destination IP address	Destination address of the IP packets	
Service	Name of the IP/ICMP service or service group used. Using the service definitions, you can define packet filter rules Here, you select one of the services you defined in the IP services dialog: • IP services or • ICMP services If you have not yet defined any services or want to define a further service, click the "IP/MAC services definition..." button.	The drop-down list box displays the configured services and service groups you can select. No entry means: No service is checked, the rule applies to all services. Note: So that the predefined IP services appear in the drop-down list, select this first in standard mode.
Bandwidth (Mbps)	Option for setting a bandwidth limitation. Can only be entered if the "Allow" action is selected. A packet passes through the firewall if the pass rule matches and the permitted bandwidth for this rule has not yet been exceeded.	CP x43-1 and SCALANCE S < V3.0: 0.001 ... 100 CP 1628 and SCALANCE S ≥ V3.0: 0.001 ... 1000 For global and user-specific rules: 0.001 ... 100

Name	Meaning/comment	Available options / ranges of values
Logging	Enable or disable logging for this rule.	
No.	Automatically assigned number for the rule.	
Comment	Space for your own explanation of the rule.	If a comment is marked with "AUTO", it was created for an automatic connection rule.

Table 4- 11 Directions with a CP

Available options / ranges of values		Security module		Meaning
From	To	CP x43-1 Adv.	CP 1628	
Internal	Station	x	-	Access from the internal network to the station.
	Any	x	-	Access from internal to the external network, VPN tunnel partner and the station.
External	Station	x	x	Access from the external network to the station.
	Any	x	-	Access from external to the internal network and the station.
Station	Internal	x	-	Access from the station to the internal network.
	External	x	x	Access from the station to the external network.
	Tunnel	x	x	Access from the station to the VPN tunnel partner.
Tunnel	Station	x	x	Access via the VPN tunnel partner to the station.
	Any	x	-	Access from VPN tunnel partners to the internal network and the station.
Any	External	x	-	Access from the internal network and the station to the external network.

Table 4- 12 Directions with SCALANCE S ≥ V3.0

Available options / ranges of values		Security module		
From	To	S602 V3*	S612 V3**	S623 V3
Internal	External	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
	DMZ	-	-	x
External	Internal	x	x	x
	Any	-	-	x
	Tunnel	-	-	x
	DMZ	-	-	x
Tunnel	Internal	-	x	x
	External	-	x	x
	DMZ	-	-	x

Available options / ranges of values		Security module		
Any	Internal	-	x	x
	External	-	-	x
	DMZ	-	-	x
DMZ	Internal	-	-	x
	External	-	-	x
	Any	-	-	x
	Tunnel	-	-	x

* Also valid for SCALANCE S 602 V2.

** Also valid for SCALANCE S 612 V2 and SCALANCE S 613 V2.

Order for rule evaluation by the security module

The packet filter rules are evaluated 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, external and DMZ network, the final rule is: All frames except for the frames explicitly allowed in the list are blocked.
- In rules for communication between the internal network and IPsec tunnel, the final rule is: All frames except for the frames explicitly blocked in the list are allowed.

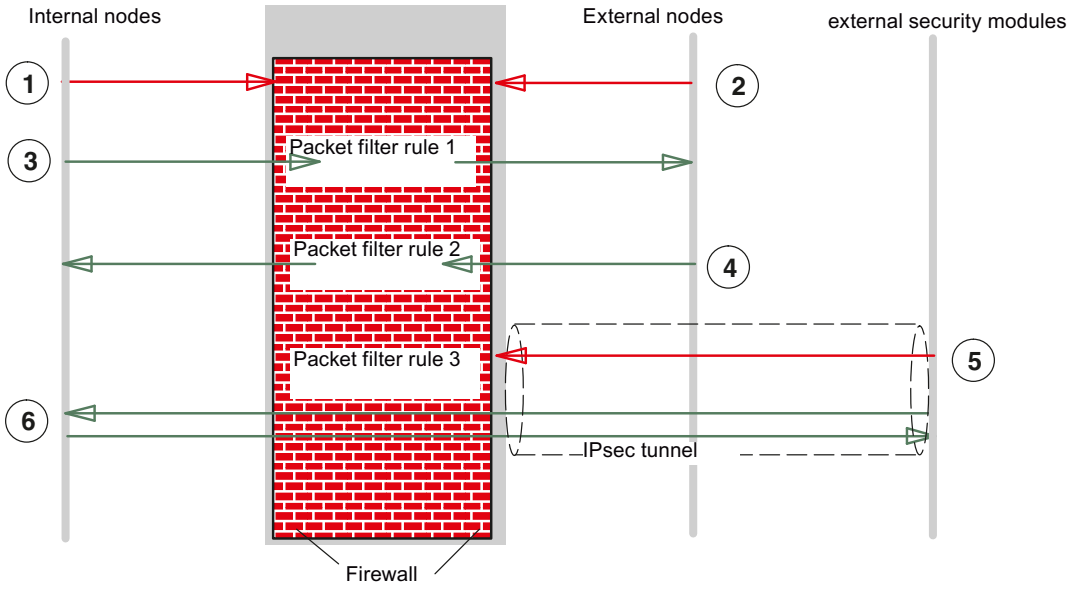
Example

Interfaces | Routing | NAT | Firewall | Time synchronization | Log settings | Nodes | VPN | DHCP-Server | SNMP | Proxy ARP

IP rules | MAC rules

Action	From	To	Source IP addre...	Destination IP address	Service	Bandwidth (Mbps)	Logging	No.	Comment
Allow	Internal	External			ServiceX1			IP-R_1	
Allow	External	Internal	196.65.254.2	197.54.199.4	ServiceX2			IP-R_2	
Drop	Tunnel	Internal			ServiceX1			IP-R_3	

The packet filter rules shown have the following effect:



① All frame types from internal to external are blocked as default, except for those explicitly allowed.
② All frame types from external to internal are blocked as default, except for those explicitly allowed.
③ IP packet filter rule 1 allows frames with the service definition "Service X1" from internal to external.
④ IP packet filter rule 2 allows frames 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 frames with the service definition "Service X1" in the VPN (IPsec tunnel).
⑥ IPsec tunnel communication is allowed as default except for the explicitly blocked frame types.

See also

MAC packet filter rules (Page 118)

Range of values for IP address, subnet mask and address of the gateway (Page 205)

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 three octets of 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.
- Address range

  For the source IP address, an address range can be specified separated by a hyphen:

  [Start IP address]-[End IP address]

For more detailed information, refer to section Range of values for IP address, subnet mask and address of the gateway (Page 205).

Table 4- 13 Examples of address ranges in IP addresses

Source IP address or destination IP address	Address range		Number of 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**	192.168.10.0	192.168.10.127	128
192.168.10.0/**26**	192.168.10.0	192.168.10.63	64
192.168.10.0/**27**	192.168.10.0	192.168.10.31	32
192.168.10.0/**28**	192.168.10.0	192.168.10.15	16
192.168.10.0/**29**	192.168.10.0	192.168.10.7	8
192.168.10.0/**30**	192.168.10.0	192.168.10.3	4
*) Note: Note that the address values 0 and 255 in the IP address have special functions (0 stands for a network address, 255 for a broadcast address). The number of actually available addresses is therefore reduced.			

4.3.7 Defining IP services

How to access this function

- Using the menu command "Options" "IP services".

  or

- From the "IP Rules" tab with the "IP services" button.

Meaning

Using the IP service definitions, you can define succinct and clear firewall rules for specific services. 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.

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

Parameters for IP services

You define the IP services using the following parameters:

Table 4- 14 IP services: Parameter

Name	Meaning/comment	Available options / ranges of 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 UDP Any
Source port	The filtering is based on the specified port number; this defines the service access at the frame sender.	Examples: *: Port is not checked 20 or 21: FTP service
Destination port	The filtering is based on the specified port number; this defines the service access at the frame recipient.	Examples: *: Port is not checked 80: Web HTTP service 102: S7 protocol - TCP/port

4.3.8 defining ICMP services

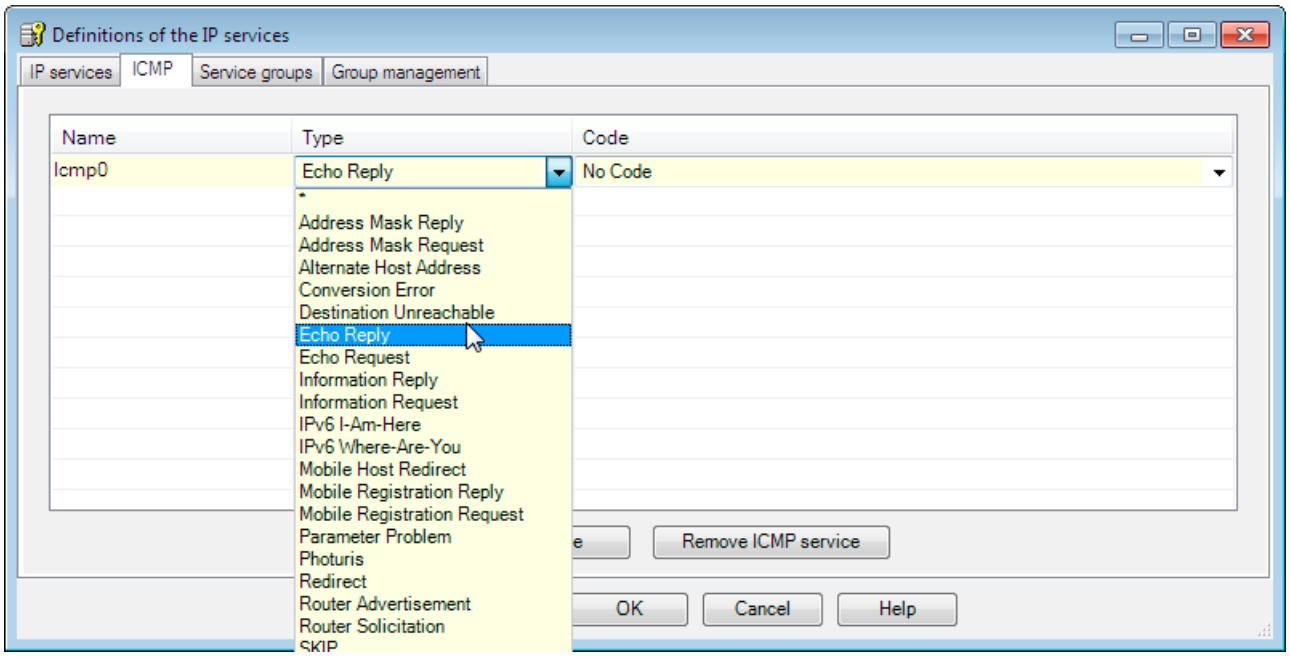
Using the ICMP service definitions, you can define firewall rules for specific ICMP services. You select a name and assign the service parameters to it. The defined services can also be grouped together under a group name. When you configure the packet filter rules, you then use this group name.

How to access this function

- Using the menu command "Options" > "IP services.." or "MAC services..", "ICMP" tab.

  or

- Using the "IP services" or "MAC services.." button, "ICMP" tab



Parameters for ICMP services

You define the ICMP services using the following parameters:

Table 4- 15 ICMP services: Parameter

Name	Meaning/comment	Available options / ranges of 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	Refer to the dialog illustration.
Code	Codes of the ICMP type	Values depend on the selected type.

4.3.9 Setting MAC packet filter rules

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

Note

No MAC rules if routing mode is enabled

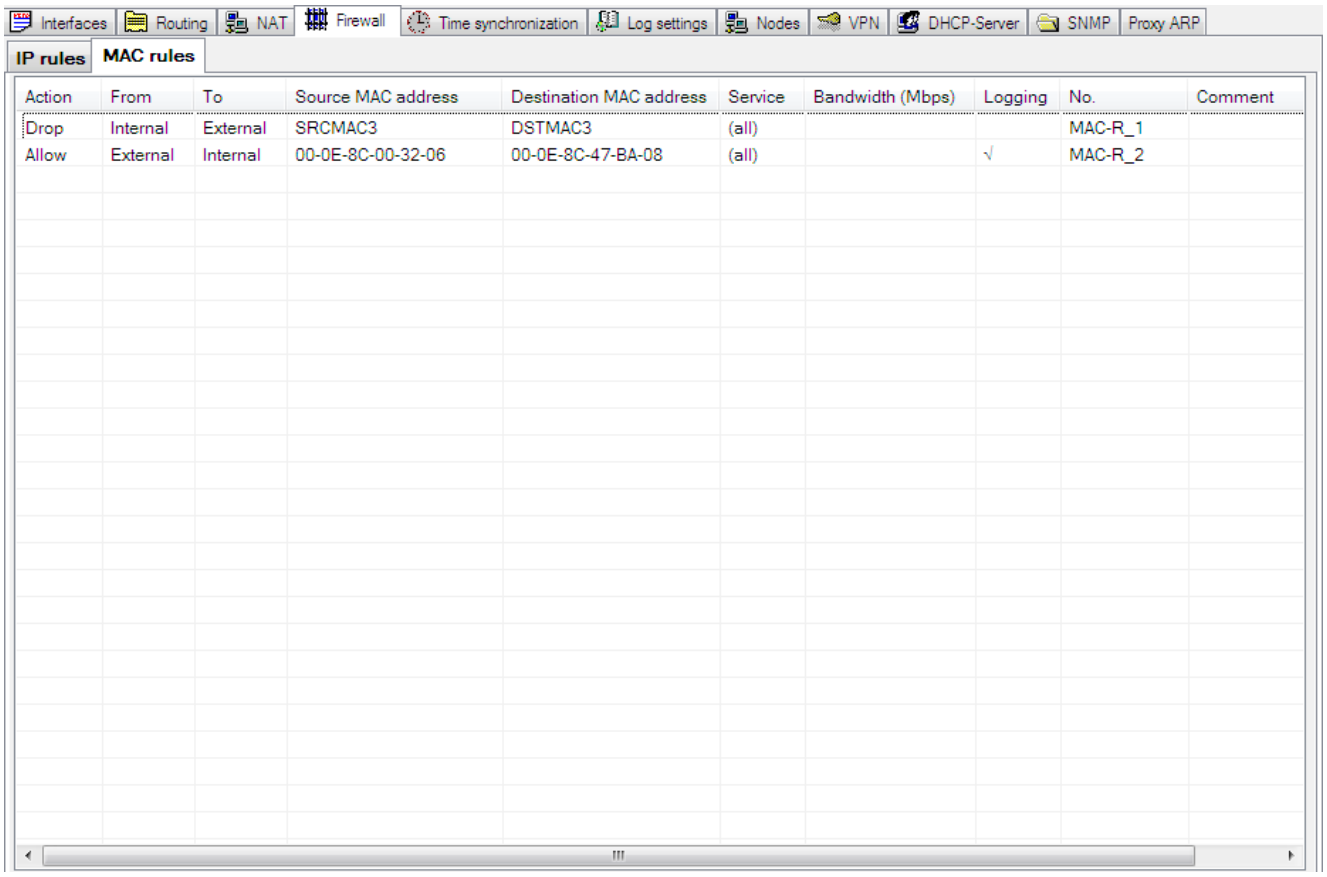
SCA.

If you have enabled the routing mode for the SCALANCE S module, MAC rules are irrelevant.

Dialog / tab

Select the module to be edited.

Select the "Edit" > "Properties..." menu command, "Firewall" > "MAC rules" tab.



Action	From	To	Source MAC address	Destination MAC address	Service	Bandwidth (Mbps)	Logging	No.	Comment
Drop	Internal	External	SRCMAC3	DSTMAC3	(all)			MAC-R_1	
Allow	External	Internal	00-0E-8C-00-32-06	00-0E-8C-47-BA-08	(all)		√	MAC-R_2	

Figure 4-7 "MAC Rules" dialog, based on an example of SCALANCE S602

Entering packet filter rules

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

Using global rule sets

Global rule sets you have assigned to the module are automatically entered in the local rule set. If the rule set appears at the end of the rule list, it is processed with the lowest priority. You can change the priority by changing the position in the rule list.

The online help explains the meaning of the individual buttons.

4.3.10 MAC packet filter rules

MAC packet filter rules are processed based on the following evaluations:

- Parameters entered in the rule;
- Priority of the rule within the rule set.

MAC packet filter rules

The configuration of a MAC rule includes the following parameters:

Table 4- 16 MAC rules: Parameter

Name	Meaning/comment	Available options / ranges of values
Action	Allow/disallow (enable/block)	• Allow Allow frames according to definition. • Drop Block frames according to definition. For automatically created connection rules: • Allow* • Drop* If you select these rules, there is no synchronization with STEP 7. Modified rules are therefore not overwritten in SCT.
From / To	The permitted communications directions.	Are described in the following tables.
Source MAC address	Source address of the MAC packets	As an alternative, you can enter symbolic names.
Destination MAC address	Destination address of the MAC packets	
Service	Name of the MAC service or service group used. "Any" groups together the directions permitted for the individual entry.	The drop-down list box displays the configured services and service groups you can select. No entry means: No service is checked, the rule applies to all services. **Note**: So that the predefined MAC services appear in the drop-down list, select this first in standard mode.

Name	Meaning/comment	Available options / ranges of values
Bandwidth (Mbps)	Option for setting a bandwidth limitation. Can only be entered if the "Allow" action is selected. A packet passes through the firewall if the pass rule matches and the permitted bandwidth for this rule has not yet been exceeded.	CP x43-1 and SCALANCE S ≤ V3.0: 0.001 ... 100 CP 1628 and SCALANCE S ≥ V3.0: 0.001 ... 1000 For global and user-specific rules: 0.001 ... 100
Logging	Enable or disable logging for this rule	
No.	Automatically assigned number for the rule.	
Comment	Space for your own explanation of the rule	If a comment is marked with "AUTO", it was created for an automatic connection rule.

Permitted directions

The following directions can be set:

Table 4- 17 Firewall directions with a CP

Available options / ranges of values		Security module		Meaning
From	To	CP x43-1 Adv.	CP 1628	
External	Station	x	x	Access from the external network to the station.
Station	External	x	x	Access from the station to the external network.
	Tunnel	x	x	Access from the station to the VPN tunnel partner.
Tunnel	Station	x	x	Access via the VPN tunnel partner to the station.

Table 4- 18 Firewall directions with SCALANCE S ≥ V3.0

Available options / ranges of values		Security module		
From	To	S602 V3*	S612 V3**	S623 V3
Internal	External	x	x	x
	Tunnel	-	x	x
	Any	-	x	x
	DMZ	-	-	x
External	Internal	x	x	x
	Any	-	-	x
	Tunnel	-	-	x
	DMZ	-	-	x
Tunnel	Internal	-	x	x
	External	-	x	x

Available options / ranges of values		Security module		
	DMZ	-	-	x
Any	Internal	-	x	x
	External	-	-	x
	DMZ	-	-	x
DMZ	Internal	-	-	x
	External	-	-	x
	Any	-	-	x
	Tunnel	-	-	x

* Also valid for SCALANCE S 602 V2.

** Also valid for SCALANCE S 612 V2 and SCALANCE S 613 V2.

Rule the evaluation by the security module

The packet filter rules are evaluated as follows:

- The list is evaluated from top to bottom; if rules are contradictory, the rule higher in the list is applied.
- The following applies to all frames not explicitly listed for the rules for communication in the direction "Internal -> External" and "External -> Internal": All frames except for the frames explicitly allowed in the list are blocked.
- The following applies to all frames not explicitly listed for the rules for communication in the direction "Internal -> Tunnel" and "Tunnel -> Internal": All frames except for the frames explicitly blocked in the list are allowed.

NOTICE
IP rules apply to IP packets, MAC rules apply to layer 2 packets For the firewall, you can define both IP rules and MAC rules. Rules for editing in the firewall are based on the Ethertype. IP packets are forwarded or blocked depending on the IP rules and layer 2 packets are forwarded or blocked depending on the MAC rules. It is not possible to filter an IP packet using a MAC firewall rule, for example based on a MAC address.

Examples

You can apply the example of an IP packet filter in Section 5.4.3 (Page 109) analogously to the MAC packet filter rules.

4.3.11 defining MAC services

How to access this function

- Using the menu command "Options" > "MAC services".

  or

- From the "MAC Rules" tab with the "MAC services..." button.

Meaning

Using the MAC service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. These services defined in this way can be grouped together under a group name. When you configure the global or local packet filter rules, you use this name.

Parameters for MAC services

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

Table 4- 19 MAC services - parameters

Name	Meaning/comment	Available options / ranges of 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: • ISO ISO identifies frames with the following properties: Lengthfield <= 05DC (hex), DSAP= userdefined SSAP= userdefined CTRL= userdefined • SNAP SNAP identifies frames with the following properties: Lengthfield <= 05DC (hex), DSAP=AA (hex), SSAP=AA (hex), CTRL=03 (hex), OUI=userdefined, OUI-Type=userdefined • PROFINET IO	• ISO • SNAP • PROFINET IO • 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 3 bytes of the MAC address = vendor identification)	

Name	Meaning/comment	Available options / ranges of values
OUI type	Protocol type/identification	
*) The protocol entries 0800 (hex) and 0806 (hex) are not accepted since these values apply to IP or ARP frames.		

Note

Processing for S7-CPs

S7-CP

Only settings for ISO frames with DSAP=SSAP=FE (hex) are processed. Other frame types are not relevant for S7 CPs and are therefore discarded even before processing by the firewall.

Special settings for SIMATIC NET services

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

- DCP (Primary Setup Tool):

  PROFINET
- SiClock :

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

4.3.12 Setting up service groups

Forming 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.

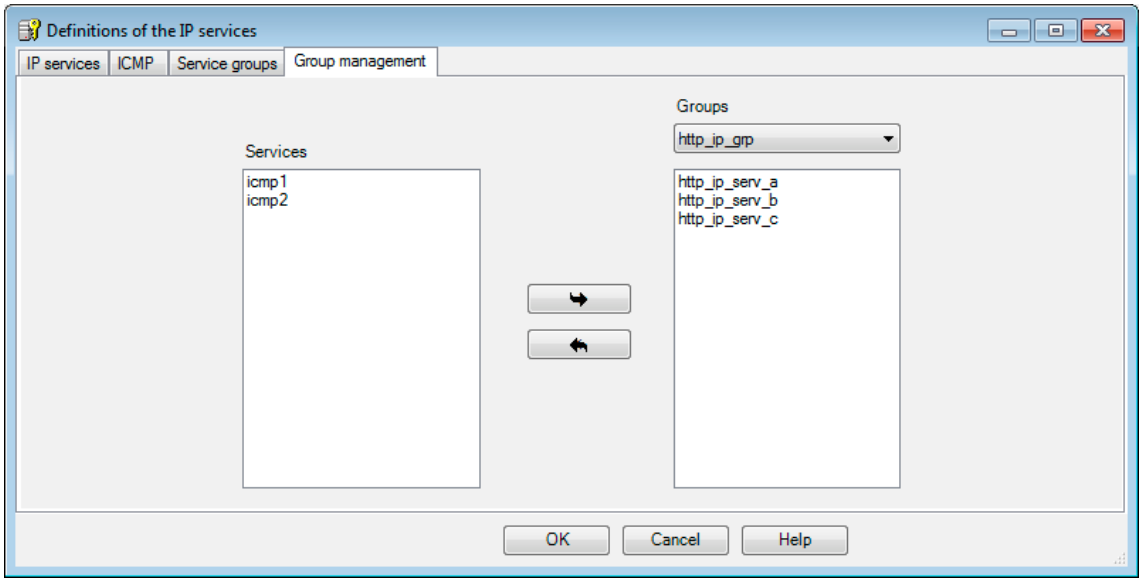
Dialogs / tabs

Open the dialog as follows:

- Using the menu command "Options" > "IP/MAC service definition".

  or

- From the "Firewall/IP rules" tab or "Firewall/MAC rules" with the "IP/MAC services definition..." button.



Configuring additional module properties 5

5.1 Security module as router

5.1.1 Overview

Meaning

By operating the security module as a router, you connect the internal network with the external network. The internal network connected by the security module therefore becomes a separate subnet.

You have the following options:

- Routing - can be set in both standard and advanced mode
- NAT/NAPT routing - can be set in advanced mode

All network queries that do not belong to a subnet are forwarded by a standard router to a different subnet. See section Default router (Page 126).

Enable routing mode - "Interfaces" tab

If you have enabled routing mode, frames intended for an existing IP address in the subnet (internal or external) are forwarded. The firewall rules for the direction of transmission also apply.

For this mode, you configure an internal IP address and an internal subnet mask for addressing the router in the internal subnet in the tab. All network queries that do not belong to a subnet are forwarded by the standard router to a different subnet.

Note: In contrast to the bridge mode of the security module, VLAN tags are lost in routing mode.

1. In the "Interfaces" tab, select the routing mode as interface routing.
2. This activates input boxes in which you enter an internal IP address and an internal subnet mask for addressing the router on the internal subnet.

5.1.2 Default router

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Routing" tab.
3. If you enter the address for the standard router, all routes are directed via this router. If you do not enter an address for the standard router, you can enter several specific routes.
4. Click the "Add route" button.
5. Enter the following values:

Parameter	Function	Example of a value
Network ID	Network ID of the subnet: Based on the network ID, the router recognizes whether a target address is inside or outside the subnet. Must not be located in the same subnet as the IP address of the security module.	196.80.96.0
Subnet mask	The subnet mask structures the network and is used to form the subnet ID.	255.255.255.0
Router IP address	IP address of the router Must be located in the same subnet as the IP address of the security module.	196.80.97.1

Application examples

S≥V3.0

- If the IP assignment configured in the "Interfaces" tab is via "PPPoE", no standard router needs to be configured because the standard route is always automatically via the PPPoE interface.
- If the address assignment configured in the "Interfaces" tab is via "Static address" and if the security module is connected to the Internet via a DSL (NAPT) router, the DSL router must be entered as the standard router.

See also

NAT/NAPT routing (Page 127)

5.1.3 NAT/NAPT routing

Requirement

- The "NAT" tab is only displayed if are in advanced mode.

Note

No return to standard mode possible

If you switch to the advanced mode and change the configuration for the current project, you can no longer switch back.

Remedy SCT standalone: You close the project without saving and open it again.

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "NAT" tab.
3. When required, enable address translation according to NAT(Network Address Translation) or NAPT (Network Address Port Translation).
4. Configure the address translation as shown in the following sections.

Address translation with NAT (Network Address Translation)

NAT is protocol for translating addresses between two address spaces. The main task is to translate private addresses into public addresses; in other words into IP addresses that are used and even routed in the Internet. As a result, the addresses of the internal network are not known to the outside in the external network. The internal nodes are only visible in the external network using the external IP address specified in the address translation list (NAT table).

If the external IP address is not the address of the security module and if the internal IP address is unique, this is known as 1:1 NAT. With 1:1 NAT, the internal address is translated to this external address without port translation. Otherwise, n:1 NAT is being used.

Address translation with NAPT (Network Address Port Translation)

The address translation with NAPT changes the target address and the target port to a communication relation.

Frames coming from the external network and intended for the IP address of the security module are translated. If the target port of the frame is identical to one of the values specified in the "External port" column, the security module replaces the target address and the target port as specified in the corresponding row of the NAPT table. With the reply, the security module uses the values for the target address and target port as contained in the initial frame as the source IP address and the source port.

The difference to NAT is that with this protocol ports can also be translated. There is no 1:1 translation of the IP address. There is now only a public IP address that is translated to a series of private IP addresses with the addition of port numbers.

Consistency check - these rules must be adhered to

When assigning addresses, remember the following rules to obtain consistent entries:

Check / rule	Check made	
	locally	project-wide
In the "Interfaces" tab, the network ID of the internal subnet must differ from the network ID of the external subnet.		x
The internal IP addresses must not be identical to the IP addresses of the module.		x
Use the part specified by the subnet mask for the IP addresses: • The external IP address must be in the same subnet range as the external IP address of the security module in the "Interfaces" tab. • The internal IP address must be in the same subnet range as the internal IP address of the security module in the "Interfaces" tab.		x
An IP address used in the NAT/NAPT address conversion list must not be a multicast or broadcast address.		x
The standard router must be in one of the two subnets of the security module; in other words, it must match either the external or internal IP address.		x
The external ports assigned for the NAPT translation are in the range > 0 and ≤ 65535. Port 123 (NTP), 443 (HTTPS), 514 (Syslog) and 500+4500 (IPsec) are excluded.	x	
The external IP address of the security module may only be used in the NAT table for the direction "Src-NAT (to external)".	x	
The internal IP address of the security module may only be used in the NAT table and not in the NAPT table.		x
Checking for duplicates in the NAT table An external IP address used in the direction "Dst-NAT (from external)" or "Src-NAT +Dst-NAT (external)" may only occur once in the NAT table.	x	
Checking for duplicates in the NAPT table • An external port number may only be entered once. Since the IP address of the security module is always used as the external IP address, multiple use would lead to ambiguities. • The port numbers or port ranges of the external ports must not overlap.	x	
As soon as the routing mode is enabled, the second addresses (IP/subnet) must be assigned to the security module.	x	
Internal NAPT ports can be in the range > 0 and ≤ 65535.	x	

Once you have completed your entries, run a consistency check.

Select the "Options" > "Consistency checks" menu command.

See also

Default router (Page 126)

5.1.4 Address translation with NAT/NAPT

Enabling NAT

The input boxes for NAT are enabled. NAT address conversions only take effect with the option described below and with entries in the address conversion list. You must also configure the firewall accordingly.

The IP address translation can take place via the following interfaces:

- External: The address translation takes place at the external port

The IP address translation can take place in both directions:

- Destination NAT (Dst-NAT): The IP address translation takes place from external to internal. Frames coming from the external subnet are checked for the specified external IP address and forwarded with the specified internal IP address into the internal network. Access from external to internal via the external address is possible.
- Source NAT (Src-NAT): The IP address translation takes place from internal to external. Frames coming from the internal subnet are checked for the specified internal IP address and forwarded to the external network with the specified external IP address. Access from internal to external is possible. In the external network, the external address is effective.
- Source and Destination NAT (Src-NAT + Dst-NAT): The IP address translation can take place from internal or external. Access from internal and external is possible. In the external network, the external address is effective.

Input options for address translation at the external port

If the address translation is to take place at the external port, you have the following options.

Translation type "Dst-NAT (from external)"

Box	Possible entries	Meaning
External IP address	• IP address in the external subnet With dynamic address assignment, this type of translation does not work.	Destination IP address in the external network via which an IP address in the internal subnet will be accessed. If the destination address in a frame matches the address entered, the address is replaced by the corresponding internal IP address. If the address entered here is not the IP address of the security module, this becomes an alias address. This means that the specified address is also registered as the address at the selected port. Make sure that no IP address conflict arises with this address.
Internal IP address	• IP address in the internal subnet	The destination IP address is replaced by internal IP address. The address translation is from external to internal.

Translation type "Src-NAT (to external)"

Box	Possible entries	Meaning
External IP address	• IP address in the external subnet • IP address of the security module if the option "Allow all internal nodes access to the outside" is not selected. With dynamic address assignment, no entry is possible.	Entry of the IP address that will be used as the new source IP address. If the address entered here is not the IP address of the security module, this becomes an alias address. This means that the specified address is also registered as the address at the selected port. Make sure that no IP address conflict arises with this address.
Internal IP address	• IP address in the internal subnet	The source IP address of the specified internal node is replaced by the specified external address. The IP address translation is therefore from internal to external.
	• Subnet or IP address range	The source IP addresses from the specified subnet or IP address range are replaced by the external IP address. The source port is replaced. The range is entered separated by a hyphen.

The following function can also be enabled:

- Allow all internal nodes access

  By selecting this option, the internal IP address is translated to the external module IP address for all frames sent from internal to external and an additional port number is assigned by the module. The use of the IP address of the external interface in the "External IP address" column is then no longer permitted.

  This behavior is indicated by an extra row being displayed at the bottom of the NAT table. The symbol "*" in the "internal IP address" column indicates that all frames sent from internal to external will be translated.

  Note: Due to this effect on the address translation list, this option is assigned to the NAT group box despite the additional assignment of a port number.

Translation type "Src-NAT + Dst-NAT (external)"

Box	Possible entries	Meaning
External IP address	• IP address in the external subnet With dynamic address assignment, this type of translation does not work.	The address translation is from internal to external: See table "Translation type Dst-NAT (from external)" The address translation is from external to internal: See table "Translation type Src-NAT (to external)"
Internal IP address	• IP address in the internal subnet	

Enabling NAPT

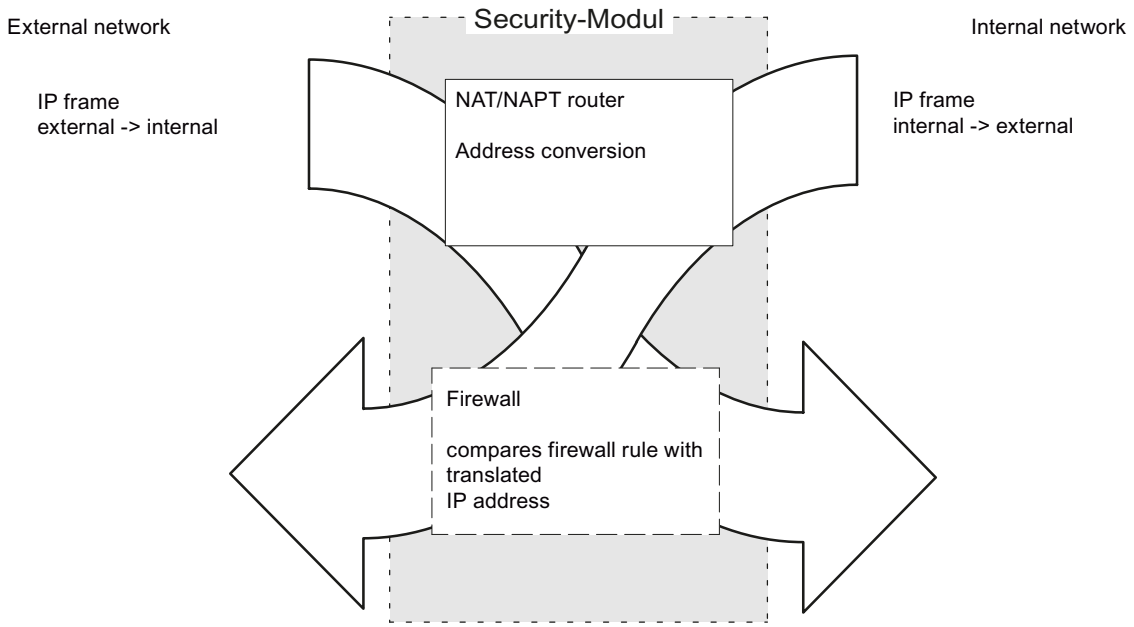
The input boxes for NAPT are enabled. NAPT translations only take effect with the option described below and with entries in the list. You must also configure the firewall accordingly (see examples).

Box	Possible entries	Meaning
External port	Port or port range Example of entering a port range: 78:99	A node in the external network can send a frame to a node in the internal subnet by using this port number.
Internal IP address	See section "IP addresses in IP packet filter rules". As an alternative, you can enter symbolic names.	IP address of the addressed node in the internal subnet.
Internal port	Port	Port number of a node in the internal subnet.

5.1.5 Relationship between NAT/NAPT router and firewall

Relationship between NAT/NAPT router and firewall

Network Address Translation (NAT) changes the IP addresses and possibly also the port numbers in IP frames. The addresses are changed before the firewall filters the frames; in other words, the IP addresses and possibly also the port numbers are changed before there is any filtering.



NOTICE
Matching NAT/NAPT settings and firewall rules Match up the settings for the NAT/NAPT router and the firewall rules so that frames with a translated address can pass through the firewall.

Stateful packet inspection

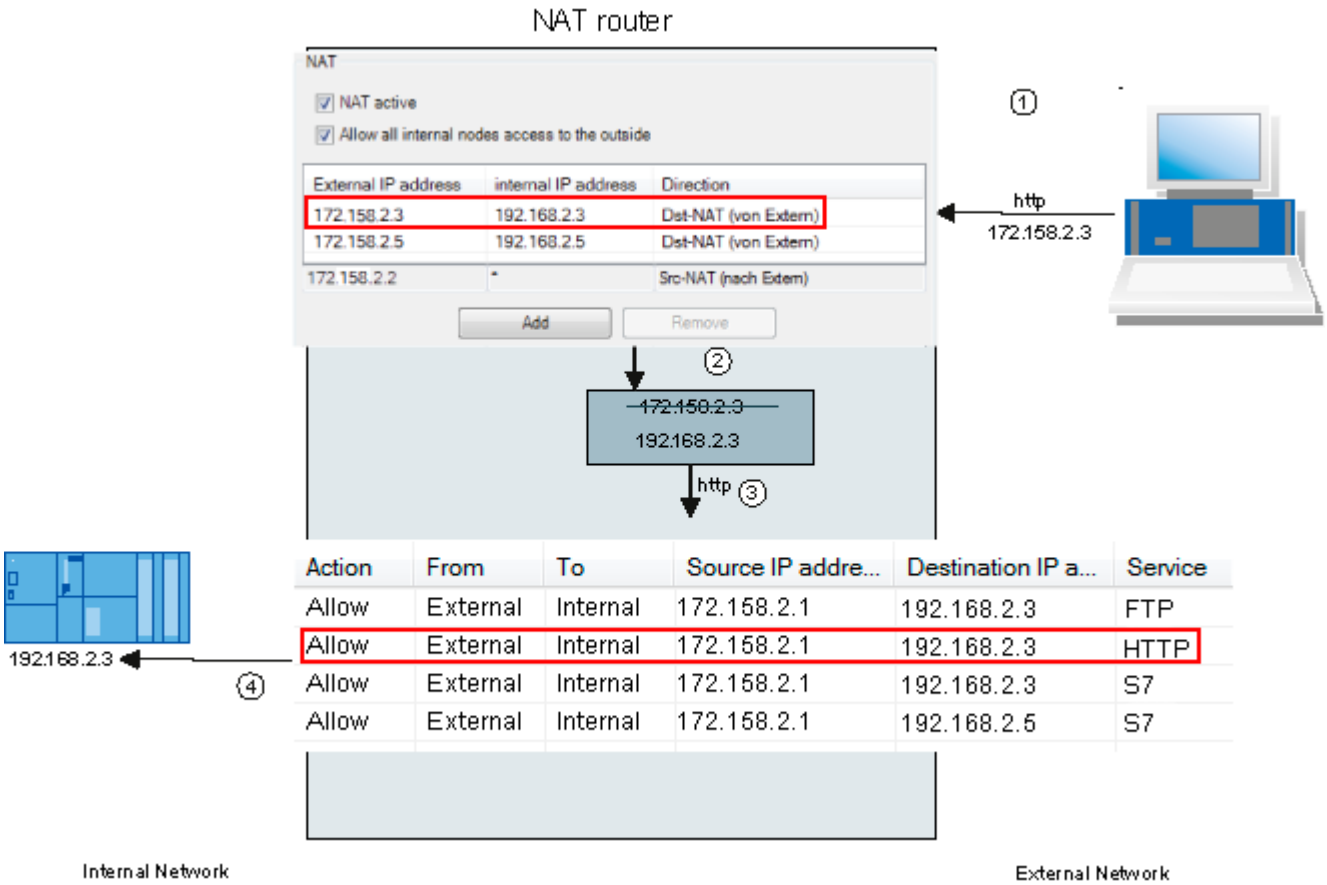
The firewall and NAT/NAPT router supports the "Stateful Packet Inspection" mechanism. As a result, reply frames can pass through the NAT/NAPT router and firewall without it being necessary for their addresses to be included in the firewall rule and the NAT/NAPT address conversion.

5.1.6 1:1 NAT routing - examples of configuration part 1

What does the example show?

The PC with the address 172.158.2.1 will access the controller with address 192.168.2.3 in the internal network. Since the address 192.168.2.3 is not a public address, this must be translated by the NAT router to an additional public address (alias address, here 172.158.2.3). The firewall ensures that the PC can only access the FTP, HTTP and S7 services of the controller.

Schematic sequence of events



NAT translation	Action
①	A device from the external network wants to send a data packet to 172.158.2.3 (HTTP application).
②	The NAT router translates the address based on the NAT table into the private IP address 192.168.2.3
③	The firewall checks how it should handle the data packet. Due to the entry "Allow" > "External" to "Internal" > "192.168.2.3" > "HTTP", all data packets coming from the PG via port 80 and addressed to 192.168.2.3 are allowed to pass.

NAT translation	Action
④	The data packet is directed into the internal network.
⑤	Due to the "Stateful Inspection" function of the firewall, the response frames are forwarded automatically.

5.1.7 NAT/NAPT Routing - examples of configuration part 2

Overview

The section contains the following examples of configuring the NAT/NAPT router:

- **Example 1: NAT address translation "Dst-NAT (from external)"**

  Application example: The internal network is a private subnet. An internal node, for example a CPU 300 as I-device, needs to be accessed. Web diagnostics or downloading of STEP 7 data from the control level needs to be allowed. The S7-300 station must not be able to access the control level.

- **Example 2: NAT address translation "Src-NAT (to external)"**

  Application example: The internal network is a private subnet. The node in the internal network is a device, for example a CPU 300 as I-device that wants to synchronize its time-of-day via an NTP server in the Internet. Web diagnostics or downloading of STEP 7 data from the control level needs to be allowed.

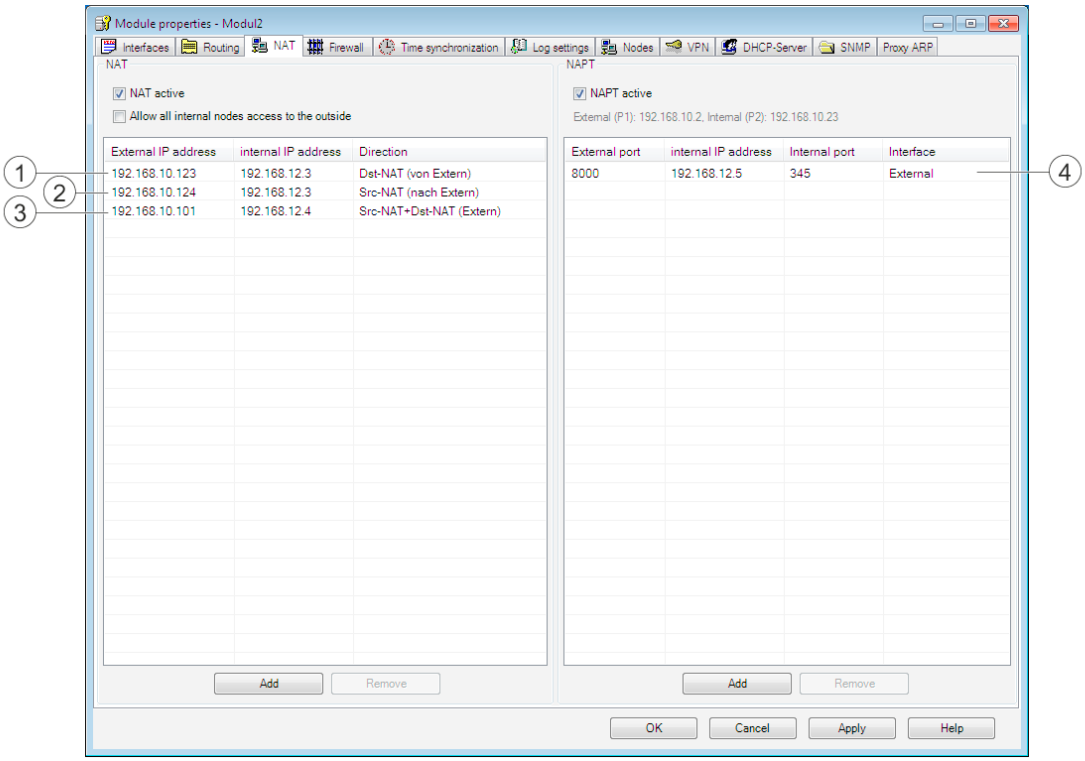
- **Example 3: NAT address translation "Src-NAT + Dst-NAT (external)"**

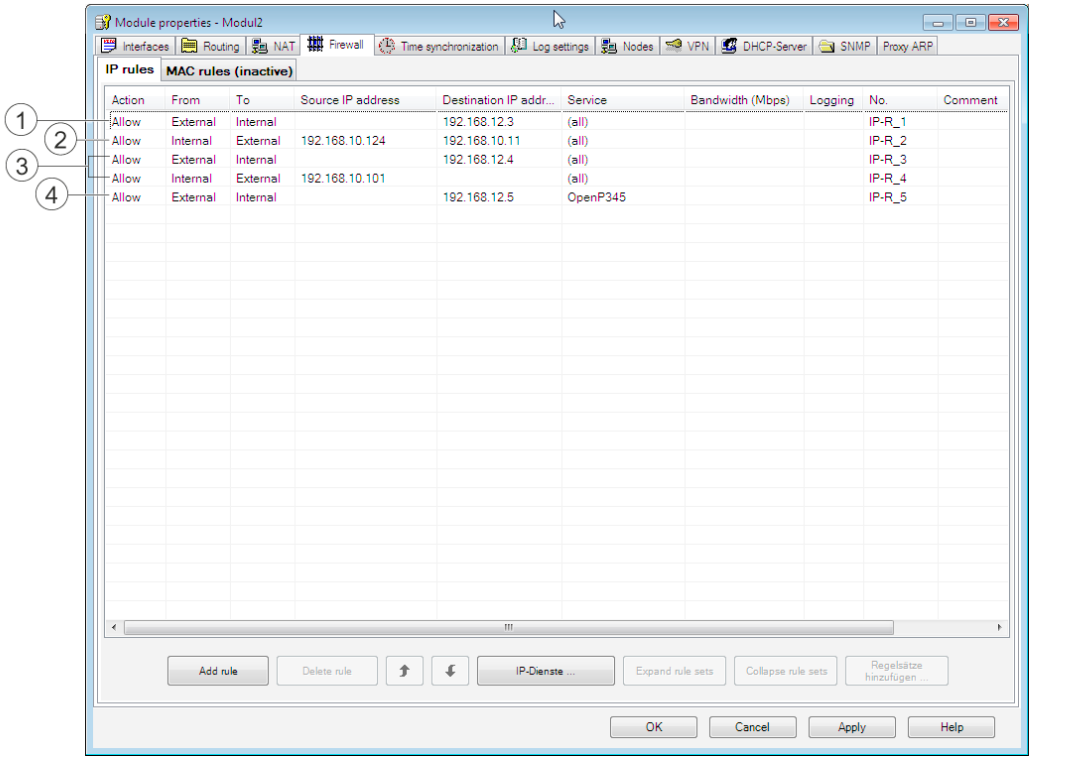
  Application example: The internal network is a private subnet. Access to selected nodes from the control level needs to be allowed. The selected nodes also need to be able to access the control level.

- Example 4: NAPT address conversion

Project engineering

In the following routing configurations, you will find address assignments according to the NAT and NAP address conversion:





Description

- **Example 1: NAT address translation "Dst-NAT (from external)"**

  A node in the external network can communicate with the node with the internal IP address 192.168.12.3 in the internal subnet by using the external IP address 192.168.10.123 as destination address.

- **Example 2: NAT address translation "Src-NAT (to external)"**

  Frames of an internal node with the internal IP address 192.168.12.3 are forwarded to the external network with the external IP address 192.168.10.124 as the source address. The firewall is set so that communication with the source IP address 192.168.10.124 from internal to external is allowed and can communicate with the node with

  IP address 192.168.10.11.

- **Example 3: NAT address translation "Src-NAT + Dst-NAT (external)"**

  In this example, the address conversion is made both for internal and external incoming frames as follows:

  – A node in the external network can communicate with the node with the internal IP address 192.168.12.4 in the internal subnet by using the external IP address 192.168.10.101 as destination address.

  – Frames of an internal node with the internal IP address 192.168.12.4 are forwarded on the external network with the external IP address 192.168.10.101 as the source address. The firewall is set so that frames with the source IP address 192.168.10.101 are allowed from internal to external.

- **Example 4: NAPT address conversion**

  Addresses are translated according to NAPT so that additional port numbers are also assigned. The destination IP address and destination port number of all TCP and UDP frames entering the external network are checked.

  – A node in the external network can send a frame to the node with IP address 192.168.12.5 and port number 345 in the internal subnet by using the external module IP address 192.168.10.1 and the external or number 8000 as the destination address.

5.1.8 NAT/NAPT Routing - examples of configuration part 3

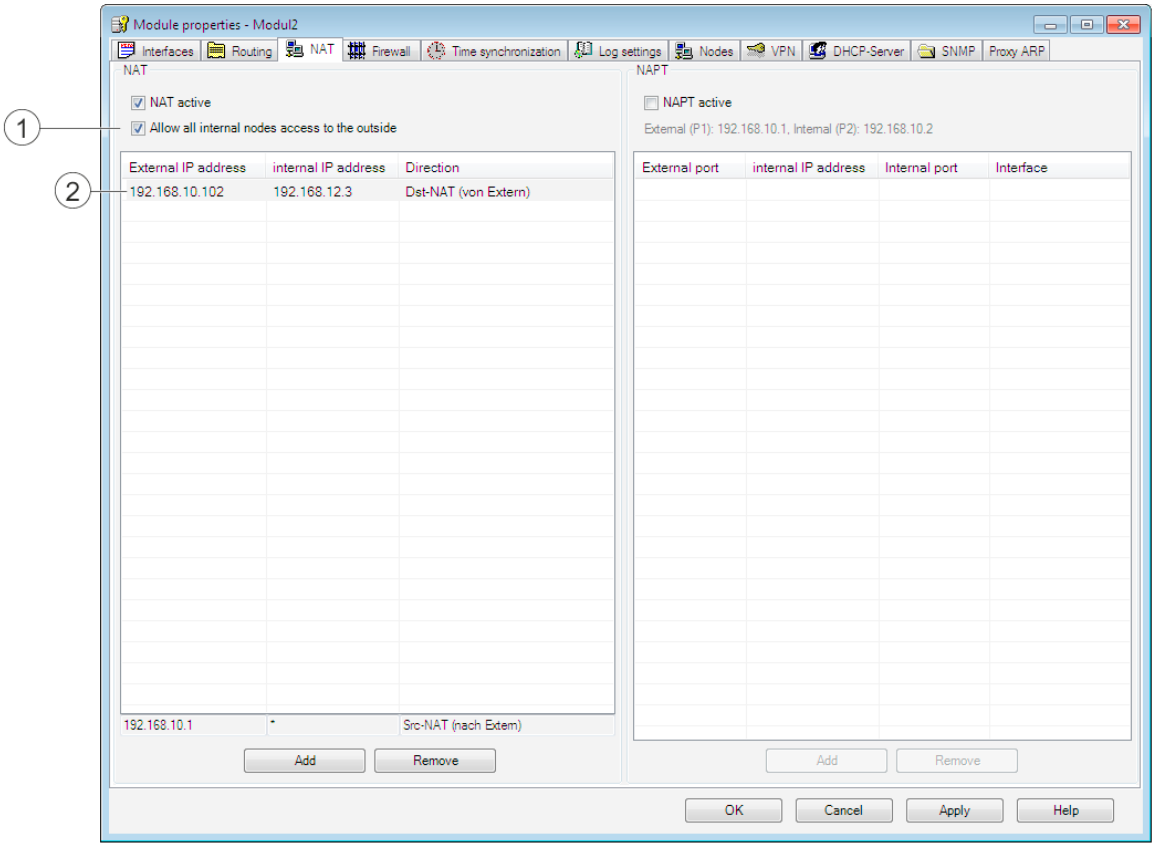
Overview

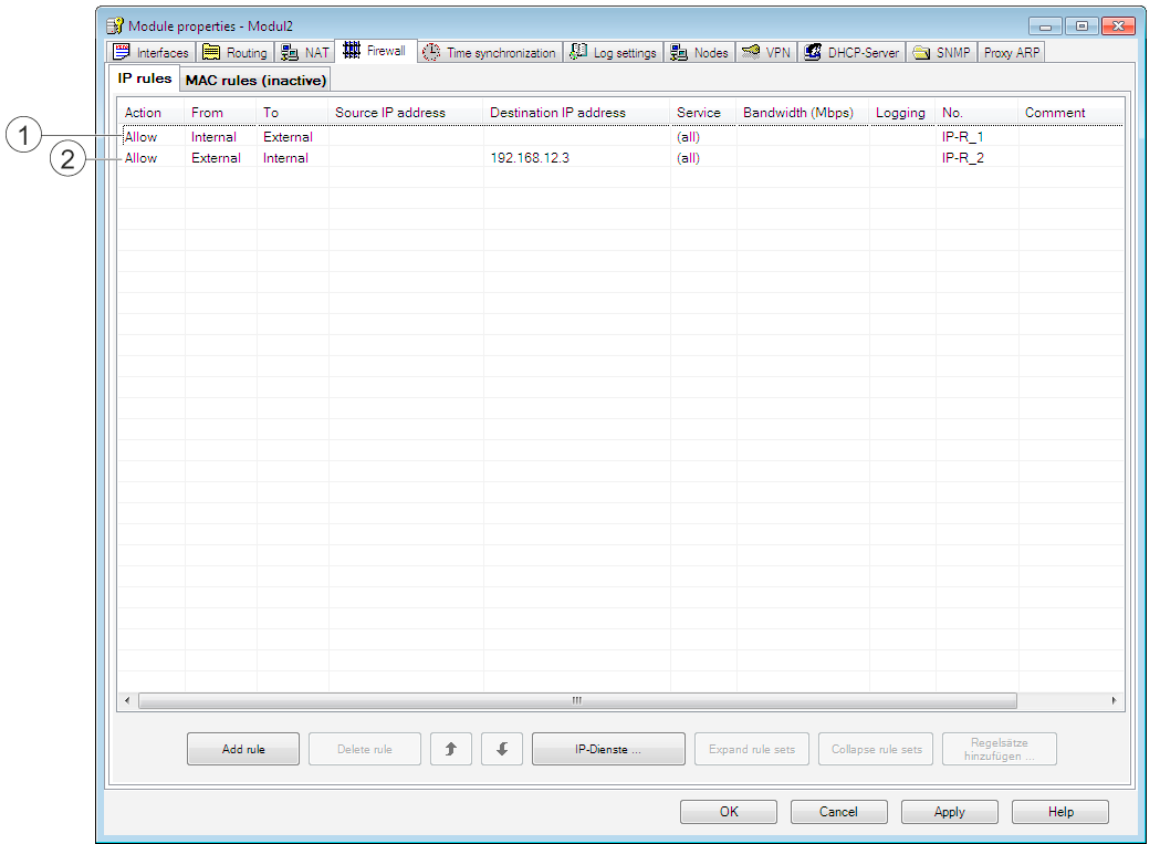
The section contains the following examples of configuring the NAT/NAPT router:

- Example 1: Allow external communication for all internal nodes
- Example 2: Also allow frames from external to internal.

Project engineering

In the following routing configurations, you will find address assignments according to the NAT address conversion:


Module properties - Modul2
Interfaces
Routing
NAT
Firewall
Time synchronization
Log settings
Nodes
VPN
DHCP-Server
SNMP
Proxy ARP
NAT
NAT active
Allow all internal nodes access to the outside
External IP address
internal IP address
Direction
192.168.10.102
192.168.12.3
Dst-NAT (von Extern)
192.168.10.1
*
Src-NAT (nach Extern)
Add
Remove
NAPT
NAPT active
External (P1): 192.168.10.1, Internal (P2): 192.168.10.2
External port
internal IP address
Internal port
Interface
Add
Remove
OK
Cancel
Apply
Help
1
2


Module properties - Modul2
Interfaces
Routing
NAT
Firewall
Time synchronization
Log settings
Nodes
VPN
DHCP-Server
SNMP
Proxy ARP
IP rules
MAC rules (inactive)
Action
From
To
Source IP address
Destination IP address
Service
Bandwidth (Mbps)
Logging
No.
Comment
Allow
Internal
External
(all)
IP-R_1
Allow
External
Internal
192.168.12.3
(all)
IP-R_2
Add rule
Delete rule
IP-Dienste ...
Expand rule sets
Collapse rule sets
Regelsätze hinzufügen ...
OK
Cancel
Apply
Help
1
2

Description

Example 1 - Allow external communication for all internal nodes

The "Allow all internal nodes access to the outside" check box is selected in the "NAT" group box.

This makes communication from internal to external possible. The address translation works so that all internal addresses are translated to the external IP address of the security module and a dynamically assigned port number.

Specifying a direction in the NAT address conversion list is now no longer relevant. All the other information relates to the communication direction external to internal.

The firewall is set so that the frames can pass from internal to external.

Example 2 - Also allow frames from external to internal.

To also allow communication from external to internal over and above the communication in example 1, entries must be made in the NAT or NAPT address conversion list. The entry in the example, means that frames to the node with IP address 192.168.10.102 will be translated to the internal IP address 192.168.12.3.

The firewall must be set accordingly. Since the NAT/NAPT translation is always made first and the translated address is then tested in a second step in the firewall, the internal IP address is entered as the destination IP address in the firewall in our example.

5.2 Security module as DHCP server

5.2.1 Overview

Overview

You can operate the security module on the internal network as a DHCP server (DHCP = Dynamic Host Configuration Protocol). This allows IP addresses to be assigned automatically to the devices connected to the internal network.

The IP addresses are either distributed dynamically from an address band you have specified or you can select a specific IP address and assign it to a particular device.

DHCP server for DMZ

S623

To be able to assign a dynamic IP address to devices in the DMZ as well, a DHCP server can be activated on the DMZ port. So that the devices in the DMZ always receive the same IP address for the firewall configuration, the address assignment must be static based on the MAC address or the client ID.

Requirement

You configure the devices in the internal network so that they obtain the IP address from a DHCP server.

Depending on the mode, the security module informs the nodes in the subnet of an IP address of the standard router or you make a router IP address known to the nodes in the subnet.

- Router IP address will be transferred

  In the following situations, the DHCP protocol of the security module will inform the nodes of the router IP address:

  – The security module is configured for router mode;

    In this case, the security module sends its own IP address as the router IP address.

  – The security module is not configured for router mode but a default router is specified in the configuration of the security module;

    In this case, the security module sends the IP address of the default router as the router IP address.

- Router IP address will not be transferred

  In the following situations, enter the router IP address manually on the nodes:

  – The security module is not configured for router mode;

  – No default router is specified in the configuration of the security module.

See also

Consistency checks (Page 47)

5.2.2 Configuring a DHCP server

Requirement

The "DHCP server" tab is only displayed if you have activated advanced mode.

Note

No return to standard mode possible

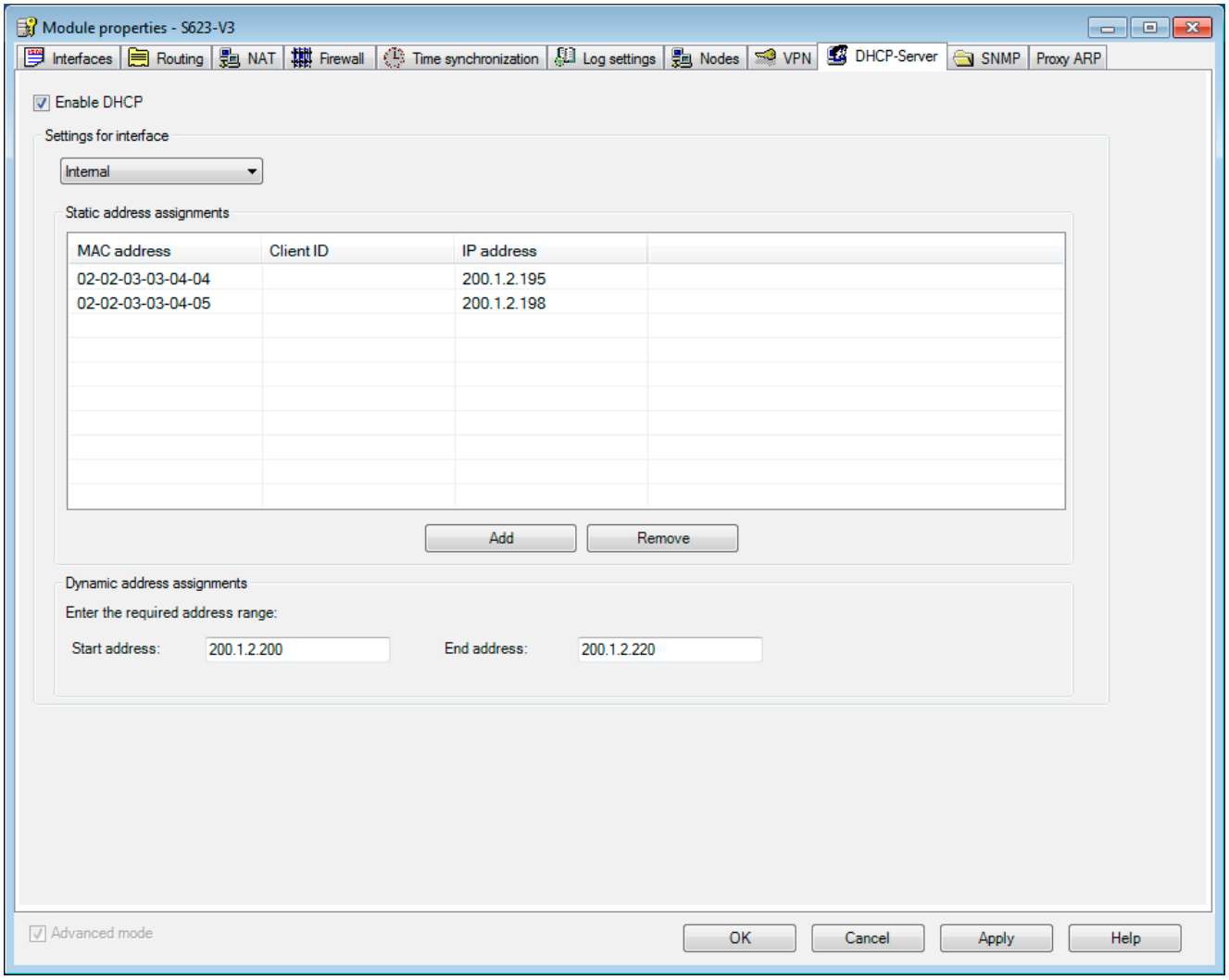
If you switch to the advanced mode and change the configuration for the current project, you can no longer switch back.

Remedy SCT standalone: You close the project without saving and open it again.

How to access this function

1. Select the module to be edited.

2. Select the "Edit" > "Properties..." menu command, "DHCP server" tab.



3. Select the "Enable DHCP" check box.
4. Select the interface for which you want to make the DHCP settings.
5. Make the address assignment. You have the following configuration options:

- Static address assignment

  Devices with a specific MAC address or client ID are assigned the specified IP addresses. You specify these addresses by entering the devices in the address list in the "Static address assignments" group box.

- Dynamic address assignment

  Devices whose MAC address or whose client ID was not specified specifically, are assigned a random IP address from a specified address range. You set this address range in the "Dynamic address assignments" group box.

NOTICE
Dynamic address assignment - reaction after interrupting the power supply Please note that dynamically assigned IP addresses are not saved if the power supply is interrupted. On return of the power, you must therefore make sure that the nodes request an IP address again. You should therefore only use dynamic address assignment for the following nodes: • Nodes that are used temporarily in the subnet (such as service devices); • Nodes that have been assigned an IP address and send this as the "preferred address" the next time they request an address from the DHCP server (for example PC stations). For nodes in permanent operation, use of a static address assignment by specifying a client ID should be preferred (recommended for S7-CPs because it is simpler to replace modules) or the MAC address.

Symbolic names are supported

You can also enter the IP or MAC addresses as symbolic names in the function described here.

Consistency check - these rules must be adhered to

Remember the following rules when making the entries.

Check / rule	Check made[1)]	
	locally	Project-/module-wide
The IP addresses assigned in the address list in the "Static address assignments" group box must not be in the range of the dynamic IP addresses.		x
Symbolic names must have a numeric address assignment. If you assign symbolic names for the first time here, you must still make the address assignment in the "Symbolic names" dialog.		x
IP addresses, MAC addresses and client IDs may only occur once in the "Static IP addresses" table (related to the security module).		x
For the statically assigned IP addresses, you must specify either the MAC address or the client ID (computer name).	x	

Check / rule	Check made[1]	
	locally	Project-/module-wide
The client ID is a string with a maximum of 63 characters. Only the following characters may be used: a-z, A-Z, 0-9 and - (dash). Note In SIMATIC S7, a client ID can be assigned to the devices on the Ethernet interface to allow them to obtain an IP address using DHCP. With PCs, the procedure depends on the operating system being used; it is advisable to use the MAC address here for the assignment.	x	
For the statically assigned IP addresses, you must specify the IP address.	x	
The following IP addresses must not be in the range of the free IP address range (dynamic IP addresses): • All router addresses in the "Routing" tab • NTP server • Syslog server • Default router • Security module address(es)		x
DHCP is supported by the security module on the interface to the internal subnet. The following additional requirements for IP addresses in the range of the free IP address range (dynamic IP addresses) result from operational behavior of the security module: • Bridge mode The free IP address range must be in the network defined by the security module. • Routing mode The free IP address range must be in the internal subnet defined by the security module.		x
The free IP address range must be fully specified by entering the start IP address and the end IP address. The end IP address must be higher than the start IP address.	x	
The IP addresses you enter in the address list in the "Static address assignments" group box must be in the address range of the internal subnet of the security module.		x

Legend:

[1] Note the explanations in the section Consistency checks (Page 47).

5.3 Time synchronization

5.3.1 Overview

Meaning

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

The following alternatives can be configured:

- The module time is set automatically to the PC time when a configuration is downloaded. SCA.
- Automatic setting and periodic synchronization of the time using a Network Time Protocol server (NTP server).

Note

Time-of-day synchronization relates solely to the security module and cannot be used to synchronize devices in the internal network of the security module.

Synchronization by an NTP server

NOTICE
Allowing frames explicitly If the NTP server cannot be reached by the security module, you will need to allow the frames from the NTP server explicitly in the firewall (UDP, port 123).

The following rules apply when creating the NTP server:

- NTP servers can be created throughout project using the SCT menu "Options" > "Definition of the NTP servers". On the properties tab "Time-of-day synchronization" assign an NTP server to a security module. If different security modules in the SCT project use the same NTP server, its data only needs to be entered once.
- You can create 32 NTP servers throughout the project.
- You can assign a maximum of 4 NTP servers to one security module.
- Symbolic names for the IP address of the NTP server are not supported.
- The IP address and the update interval of NTP servers already created in STEP 7 are migrated to SCT. CP
- If you select "NTP (secure)", the security module only accepts the time from suitably configured secure NTP servers. A mixed configuration of non-secure and secure NTP servers on a security module is not possible. CP

5.3.2 Configuring time keeping

How to access this function

Menu command SCT: "Options" > "Definition of the NTP servers...".

Menu command STEP 7 (if the option " Activate NTP time-of-day synchronization" is enabled): "Time-of-day synchronization" > " Activate NTP time-of-day synchronization", "Run" button.

Alternatives for time synchronization

The following alternatives can be configured:

Table 5- 1 Time synchronization for CPs

Possible selection	Meaning / effect
No time synchronization	No time synchronization via a PC or an NTP server.
Time-of-day synchronization with NTP	Automatic setting and periodic synchronization of the time using an NTP server.
Time synchronization using NTP (secured)	Automatic setting and periodic synchronization of the time using a suitably configured NTP server.

Table 5- 2 Time synchronization for SCALANCE S ≥ V3.0

Possible selection	Meaning / effect
No time synchronization	No time synchronization via a PC or an NTP server.
Set time with each download	The module time is set automatically to the PC time when a configuration is downloaded.
Time-of-day synchronization with NTP	Automatic setting of the time using an NTP server.

Selecting the mode of time-of-day synchronization

Follow these steps:

1. Select the synchronization mode.

2. For SCALANCE S < V3.0: For synchronization by an NTP server, enter the update interval in seconds. For SCALANCE S ≥ V3.0, the time interval for querying the NTP server is specified automatically.

   Note

   CP

   NTP servers created in STEP 7 are automatically migrated to SCT with the update interval. The update interval can only be changed in STEP 7.

3. Using the "Add" button, assign the security module an existing NTP server of the same type as selected in the "Synchronization mode" box.

   If no NTP servers exist yet, create an NTP server with the "NTP server..." button.

5.3.3 Adding an entry

Adding an NTP server to the NTP list

Click the "Add..." button to create a new server.

Editing the NTP server from the NTP list

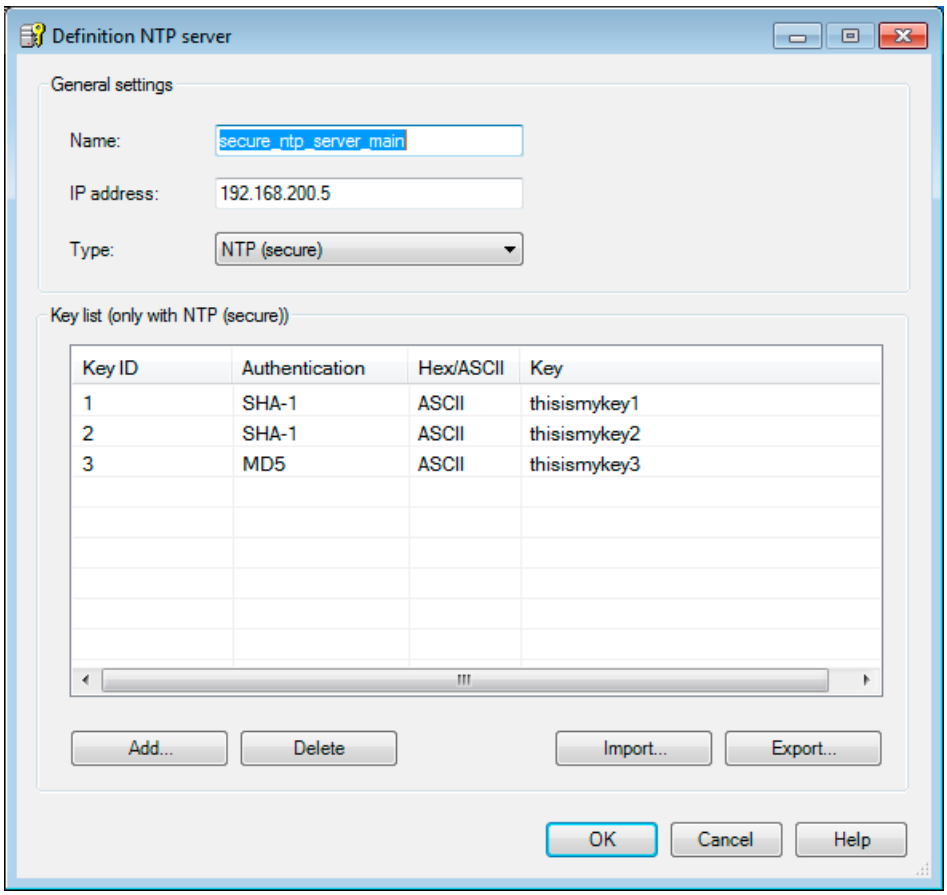
Click the "Properties..." button to edit an existing server.

Result: The "Definition NTP server" dialog opens.

5.3.4 Defining an NTP server

How to define a new NTP server:

1. Enter a name for the NTP server.



2. Enter the IP address of the NTP server.
3. Select the Type.

Settings for NTP (secure)

CP

1. Click the "Add" button.
2. Enter the following data:

Property	Meaning
Key ID	Numeric value between 1 and 65534.
Authentication	Select the authentication algorithm.
Hex/ASCII	Select the format for the NTP key.
Key	Enter the NTP key with the following lengths: Hex: 22 ... 40 characters ASCII: 11 ... 20 characters
Delete	Use the button to delete the selected entry.

Importing/exporting NTP servers

Using the "Import" or "Export" buttons, you can export the key list of the currently displayed NTP server and import the file into an NTP server or vice versa.

5.4 SNMP

5.4.1 Overview

What is SNMP?

The security module supports the transfer of management information using the Simple Network Management Protocol (SNMP). To allow this, an SNMP agent is installed on the security module that receives and responds to SNMP queries. The information on the properties of SNMPcompliant devices is entered in MIB files (MIB = Management Information Base) for which the user must have the required rights.

In SNMPv1, the "community string" is also sent. The "community string" is like a password that is sent along with the SNMP query. If the community string is correct, the security module replies with the required information. If the string is incorrect, the security module discards the query and does not reply.

In SNMPv3, the data can be transferred encrypted.

5.4.2 Enabling SNMP

Requirement

- The "SNMP" tab is only displayed if you have activated advanced mode.

  Note
  No return to standard mode possible

  If you switch to the advanced mode and change the configuration for the current project, you can no longer switch back.

  Remedy SCT standalone: You close the project without saving and open it again.

- STEP 7: In the "SNMP" tab, the "Enable SNMP" check box is selected. CP

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "SNMP" tab.
3. For SCALANCE S: Select the "Enable SNMP" check box.
4. Select one of the following SNMP protocol versions:

- SNMPv1

  The security module uses the following default values for the community strings to control the access rights in the SNMP agent:

  – For read access: public
  – For read and write access: private

  Note
  Overwriting the default values for the community strings

  To increase security, overwrite the default values of the community string with a new name.

  To enable write access using SNMP, select the option "Allow write access via community string: "private"".

- SNMPv3

  Select either an authentication method or an authentication and encryption method.

  – Authentication algorithm: none, MD5, SHA-1
  – Encryption algorithm: none, AES-128, DES

1. Assign a role to the user for which the suitable SNMP rights are enabled. You will find an overview of SNMP rights in the section Managing rights (Page 56).

5.5 Proxy ARP

S≥V3.0

Overview

Proxy ARP allows routers to respond to ARP queries for hosts. The hosts are in networks separated by routers but use the same IP address range.

If PC1 sends an ARP request to PC2, it receives a response and the hardware address of the interface (MAC of the port on the router) on which the query was received from the router located in between and not from PC2. The querying PC1 then sends its data to the router that then forwards it to PC2.

How to access this function

Only for internal port and in bridge mode.

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Proxy ARP" tab.
3. If the security module is to respond to an ARP query from its own LAN as a substitute for the specific connection partner, enter the corresponding IP address.

Secure communication in the VPN via an IPsec tunnel

6

In this section, you will learn how to connect IP subnets protected by the security module by dragging them to a VPN (Virtual Private Network).

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

Further information

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.

See also

Online functions - test, diagnostics, and logging (Page 193)

6.1 VPN with security modules

Secure connection through an unprotected network

For security modules that protect the internal network, IPsec tunnels provide a secure data connection through the non-secure external network.

Due to the data exchange via IPsec, the following security aspects are implemented for the communication.

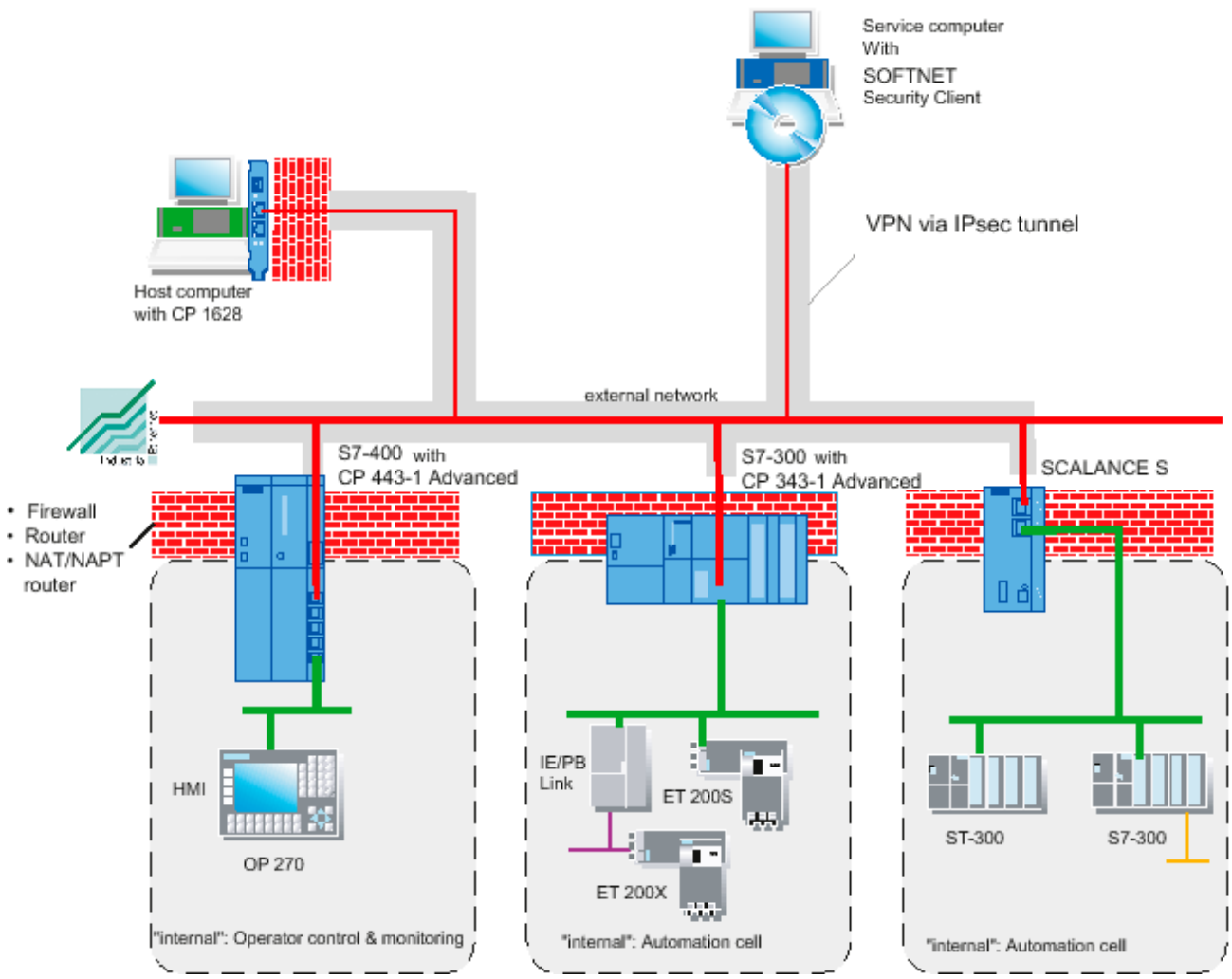
- Confidentiality

  Makes sure that the data is transferred encrypted.
- Integrity

  Makes sure that the data has not been changed.
- Authenticity

  Makes sure that the VPN endpoints are also trustworthy.

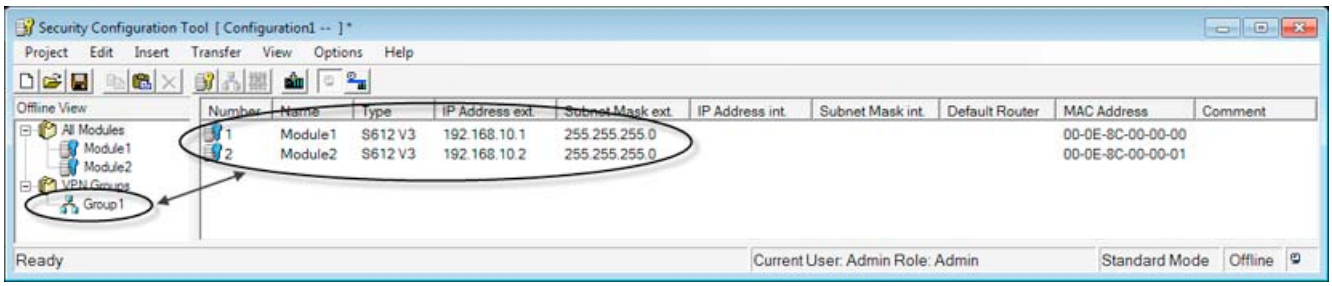
The security module uses the IPsec protocol for tunneling (tunnel mode of IPsec).



Tunnel connections exist between modules in the same group (VPN)

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

IPsec tunnels are established automatically between all security modules and SOFTNET Security Client modules that belong to the same group. A security module can belong to several different groups at the same time in one project.



NOTICE
If the name of a security module is changed, all the security modules of the groups to which the changed security module belongs must be reconfigured (menu command "Transfer" > "To all modules...").
If the name of a group is changed, all security modules of this group must be reconfigured in (menu command "Transfer" > "To all modules...").

NOTICE
Layer 2 frames are also tunneled when there is a router between two security modules. To make this possible, however, the MAC addresses of the communications partners must be configured statically in the Security Configuration Tool and, where necessary, static ARP entries must be entered on the communications devices.
The following applies in general: Non-IP frames are transferred through a tunnel only when the devices that send or receive the frames were able to communicate previously; in other words, without using the security modules.

6.2 Authentication methods

Authentication methods

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

  Authentication is achieved using a previously agreed character string that is distributed to all modules in the group.

  Enter a password in the "Preshared key" box in the "Group properties" dialog.

- Certificate

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

  – When a group is generated, a group certificate is generated (group certificate = CA certificate).

  – Each security module in the group receives a certificate signed with the key of the group CA.

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

  The certificates are generated by a certification function in the Security Configuration Tool.

NOTICE
Restriction in VLAN operation With IP frames through the VPN tunnel of the security module, no VLAN tagging is transferred. The VLAN tags included in IP frames are lost when they pass through the security modules because IPsec is used to transfer the IP frames. As default, no IP broadcast or IP multicast frames can be transferred with IPsec through a layer 3 VPN tunnel. Through a layer 2 VPN tunnel of the security module, IP broadcast or IP multicast frames are packaged just like MAC packets including the Ethernet header in UDP and transferred. With these packets, the VLAN tagging is therefore retained.

6.3 VPN groups

6.3.1 Modes of VPN groups

VPN modes

Security modules can belong to several VPN groups at the same time and, depending on the security module, can also operate in different modes.

Rules for forming groups

Remember the following rules if you want to create VPN groups:

- For SCALANCE S 612/613

  The first assigned module in a VPN group decides which other modules can be added to it.

  If the first SCALANCE S module added is in routing mode, you can only add other SCALANCE S modules that have routing enabled on them. If the first SCALANCE S module added is in bridge mode, you can only add other SCALANCE S modules in bridge mode. If you want to change the mode of a VPN group, you will have to remove all the modules contained in the group and add them again. A CP can be added to a group with a SCALANCE S in bridge or routing mode.

- For CP and SCALANCE S 623

  If a CP or SCALANCE S 623 is inserted in a VPN group as the first module, the VPN group will be in bridge mode. The next security module inserted decides the group mode. If the security module is in routing mode, only security modules can be then inserted that are also in routing mode.

  A CP or SCALANCE S 623 can be assigned to several VPN groups at the same time and use different modes. The CP or the SCALANCE S 623 is then operated in mixed mode.

- It is not possible to add a SCALANCE M module to a VPN group that contains a module in bridge mode.

Refer to the following table to see which modules can grouped together in a VPN group:

Table 6- 1 Security modules and VPN modes

Module	Can be included in a VPN group in...		
	Bridge mode	Routing mode	Mixed mode
SCALANCE S 612/613 in bridge mode	x	-	-
SCALANCE S 612/613 in routing mode	-	x	-
SCALANCE S 623 in bridge mode	x	x	x
SCALANCE S 623 in routing mode	x	x	x
CP x43 Adv.	x	x	x

Module	Can be included in a VPN group in...		
	Bridge mode	Routing mode	Mixed mode
CP 1628	x	x	x
SOFTNET Security Client 2005	x	-	-
SOFTNET Security Client 2008	x	x	-
SOFTNET Security Client V3.0	x	x	-
SOFTNET Security Client V4.0	x	x	x
SCALANCE M	-	x	-

6.3.2 Creating groups and assigning modules

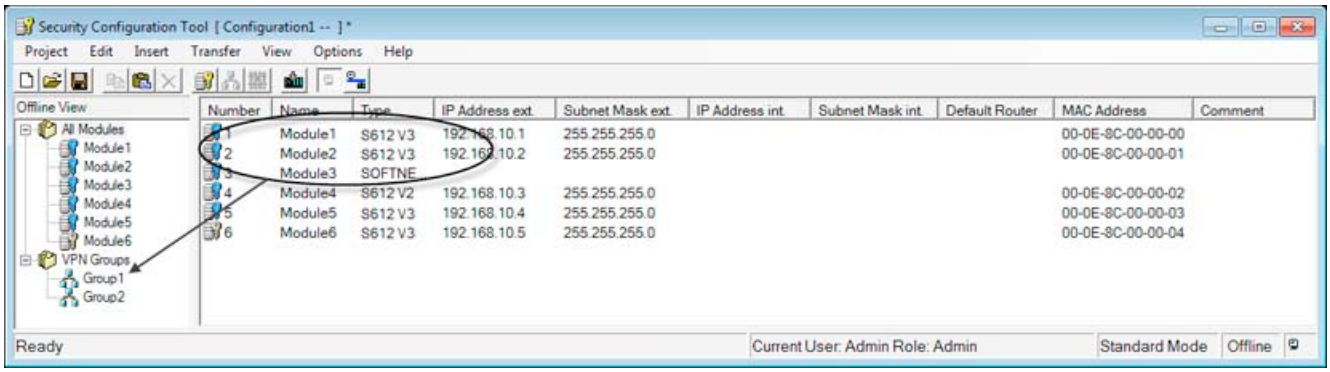
Requirement

NOTICE
Current date and current time of day on the security modules When using secure communication (for example HTTPS, VPN...), make sure that the security modules involved have the current time of day and the current date. Otherwise the certificates used will not be evaluated as valid and the secure communication will not work.

How to access this function

1. Create a group with the "Insert" > "Group" menu command.

2. Assign the security modules and SOFTNET Security Client modules intended for a VPN group to the group. by dragging the module to the required group with the mouse.



Configuring properties

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

- **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.

Note

Setting parameters for SCALANCE M or other VPN clients

To set the parameters for SCALANCE M or other VPN clients, you configure VPN properties for the specific modules in advanced mode.

Displaying all configured groups and their properties

- Select the "VPN groups" object in the navigation area.

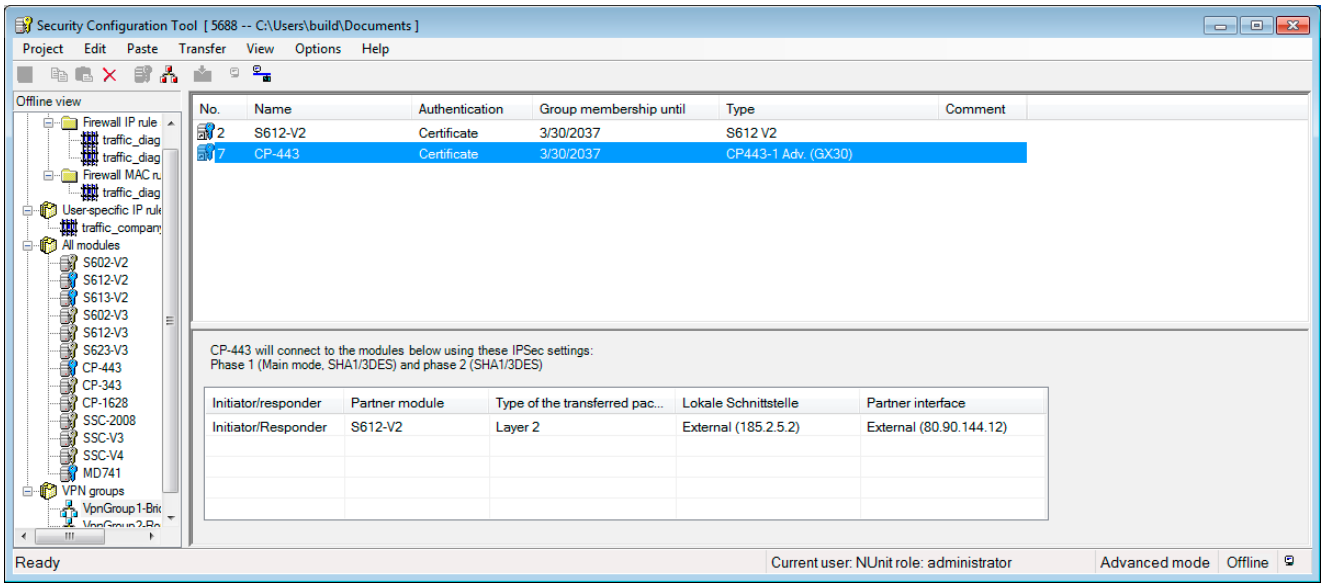
The following properties of the groups are displayed in columns:

Property/column	Meaning	Comment/selection
Group Name	Group Name	Freely selectable
Authentication	Type of authentication	• Preshared key • Certificate
Group membership until...	Life of certificates	See section "Setting the lifetime of certificates"
Comment	Comment	Freely selectable

Displaying and configuring VPN connection details

1. In the navigation area, select the VPN group you want to edit.
2. Click on a module in the content area.

   Result: The preview area displays the other VPN group members to each of which the selected module establishes a VPN connection.
3. Select the interface via which the VPN group members will communicate.



Setting the life of certificates

Open the dialog in which you can set the expiry date of the certificate as follows:

1. In the navigation area, select the VPN group you want to edit.

2. Right-click and select "Properties" in the shortcut menu.

Note

Expiry of a certificate

Communication through the VPN tunnel continues after the certificate has expired until the tunnel is terminated or the SA lifetime expires. For more information on certificates, refer to section Managing certificates (Page 59).

6.4 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 learning mode is active for all modules.

Opening the dialog for displaying default values

1. Select the required group.
2. Select the "Edit" > "Properties" menu command.

The display is identical to the dialog in advanced mode; you cannot, however, change the values.

6.5 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 described in this section, change to advanced mode.

Note

No return to standard mode possible

If you switch to the advanced mode and change the configuration for the current project, you can no longer switch back.

Remedy SCT standalone: You close the project without saving and open it again.

6.5.1 Configuring group properties

Group properties

NOTICE
Knowledge of IPsec necessary 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.

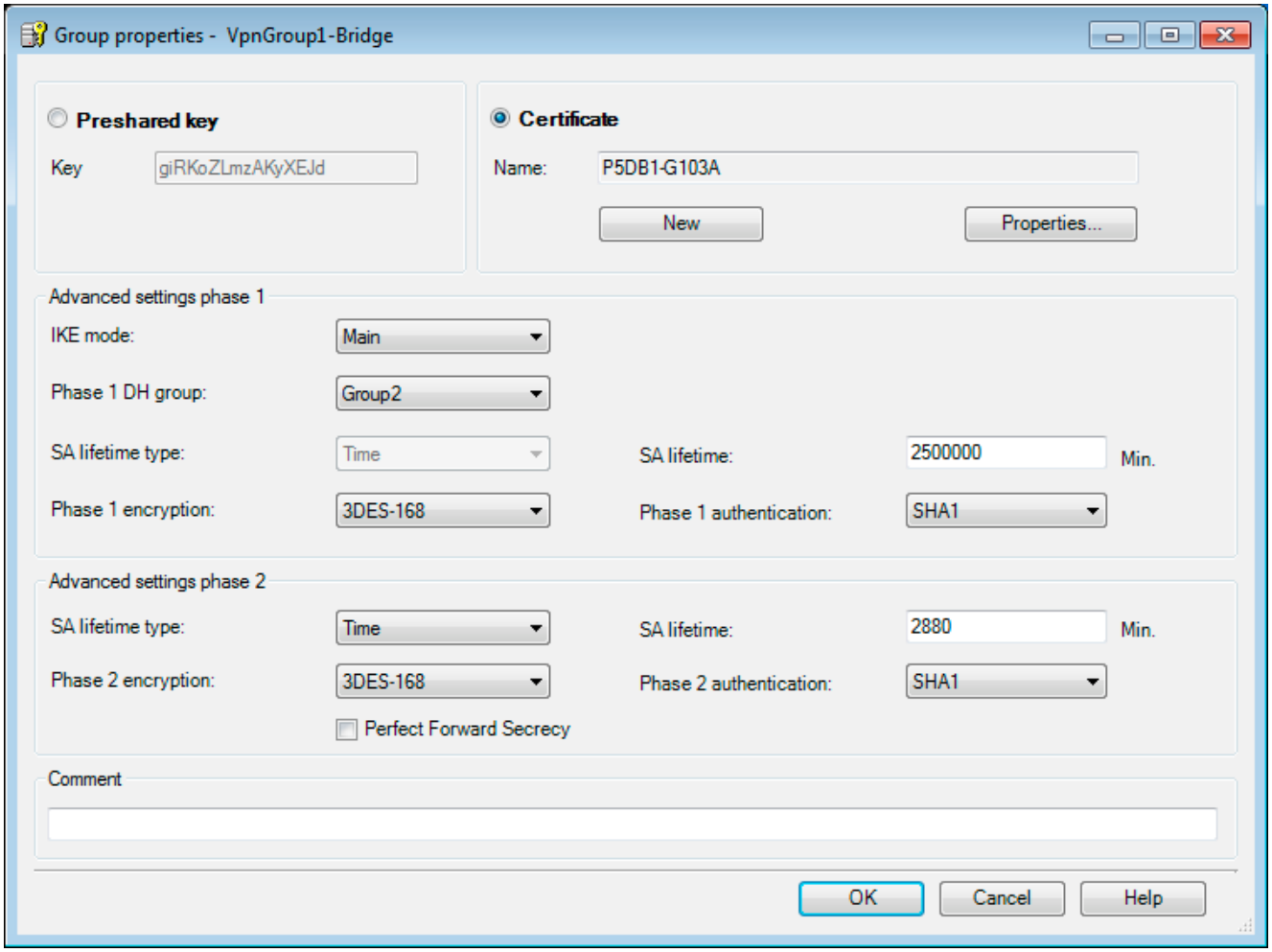
The following group properties can be set in advanced mode:

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

How to access this function

1. In the navigation area, select the VPN group you want to edit.

2. Select the "Edit" > "Properties..." menu command.



3. Select whether a preshared key or certificate will be used for authentication. For more detailed information, refer to section Authentication methods (Page 156).

Parameters for advanced settings phase 1 - IKE settings

Phase 1: Key exchange (IKE = Internet Key Exchange):

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

Parameter	Description
IKE mode	Key exchange method: • Main mode • Aggressive mode 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	Diffie-Hellman key agreement: • Group 1 • Group 2 • Group 5 Diffie-Hellman groups (selectable cryptographic algorithms in the Oakley key exchange protocol).
SA lifetime type	Phase 1 Security Association (SA): • Time: Time limit in minutes The lifetime of the current key material is limited in time. When the time expires, the key material is renegotiated.
SA lifetime	Numeric value: Range of values for time: 1440 ... 2500000 minutes (default: 2500000)
Phase 1 encryption	Encryption algorithm: • DES: Data Encryption Standard (56 bit key length, mode CBC) • 3DES-168: Triple DES (168-bit key length, mode CBC) • AES-128, 192, 256: Advanced Encryption Standard (128-bit, 192-bit or 256-bit key length, mode CBC)
Phase 1 authentication	Authentication algorithm;: • MD5: Message Digest Algorithm 5 • SHA1: Secure Hash Algorithm 1

Parameters for advanced settings phase 2 - IPsec settings

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

Here, you set the parameters for the protocol of the IPsec data exchange. The data exchange is in "quick mode". The entire communication during this phase is encrypted using the standardized security protocol ESP for which you can set the following protocol parameters:

Parameter	Description
SA lifetime type	Phase 2 Security Association (SA): • Time: Time limit in minutes The use of the current key material has a time limit. When the time expires, the key material is renegotiated. • Limit: Limitation of the data volume in MB
SA lifetime	Numeric value: • Range of values for time: 60 ... 16666666 minutes (default: 2880) • Range of values for limit: 2000 ... 500000 MB (default: 4000)
Phase 2 Encryption	Encryption algorithm: • DES: Data Encryption Standard (56 bit key length, mode CBC) • 3DES-168: Triple DES (168-bit key length, mode CBC) • AES-128: Advanced Encryption Standard (128-bit key length, mode CBC)
Phase 2 authentication	Authentication algorithm;: • MD5: Message Digest Algorithm 5 • SHA1: Secure Hash Algorithm 1
Perfect Forward Secrecy	Select whether or not before each time an IPsec-SA is renegotiated, the key is negotiated again using the Diffie-Hellman method. Due to the Perfect Forward Secrecy, it is guaranteed that the new key cannot be ascertained from the previously generated keys.

6.5.2 Including security module in configured group

The configured group properties are adopted for security modules 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. Add the new security modules to the group.
2. Download the configuration to the new modules.

- **Case b:** When you have changed group properties

1. Add the new security modules to the group.
2. Download the configuration to all modules that belong to the group.

Advantage

Existing security modules that have already been commissioned do not need to be reconfigured and downloaded. Active communication is not influenced or interrupted.

Settings for nodes with an unknown IP address

Nodes whose IP address is unknown at the time of configuration (unknown peers) can be inserted in an existing VPN group. Since the nodes are usually mobile and obtain their IP addresses dynamically (for example a SOFTNET security client or SCALANCE M), the VPN tunnel can only be established if you set the parameters for Phase 1 according to one of the following tables. If you use other settings, you cannot establish a VPN tunnel to the end device.

Table 6- 2 Encryption parameter 1

Parameter	Setting
Phase 1 encryption	AES-256
Phase 1 DH group	Group2
Phase 1 authentication	SHA1
Authentication method	Certificate
SA lifetime	1 … 2500000 minutes

Table 6- 3 Encryption parameter 2

Parameter	Setting
Phase 1 encryption	3DES-168
Phase 1 DH group	Group2
Phase 1 authentication	SHA1
Authentication method	Certificate
SA lifetime	1 … 2500000 minutes

Table 6- 4 Encryption parameter 3

Parameter	Setting
Phase 1 encryption	DES
Phase 1 DH group	Group2
Phase 1 authentication	MD5
Authentication method	Certificate
SA lifetime	1 … 2500000 minutes

Table 6- 5 Encryption parameter 4

Parameter	Setting
Phase 1 encryption	3DES-168
Phase 1 DH group	Group2
Phase 1 authentication	SHA1
Authentication method	Preshared key
SA lifetime	1 … 2500000 minutes

Additional restrictions for the SOFTNET Security Client

For the SOFTNET security client, the following restrictions also apply:

Parameter	Setting / special feature
Phase 1 encryption	AES-256 possible only with Windows 7
Phase 1 SA lifetime	1440 to 2879 minutes
SA lifetime type	Must be selected identical for both phases
Phase 2 encryption	No AES 128 possible
Phase 2 SA lifetime	1440 to 2879 minutes
Phase 2 authentication	No MD5 possible

Including active nodes in a VPN group

If an active node is added to an existing VPN group, this can reach the group members without needing to download the project to all members of the VPN group again.

NOTICE
If you remove an active node from an existing VPN group, this can still establish a connection to the group members even if you have downloaded the project to all members of the VPN group again. If you do not want the removed active node to be able to establish the connection any longer, renew the CA group certificate and download the project again to the members of the VPN group. The certificate can be renewed in the group properties of the VPN group or in the certificate manager, "Certification authorities" tab.

6.5.3 Configuring module-specific VPN properties

Meaning

You can configure the following module-specific properties for data exchange over the IPsec tunnel in the VPN:

- Dead peer detection
- Permission to initiate connection establishment
- Public IP address for communication via Internet gateways

Requirement

You can only make settings in the "VPN" tab if the security module you are configuring is in a VPN group.

How to access this function

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "VPN" tab.

Dead peer detection (DPD)

As default, DPD is enabled.

If DPD is enabled, the modules exchange additional messages at selectable intervals. This means that it can be recognized whether the IPsec connection is still valid or possibly needs to be re-established. If there is no longer a connection, the security associations (SA) of phase 2 are terminated prematurely. If DPD is disabled, the SA is ended only after the SA lifetime has expired. For information on the SA lifetime settings, refer to the configuration of the group properties.

Permission to initiate connection establishment

You can restrict the permission for initiating the VPN connection establishment to certain modules in the VPN.

The decisive factor the setting of the parameter described is the assignment of the IP address for the gateway of the module you are configuring. If a static IP address is assigned, the module can be found by the partner. If the IP address is assigned dynamically, and therefore changes constantly, the partner cannot establish a connection as things stand.

Mode	Meaning
Start connection to remote VPN gateway (standard)	If this option is selected, the module is "active", in other words, it attempts to establish the connection to the partner. This option is recommended when you obtain a dynamic IP address from the provider for the gateway of the security module you are configuring. The partner is addressed over its configured WAN IP address or its external module IP address.
Wait for connection from remote VPN gateway	If this option is selected, the module is "passive", in other words, it waits for the partner to initiate the connection. This option is recommended when you have been assigned a static IP address by the provider for the gateway of the security module you are configuring. With this, connection establishment attempts are started only by the partner with a dynamic WAN IP address.

NOTICE
Make sure that you do not set all the modules in a VPN group to "Wait for connection from remote VPN gateway" otherwise a connection will never be established.

WAN IP address - IP addresses of the modules and gateways in a VPN over Internet

When operating a VPN with IPsec tunnel over the Internet, additional IP addresses are generally required for the Internet gateways such as DSL routers. The individual security or SCALANCE M modules must know the external IP addresses of the partner modules in the VPN.

Note

To use a WAN as an external, public network, enter the IP address you received from the provider as "IP address ext." via which the security module will then be reachable in the WAN (Internet). To allow the security module to send packets via the WAN (Internet), you need to enter your DSL router as "Standard router".

If you use a DSL router as Internet gateway, the following ports (at least) must be opened on it:

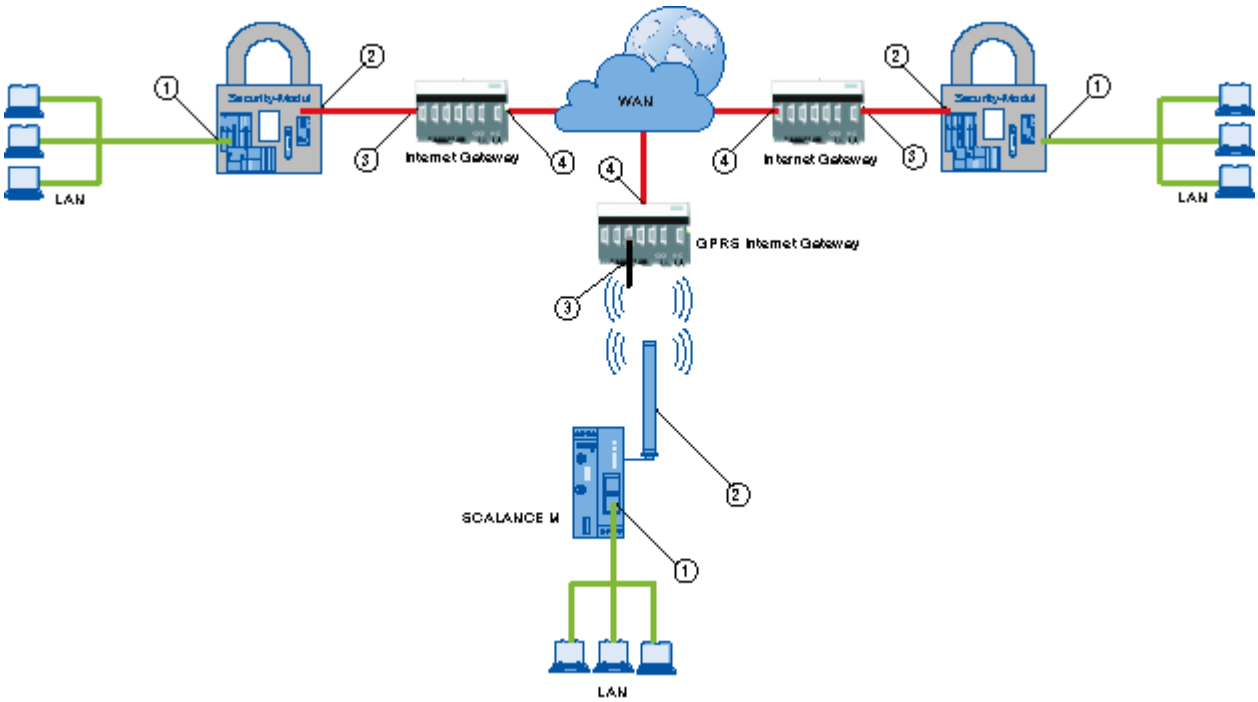
- Port 500 (ISAKMP)
- Port 4500 (NAT-T)

With SCALANCE S, for configuration downloads (via the WAN without active tunnel), port 443 (HTTPS) must also be open.

To allow this, when you configure the module, you have the option of assigning an external IP address as a "WAN IP address". When you download the module configuration, the group members are then informed of the WAN IP addresses of the partner modules.

You can choose whether the external IP address or the WAN IP address is used by clicking on the relevant security module within a VPN group and selecting the address in the content area. For more detailed information, refer to section Creating groups and assigning modules (Page 158).

If you do not enter a WAN IP address, the external IP address of the module is used.



① Internal IP address - of a module
② External IP address - of a module
③ Internal IP address - of an Internet gateway (for example GPRS gateway)
④ External IP address (WAN IP address) - of an Internet gateway (for example DSL router)

6.6 Configuring internal network nodes

Configuring internal network nodes

Each security module must know the network nodes in the entire internal network to be able to recognize the authenticity of a frame.

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

SCA.

The security module allows network nodes to be learned automatically or configured statically.

Nodes when security modules are in bridge mode

- SCALANCE S

  For a SCALANCE S in bridge mode, you can configure the static internal subnets and internal IP/MAC nodes here and enable or disable the automatic learning of internal nodes.

- CP 1628

  You can configure the static NDIS nodes by entering the NDIS nodes that can be reached through the VPN tunnel. The automatic learning of internal nodes is always enabled.

Security module in routing mode and members of a VPN group

- SCALANCE S

  Enter the internal nodes / complete subnets that will be reachable through the VPN tunnel.

  In routing mode, complete subnets are tunneled; here learning network nodes is not necessary.

- CP x43-1 Adv.

  Select the subnets of the CPU to which the VPN connection partners in a routing relation with the CP (SCALANCE S in routing mode and SCALANCE M) may have access.

6.6.1 How the learning mode works

Finding nodes for tunnel communication automatically (with SCALANCE S bridge mode only)

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

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

Requirements

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.

- PROFINET nodes

  Using DCP (Discovery and basic Configuration Protocol), it is possible to find PROFINET nodes.

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

Subnets

Subnets located downstream from internal routers must also be configured.

Enabling/disabling the learning mode

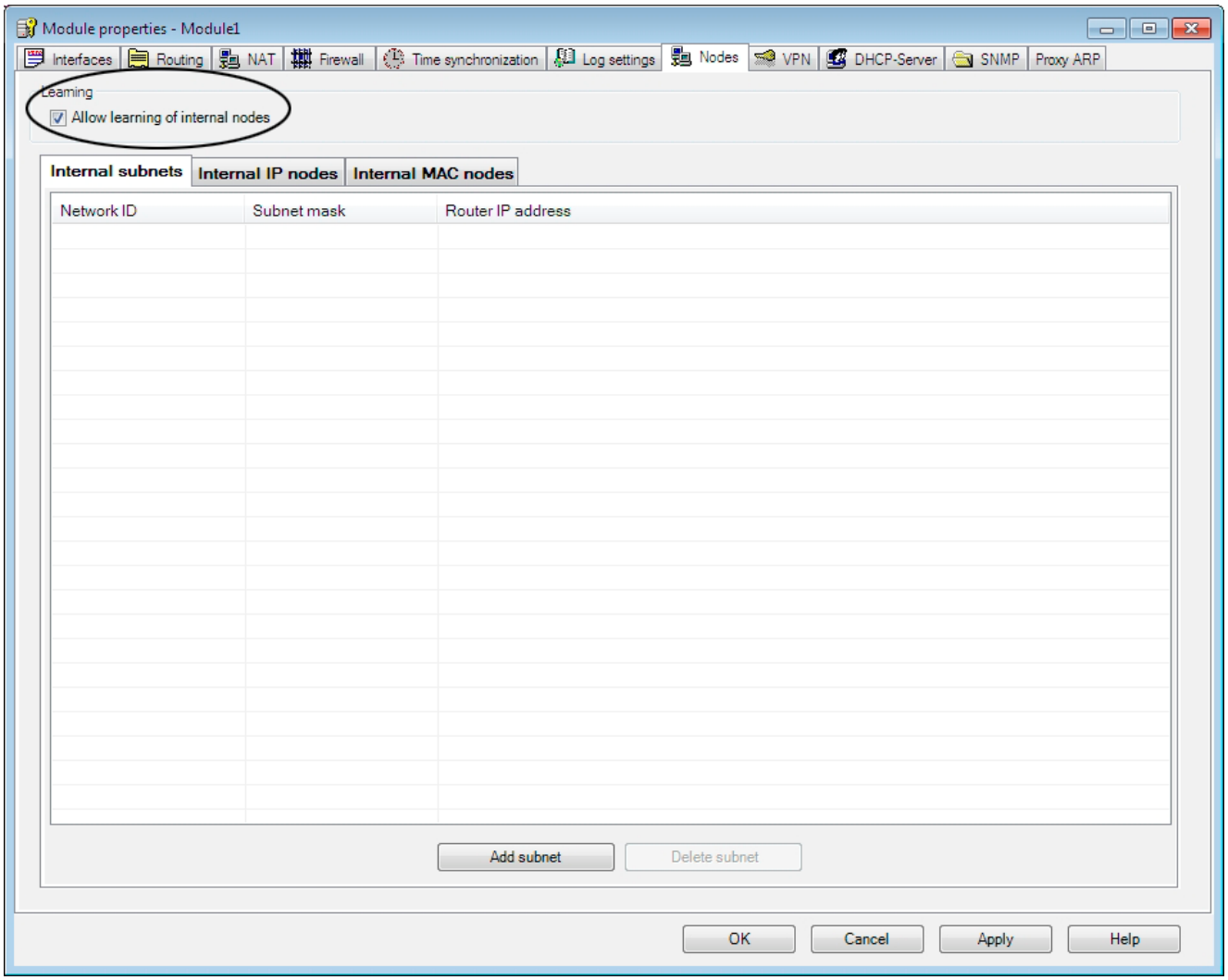
The learning function is enabled in the configuration as default for every security module by the Security Configuration Tool configuration software.

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

How to access the function

SCA.

1. Select the module.
2. Select the "Edit" > "Properties..." menu command, "Nodes" tab.



When is it useful to disable the automatic learning mode?

The default settings for the security module 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 security module 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. The information relating to VPN configuration limits relates only to nodes that communicate over VPN in the internal network.

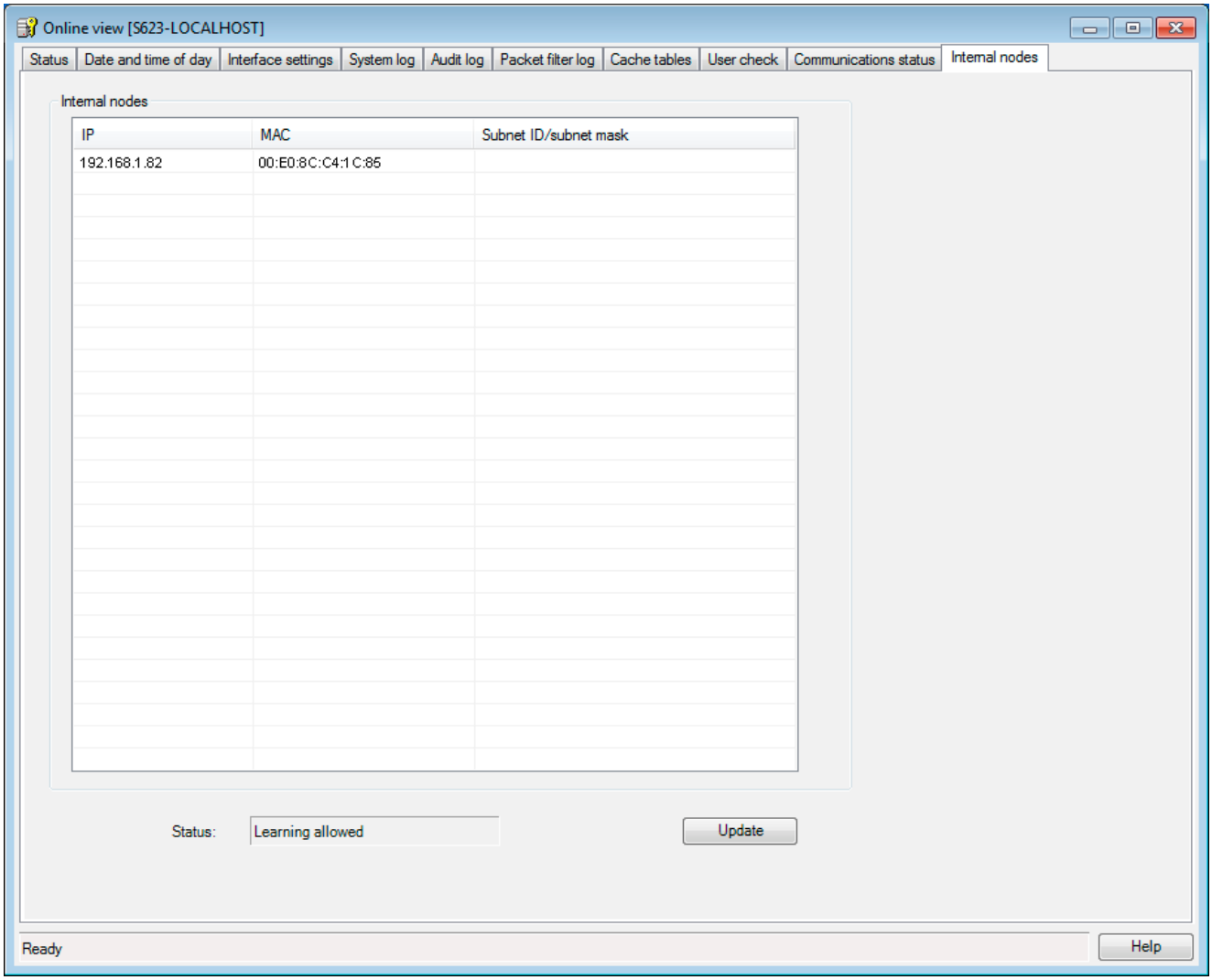
NOTICE
If more than 128 internal nodes are being operated, the permitted configuration limits are exceeded and an illegal operating status results. Due to the dynamics in the network traffic, this causes internal nodes that have already been learned to be replaced by new previously unknown internal nodes.

6.6.2 Displaying the detected internal nodes

All network nodes found are displayed in the Security Configuration Tool.

1. Change to "Online" mode.

2. Select the "Edit" > "Online diagnostics..." menu command, "Internal nodes" tab.



Nodes that cannot be learnt

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

You must also configure subnets located in the internal network of the security module.

How to access this tab

1. Select the module.
2. Select the "Edit" > "Properties..." menu command, "Nodes" tab.
3. Here, in the individual tabs, enter the required address parameters for all network nodes to be protected by the selected security module.

Effects when using the SOFTNET Security Client

If you configure nodes statically, you will also need to redownload the configuration for a SOFTNET Security Client used in the VPN.

Depending on the security module and mode, various tabs are available that are described in the online help.

SOFTNET Security Client 7

With the SOFTNET Security Client PC software, secure remote access is possible from PCs/PGs to automation systems protected by security modules via public networks.

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 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.

See also

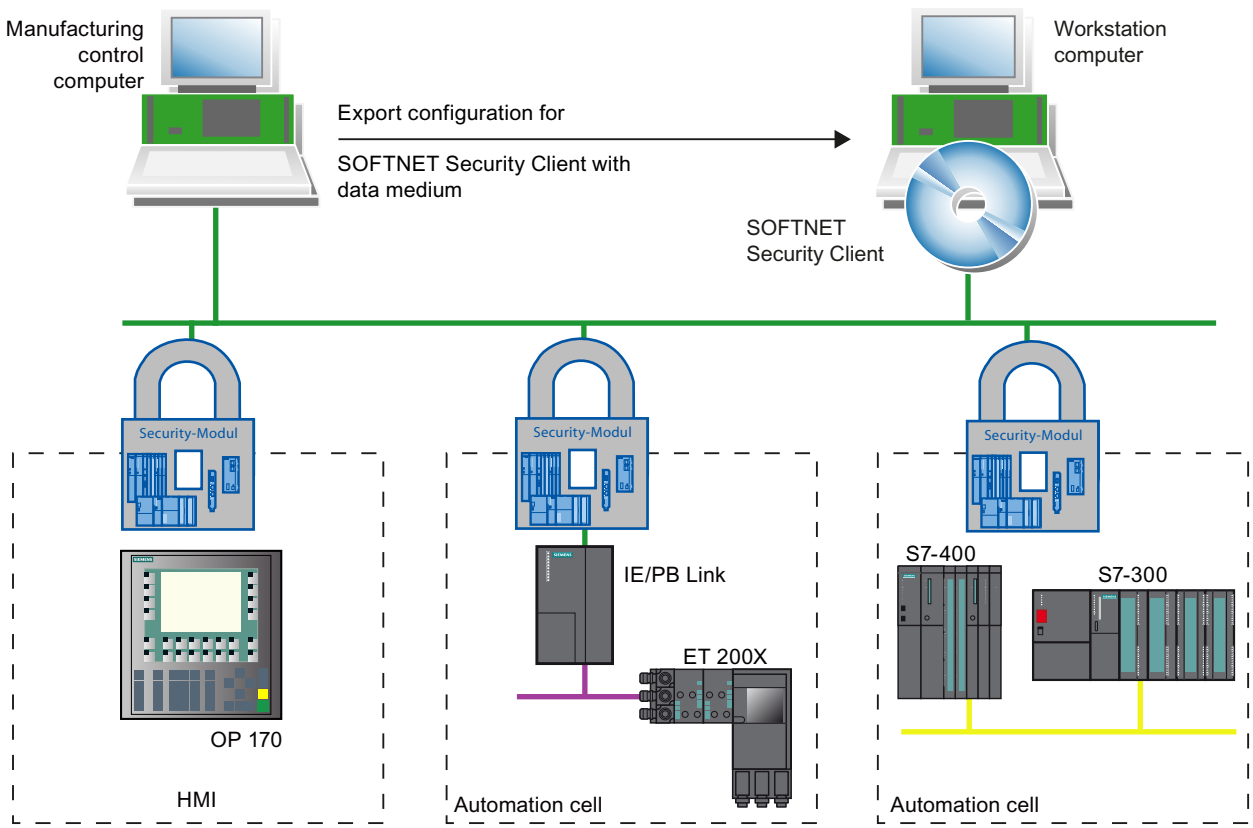
Secure communication in the VPN via an IPsec tunnel (Page 153)

7.1 Using the SOFTNET Security Client

Area of application - access over VPN

With the SOFTNET Security Client, you configure a PG/PC so that it can automatically establish secure IPsec tunnel connection in the VPN (Virtual Private Network) with one or more security modules.

PG/PC applications such as NCM Diagnostics or STEP 7 can access devices or networks in an internal network protected by the security module via a secure tunnel connection.



Automatic communication over VPN

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

NOTICE
Via the IPsec tunnel, IP-based communication is possible only between SSC and the security modules as well the internal nodes behind the security modules. Layer 2 communication is not possible with the SSC.

Operation

The SOFTNET Security Client PC software is used for configuration of the security properties required for communication with devices protected by security modules. Following configuration, the SOFTNET Security Client runs in the background - visible as an icon in the symbol bar on the 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 obtains 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 on and addresses downstream from the security 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 the security modules. Afterwards, the SOFTNET Security Client identifies the IP addresses of the internal nodes and enters these in special filter lists of the security policy.

Result: Applications such as STEP 7 communicate with the programmable controllers via VPN.

NOTICE
On a Windows system, the IP security policies are stored separately for specific users. Only one IP security policy can ever be valid at one time for a user. If you do not want an existing IP security policy to be overwritten by installing the SOFTNET Security Client, you should install and use the SOFTNET Security Client under a user specifically set up for it.

Supported operating systems

The SOFTNET Security Client is suitable for use with the following operating systems:

- Microsoft Windows XP 32-bit + Service Pack 3
- Microsoft Windows 7 Professional 32/64-bit
- Microsoft Windows 7 Professional 32/64-bit + Service Pack 1
- Microsoft Windows 7 Ultimate 32/64-bit
- Microsoft Windows 7 Ultimate 32/64-bit + Service Pack 1

Response to problems

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

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

7.2 Installation and commissioning of the SOFTNET Security Client

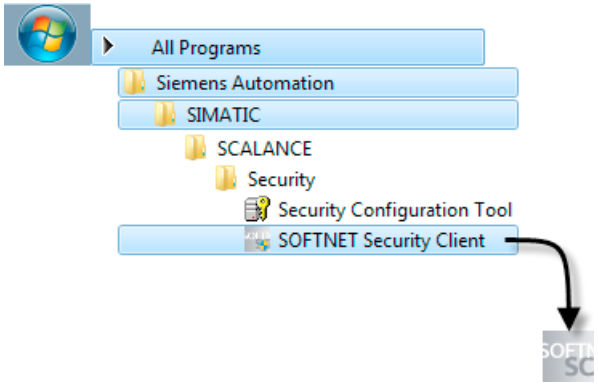
7.2.1 Installing and starting SOFTNET Security Client

You install the SOFTNET Security Client PC software from the product CD.

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;

   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.exe file. You can then select the entry "Installation SOFTNET Security Client" directly

Following installation and startup of the SOFTNET Security Client, the symbol 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 as follows:

- Export of a security configuration from the Security Configuration Tool.
- Import of the security configuration in its own user interface as described in the next section.

Startup behavior

Downloading the security rules can take up to 15 minutes. The CPU usage of the PG/PC is 100% during this time.

Exiting SOFTNET Security Client

You exit SOFTNET Security Client as follows:

- Right-click on the SOFTNET Security Client symbol and select the option "Exit SOFTNET Security Client".
- Click the "Exit" button in the open user interface.

Result: If SOFTNET Security Client is exited and the security policy is deactivated.

7.2.2 Uninstalling SOFTNET Security Client

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

7.3 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 security modules, you do not need to configure any further properties.

Assign the SSC module to the VPN group or groups in which an IPsec tunnel is to be set up to the PG/PC. The group properties you configured for these groups are adopted.

NOTICE
Refer to the information on parameters in section Including security module in configured group (Page 165).

Note

If you create several SOFTNET Security Clients within a group, no tunnels are set up between these clients but only from the relevant client to the security modules.

Configuration files for the SOFTNET Security Client

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

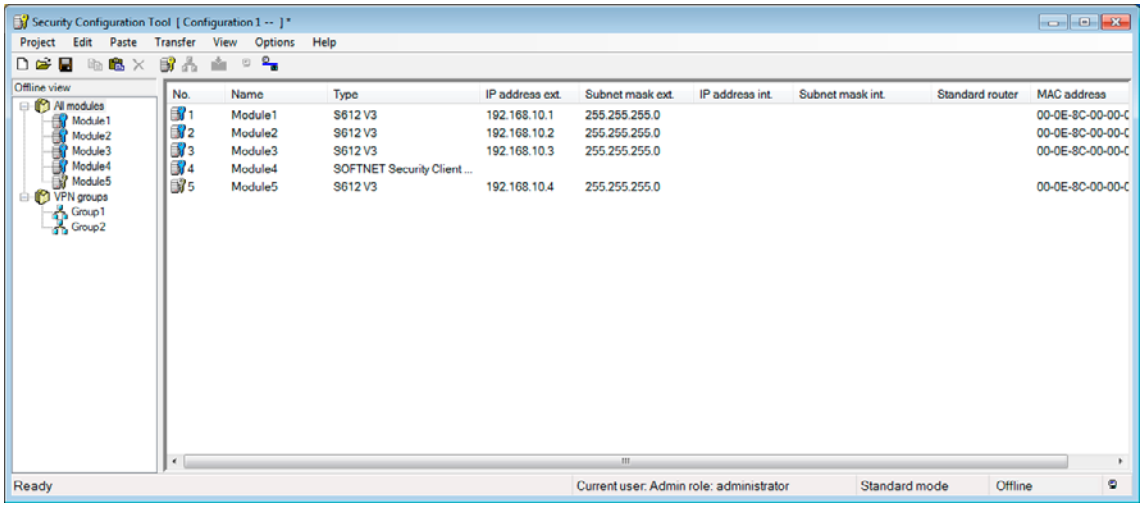
The configuration is stored in the following file types:

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

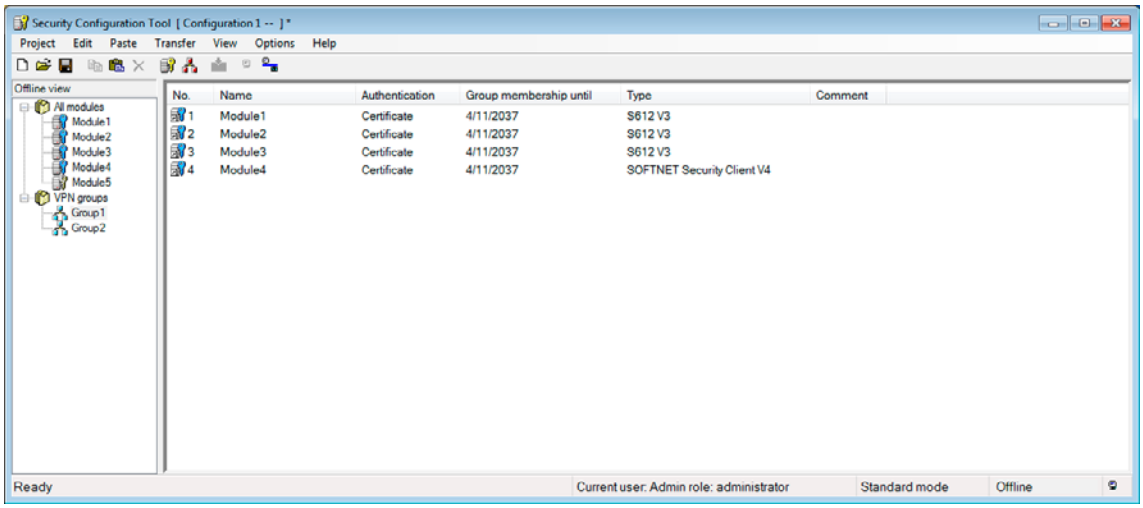
Procedure

To generate the configuration files, perform the following steps in SCT:

1. Create a module of the type SOFTNET Security Client.



2. Assign the module to the VPN groups in which the PG/PC will communicate over IPsec tunnels.



3. Select the "Transfer" > "To module..." menu command in the shortcut menu of the SOFTNET Security Client.
4. Select the storage location for the configuration files.
5. If you selected certificate as the authentication method, specify a password for the certificate of the VPN configuration. If you do not assign a password, the project name (not the project password) is used as the password.

   Result: Export of the configuration files is completed.
6. Adopt the files of the type *.dat, *.p12, *.cer on the PG/PC on which you want to operate the SOFTNET Security Client.

7.4 Working with SOFTNET Security Client

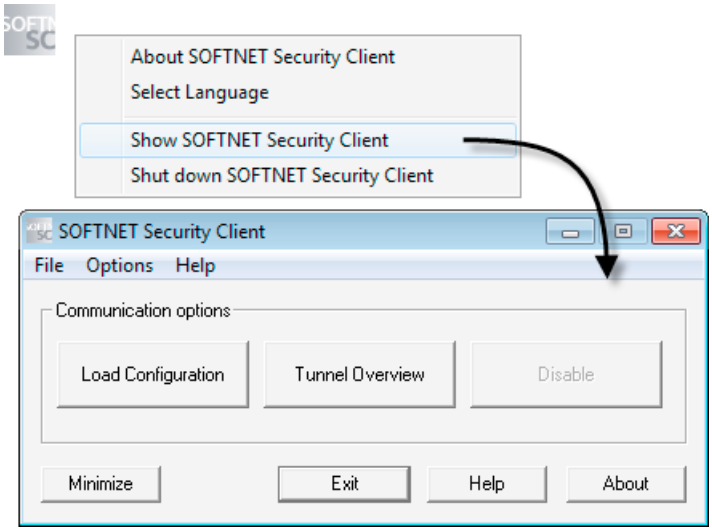
Configurable properties

You can use the following individual services:

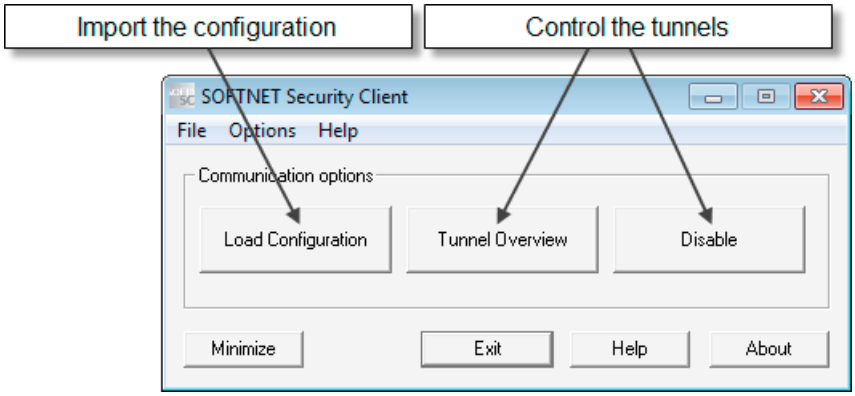
- Setting up secure IPsec tunnel communication (VPN) between the PC/PG and all security modules or individual security modules of a project. The PC/PG can access the security module and the internal nodes via this IPsec tunnel.
- Enable and disable existing secure connections;
- Setting up connections after adding end devices later. The learning mode must be enabled for this.
- Check a configuration; in other words, which connections are set up or possible.

How to open SOFTNET Security Client for configuration

Double-click on the symbol in the Windows taskbar or select the menu command "Open SOFTNET Security Client" from the shortcut menu.



With the buttons, you can activate the following functions:



Button	Meaning
Downloading configuration data	Dialog for selecting a configuration file for import Select a file and click the "Open" button. Result: The configuration is read in. In the dialog, you are asked whether you want to set up the tunnels for all security modules immediately. If IP addresses of the security modules are entered in the configuration or if the learning mode is active, the tunnels for all configured or detected addresses are set up. This procedure is fast and efficient particularly with small configurations. As an option, you can set up all tunnels in the "Tunnel Overview" dialog. Note: You can import the configuration files from several projects created in SCT one after the other (see also the explanation of the procedure below).
Tunnel Overview	Dialog for setting up and editing the tunnels This is the dialog in which you actually configure the SOFTNET Security Client. A list of secure tunnels along with the IP addresses of the security modules is displayed. If you have more than one network adapter on your PG/PC, the SOFTNET Security Client automatically selects one via which an attempt is made to set up a tunnel. In some cases, the SOFTNET Security Client does not find an adapter to suit your node and enters any one of the adapters. In this case, you will need to adapt the network adapter setting manually in the context menu of the nodes and security modules in the "Network adapter" dialog.
Disable	Disable all secure tunnels
Minimize	The user interface of the SOFTNET Security Client is closed The symbol for the SOFTNET Security Client remains displayed in the Windows taskbar.
Exit	The SOFTNET Security Client is closed and all tunnels disabled.
Help	Open online help
Info	Information on the version of the SOFTNET Security Client Details: List of all the files required for the SOFTNET Security Client to function with feedback as to whether these could be found on the system

7.5 Setting up and editing tunnels

Setting up secure connections to all security modules

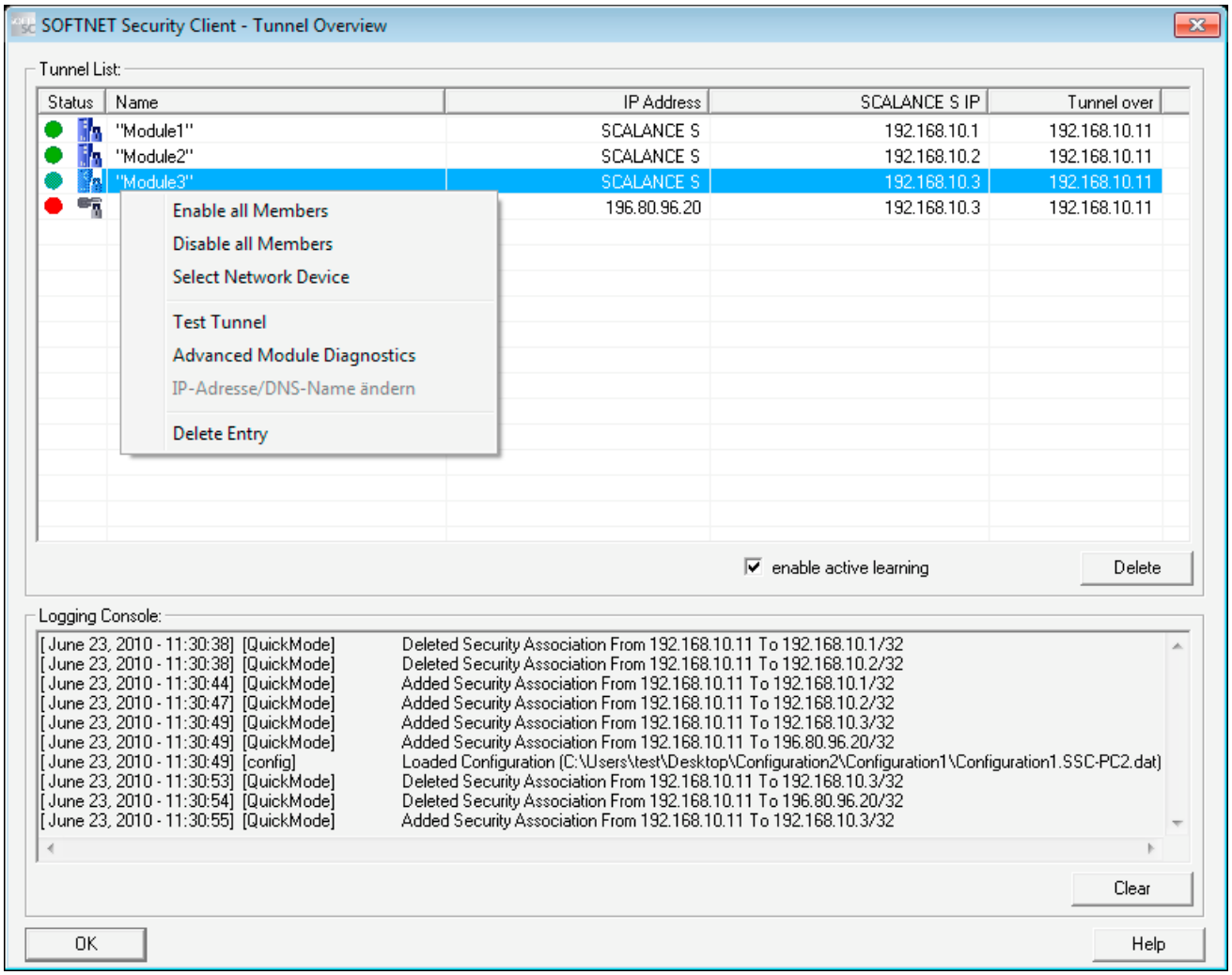
In the dialog for importing the configuration, select whether or not the tunnels will be set up for all security modules immediately. This results in the following possibilities:

- Enable tunnels automatically

  If IP addresses of the security 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 for setting up tunnels.

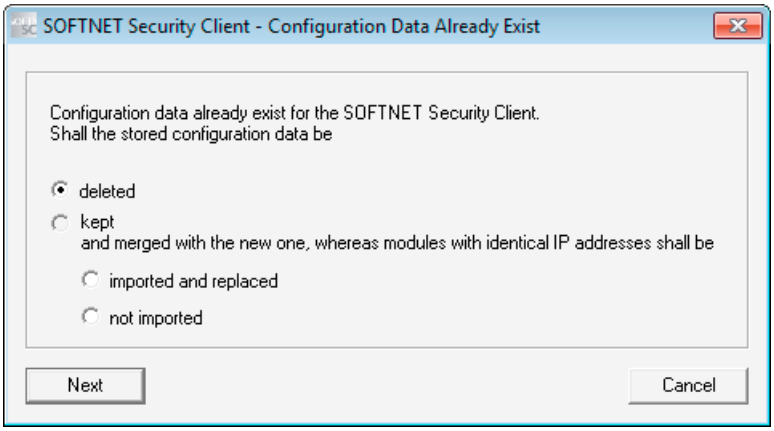


How to set up tunnel connections

1. With the "Load Configuration Data" button, open the dialog for importing the configuration file.
2. Select the configuration file created with SCT.

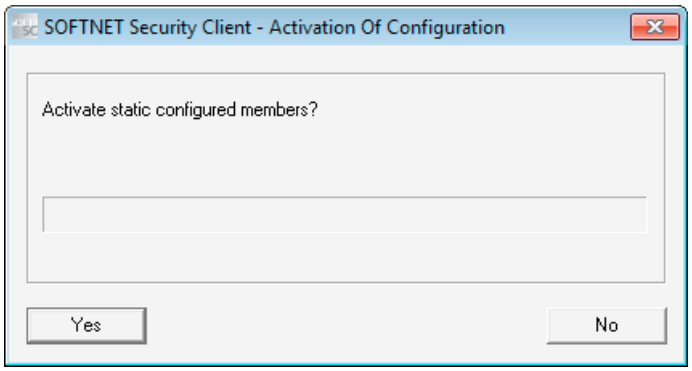
   You can read in configuration data from several projects at the same time. If there is already configuration data in the SOFTNET Security client, select one of the following options:

   – "deleted": Only the last downloaded configuration data is available.
   – "imported and replaced": If you have modified configuration data, for example, you have only changed the configuration in project a, project b and c remain unchanged.
   – "not imported": is useful if a security module has been added to a project and you do not want to lose internal nodes that have already been learned.



3. If you have selected "certificate" as the authentication method in SCT, enter the password.
4. Decide whether or not to enable the tunnel connections for the nodes included in the configuration (statically configured nodes).

   If you do not enable the tunnel connections here, you can do this at any time in the tunnel dialog described below.

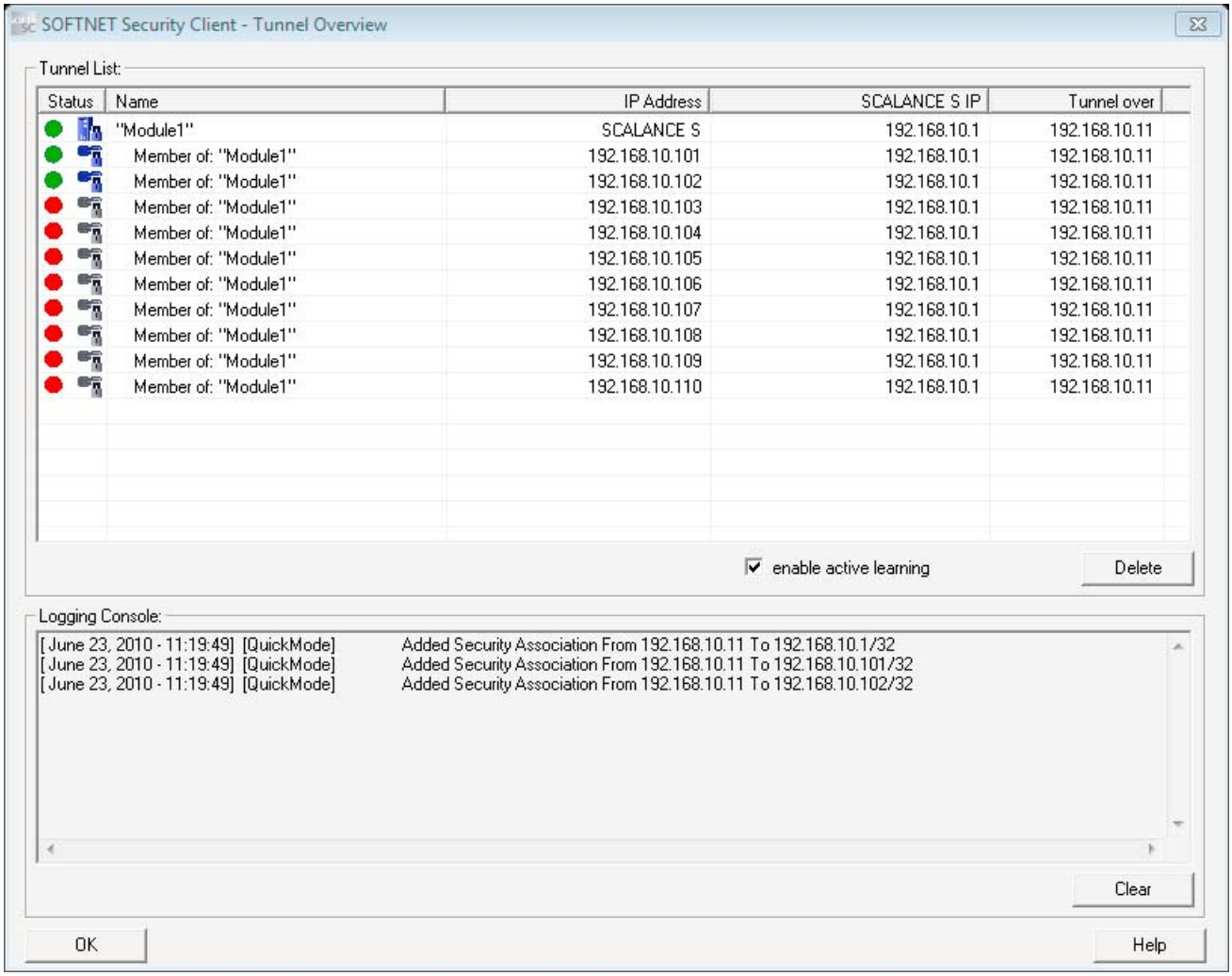


   If you have decided to enable the tunnel connections, the tunnel connections between the SOFTNET Security Client and the security modules are now established.

   This can take several seconds.

5. Open the "Tunnel Overview" dialog.

   The table displays the modules and nodes with status information about the tunnel connections.



6. If nodes are not displayed in the table, use the command line to send a ping command to the missing nodes.

   Result: The node is learned by the security module and passed on to the SOFTNET Security Client.

   Note:

   If the dialog is not open while a node is detected, the dialog is displayed automatically.

   Note

   Statically configured nodes and subnets

   If you configure nodes or subnets statically, you will also need to redownload the configuration for a SOFTNET Security Client used in the VPN.

7. Enable the nodes for which no tunnel connection has yet been established.

After successful establishment of the connection, start the application that will establish a communication connection to one of the nodes, for example STEP 7.

NOTICE
If there are several network adapters in the PG/PC, SSC automatically selects the network adapter to establish a tunnel. If there is no network adapter suitable for the project, SSC automatically enters one. In this case, adapt the setting for the network adapter using the shortcut menu of the nodes and security modules.

Meaning of the parameters

Table 7- 1 Meaning of the parameters in the "Tunnel Overview" dialog box

Parameter	Meaning / range of values
Status	You will find possible status displays in the following table.
Name	Name of the module or node adopted from the SCT configuration.
IP address int. / subnet	If there are internal nodes / subnets, the IP address of the internal node or the network ID of the internal subnet is displayed.
Tunnel endpoint IP	IP address of the assigned security module.
Tunnel over...	If the PC is operated with more than one network adapter, the assigned IP address via which the VPN tunnel is established is displayed.

Table 7- 2 Status displays

Symbol	Meaning
	There is no connection to the module or node.
	There are more nodes that are not displayed. Double-click on the symbol to display further nodes.
	The node is not enabled.
	The node is enabled.
	Disabled security module.
	Enabled security module.
	Disabled SCALANCE M module.
	Enabled SCALANCE M module.
	Internal subnet disabled.
	Internal subnet enabled.
	Module / node cannot be reached.
	Module / node can be reached.
	Reachability test disabled.

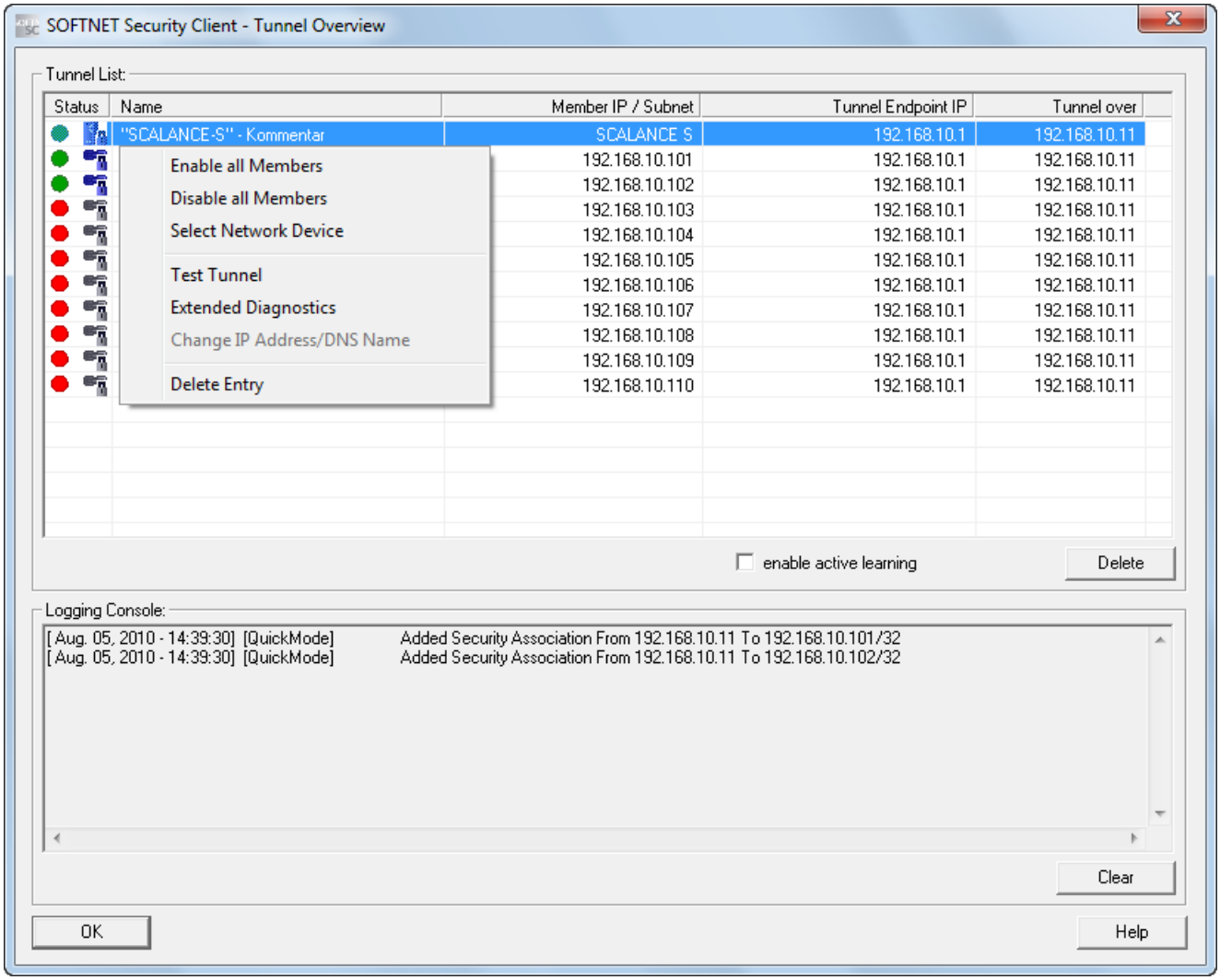
"enable active learning" check box

If the learning mode is enabled in the configuration of the security modules, this can also be enabled for the SOFTNET Security Client. This automatically provides you with the information about the internal nodes of the security module.

Otherwise the "enable active learning" check box is disabled.

Selecting and working with a tunnel entry

Select an entry in the "Tunnel Overview" dialog and open further options using the shortcut menu.



NOTICE
If several IP addresses are used for a network adapter, assign the IP address to each entry in the "Tunnel Overview" dialog.

"Delete All" button

The IP security policy and all entries not set up using SSC are deleted.

Enabling and disabling existing secure connections

You can disable secure connections that have been set up using the "Disable" button. After clicking the button, the text of the button changes to "Enable" and the symbol in the status bar is replaced.

Result: The security policy is disabled on the PC.

To undo the change and to enable the tunnels that have been set up again, click the "Enable" button.

Logging Console

In the "Settings" dialog, you can select which entries are displayed in the logging console.

- Diagnostics information about connection establishment with the configured security modules / SCALANCE M modules and internal nodes / subnets.
- Date and time stamp at the time of the events
- Establishment and termination of a security association
- Negative reachability test (test ping) to the configured nodes

"Clear" button

Deletes all entries in the logging console.

Global settings for the SOFTNET Security Client

1. Select the menu command "Options" > "Settings" in the main dialog of the SOFTNET Security Client.
2. Make the global settings that will be retained after closing and opening the SOFTNET Security Client.

You will find the functions in the following table:

Function	Description / options
Log file size (logging console)	Log file size of the source file containing the messages that are output filtered in the logging console of the tunnel overview and are restricted to a specific number.
Number of messages to be displayed in the logging console of the tunnel overview.	Number of messages that will be extracted from the log file of the source file and displayed in the logging console of the tunnel overview.

Function	Description / options
Output the following log messages in the logging console of the tunnel overview: • Display of the negative reachability test (ping) • Creation/deletion of security associations (quick modes) • Creation / deletion of main modes • Download configuration files • Learn internal nodes	Optional messages displayed in the logging console of the tunnel overview.
Log file size (debug log files)	Log file size of the source files for debug messages of the SOFTNET Security Client (can be requested from Customer Support to make analyses easier)
Reachability test, wait time for reply	Selectable wait time for a ping that will establish whether a tunnel partner can be reached. It is important to make this setting especially for tunnels with slow transmission paths (UMTS, GPRS, etc.) on which the delay of the data packets is significantly higher. This therefore directly influences the display of the reachability in the tunnel overview.
Disable reachability test globally	If you enable this function, the reachability test is disabled globally for all the configurations contained in the SOFTNET Security Client. Advantage: No additional packets create data traffic Disadvantage: In the tunnel overview, there is no feedback message to indicate whether a tunnel partner can be reached or not.

Expanded module diagnostics

Select the menu command "Options" > "Advanced Module Diagnostics" in the main dialog of the SOFTNET Security Client.

The view is used only for diagnostics of the system status relating to the configured security modules and can be useful when contacting Customer Support for help.

- Security module

  Select the module for which the current system status will be diagnosed.

- Routing settings (module-specific parameters)

  Shows the settings for interfaces and internal nodes/subnets detected in the configuration.

- Active main modes / active quick modes

  If you have set up main modes or quick modes for the selected module on the PG/PC, the details are displayed here. This also includes the total number of main modes or quick modes found on the system for the selected module.

- Routing settings (network settings of the computer)

  Shows the current routing settings of the computer.

  You can obtain additional routing information with the "Show all routing settings" option.
- Assigned IP addresses

  List of the network interfaces known to the computer in conjunction with the configured or assigned IP addresses.

Online functions - test, diagnostics, and logging 8

For test and monitoring purposes, the security module has diagnostic and logging functions.

- Diagnostic functions

  These include various system and status functions that you can use in online mode.

- Logging functions

  This involves the recording of system and security events.

The events are logged in the buffer areas of the security module or a server. These functions can only be assigned parameters and evaluated when there is a network connection to the selected security module.

Recording events with logging functions

You select the events to be logged in the log settings for the relevant security module.

You can configure the following variants for logging:

- Local logging

  In this variant, you log events in the local buffer of the security module. You can then access these logs, display them and archive them on the service station in the online dialog of the Security Configuration Tool.

- Network Syslog

  With Network Syslog, you use a Syslog server that exists in the network. This logs the events according to the configuration in the log settings for the relevant security module.

Archiving log data and reading in from a file

You can save the logged events for archiving in a log file and also open this in offline mode. For more detailed information, refer to section Overview of the functions in the online dialog (Page 194).

8.1 Overview of the functions in the online dialog

In the Security Configuration Tool, the security module provides the following functions in the online dialog:

Table 8- 1 Functions and logging in online diagnostics

Function / tab in the online dialog		Meaning
System and status functions		
	Status	Display of the device status of the security module selected in the project.
SCA.	Date and time of day	Date and time setting.
S≥V3.0	Interface settings	Overview of the settings of the individual interfaces.
S≥V3.0	Cache tables	Display of the ARP table of the security module.
S≥V3.0	User check	Shows the users logged on to the Internet page for user-specific IP rule sets.
~~S602~~	Communication Status	Display of the communication status and the internal nodes for other security modules belonging to the VPN group.
~~S602~~ ~~PC-CP~~	Internal nodes	Display of the internal network nodes of the security module.
S7-CP	Dynamically updated firewall rules	Display of the IP addresses that are enabled dynamically via FTP or HTTP when using IP access control lists or that were loaded later by the user.
Logging functions		
	System log	Display of logged system events.
	Audit log	Display of logged security events.
	Packet filter log	Displays logged data packets as well as starting and stopping packet logging.

For more detailed information on the possible settings, in the individual tabs, refer to the online help.

Requirements for access

To be able to use the online functions with a security module, the following requirements must be met:

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

---

Note

Effects of the mode of the Security Configuration Tool

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

How to access this function

1. Change the mode using the "View" > "Online" menu command.
2. Select the module to be edited.
3. Select the "Edit" > "Online Diagnostics..." menu command.

   When you open one of the tabs for logging functions, you will see the current status of the logging function of the selected security module in the lower part of the tab:

- Buffer settings: Ring buffer / one-shot buffer

  The current logging status originates from the loaded configuration of from the online function if this has been run once.

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 security 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 that you make in online mode (for example settings for the logging memory) are not stored in the configuration on the security module. Following a module restart, the settings from the configuration are therefore always effective.

8.2 Logging events

Overview

Events on the security module can be logged. Depending on the event type, they are stored in volatile or non-volatile buffers. As an alternative, you can also record on a network server.

Configuration in standard mode and in advanced mode

The options that can be selected in the Security Configuration Tool depend on the selected view:

- Standard mode

  "Local logging" is enabled as default in standard mode; packet filter events can be enabled globally in the "Firewall" tab. "Network Syslog" is not possible in this view.

- Advanced mode

  All logging functions can be enabled or disabled; packet filter events must be enabled selectively in the "Firewall" tab (local or global rules).

Logging procedures and event classes

During configuration, you can specify which data should be logged. As a result, you enable logging as soon as you download the configuration to the security module.

During configuration, you also select one or both of the possible logging procedures:

- Local logging
- Network Syslog

The security module recognizes the following events for both logging methods:

Function / tab in the online dialog	How it works
Packet filter events (firewall)	The packet filter log records certain packets of the data traffic. Data packets are only logged if they match a configured packet filter rule (firewall) or to which the basic protection reacts (corrupt or invalid packets). This is only possible when logging is enabled for the packet filter rule.
Audit events	The audit log automatically records security-relevant events, for example user actions such as enabling or disabling packet logging or actions for which a user has not been authenticated correctly by password.
System events	The system log automatically logs successive system events, for example the start of a process. The logging can be scaled based on event classes.
	Line diagnostics: Line diagnostics can also be configured. Line diagnostics returns messages as soon as the number of bad packets exceeds a selectable limit. CP

Storage of logged data in local logging

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.

Enabling or disabling logging

In "offline" mode, you can enable local logging for the event classes in the log settings and can select the storage mode. These log settings are loaded on the module with the configuration and take effect when the security module starts up.

When required, you can also enable or disable local logging of packet filter events and system events in the online functions. This does not change the settings in the project configuration.

8.2.1 Local logging - settings in the configuration

In "offline" mode, you can enable the event classes in the log settings and can select the storage mode. These log settings are loaded on the module with the configuration and take effect when the security module 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.

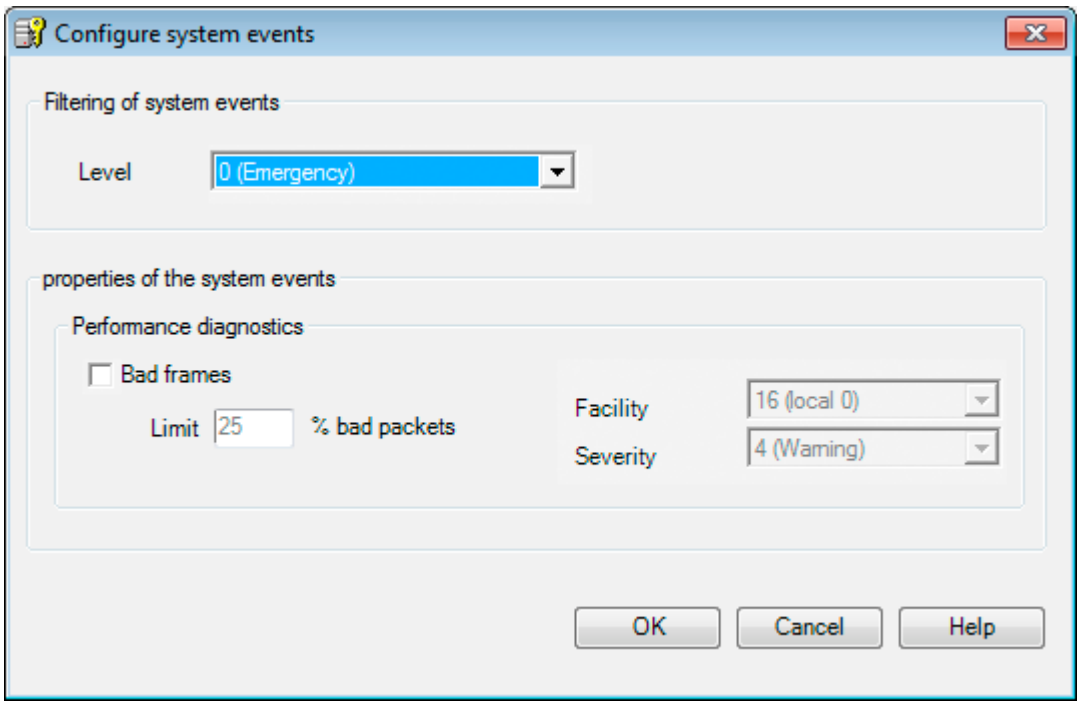
Log settings in standard mode

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

1. Select the module to be edited.
2. Select the "Edit" > "Properties..." menu command, "Log settings" tab.

The following dialog shows the default settings for the security module; the dialog for configuration of the logging of system events is also opened:



Configuring event classes

Table 8- 2 Local log - overview of the functions

Function / tab in the online dialog	Project engineering	Remarks
Packet filter events (firewall)	You enable options using the check boxes. You select the storage mode using the check boxes.	Packet filter log data is not retentive The data is stored in volatile memory on the security module and is therefore no longer available after the power supply has been turned off.
Audit events (always enabled)	Logging is always enabled. The logged information is always stored in the ring buffer.	Audit log data is retentive The data is stored in a retentive memory of the security module and is therefore still available after turning off the power supply.
System events	You enable options using the check boxes. You select the storage mode using the check boxes. To configure the event filter and line diagnostics, open a further dialog with the "Configure..." button.	System log data is not retentive The data is stored in volatile memory on the security module and is therefore no longer available after the power supply has been turned off.

Function / tab in the online dialog	Project engineering	Remarks
Filtering of the system events	In this sub-dialog, set a filter level for the system events. As default, the following values are set: • SCALANCE S: Level 0 • CP: Level 3	Select "Error" as the filter level or a higher value to stop logging of general, uncritical events. **Note on CPs** For a CP, select only level 3 or level 6. • If you select level 3, the error messages of levels 0 to 3 are output. • If you select level 6, the error messages of levels 0 to 6 are output.
Line diagnostics CP	Line diagnostics generates a special system event. Set the percentage of bad frames as of which a system event is generated. Assign a facility and a severity to the system event.	Using the severity, you weight the system events of line diagnostics relative to the severity of the other system events. **Note** Assign the system events of line diagnostics a lower severity than the filtering of system events. Otherwise, these events will not pass through the filter and are not logged.

8.2.2 Network Syslog - settings in the configuration

You can configure the security module as a client that sends logging information to a Syslog server. The Syslog server can be in the local internal or external subnet. The implementation corresponds to RFC 3164.

Note

Firewall - Syslog server not active in the external network

If the Syslog server is not enabled on the addressed computer, this computer generally returns ICMP responses "port not reachable". If these reply frames are logged due to the firewall configuration and sent to the Syslog server, the procedure can become never ending (storm of events).

Remedies:

- Start the Syslog server;
- Change the firewall rules;
- Take the computer with the disabled Syslog server out of the network;

Making the log settings

1. Change the mode with the menu command "View" > "Advanced mode".

Note

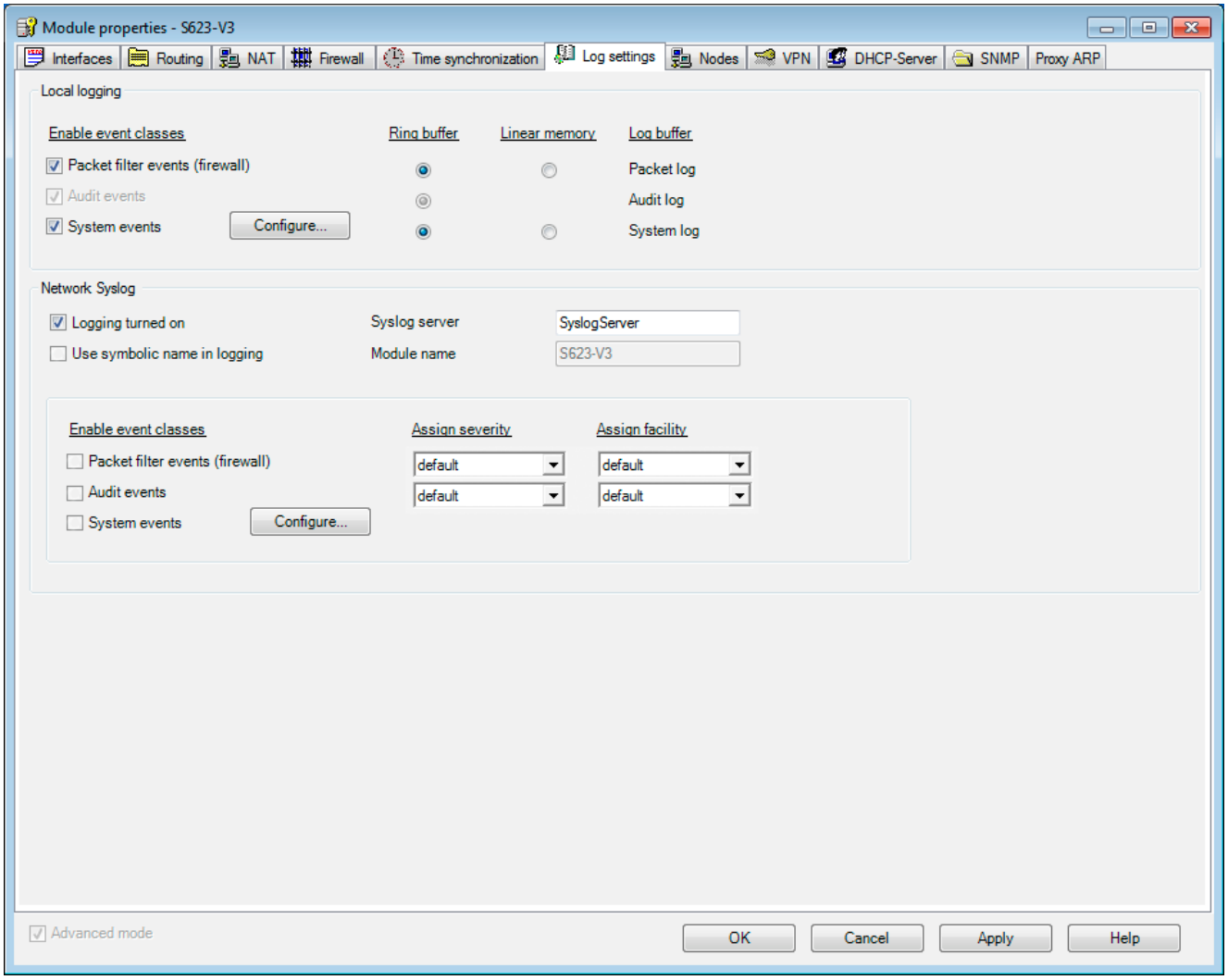
No return to standard mode possible

If you switch to the advanced mode and change the configuration for the current project, you can no longer switch back.

Remedy SCT standalone: You close the project without saving and open it again.

2. Select the module to be edited.
3. Select the "Edit" > "Properties..." menu command, "Log settings" tab.

The following dialog shows the standard settings for the security module when logging is enabled for the network Syslog:



Establishing a connection to the Syslog server

For SCALANCE S: The security module uses the configured module name as the hostname to identify itself to the Syslog server.

For CPs: The security module uses its own IP address as the hostname to identify itself to the Syslog server.

Enter the IP address of the Syslog server in the "Syslog server" box. You can enter the IP address either as a symbolic name or as a numeric name.

The Syslog server must be reachable from the security module using the specified IP address, if necessary using the router configuration in the "Routing" tab. If the Syslog server cannot be reached, the sending of Syslog information is disabled. You can recognize this operating situation based on the system messages. To enable the sending of Syslog information again, you may need to update the routing information and restart the security module.

Use symbolic names in log

If you enable the "Use symbolic name in logging" option, the address information of the log frames transferred to the Syslog server is replaced by symbolic names. The security module checks whether corresponding symbolic names have been configured and enters these in the log frame.

Note

Longer a processing time when using symbolic names

If the "Use symbolic name in logging" option is selected, the processing time on the security module is increased.

The module names are automatically used as symbolic names for the IP addresses of the security modules. In routing mode, these names have a port name added to them as follows: "Modulename-P1", "Modulename-P2" etc.

Configuring event classes

Table 8- 3 Network Syslog - overview of the functions

Function / tab in the online dialog	Project engineering	Remarks
Packet filter events (firewall)	You enable this using the check box. By setting facility and severity, Syslog messages can be classified according to their origin and their severity. The assignment is made in drop-down lists. Each event is assigned the severity and facility you set here.	Which value you select here, depends on the evaluation in the Syslog server. This allows you to adapt to the requirements in the Syslog server. If you leave the default setting, the security module specifies which combination of facility and severity is displayed for the event.
Audit events	You enable this using the check box. The severity and facility are assigned in drop-down lists. Each event is assigned the severity and facility you set here.	The value you select here for the severity and facility, depends on the evaluation in the Syslog server. This allows you to adapt to the requirements in the Syslog server. If you leave the default setting, the security module specifies which combination of facility and severity is displayed for the event.
System events	You enable this using the check box.	To configure the event filter and line diagnostics, open a further dialog with the "Configure..." button.
Filtering of the system events	In this dialog, set a filter level for the system events. As default, the following values are set: • SCALANCE S: Level 0 • CP: Level 3	Select "Error" as the filter level or a higher value to stop logging of general, uncritical events. **Note on CPs** For a CP, select only level 3 or level 6. • If you select level 3, the error messages of levels 0 to 3 are output. • If you select level 6, the error messages of levels 0 to 6 are output.
Line diagnostics SP	Line diagnostics generates a special system event. Set the percentage of bad frames as of which a system event is generated. Assign a facility and a severity to the system event.	Using the severity, you weight the system events of line diagnostics relative to the severity of the other system events. **Note** Assign the system events of line diagnostics a lower severity than the filtering of system events. Otherwise, these events will not pass through the filter and are not recorded by the Syslog server.

8.2.3 Configuring packet logging

Configuring logging in standard mode

You will find information on logging IP and MAC rule sets in the section CPs in standard mode (Page 83) in the relevant subsection of the security module.

Configuring logging 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 "Log" column in the "Firewall" tab.

Appendix A

A.1 DNS compliance

DNS-compliance according to RFC1035 involves the following rules:

- Restriction to 255 characters in total (letters, numbers, dash or period);
- The name must begin with a letter;
- The must end with a letter or a number;
- A separate name within the name, in other words a string between two periods may be a maximum of 63 characters long:
- No special characters such as umlauts, brackets, underscores, slashes or spaces etc.

A.2 Range of values for IP address, subnet mask and address of the gateway

Range of values for IP address

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

Range of values for subnet mask

The subnet mask consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 255.255.0.0

The binary representation of the 4 subnet mask decimal numbers must contain a series of consecutive 1s from the left and a series of consecutive 0s from the right.

The 1s specify the network number within the IP address. The 0s specify the host address within the IP address.

Example:

Correct values:

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

Incorrect value:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

Relationship between the IP address and subnet mask

The first decimal number of the IP address (from the left) determines the structure of the subnet mask with regard to the number of "1" values (binary) as follows (where "x" is the host address):

First decimal number of the IP address	Subnet mask
0 through 126	255.x.x.x
128 through 191	255.255.x.x
192 through 223	255.255.255.x

Note:

You can also enter a value between 224 and 255 for the first decimal number of the IP address. This is, however, not advisable since STEP 7 does not run an address check for these values.

Value range for gateway address

The address consists of four decimal numbers taken from the range 0 to 255, each number being separated by a period; example: 141.80.0.1

Range of values for IP address and gateway address

The only parts of the IP address and network transition address that may differ are those in which "0" appears in the subnet mask.

Example:

You have entered the following: 255.255.255.0 for the subnet mask; 141.30.0.5 for the IP address and 141.30.128.0 for the gateway address. Only the fourth decimal number of the IP address and gateway address may be different. In the example, however, the 3rd position is different.

You must, therefore, change one of the following in the example:

The subnet mask to: 255.255.0.0 or

the IP address to 141.30.128.5 or

the gateway address to: 141.30.0.0

A.3 MAC address

Note on the structure of the MAC address:

The MAC address consists of a fixed and a variable part. The fixed part ("basic MAC address") identifies the manufacturer (Siemens, 3COM, ...). The variable part of the MAC address distinguishes the various Ethernet nodes.

References

B

B.1 Introduction

Where to find Siemens documentation

You will find the order numbers for Siemens documentation in the catalogs "SIMATIC NET Industrial Communication, catalog IK PI" and "SIMATIC Products for Totally Integrated Automation and Micro Automation, catalog ST 70".

You can request these catalogs and additional information from your Siemens representative.

Some of the documents listed here are also on the SIMATIC NET Manual Collection CD supplied with every device.

You will find many SIMATIC NET manuals on the Internet pages of Siemens Customer Support for automation.

Link to Customer Support (http://support.automation.siemens.com/WW/view/en)

Enter the ID of the relevant manual as the search item. The ID is listed below some of the reference entries in brackets.

Manuals that are included in the online documentation of the STEP 7 installation on your PG/PC can be found in the start menu ("Start" > "SIMATIC" > "Documentation").

You will find an overview of the SIMATIC documentation on the Internet.

Link to the documentation:
(http://www.automation.siemens.com/simatic/portal/html_00/techdoku.htm)

B.2 S7 CPs / On configuring, commissioning and using the CP

B.2.1 /1/

SIMATIC NET
S7 CPs for Industrial Ethernet
Configuring and Commissioning
Manual Part - General Application
Configuration Manual
Siemens AG
(SIMATIC NET Manual Collection)
On the Internet under the following entry ID:
30374198 (http://support.automation.siemens.com/WW/view/en/30374198)

B.2.2 /2/

SIMATIC NET

S7CPs for Industrial Ethernet

Manual Part B

Manual

Siemens AG

(SIMATIC NET Manual Collection)

You will find the manuals for the individual CPs under the following entry IDs:

CP 343-1 Advanced (GX31): 28017299
(http://support.automation.siemens.com/WW/view/en/28017299)

CP 443-1 Advanced (GX30): 59187252
(http://support.automation.siemens.com/WW/view/en/59187252)

B.3 For configuration with STEP 7 / NCM S7

B.3.1 /3/

SIMATIC NET
NCM S7 for Industrial Ethernet
Primer
Siemens AG
(part of the online documentation in STEP 7)

B.3.2 /4/

SIMATIC NET
Commissioning PC Stations - instructions and getting started
Configuration manual
Siemens AG
(SIMATIC NET Manual Collection)
On the Internet under following entry ID:
13542666 (http://support.automation.siemens.com/WW/view/en/13542666)

B.3.3 /5/

SIMATIC
Configuring Hardware and Connections with STEP 7
Siemens AG
Part of the documentation package "STEP 7 Basic Knowledge"
(Part of the online documentation in STEP 7)

B.4 S7 CPs On installing and commissioning the CP

B.4.1 /6/

SIMATIC S7
Automation System S7-300

- CPU 31xC and 31x Installation: Operating instructions
  Entry ID: 13008499 (http://support.automation.siemens.com/WW/view/en/13008499)
- Module Data: Reference manual
  Entry ID: 8859629 (http://support.automation.siemens.com/WW/view/en/8859629)

Siemens AG

and

SIMATIC S7
Automation System S7-400, M7-400

- Installation: Installation manual
  Entry ID: 1117849 (http://support.automation.siemens.com/WW/view/en/1117849)
- Module Data: Reference manual
  Entry ID: 1117740 (http://support.automation.siemens.com/WW/view/en/1117740)

Siemens AG

B.5 On setting up and operating an Industrial Ethernet network

B.5.1 /7/

SIMATIC NET
Twisted-Pair and Fiber-Optic Networks Manual
Siemens AG
(SIMATIC NET Manual Collection)

B.6 SIMATIC and STEP 7 basics

B.6.1 /8/

SIMATIC
Communication with SIMATIC
system manual
Siemens AG
Entry ID:
25074283 (http://support.automation.siemens.com/WW/view/en/25074283)

B.6.2 /9/

Documentation package "STEP 7 Basic Knowledge"

- Working with STEP 7 Getting Started (ID: 18652511 (http://support.automation.siemens.com/WW/view/en/18652511))
- Programming with STEP 7 (ID: 18652056 (http://support.automation.siemens.com/WW/view/en/18652056))
- Configuring Hardware and Connections with STEP 7 (ID: 18652631 (http://support.automation.siemens.com/WW/view/en/18652631))
- From S5 to S7, Converter Manual (ID: 1118413 (http://support.automation.siemens.com/WW/view/en/1118413))

Siemens AG
Order number 6ES7 810-4CA08-8AW0

(part of the online documentation in STEP 7)

B.7 Industrial Communication Volume 2

B.7.1 /10/

SIMATIC NET
Industrial Ethernet Network Manual
Siemens AG

(SIMATIC NET Manual Collection)

On the Internet under the following entry ID: 27069465
(http://support.automation.siemens.com/WW/view/en/27069465)

B.8 On the configuration of PC stations / PGs

B.8.1 /11/

SIMATIC NET
Commissioning PC Stations - Manual and Getting Started

Configuration Manual
Siemens AG

(SIMATIC NET Manual Collection)

On the Internet under the following entry ID: 13542666
(http://support.automation.siemens.com/WW/view/en/13542666)

B.9 On configuration of PC CPs

B.9.1 /12/

SIMATIC NET Industrial Ethernet CP 1628

Compact Operating Instructions
Siemens AG

(SIMATIC NET Manual Collection)

On the Internet under the following entry ID: 56714413
(http://support.automation.siemens.com/WW/view/en/56714413)

B.10 SIMATIC NET Industrial Ethernet Security

B.10.1 /13/

SIMATIC NET Industrial Ethernet Security
SCALANCE S as of V3.0

Commissioning and installation manual
Siemens AG

(SIMATIC NET Manual Collection)

On the Internet under the following entry ID: 56576669
(http://support.automation.siemens.com/WW/view/en/56576669)

B.10.2 /14/

SIMATIC NET Industrial Ethernet Security
EDGE/GPRS router SCALANCE MD741-1

System Manual
Siemens AG

(SIMATIC NET Manual Collection)

On the Internet under the following entry ID: 31385703
(http://support.automation.siemens.com/WW/view/en/31385703)

B.10.3 /15/

SIMATIC NET
Telecontrol SCALANCE M875

Operating Instructions
Siemens AG

(SIMATIC NET Manual Collection)

On the Internet under the following entry ID: 58122394
(http://support.automation.siemens.com/WW/view/en/58122394)

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W